А. Л. ГОРОДЕНЦЕВ*

Алгебра – 1

учебник для студентов-математиков первого курса

Это первая часть интенсивного двухгодичного курса алгебры для студентов, профессионально изучающих математику и физику. Основу курса составляют лекции, читавшиеся в Независимом Московском университете и на факультете математики Высшей школы экономики, а также материалы сопровождавших их семинарских занятий. Большинство встречающихся в тексте упражнений существенно для понимания и используется в дальнейшем (некоторые из них снабжены указаниями, помещёнными в конце книги).

Москва,
май 2011

*Факультет математики Высшей школы экономики,
Группа математической физики ИТЭФ, Независимый Московский университет
mailto: gorod@itep.ru , gorodentsev@hse.ru
http://wwwth.itep.ru/~gorod

Стандартные обозначения и сокращения

$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$	натуральные, целые, рациональные, действительные и комплексные числа, и кватернионы
$\Rightarrow$ и $\iff$	«влечёт» и «равносильно»;
$\forall$, $\exists$ и $:$	«для любого», «существует» и «такой, что»
$\mathrm{Hom}(X, Y)$	множество отображений или гомоморфизмов $X \longrightarrow Y$
$\mathrm{End}(X) = \mathrm{Hom}(X, X)$	множество отображений или гомоморфизмов $X \longrightarrow X$
$\mathrm{Aut}\,(X) \subset \mathrm{End}(X)$	группа *обратимых* отображений $X \longrightarrow X$
$\lvert M\rvert$, $\lvert G\rvert$, $\lvert\lambda\rvert$	число элементов в конечном множестве M, порядок группы G и количество клеток в диаграмме Юнга λ
$\lvert pq\rvert$, $\lvert v\rvert$, $\lvert\lvert v\rvert\rvert$	расстояние между точками p и q и длина (норма) вектора v
$a \,\vdots\, b$ (или $b \mid a$)	a нацело делится на b (или b нацело делит a)
$a \equiv b \pmod n$	a сравнимо с b по модулю n (т. е. $(a-b) \,\vdots\, n$)
$\mathbb{Z}/(n)$, $\mathbb{F}_q$	кольцо и аддитивная группа вычетов по модулю n и конечное поле из q элементов
нод, нок, чум	наибольший общий делитель, наименьшее общее кратное, частично упорядоченное множество
S_n	симметрическая группа $\mathrm{Aut}\,\big(\{1, 2, \dots, n\}\big)$
$(\sigma_1, \sigma_2, \dots, \sigma_n) \in S_n$	перестановка $k \mapsto \sigma_k$
$\lvert i_1, i_2, \dots, i_m\rangle \in S_n$	циклическая перестановка $i_1 \mapsto i_2 \mapsto \cdots \mapsto i_m \mapsto i_1$
$K[x]$ и $K[[x]]$	кольца многочленов и формальных степенных рядов с коэффициентами в коммутативном кольце K
$\Bbbk[x_1, x_2, \dots, x_n]_{\leqslant m}$	пространство многочленов степени не выше m от переменных $x_1, x_2, \dots, x_n$ с коэффициентами в $\Bbbk$
$\Bbbk\,\langle \xi_1, \xi_2, \dots, \xi_n\rangle$	кольцо грассмановых многочленов от (антикоммутирующих) переменных $\xi_1, \xi_2, \dots, \xi_n$
$\mathbb{F}^*$, K^*	мультипликативные группы ненулевых элементов поля $\mathbb{F}$ и обратимых элементов кольца K
V^*, F^*	двойственное пространство и двойственный или евклидово или эрмитово сопряжённый оператор

$\mathrm{Mat}_{m\times n}(K)$, $\mathrm{Mat}_n(K)$	модуль матриц из m строк и n столбцов и алгебра квадратных $n\times n$ матриц с элементами из кольца K
M^t , λ^t	транспонированная матрица и транспонированная (сопряжённая) диаграмма Юнга
$\langle\xi,v\rangle=\xi(v)=\mathrm{ev}_v(\xi)$	свёртка вектора $v\in V$ с ковектором $\xi\in V^*$
(v,w)	евклидово или эрмитово скалярное произведение векторов v и w
$\mathrm{GL}(V)$, $\mathrm{PGL}(V)$, $\mathrm{O}(V)$, $\mathrm{U}(V)$	группы линейных, проективных, ортогональных и унитарных преобразований пространства V
$\mathrm{SL}(V)$, $\mathrm{SO}(V)$, $\mathrm{SU}(V)$	группы линейных, ортогональных и унитарных преобразований определителя 1
GL_n , PGL_n , SL_n , и т. д.	соответствующие предыдущим группы $n\times n$ матриц
S^nV^*	пространство однородных многочленов степени n на векторном пространстве V
$\mathbb{A}(V)$, $\mathbb{P}(V)$	аффинизация и проективизация векторного пространства V
$V(f)\subset\mathbb{P}(V)$	гиперповерхность, заданная уравнением $f(v)=0$
Q , q , $\widetilde{q}$, $\widehat{q}$	квадрика $Q=V(q)\subset\mathbb{P}(V)$, задаваемая уравнением $q(v)=0$, где $q\in S^2V^*$ квадратичная форма с поляризацией $\widetilde{q}:V\times V\longrightarrow\mathbb{F}$ и корреляцией $\widehat{q}:V\longrightarrow V^*$
$\mathsf{T}V$, SV , ΛV	тензорная, симметрическая и внешняя алгебры векторного пространства V

Раздел I
Множества, отображения, разбиения

§1. Множества и отображения

1.1. Множества. В этом курсе мы не будем заниматься основаниями теории множеств, полагаясь на имеющееся у читателя школьное интуитивное представление о множестве как об «абстрактной совокупности объектов произвольной природы[1]». Напомним, однако, что всякое множество состоит из *элементов*, которые мы часто будем называть *точками*. Все точки в любом множестве, по определению, различны.

Множество задано, как только про любой объект можно сказать, является он точкой данного множества или нет. Принадлежность точки x множеству X записывается как $x \in X$. Два множества *равны*, если они состоят из одних и тех же элементов. Существует единственное множество, не содержащее ни одного элемента. Оно называется *пустым* и обозначается $\varnothing$. Для конечного множества X мы обозначаем через $|X|$ количество элементов в этом множестве.

Множество X называется *подмножеством* множества Y, если каждый элемент $x \in X$ лежит также и в Y. В этом случае пишут $X \subset Y$. Отметим, что пустое множество является подмножеством любого множества и всякое множество является подмножеством самого себя. Непустые подмножества, отличные от всего множества называются *собственными подмножествами*.

Упражнение 1.1. Сколько всего подмножеств (включая несобственные) имеется у множества, состоящего из n элементов?

Для любых двух множеств X и Y множество $X \cup Y$, состоящее из всех элементов, принадлежащих хотя бы одному из них, называется их *объединением*; множество $X \cap Y$, состоящее из всех элементов, принадлежащих одновременно каждому из них, называется их *пересечением*; множество $X \smallsetminus Y$, состоящее из всех элементов множества X, которые не содержатся в Y, называется их *разностью*.

---

[1] строго говоря, теория множеств начинается с фиксации некоторого набора выразительных средств — *языка теории множеств*, похожего на язык программирования, и ограничивается только такими «совокупностями объектов», которые можно описать посредством этого языка; одним из требований к такому языку является возможность выразить на нём теоремы из стандартных курсов алгебры, геометрии и анализа; так что построению строгих оснований теории множеств разумно предпослать изучение хотя бы части таковых теорем

Упражнение 1.2. Проверьте, что операция пересечения выражается через разность по формуле $X \cap Y = X \smallsetminus (X \smallsetminus Y)$. Можно ли выразить разность через пересечение и объединение?

Если множество X является объединением непересекающихся подмножеств Y и Z, то говорят, что X является *дизъюнктным объединением* Y и Z и пишут $X = Y \sqcup Z$.

Множество $X \times Y$, элементами которого являются, по определению, всевозможные пары (x, y) с $x \in X$, $y \in Y$, называется *декартовым* (или *прямым*) *произведением* множеств X и Y.

1.2. Отображения. Отображение $f : X \longrightarrow Y$ из множества X в множество Y — это правило, которое сопоставляет каждой точке $x \in X$ некоторую однозначно определяемую по x точку $y = f(x) \in Y$, которая называется *образом* точки x при отображении f.

Множество всех точек $x \in X$, образ которых равен данной точке $y \in Y$, называется *полным прообразом* точки y (или *слоем* отображения f над y) и обозначается

$$f^{-1}(y) \overset{\text{def}}{=} \{x \in X \mid f(x) = y\}\,.$$

Полные прообразы различных точек не пересекаются и могут быть как пустыми, так и состоять из многих точек. Множество всех $y \in Y$, имеющих непустой прообраз, называется *образом отображения* $X \xrightarrow{f} Y$ и обозначается

$$\operatorname{im}(f) \overset{\text{def}}{=} \{y \in Y \mid f^{-1}(y) \neq \varnothing\} = \{y \in Y \mid \exists\, x \in X : f(x) = y\}\,.$$

Два отображения $f : X \longrightarrow Y$ и $g : X \longrightarrow Y$ *равны*, если их значения в каждой точке одинаковы: $\forall\, x \in X \;\; f(x) = g(x)$. Множество всех отображений из множества X в множество Y обозначается $\operatorname{Hom}(X, Y)$.

Отображения $X \longrightarrow X$ из множества X в себя обычно называют *эндоморфизмами* множества X. Множество всех эндоморфизмов множества X обозначается $\operatorname{End}(X) = \operatorname{Hom}(X, X)$. Отметим, что у всякого множества X имеется *тождественный эндоморфизм* $\operatorname{Id}_X : X \longrightarrow X$, который переводит каждый элемент в самого себя: $\forall\, x \in X \;\; \operatorname{Id}_X(x) = x$.

Отображение $f : X \longrightarrow Y$ называется *наложением* (а также *сюрьектцией* или *эпиморфизмом*), если $\operatorname{im}(f) = Y$, т. е. когда прообраз каждой точки $y \in Y$ не пуст. Мы будем изображать сюрьективные отображения стрелками $X \twoheadrightarrow Y$.

Отображение f называется *вложением* (а также *инъекцией*, или *мономорфизмом*), если $f(x_1) \neq f(x_2)$ при $x_1 \neq x_2$, т. е. когда прообраз каждой точки $y \in Y$ содержит не более одного элемента. Инъективные отображения мы обозначает стрелками $X \hookrightarrow Y$.

Упражнение 1.3. Перечислите все отображения

$$\{0, 1, 2\} \longrightarrow \{0, 1\} \quad \text{и} \quad \{0, 1\} \longrightarrow \{0, 1, 2\}\,.$$

Сколько среди них вложений и сколько наложений?

Отображение $f : X \longrightarrow Y$, которое является одновременно и вложением и наложением, называется *взаимно однозначным* (а также *биекцией* или *изоморфизмом*). Иными словами, биективность отображения f означает, что для каждого $y \in Y$ существует единственный $x \in X$, такой что $f(x) = y$. Мы будем обозначать биекции стрелками $X \xrightarrow{\sim} Y$.

Упражнение 1.4. Какие из отображений:

$$\mathbb{Z} \xrightarrow{x \mapsto x^2} \mathbb{Z}\,; \quad \mathbb{N} \xrightarrow{x \mapsto x^2} \mathbb{N}\,; \quad \mathbb{Z} \xrightarrow{x \mapsto 7x} \mathbb{Z}\,; \quad \mathbb{R} \xrightarrow{x \mapsto 7x} \mathbb{R}$$

являются а) биекциями, б) инъекциями, в) сюрьекциями?

Взаимно однозначные отображения $X \xrightarrow{\sim} X$ данного множества X в себя обычно называют *автоморфизмами* этого множества. Автоморфизмы можно воспринимать как *перестановки* элементов множества X. Множество всех автоморфизмов множества X обозначается через $\mathrm{Aut}\,(X)$.

1.2.1. Запись отображений словами. Пусть

$$X = \{x_1, x_2, \dots, x_n\}\,, \quad Y = \{y_1, y_2, \dots, y_m\}\,.$$

Сопоставим каждому отображению $X \xrightarrow{f} Y$ выписанный в ряд слева направо набор его значений:

$$w(f) \overset{\text{def}}{=} (f(x_1),\, f(x_2),\, \dots\,,\, f(x_n)) \tag{1-1}$$

и будем воспринимать его как n-буквенное слово, написанное при помощи m-буквенного алфавита $Y = \{y_1, y_2, \dots, y_m\}\,$.

Например, отображениям $\{1,\,2\} \xrightarrow{f} \{1,\,2,\,3\}$ и $\{1,\,2,\,3\} \xrightarrow{g} \{1,\,2,\,3\}$

$$f: \begin{tikzcd}[row sep=small] & 1 \\ 1 \arrow[ddr] & \\ & 2 \\ 2 \arrow[ur] & \\ & 3 \end{tikzcd} \qquad g: \begin{tikzcd}[row sep=small] 1 \arrow[r] & 1 \\ 2 \arrow[r] & 2 \\ 3 \arrow[ur] & 3 \end{tikzcd}$$

сопоставятся при этом слова $w(f) = (3, 2)$ и $w(g) = (1, 2, 2)$, составленные из букв трёхбуквенного алфавита $\{1,\,2,\,3\}$.

Таким образом мы получаем биекцию

$$w : \mathrm{Hom}(X, Y) \xrightarrow{\sim} \{\text{слова из } |X| \text{ букв в алфавите } Y\}\,. \tag{1-2}$$

Инъективные отображения записываются при этом словами, в которых нет повторяющихся букв, а сюрьективные отображения — словами, в которых используются все без исключения буквы алфавита Y. Взаимно однозначным отображениям отвечают слова, в которых задействованы все буквы алфавита Y, причём каждая — ровно по одному разу.

Предложение 1.1
Если множество X состоит из n элементов, а множество Y — из m, то множество $\mathrm{Hom}(X,Y)$ состоит из m^n элементов.

Доказательство. Обозначим через $W_m(n)$ количество всех n-буквенных слов, которые можно написать при помощи алфавита из m букв. Выпишем все эти слова на m страницах, поместив на i-тую страницу все слова, начинающиеся на i-тую букву алфавита. В результате на каждой странице окажется ровно по $W_m(n-1)$ слов. Поэтому $W_m(n) = m \cdot W_m(n-1) = m^2 \cdot W(n-2) = \cdots = m^{n-1} \cdot W(1) = m^n$. □

Предложение 1.2
У n-элементного множества имеется ровно $n!$ автоморфизмов.

Доказательство. Пусть $X = \{x_1, x_2, \dots, x_n\}$. Биекции $X \xrightarrow{f} X$ записываются n-буквенными словами в n-буквеном алфавите $x_1, x_2, \dots, x_n$, содержащими каждую букву x_i ровно по одному разу. Обозначим количество таких слов через $V(n)$ и выпишем их по алфавиту на n страницах, поместив на i-тую страницу все слова, начинающиеся на x_i. Тогда на каждой странице будет ровно $V(n-1)$ слов, откуда $V(n) = n \cdot V(n-1) = n \cdot (n-1) \cdot V(n-2) = \cdots = n \cdot (n-1) \cdot (n-2) \cdot \cdots \cdot 2 \cdot 1 = n!$. □

Упражнение 1.5 (принцип Дирихле). Покажите, что следующие три условия на множество X попарно равносильны друг другу:

а) X бесконечно;

б) $\exists$ вложение $X \hookrightarrow X$, не являющееся наложением;

в) $\exists$ наложение $X \twoheadrightarrow X$, не являющееся вложением.

Упражнение 1.6. Счётно ли множество $\mathrm{Aut}\,(\mathbb{N})$?

1.3. Разбиения. Со всяким отображением $X \xrightarrow{f} Y$ связано разбиение множества X в объединение непересекающихся подмножеств — полных прообразов различных точек $y \in Y$. Поэтому задать отображение $X \xrightarrow{f} Y$ — это то же самое, что представить X в виде дизъюнктного объединения непустых подмножеств, занумерованных точками $y \in \mathrm{im}\,(f)$:

$$X = \bigsqcup_{y \in \mathrm{im}\,(f)} f^{-1}(y)\,. \tag{1-3}$$

Такой взгляд на отображения часто оказывается полезным при подсчёте числа элементов в том или ином множестве.

Допустим, к примеру, что все непустые слои отображения $X \xrightarrow{f} Y$ состоят из одного и того же числа точек $m = |f^{-1}(y)|$. Тогда число элементов в образе отображения f связано с числом элементов в множестве X формулой

$$|X| = m \cdot |\mathrm{im}\, f|\,. \tag{1-4}$$

У этой простой формулы имеется множество приложений.

1.3.1. Пример: другое доказательство предл. 1.1. Зафиксируем какую-нибудь точку $x \in X$ и рассмотрим *отображение вычисления*[1]

$$\mathrm{ev}_x : \mathrm{Hom}(X, Y) \xrightarrow{f \mapsto f(x)} Y \,, \tag{1-5}$$

которое сопоставляет отображению $X \xrightarrow{f} Y$ его значение в точке x.

Прообраз ev_x^{-1} любой точки $y \in Y$ можно отождествить с множеством всех отображений из $(n-1)$-элементного множества $X \smallsetminus \{x\}$ в Y:

$$\mathrm{ev}_x^{-1}(y) = \{X \xrightarrow{f} Y \mid f(x) = y\} = \mathrm{Hom}\left(X \smallsetminus \{x\}\,,\, Y\right)\,.$$

Поэтому $\mathrm{im}\,\mathrm{ev}_x = Y$ и применима формула (1-4), согласно которой

$$|\mathrm{Hom}(X, Y)| = |\mathrm{Hom}\left(X \smallsetminus \{x\}\,,\, Y\right)| \cdot |Y|\,.$$

Таким образом, при добавлению к множеству X одной точки, количество отображений из X в Y увеличивается в $|Y|$ раз. Отсюда $\mathrm{Hom}(X, Y) = |Y|^{|X|}$ (по этой причине множество отображений $\mathrm{Hom}(X, Y)$ часто обозначают через Y^X).

1.3.2. Пример: другое доказательство предл. 1.2. Положим в предыдущем рассуждении $Y = X$ и ограничим отображение вычисления (1-5) на подмножество биекций $\mathrm{Aut}\,(X) \subset \mathrm{Hom}(X, X)$. Получим отображение

$$\mathrm{ev}_x : \mathrm{Aut}\,(X) \xrightarrow{f \mapsto f(x)} X\,.$$

Любой элемент его слоя $\mathrm{ev}_x^{-1}(x')$ над произвольной точкой $x' \in X$ представляет собою биекцию $X \longrightarrow X$, которая сначала как-то переставляет точки $(n-1)$-элементного множества $X \smallsetminus \{x\}$, а затем переставляет между собой две точки x и x', оставляя все остальные точки на месте. Поэтому все слои непусты и состоят из одного и того же числа элементов, равного количеству автоморфизмов $(n-1)$-элементного множества $X \smallsetminus \{x\}$. По формуле (1-4)

$$|\mathrm{Aut}\,(X)| = |\mathrm{Aut}\,(X \smallsetminus \{x\})| \cdot |X|\,,$$

т. е. при добавлении к $(n-1)$-элементному множеству n-той точки количество эндоморфизмов увеличивается в n раз. Если $|X| = n$, получаем

$$|\mathrm{Aut}\,(X)| = n \cdot (n-1) \cdot (n-2) \cdot \;\cdots\; \cdot 1 = n!$$

1.3.3. Пример: мультиномиальные коэффициенты. При раскрытии скобок в выражении $(a_1 + a_2 + \;\cdots\; + a_k)^n$ получится сумма одночленов вида $a_1^{m_1} a_2^{m_2} \cdots a_k^{m_k}$, где каждый показатель m_i заключен в пределах $0 \leqslant m_i \leqslant n$, а общая степень $m_1 + m_2 + \;\cdots\; + m_k = n$. Коэффициент, возникающий при

[1] обозначение «ev» является сокращением слова *evaluation*

таком одночлене после приведения подобных слагаемых, называется *мультиномиальным коэффициентом* и обозначается $\binom{n}{m_1 \dots m_k}$. Таким образом,

$$(a_1 + a_2 + \cdots + a_k)^n = \sum_{\substack{m_1+m_2+\cdots+m_k=n \\ 0 \leqslant m_i \leqslant n}} \binom{n}{m_1 \dots m_k} \cdot a_1^{m_1} a_2^{m_2} \cdots a_k^{m_k} , \qquad (1\text{-}6)$$

Чтобы явно выразить мультиномиальный коэффициент $\binom{n}{m_1 \dots m_k}$ через показатели $m_1, m_2, \dots, m_k$, заметим, что перемножение n скобок

$$(a_1 + a_2 + \cdots + a_k)(a_1 + a_2 + \cdots + a_k) \cdots (a_1 + a_2 + \cdots + a_k)$$

заключается в последовательном выборе внутри каждой из скобок какой-нибудь одной буквы и перемножении этих букв — выписывании их слева направо друг за другом в одно n-буквенное слово. После чего все такие слова, полученные из всех возможных выборов букв в каждой из скобок, суммируются. Подобные слагаемые, вносящие вклад в коэффициент при $a_1^{m_1} a_2^{m_2} \cdots a_k^{m_k}$ — это всевозможные слова, состоящие ровно из m_1 букв a_1, m_2 букв a_2, … , m_k букв a_k. Количество таких слов легко подсчитать по формуле (1-4).

А именно, сделаем на время m_1 букв a_1 попарно разными, снабдив каждую из них дополнительным верхним индексом; аналогично поступим с m_2 буквами a_2, m_3 буквами a_3 и т. д. В результате получится набор из $n = m_1 + m_2 + \cdots + m_k$ попарно различных букв:

$$\underbrace{a_1^{(1)}, a_1^{(2)}, \dots, a_1^{(m_1)}}_{m_1 \text{ меченых букв } a_1}, \underbrace{a_2^{(1)}, a_2^{(2)}, \dots, a_2^{(m_2)}}_{m_2 \text{ меченых букв } a_2}, \dots \dots \dots, \underbrace{a_k^{(1)}, a_k^{(2)}, \dots, a_k^{(m_k)}}_{m_k \text{ меченых букв } a_k} .$$

Обозначим через X множество всех n-буквенных слов, которые можно написать этими n различными буквами, используя каждую букву ровно по одному разу. Как мы уже знаем, $|X| = n!$. В качестве Y возьмём интересующее нас множество слов из m_1 одинаковых букв a_1, m_2 одинаковых букв a_2, … , m_k одинаковых букв a_k и рассмотрим отображение $X \xrightarrow{f} Y$, которое в каждом слове стирает у всех букв верхние индексы. Это отображение эпиморфно, и полный прообраз каждого слова $y \in Y$ состоит из $m_1! \cdot m_2! \cdot \cdots \cdot m_k!$ слов, которые получаются из какого-нибудь одного слова $x \in X$, переходящего в y, всевозможными перестановками m_1 верхних индексов у букв a_1, m_2 верхних индексов у букв a_2, … , m_k верхних индексов у букв a_k.

Таким образом, формула (1-4) применима и приводит к равенству

$$\binom{n}{m_1 \dots m_k} = \frac{n!}{m_1! \cdot m_2! \cdot \cdots \cdot m_k!} , \qquad (1\text{-}7)$$

которое позволяет переписать разложение (1-6) в виде

$$(a_1 + a_2 + \cdots + a_k)^n = \sum_{\substack{m_1+m_2+\cdots+m_k=n \\ 0 \leqslant m_i \leqslant n}} \frac{n! \cdot a_1^{m_1} a_2^{m_2} \cdots a_k^{m_k}}{m_1! \cdot m_2! \cdot \cdots \cdot m_k!} . \qquad (1\text{-}8)$$

В частности, при $k = 2$ мы получаем известную формулу для раскрытия бинома с натуральным показателем[1]:

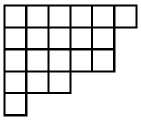
$$(a+b)^n = \sum_{k=0}^{n} \frac{n! \cdot a^k b^{n-k}}{k!(n-k)!}\,. \tag{1-9}$$

Упражнение 1.7. Сколько всего слагаемых в правой части формулы (1-8) ?

1.3.4. Пример: диаграммы Юнга. Разбиение конечного множества $X = \{1,\,2,\,\dots\,,\,n\}$ в объединение непересекающихся подмножеств

$$X = X_1 \sqcup X_1 \sqcup X_2 \sqcup \,\dots\, \sqcup X_k\,. \tag{1-10}$$

часто бывает удобно кодировать следующим образом. Условимся нумеровать подмножества в порядке нестрогого убывания их размера и обозначим количество элементов в i-том подмножестве через $\lambda_i = |X_i|$. Будем называть невозрастающую последовательность чисел $\lambda = (\lambda_1, \lambda_2, \dots, \lambda_n)$ *формой* разбиения (1-10). Форму разбиения удобно представлять себе в виде *диаграммы Юнга* — картинки вида



, (1-11)

составленной из выровненных по левому краю горизонтальных полос длины $\lambda_1 \geqslant \lambda_2 \geqslant \cdots \geqslant \lambda_k$. Так, диаграмма Юнга (1-11) отвечает разбиению формы $\lambda = (6,5,5,3,1)$. Общее число клеток в диаграмме λ называется *весом* диаграммы и обозначается $|\lambda| = \sum \lambda_i$.

Будем называть *заполнением* диаграммы λ множеством X с $|X| = |\lambda|$ произвольную расстановку элементов множества X в клетки диаграммы по одному элементу в каждую клетку. Таким образом, всего имеется $n!$ различных заполнений диаграммы λ множеством X.

Объединяя элементы, стоящие в i-той строке диаграммы в одно подмножество X_i, мы получаем разбиение множества X в дизъюнктное объединение k непересекающихся подмножеств $X_1, X_2, \dots, X_k$. Ясно, что любое разбиение (1-10) можно получить таким образом, так что мы получаем сюрьективное отображение из множества заполнений диаграммы λ в множество разбиений множества X формы λ. Покажем, что все слои этого отображения состоят из одного и того же числа элементов.

Два заполнения приводят к одинаковым разбиениям тогда и только тогда, когда они получаются друг из друга перестановками элементов внутри строк и перестановками строк одинаковой длины между собою как единого целого. Если обозначить через m_i число строк длины i в диаграмме λ (отметим, что

[1]это частный случай *формулы Ньютона*, которую в полной общности мы обсудим в n° 5.5, когда будем заниматься степенными рядами

многие $m_i = 0$, поскольку $|\lambda| = n = m_1 + 2m_2 + \cdots + nm_n$), то перестановок первого типа будет $\prod\limits_{i=1}^{n} \lambda_i! = \prod\limits_{i=1}^{n} (i!)^{m_i}$ штук, а второго типа — $\prod\limits_{i=1}^{n} m_i!$ штук. Так как все эти перестановки действуют независимо друг от друга, каждый слой нашего отображения состоит из

$$\prod_{i=1}^{n} (i!)^{m_i} m_i!$$

Из формулы (1-4) вытекает

Предложение 1.3

Число разбиений n-элементного множества X в дизъюнктное объединение m_1 1-элементных, m_2 2-элементных, … , m_n n-элементных подмножеств равно

$$\frac{n!}{\prod\limits_{i=1}^{n} m_i! \cdot (i!)^{m_i}} . \tag{1-12}$$

1.4. Классы эквивалентности. Альтернативный способ задавать разбиение данного множества X в дизъюнктное объединение подмножеств состоит в том, чтобы объявить элементы, входящие в одно подмножество такого разбиения «эквивалентными». Формализуется это так.

Назовём *бинарным отношением* на множестве X произвольное подмножество $R \subset X \times X$ в множестве всех упорядоченных пар

$$X \times X = \{(x_1, x_2) \mid x_1, x_2 \in X\} .$$

Принадлежность пары (x_1, x_2) отношению R обычно записывают как $x_1 \underset{R}{\sim} x_2$.

Например, на множестве целых чисел $X = \mathbb{Z}$ часто рассматривают бинарные отношения

$$\text{равенство} \qquad x_1 \underset{R}{\sim} x_2 \overset{\text{def}}{\iff} x_1 = x_2 \tag{1-13}$$

$$\text{неравенство} \qquad x_1 \underset{R}{\sim} x_2 \overset{\text{def}}{\iff} x_1 \leqslant x_2 \tag{1-14}$$

$$\text{делимость} \qquad x_1 \underset{R}{\sim} x_2 \overset{\text{def}}{\iff} x_1 | x_2 \tag{1-15}$$

$$\text{сравнимость по модулю } n \qquad x_1 \underset{R}{\sim} x_2 \overset{\text{def}}{\iff} x_1 \equiv x_2 \pmod{n} \tag{1-16}$$

(последнее условие $x_1 \equiv x_2 \pmod{n}$ читается как «x_1 сравнимо с x_2 по модулю n» и по определению означает, что x_1 и x_2 имеют одинаковые остатки от деления на n, т. е. $(x_1 - x_2) \,\vdots\, n$).

Определение 1.1

Бинарное отношение $\underset{R}{\sim}$ называется *эквивалентностью*, если оно обладает следующими тремя свойствами:

$$\begin{aligned}
&\textit{рефлексивность}: && \forall\, x \in X \;\; x \underset{R}{\sim} x \\
&\textit{транзитивность}: && \forall\, x_1, x_2, x_3 \in X \text{ из } x_1 \underset{R}{\sim} x_2 \text{ и } x_2 \underset{R}{\sim} x_3 \text{ вытекает } x_1 \underset{R}{\sim} x_3 \\
&\textit{симметричность}: && \forall\, x_1, x_2 \in X \;\; x_1 \underset{R}{\sim} x_2 \iff x_2 \underset{R}{\sim} x_1 .
\end{aligned}$$

Среди перечисленных выше бинарных отношений на множестве $\mathbb{Z}$ отношения (1-13) и (1-16) являются эквивалентностями, а (1-14) и (1-15) не являются (они несимметричны).

Если множество X разбито в объединение непересекающихся подмножеств, то отношение $x_1 \sim x_2$, означающее, что x_1 и x_2 лежат в одном и том же подмножестве этого разбиения, очевидно, является эквивалентностью.

Наоборот, пусть на множестве X задано какое-нибудь отношение эквивалентности R. Рассмотрим для каждого $x \in X$ подмножество в X, состоящее из всех элементов, эквивалентных x. Оно называется *классом эквивалентности* элемента x и обозначается

$$[x]_R = \{z \in X \mid x \underset{R}{\sim} z\} = \{z \in X \mid z \underset{R}{\sim} x\}$$

(второе равенство выполняется благодаря симметричности отношения R). Два класса $[x]_R$ и $[y]_R$ либо вообще не пересекаются, либо полностью совпадают. В самом деле, если существует элемент z, эквивалентный и x и y, то в силу симметричности и транзитивности отношения $\underset{R}{\sim}$ элементы x и y будут эквивалентны между собой, а значит, любой элемент, эквивалентный x, будет эквивалентен также и y, и наоборот. Таким образом, множество X распадается в дизъюнктное объединение различных классов эквивалентности.

Множество классов эквивалентности по отношению $R \subset X \times X$ обозначается X/R и называется *фактором* множества X по отношению R. Сюрьективное отображение

$$X \xrightarrow{x \mapsto [x]} X/R\,, \tag{1-17}$$

сопоставляющее каждому элементу $x \in X$ его класс эквивалентности $[x] \in X/R$, называется *отображением факторизации*. Слои этого отображения суть классы эквивалентных элементов. Наоборот, любое сюрьективное отображение

$$X \xrightarrow{f} Y$$

является отображением факторизации по отношению эквивалентности

$$x_1 \sim x_2 \iff f(x_1) = f(x_2)\,.$$

1.4.1. Пример: классы вычетов. Фиксируем ненулевое целое число $n \in \mathbb{Z}$. Фактор множества целых чисел $\mathbb{Z}$ по отношению сравнимости по модулю n из (1-16) обозначается $\mathbb{Z}/(n)$ или $\mathbb{Z}/n\mathbb{Z}$. Мы будем записывать его элементы символами $[z]_n$, где $z \in \mathbb{Z}$. Класс эквивалентности

$$[z]_n \overset{\text{def}}{=} \{x \in \mathbb{Z} \mid z - x \,\vdots\, n\} \tag{1-18}$$

называется *классом вычетов по модулю* n и состоит из всех целых чисел, имеющих тот же остаток[1] от деления на n, что и число z. Таким образом, $\mathbb{Z}/(n)$ состоит из n различных классов

$$[0]_n\,,\ [1]_n\,,\ \dots\,,\ [n-1]_n\,,$$

которые можно, при желании, считать остатками от деления на n. Отображение факторизации

$$\mathbb{Z} \xrightarrow{z\mapsto[z]_n} \mathbb{Z}/(n)$$

называется *приведением по модулю* n. На языке остатков, оно сопоставляет каждому целому числу его остаток от деления на n.

Подчеркнём, однако, при практических вычислениях с вычетами гораздо удобнее воспринимать их не как остатки, а как *непересекающиеся подмножества*, образующие разбиение множества $\mathbb{Z}$, поскольку возможность по разному записывать один и тот же класс иногда сильно упрощает вычисления. Например, остаток от деления 12^{100} на 13 можно искать как

$$\left[12^{100}\right]_{13} = [12]_{13}^{100} = [-1]_{13}^{100} = \left[(-1)^{100}\right]_{13} = [1]_{13}\,.$$

Упражнение 1.8. Докажите правомочность этого вычисления. Точнее, проверьте, что классы $[x+y]_n$ и $[xy]_n$ не зависят от выбора элементов $x\in[x]_n$ и $y\in[y]_n$ и, стало быть, правила

$$[x]_n + [y]_n \overset{\text{def}}{=} [x+y]_n \tag{1-19}$$

$$[x]_n \cdot [y]_n \overset{\text{def}}{=} [xy]_n \tag{1-20}$$

корректно определяют на множестве классов вычетов $\mathbb{Z}/(n)$ операции сложения и умножения. Именно такое умножение $[12]^{100} = \underbrace{[12]\cdot[12]\cdot\,\cdots\,\cdot[12]}_{100} = \left[12^{100}\right]$ и использовано в предыдущей формуле.

1.4.2. Пример: повороты. Обозначим через SO_2 множество поворотов декартовой плоскости $\mathbb{R}^2$ вокруг начала координат. Отображение

$$\mathbb{R} \xrightarrow{\alpha\mapsto T_\alpha} \mathrm{SO}_2\,, \tag{1-21}$$

сопоставляющее вещественному числу α поворот $T_\alpha : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ на угол α против часовой стрелки вокруг начала координат, является факторизацией по отношению эквивалентности

$$\alpha \underset{R}{\sim} \beta \iff \alpha-\beta = 2\pi k \quad \text{с} \quad k\in\mathbb{Z}\,.$$

[1]где под *остатком* от деления числа x на число n понимается разность между x и наибольшим не превосходящим x числом вида nk с $k\in\mathbb{Z}$

Выбирая в каждом классе эквивалентности $[\alpha]$ наименьшее неотрицательное число $\alpha_{\min} \in [\alpha]$ и откладывая на единичной окружности S^1 с центром в начале координат дугу длины $\alpha_{\min}$, начинающуюся в точке $(1, 0)$ и идущую против часовой стрелки, мы получаем биекцию $\mathrm{SO}_2 \simeq S^1$ между поворотами и точками единичной окружности. Таким образом, отображение (1-21) можно воспринимать как наматывание числовой прямой $\mathbb{R}$ на единичную окружность S^1.

Если зафиксировать $n \in \mathbb{N}$ и вместо отображения (1-21) рассмотреть отображение

$$\mathbb{R} \xrightarrow{\alpha \mapsto T_{2\pi\alpha/n}} S^1 , \tag{1-22}$$

сопоставляющее числу $\alpha \in \mathbb{R}$ поворот на угол $\frac{2\pi}{n}\alpha$, то мы получим отображение факторизации по отношению эквивалентности

$$\alpha \underset{R}{\sim} \beta \iff \alpha - \beta = nk \quad \text{с} \quad k \in \mathbb{Z},$$

ограничение которого на множество целых чисел $\mathbb{Z} \subset \mathbb{R}$ совпадает с отношением сравнимости по модулю n из предыдущего примера.

Таким образом, классы вычетов по модулю n можно воспринимать как повороты на углы, кратные $2\pi/n$, и представлять себе как «циферблат», состоящий из n равномерно нанесённых на единичную окружность делений. Сложение вычетов из упр. 1.8 превращается при этом в обычное «сложение часов» на циферблате.

1.4.3. Неявное задание эквивалентности. Для любого семейства отношений эквивалентности $R_\nu \subset X \times X$ пересечение $\bigcap\limits_\nu R_\nu \subset X \times X$ также является отношением эквивалентности. В самом деле, если каждое из множеств $R_\nu \subset X \times X$ содержит диагональ $\Delta = \{(x, x)\} \subset X \times X$, переходит в себя при симметрии $(x, y) \leftrightarrows (y, x)$ и вместе с каждой парой точек вида (x, y), (y, z) содержит также и точку (x, z), то этими свойствами обладает и пересечение $\bigcap\limits_\nu R_\nu$ всех этих множеств. Поэтому для любого подмножества

$$R \subset X \times X$$

существует *наименьшее по включению* отношение эквивалентности $\overline{R}$, содержащее R, а именно, пересечение всех содержащих R отношений эквивалентности. Отношение $\overline{R}$ называется эквивалентностью, *порождённой* отношением R.

Отметим, что по наугад выбранному множеству R часто бывает трудно судить о том, как устроена порождённая им эквивалентность $\overline{R}$. Даже выяснить, не являются ли все точки эквивалентными друг другу[1], может быть не просто.

1.4.4. Пример: дроби. Множество рациональных чисел $\mathbb{Q}$ обычно определяют как множество дробей a/b с $a, b \in \mathbb{Z}$ и $b \neq 0$. При этом под *дробью*

[1] т. е. существует ли хоть одна собственная (отличная от всего произведения $X \times X$) эквивалентность, содержащая R

понимается класс эквивалентности упорядоченных пар $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ по минимальному отношению эквивалентности, содержащему все отождествления

$$(a, b) \sim (ac, bc) \qquad \forall\, c \neq 0\,. \tag{1-23}$$

Отношения (1-23) выражают собою равенства дробей $a/b = ac/bc$, но сами по себе не образуют эквивалентности. Например, при $a_1b_2 = a_2b_1$ в двухшаговой цепочке отождествлений (1-23)

$$(a_1, b_1) \sim (a_1b_2, b_1b_2) = (a_2b_1, b_1b_2) \sim (a_2, b_2)$$

самый левый и самый правый элементы нельзя напрямую отождествить по правилу (1-23). Таким образом, отношение эквивалентности, порождённое отождествлениями (1-23) содержит также отождествления

$$(a_1, b_1) \sim (a_2, b_2) \quad \text{при} \quad a_1b_2 = a_2b_1\,. \tag{1-24}$$

Оказывается, что к ним уже больше ничего добавлять не надо.

Упражнение 1.9. Проверьте, что набор отношений (1-24) рефлексивен, симметричен и транзитивен (и, тем самым, полностью описывает минимальное отношение эквивалентности, содержащее все отождествления (1-23)).

1.5. Композиции отображений. Отображение $X \longrightarrow Z$, получающееся в результате последовательного выполнения двух отображений

$$X \xrightarrow{f} Y \xrightarrow{g} Z$$

называется *композицией* отображений g и f и обозначается $g{\circ}f$ или просто gf. Таким образом,

$$\forall\, x \in X \;\; gf(x) \stackrel{\text{def}}{=} g(f(x))\,.$$

Композиция gf определена только тогда, когда образ f содержится в множестве, на котором определено отображение g.

Упражнение 1.10. Приведите пример ситуации, когда композиция gf определена, а fg — нет.

Композицию трёх отображений $X \xrightarrow{h} Y \xrightarrow{g} Z \xrightarrow{f} T$ можно вычислять двумя способами: как $(fg)h$ или как $f(gh)$. В обоих случаях получится отображение, переводящее точку $x \in X$ в точку $f(g(h(x))) \in T$. Иначе говоря, композиция отображений *ассоциативна*[1]:

$$(fg)h = f(gh)\,.$$

Таким образом, композиция нескольких отображений $f_1f_2\ldots f_m$ (если она определена) не зависит от расстановки скобок.

[1] ассоциативность также называют *сочетательным законом*

Хотя мы и обозначаем композицию отображений точно так же, как произведение, обращаться с формулами, включающими в себя композиции, надо с осторожностью: некоторые привычные по вычислениям с числами преобразования недопустимы при работе с композициями отображений.

Например, умножение чисел *коммутативно*[1]: $fg = gf$, а композиция отображений, как правило, нет (хотя бы уже потому, что одна из частей этого равенства может быть определена, а другая — нет).

Упражнение 1.11. Рассмотрим на плоскости пару различных прямых ℓ_1, ℓ_2, пересекающихся в точке O, и обозначим через σ_1 и σ_2 осевые симметрии относительно этих прямых. Явно опишите движения плоскости, задаваемые композициями $\sigma_1\sigma_2$ и $\sigma_2\sigma_1$. При каком условии на прямые выполняется равенство $\sigma_1\sigma_2 = \sigma_2\sigma_1$?

Чтобы почувствовать отличие алгебраических свойств композиции от свойств умножения чисел, поучительно взглянуть на «таблицу умножения» отображений из двухэлементного множества $X = \{1,2\}$ в себя.

Есть ровно четыре таких отображения, причём все композиции между ними определены. Если обозначать отображение $f \in \mathrm{End}(X)$ двухбуквенным словом $(f(1),\ f(2))$ (как в n° 1.2.1), то эти четыре эндоморфизма запишутся словами

$$(1,1)\,,\ (1,2) = \mathrm{Id}_X\,,\ (2,1)\,,\ (2,2)\,.$$

Значения композиций gf представлены в таблице:

$g\diagdown f$	$(1,1)$	$(1,2)$	$(2,1)$	$(2,2)$
$(1,1)$	$(1,1)$	$(1,1)$	$(1,1)$	$(1,1)$
$(1,2)$	$(1,1)$	$(1,2)$	$(2,1)$	$(2,2)$
$(2,1)$	$(2,2)$	$(2,1)$	$(1,2)$	$(1,1)$
$(2,2)$	$(2,2)$	$(2,2)$	$(2,2)$	$(2,2)$

(1-25)

Обратите внимание на то, что $(2,2)\circ(1,1) \neq (1,1)\circ(2,2)$, а также на то, что в верхней и нижней строках все произведения одинаковы, но «сократить общий множитель» при этом нельзя, т. е. из равенства $fg_1 = fg_2$, вообще говоря, не следует равенство $g_1 = g_2$, как не следует оно и из равенства $g_1 f = g_2 f$.

Упражнение 1.12 (левые обратные отображения). Покажите, что следующие три условия на отображение $X \xrightarrow{f} Y$ эквивалентны:

а) f инъективно

б) $\exists\, Y \xrightarrow{g} X \ :\ gf = \mathrm{Id}_X$ (любое такое g называется *левым обратным* к f)

в) $\forall$ отображений $g_1, g_2 : Z \longrightarrow X$ из $fg_1 = fg_2$ вытекает $g_1 = g_2$

и выясните, сколько левых обратных отображений имеется у заданного вложения n-элементного множества в m-элементное.

Упражнение 1.13 (правые обратные отображения). Покажите, что следующие три условия на отображение $X \xrightarrow{f} Y$ эквивалентны:

[1] коммутативность также называют *переместительным законом*

а) f сюрьективно

б) $\exists\, Y \xrightarrow{g} X \,:\, fg = \mathrm{Id}_Y$ (любое такое g называется *правым обратным* к f)

в) $\forall$ отображений $g_1, g_2 : Z \longrightarrow X$ из $g_1 f = g_2 f$ вытекает $g_1 = g_2$

и выясните, сколько правых обратных отображений имеется у заданного наложения m-элементного множества на n-элементное.

1.5.1. Обратимые отображения. Если отображение $X \xrightarrow{g} Y$ биективно, то прообраз $g^{-1}(y) \subset X$ каждой точки $y \in Y$ состоит ровно из одной точки, и правило $y \mapsto g^{-1}(y)$ определяет отображение $X \xleftarrow{g^{-1}} Y$, такое что

$$g \circ g^{-1} = \mathrm{Id}_Y \qquad \text{и} \qquad g^{-1} \circ g = \mathrm{Id}_X \,,$$

Таким образом, g^{-1} является одновременно и левым и правым обратным к g в смысле упр. 1.12 и упр. 1.13. Отображение g^{-1} называется *двусторонним обратным* к g.

Предложение 1.4

Следующие условия на отображение $X \xrightarrow{g} Y$ попарно эквивалентны:

(1) g взаимно однозначно

(2) существует отображение $X \xleftarrow{g'} Y$, такое что $g \circ g' = \mathrm{Id}_Y$ и $g' \circ g = \mathrm{Id}_X$

(3) g обладает левым и правым обратными отображениями[1].

При выполнении этих условий любое отображение g' из (2) и любые левые и правые обратные к g отображения из (3) совпадают друг с другом и с отображением g^{-1} описанным выше.

Доказательство. Импликация (1) $\Rightarrow$ (2) уже была установлена. Импликация (2) $\Rightarrow$ (3) очевидна. Докажем, что (3) $\Rightarrow$ (2).

Если у $X \xrightarrow{g} Y$ есть левое обратное $X \xleftarrow{f} Y$ (такое что $f \circ g = \mathrm{Id}_X$) и правое обратное $X \xleftarrow{h} Y$ (такое что $g \circ h = \mathrm{Id}_Y$), то

$$f = f \circ \mathrm{Id}_Y = f \circ (g \circ h) = (f \circ g) \circ h = \mathrm{Id}_X \circ h = h \,, \tag{1-26}$$

и условие (2) выполняется для $g' = f = h$.

Остаётся показать, что (2) $\Rightarrow$ (1) и доказать равенство $g' = g^{-1}$. Поскольку $g(g'(y)) = y$ для любого $y \in Y$, прообраз $g^{-1}(y)$ каждой точки $y \in Y$ содержит точку $g'(y)$. С другой стороны, для любого $x \in g^{-1}(y)$

$$x = \mathrm{Id}_X(x) = g'(g(x)) = g'(y)\,.$$

Поэтому $f^{-1}(y)$ состоит из единственной точки $g'(y)$. Следовательно, g — биекция, и $g' = g^{-1}$. $\square$

[1] обратите внимание, что в этом условии не требуется совпадения левого обратного отображения с правым обратным отображением

1.6. Группы преобразований. Непустой набор G взаимно однозначных отображений множества X в себя называется *группой преобразований* множества X, если вместе с каждым отображением $g \in G$ в G лежит и обратное к нему отображение g^{-1}, а вместе с каждыми двумя отображениями $f, g \in G$ в G лежит и их композиция fg. Эти условия гарантируют, что тождественное преобразование Id_X тоже лежит в G, поскольку $\mathrm{Id}_X = g^{-1}g$ для любого $g \in G$.

Если группа преобразований G конечна, число элементов в ней обозначается $|G|$ и называется *порядком* группы G.

Если подмножество $H \subset G$ тоже является группой, то H называются *подгруппой* группы G.

1.6.1. Пример: группы перестановок. Множество $\mathrm{Aut}\,(X)$ всех взаимно однозначных отображений $X \longrightarrow X$ является группой. Эта группа называется *симметрической группой* (или *группой перестановок*) множества X. Все прочие группы преобразований множества X являются подгруппами этой группы.

Группа перестановок n-элементного множества $\{1, 2, \dots, n\}$ обозначается S_n и называется n-той *симметрической группой*. Согласно предл. 1.2 $|S_n| = n!$.

Перестановку $\{1, 2, \dots, n\} \xrightarrow{\sigma} \{1, 2, \dots, n\}$ мы будем записывать строчкой $(\sigma_1, \sigma_2, \dots, \sigma_n)$ её значений $\sigma_i = \sigma(i)$, как в n° 1.2.1. Например, перестановки $\sigma = (3,4,2,1)$ и $\tau = (2,3,4,1)$ — это отображения

$$\begin{array}{cccccccccccc} & 1 & 2 & 3 & 4 & & & 1 & 2 & 3 & 4 \\ \sigma: & \downarrow & \downarrow & \downarrow & \downarrow & , & \tau: & \downarrow & \downarrow & \downarrow & \downarrow \\ & 3 & 4 & 2 & 1 & & & 2 & 3 & 4 & 1 \end{array}$$

а их композиции записываются как $\sigma\tau = (4,2,1,3)$ и $\tau\sigma = (4,1,3,2)$.

Упражнение 1.14. Составьте таблицу умножения шести элементов группы S_3, аналогичную таблице (1-25) на стр. 16.

1.6.2. Пример: абелевы группы. Группа G, в которой любые два элемента перестановочны, т. е. удовлетворяют соотношению $fg = gh$, называется *коммутативной* или *абелевой*. Примерами абелевых групп являются группы параллельных переносов плоскости или пространства, а также группа SO_2 поворотов плоскости вокруг фиксированной точки. Для каждого натурального $n \geqslant 2$ n поворотов на углы, кратные $2\pi/n$, образуют в группе SO_2 конечную подгруппу. Она называется *циклической группой порядка n*.

Задачи для самостоятельного решения к §1

Задача 1.1. Сколько разных слов (не обязательно осмысленных) можно получить переставляя буквы в словах а) шнурок б) курок в) колобок г) $\underbrace{\text{аа}\dots\text{а}}_{a}\underbrace{\text{бб}\dots\text{б}}_{b}$ д) $\underbrace{\text{б}_1\text{б}_1\dots\text{б}_1}_{k_1}\underbrace{\text{б}_2\text{б}_2\dots\text{б}_2}_{k_2}\dots\dots\dots\underbrace{\text{б}_m\text{б}_m\dots\text{б}_m}_{k_m}$?

Задача 1.2. Раскройте скобки и приведите подобные слагаемые в выражениях
а) $(a_1+a_2+\cdots+a_m)^2$ б) $(a+b+c)^3$ в) $(a+b)^n$ г) $(a_1+a_2+\cdots+a_m)^n$.

Задача 1.3. Сколько имеется различных одночленов от n переменных полной степени[1] а) ровно d б) не больше d?

Задача 1.4. Цело ли число $1000!/\left(100!^{10}\right)$?

Задача 1.5. Покажите, что при простом $p\in\mathbb{N}$ все биномиальные коэффициенты $\binom{p}{k}$ с $1\leqslant k\leqslant(p-1)$ нацело делятся на p .

Задача 1.6. Вычислите суммы: а) $\binom{n}{0}+\binom{n}{1}+\cdots+\binom{n}{n}$ б) $\binom{n}{0}+\binom{n-1}{1}+\binom{n-2}{2}+\cdots$
в) $\binom{k}{k}+\binom{k+1}{k}+\cdots+\binom{k+n}{k}$ г) $\binom{n}{0}-\binom{n}{1}+\binom{n}{2}-\binom{n}{3}+\cdots+(-1)^n\binom{n}{n}$
д) $\binom{n}{1}+2\binom{n}{2}+\cdots+n\binom{n}{n}$ е) $\binom{n}{0}+2\binom{n}{1}+\cdots+(n+1)\binom{n}{n}$ ж) $\binom{n}{0}^2+\binom{n}{1}^2+\cdots+\binom{n}{n}^2$.

Задача 1.7. Сколько имеется отображений из пятиэлементного множества в двухэлементное, таких чтобы у каждой точки было не менее двух прообразов?

Задача 1.8. Фиксируем натуральные числа m и n. Сколько решений имеет уравнение $x_1+x_2+\cdots+x_m=n$ а) в натуральных б) в целых неотрицательных числах?

Задача 1.9. Фиксируем натуральные числа m и n. Сколько имеется отображений

$$\{1,\,2,\,\ldots,\,m\}\longrightarrow\{1,\,2,\,\ldots,\,n\}$$

а) произвольных? б) биективных? в) возрастающих[2]? г) инъективных?
д) неубывающих[3]? е) сюрьективных неубывающих? ж) сюрьективных?

Задача 1.10. Сколько существует диаграмм Юнга:
а) веса 6 ? б) веса 7, содержащих не более трёх строк?
в) без ограничений на вес, но содержащих не более p строк и q столбцов?

Задача 1.11. Имеются 4 попарно отличающихся друг от друга чашки, 4 совершенно одинаковых стакана, 10 совершенно одинаковых кусков сахара и 7 попарно разноцветных соломинок. Сколькими способами можно разложить:
а) соломинки по чашкам? б) сахар по чашкам? в) сахар по стаканам?
г) соломинки по стаканам?

Задача 1.12. Как изменятся ответы в предыдущей задаче, если потребовать, чтобы после раскладывания пустых ёмкостей не оставалось?

Задача 1.13. Стороны плоского проволочного правильного n-угольника раскрашивают в n цветов — каждую сторону в свой цвет. Сколько различных игрушек при этом получится?

---

[1] напомним, что *полной степенью* одночлена $x_1^{m_1}x_2^{m_2}\cdots x_n^{m_n}$ называется сумма $\sum\limits_{i=1}^{n}m_i$

[2] напомним, что отображение упорядоченных множеств $M\xrightarrow{f}N$ называется *возрастающим*, если $x_1<x_2\Rightarrow f(x_1)<f(x_2)\ \forall\,x_1,x_2\in M$

[3] отображение f называется *неубывающим*, если $x_1\leqslant x_2\Rightarrow f(x_1)\leqslant f(x_2)$

Задача 1.14. Сколько бус можно сделать из 5 красных, 7 синих и 11 белых бусин одинаковой формы?

Задача 1.15. Каждую грань а) кубика б) правильного тетраэдра красят одним из шести фиксированных цветов, так чтобы все грани получились разноцветные. Сколько различных игрушек можно получить таким образом?

Задача 1.16. Сколько разных безделушек получится при склейке пары крашеных кубиков из предыдущей задачи по наугад выбираемой грани?

Задача 1.17* (задача Л. Г. Макар-Лиманова). Торговец газировкой коротает время манипулируя пятнадцатью одноразовыми стаканчиками, сложенными перед ним в несколько стопок. Одна манипуляция заключается в том, что он берёт верхний стаканчик из каждой стопки и составляет из них новую стопку[1]. Как разложатся стаканчики после 1000 таких манипуляций?

Задача 1.18 (полные чумы). Множество $\mathfrak{P}$ называется *частично упорядоченным* (сокращённо чумом) если на нём задано бинарное отношение $x \leqslant y$, которое рефлексивно[2], транзитивно[3] и *кососимметрично*: из $x \leqslant y$ и $y \leqslant x$ следует, что $x = y$. чум $\mathfrak{P}$ *локально конечен*, если $\forall\ x, y \in \mathfrak{P} \times \mathfrak{P}$ множество $[x, y] \stackrel{\text{def}}{=} \{\, z \mid x \leqslant z \leqslant y \,\}$ конечно. Подмножество L чума M называется *линейно упорядоченным*, если любые два его элемента сравнимы, т. е. $\forall\ a, b \in L$ имеет место отношение $a \leqslant b$ или $b \leqslant a$. чум M называется *полным*, если каждое его линейно упорядоченное подмножество $U \subset M$ обладает *верхней гранью*, т. е. существует $m \in M$, такой что $u \leqslant m \ \ \forall u \in U$ (подчеркнём, что ни единственности, ни «минимальности» верхней грани не требуется). Покажите, что всякое отображение $M \xrightarrow{f} M$ из полного чума в себя, такое что $x \leqslant f(x) \ \ \forall x \in M$, имеет неподвижную точку, т. е. $\exists\ x_0 \in M : f(x_0) = x_0$.

Задача 1.19 (лемма Цорна). Аксиома выбора[4] утверждает, что в любом множестве непустых множеств можно выбрать по одному элементу из каждого множества[5]. Выведите из аксиомы выбора и зад. 1.18, что в любом полном чуме есть максимальный элемент[6].

[1] стопка может состоять и из единственного стакана, который в этом случае и будет верхним

[2] т. е. $x \leqslant x \ \forall x$

[3] т. е. из $x \leqslant y$ и $y \leqslant z$ следует, что $x \leqslant z$

[4] эта аксиома входит в один из общепринятых вариантов аксиоматики теории множеств

[5] иначе говоря, для любого множества $\mathfrak{M}$, элементы которого сами суть непустые множества, существует отображение f из $\mathfrak{M}$ в объединение всех множеств $M \in \mathfrak{M}$, такое что $f(M) \in M \ \ \forall M \in \mathfrak{M}$

[6] решение этой задачи имеется в книгах: *Ван Дер Варден. Алгебра.* М. «Мир» (1976), стр. 246–249, *П. С. Александров. Введение в теорию множеств и общую топологию.* М. «Наука» (1977), стр. 80–83.

Раздел II
Числа и функции

§2. Числовые поля и кольца

2.1. Поля. Говоря вольно, поле — это числовая область, в которой определены четыре стандартных арифметических операции — сложение, вычитание, умножение и деление, обладающие привычными свойствами соответствующих действий над рациональными числами. Аксиоматизация этих свойств приводит к следующему формальному определению.

Определение 2.1
Множество $\mathbb{F}$ с двумя операциями $\mathbb{F}\times\mathbb{F}\longrightarrow\mathbb{F}$: *сложением* $(a,b)\mapsto a+b$ и *умножением* $(a,b)\mapsto ab$, называется *полем*, если выполняются следующие три набора аксиом:

свойства сложения

коммутативность: $a+b=b+a \quad \forall\, a,b\in\mathbb{F}$ (2-1)

ассоциативность: $a+(b+c)=(a+b)+c \quad \forall\, a,b,c\in\mathbb{F}$ (2-2)

наличие нуля: $\exists\, 0\in\mathbb{F}: \quad a+0=a \quad \forall\, a\in\mathbb{F}$ (2-3)

наличие противоположных: $\forall\, a\in\mathbb{F} \quad \exists\, (-a)\in\mathbb{F}: \quad a+(-a)=0$ (2-4)

свойства умножения

коммутативность: $ab=ba \quad \forall\, a,b\in\mathbb{F}$ (2-5)

ассоциативность: $a(bc)=(ab)c \quad \forall\, a,b,c\in\mathbb{F}$ (2-6)

наличие единицы: $\exists\, 1\in\mathbb{F}: \quad 1\,a=a \quad \forall\, a\in\mathbb{F}$ (2-7)

наличие обратных: $\forall\, a\in\mathbb{F} \quad \exists\, a^{-1}\in\mathbb{F}: \quad aa^{-1}=1$ (2-8)

свойства, связывающие сложение с умножением

дистрибутивность: $a(b+c)=ab+ac \quad \forall\, a,b\in\mathbb{F}$ (2-9)

нетривиальность: $0\neq 1$ (2-10)

2.1.1. Пример: поле из двух элементов. Простейшим объектом, удовлетворяющим всем аксиомам из опр. 2.1 является поле $\mathbb{F}_2$, состоящее из 0 и 1, таких что $0+1=1\cdot 1=1$, а все остальные суммы и произведения равны нулю (включая $1+1=0$).

Упражнение 2.1. Проверьте, что $\mathbb{F}_2$ действительно является полем.

Элементы этого поля можно воспринимать как классы вычетов по модулю 2, а операции сложения и умножения — как операции сложения и умножения классов вычетов, определённые формулами (1-19) и (1-20) из упр. 1.8 на стр. 13.

С другой стороны, элементы поля $\mathbb{F}_2$ могут интерпретироваться как

$$\text{«ложь»} = 0 \quad \text{и} \quad \text{«истина»} = 1$$

сложение — как логическое «исключающее или[1]», а умножение — как логическое «и[2]». В такой интерпретации все алгебраические вычисления в поле $\mathbb{F}_2$ превращаются в логические манипуляции с высказываниями.

Упражнение 2.2. Напишите над полем $\mathbb{F}_2$ многочлен от x, равный «не x», а также многочлен от x и y, равный «x или[3] y».

2.1.2. Пример: рациональные числа. Напомним (см. n° 1.4.3), что поле рациональных чисел $\mathbb{Q}$ можно определить как множество дробей p/q, где под «дробью» понимается класс эквивалентности упорядоченных пар (p,q) с $p,q \in \mathbb{Z}$ и $q \neq 0$ отношению

$$(a_1,b_1) \sim (a_2,b_2) \quad \text{при} \quad a_1b_2 = a_2b_1\,,$$

которое является минимальным отношением эквивалентности, содержащим все отождествления $(a,b) \sim (ac,bc)$ для любых $c \neq 0$.

Сложение и умножение дробей определяется формулами

$$\frac{p}{q} + \frac{r}{s} = \frac{ps+qr}{qs}\,, \quad \frac{p}{q} \cdot \frac{r}{s} = \frac{pr}{qs} \tag{2-11}$$

Упражнение 2.3. Проверьте, что эти определения корректны (не зависят от выбора представителей в классах) и удовлетворяют аксиомам поля.

2.1.3. Пример: вещественные числа. Множество вещественных чисел $\mathbb{R}$ определяется в курсе анализа несколькими различными способами: как множество классов эквивалентности десятичных[4] дробей, как множество дедекиндовых сечений упорядоченного множества $\mathbb{Q}$, или как множество классов эквивалентности рациональных последовательностей Коши. Мы надеемся, что читатель знаком с этими определениями и понимает, как они связаны друг с другом. Отметим, что какое бы описание множества $\mathbb{R}$ ни использовалось, задание на $\mathbb{R}$ операций сложения и умножения и проверка того, что они удовлетворяют всем аксиомам из опр. 2.1, требует некоторой работы, составляющей стандартный набор теорем из начального курса анализа. Мы полагаем, что читатель знает эти теоремы.

[1] т. е. высказывание $A+B$ истинно тогда и только тогда, когда истинно *ровно одно* из высказываний A, B

[2] т. е. высказывание AB истинно тогда и только тогда, когда истинны *оба* высказывания A, B

[3] здесь имеется в виду обычное, не исключающее «или»: многочлен должен принимать значение 1 тогда и только тогда, когда *хотя бы одна* из переменных равна 1

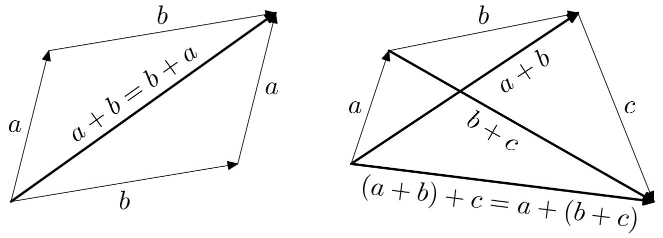
[4] или привязанных к какой-либо другой позиционной системе счисления, например, двоичных

2.2. Абелевы группы. Множество A *с одной* операцией $A \times A \longrightarrow A$, удовлетворяющей первым четырём аксиомам сложения из опр. 2.1, называется *абелевой группой*. Таким образом, всякое поле $\mathbb{F}$ является абелевой группой относительно операции сложения. Эта группа называется *аддитивной группой поля*.

Четыре аксиомы умножения из опр. 2.1 утверждают, то множество всех *ненулевых* элементов поля $\mathbb{F}$ является абелевой группой относительно операции умножения. Эту абелеву группу называют *мультипликативной группой поля* и обозначают $\mathbb{F}^*$. Роль нуля из аддитивной группы в мультипликативной группе исполняет единица. В абстрактной абелевой группе такой элемент называется *нейтральным*. Мультипликативным аналогом перехода к противоположному элементу является переход к обратному элементу.

Абелевы группы часто возникают в математике вне какого-бы ни было отношения к полям. Например, целые числа $\mathbb{Z}$ и классы вычетов $\mathbb{Z}/(n)$ по модулю n являются абелевыми группами относительно операции сложения.

2.2.1. Пример: геометрические векторы. Будем называть *геометрическим вектором* класс эквивалентности направленного отрезка (на плоскости или в пространстве) по отношению эквивалентности, отождествляющему отрезки, получающиеся друг из друга параллельным переносом. Нулевым вектором назовём класс эквивалентности точки (это единственный вектор, имеющий нулевую длину и не имеющий направления). Сложение векторов определяется стандартным образом: надо выбрать представителей векторов a и b так, чтобы конец a совпал с началом b, и объявить $a+b$ равным вектору с началом в начале a и концом в конце b. Коммутативность и ассоциативность этой операции видна из рис. рис. 2◇1



2◇1. Коммутативность и ассоциативность сложения векторов.

Нулевым элементом является нулевой вектор. Вектор $-a$, противоположный вектору a, получается из вектора a изменением его направления на противоположное.

2.2.2. Формальные свойства операции в абелевой группе. Пусть A — абелева группа, операцию в которой мы будем записывать знаком «+» (читателю настоятельно рекомендуется проговорить всё дальнейшее и на мультипликативном языке). Из аксиом (2-1)–(2-4) формально вытекает ряд других интуитивно ожидаемых свойств сложения.

Например, нейтральный элемент единственен, поскольку для любых двух таких элементов 0_1 и 0_2 мы имеем равенства $0_1 = 0_1 + 0_2 = 0_2$ (первое — в силу того, то 0_2 является нулевым элементом, второе — в силу того, то нулевым элементом является 0_1).

Элемент $-a$, противоположный к a, определяется по a однозначно (чем и оправдывается его обозначение), поскольку для любых двух таких элементов $-a$ и $-a'$ мы имеем равенства

$$-a = -a + 0 = -a + (a + (-a')) = (-a + a) + (-a)' = 0 + (-a)' = -a' .$$

В частности, для любого $a \in A$ выполняется равенство $-(-a) = a$, и в любой абелевой группе корректно определена операция *вычитания*

$$a - b \stackrel{\text{def}}{=} a + (-b) . \tag{2-12}$$

2.2.3. Формальные свойства операций в поле. Согласно предыдущему, нулевой и единичный элемент любого поля $\mathbb{F}$ определяются своими свойствами однозначно, а противоположный элемент $-a$ и обратный элемент a^{-1} однозначно определяются элементом a. Кроме того, наряду со сложением, умножением и вычитанием (2-12) в поле определена операция *деления* на любые ненулевые элементы b

$$a/b \stackrel{\text{def}}{=} ab^{-1} . \tag{2-13}$$

Далее, из аксиомы дистрибутивности (2-9) вытекает, что $0{\cdot}a = 0$ для любого $a \in \mathbb{F}$. В самом деле, обозначим $a \cdot 0$ через b. Тогда

$$b + a = a \cdot 0 + a = a \cdot 0 + a \cdot 1 = a(0 + 1) = a \cdot 1 = a ,$$

и, прибавляя к обеим частям этого равенства $(-a)$, получаем $b = 0$.

Из дистрибутивности следует также, что результатом умножения произвольного $a \in \mathbb{F}$ на противоположный единице элемент -1 является элемент, противоположный к a, т. е. $(-1) \cdot a = (-a)$. Действительно,

$$(-1) \cdot a + a = (-1) \cdot a + 1 \cdot a = ((-1) + 1) \cdot a = 0 \cdot a = 0 ,$$

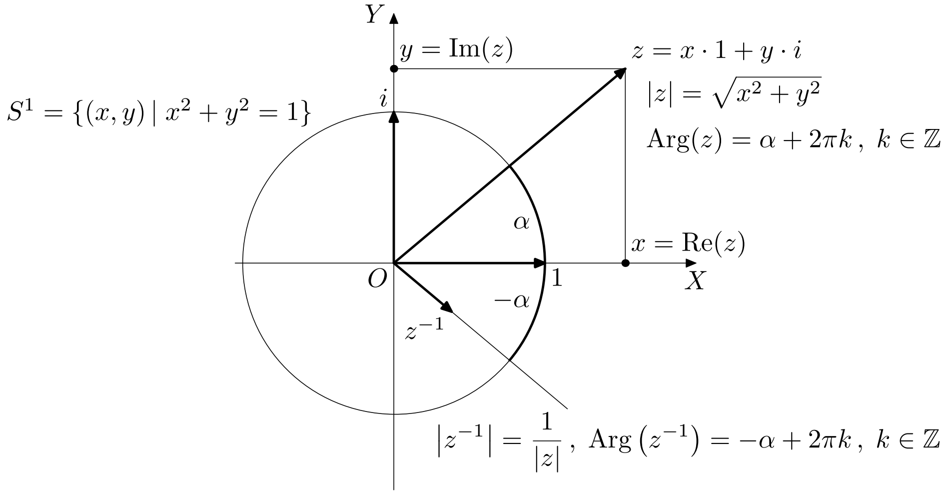
откуда $(-1) \cdot a = -a$.

Аксиома нетривиальности (2-10) равносильна требованию $\mathbb{F} \neq \{0\}$, поскольку при $0 = 1$ мы имели бы $a = a \cdot 1 = a \cdot 0 = 0 \; \forall \, a \in \mathbb{F}$.

2.3. Поле комплексных чисел. Обозначим через $\mathbb{C}$ вещественную координатную плоскость $\mathbb{R}^2$ с фиксированной прямоугольной системой координат OXY с началом в точке $O = (0, 0)$ и координатными осями OX и OY, направленными вдоль базисных векторов $(1, 0)$ и $(0, 1)$ (см. рис. 2◇2).

Точки z этой плоскости называются *комплексными числами*. Координаты (x, y) комплексного числа $z \in \mathbb{C}$ обозначаются через $\mathrm{Re}\,(z) = x$, $\mathrm{Im}\,(z) = y$ и называются *действительной* и *мнимой* частями числа z. Расстояние от z до начала координат $|z| = \sqrt{x^2 + y^2}$ называется *модулем* комплексного числа z .

Имеется взаимно однозначное соответствие между комплексными числами и векторами на плоскости, сопоставляющее каждому комплексному числу $z \in \mathbb{C}$ вектор с началом в O и концом в z, обычно называемый *радиус-вектором* числа z. В дальнейшем мы не будем делать разницы между точками и их радиус векторами, обозначая через z как точку, так и её радиус вектор. При этом точке $O = (0,0)$ отвечает нулевой вектор 0, а точкам $(1,0)$ и $(0,1)$ — стандартные базисные векторы, которые мы обозначим символами 1 и i соответственно. Радиус вектор произвольной точки $z \in \mathbb{C}$ с координатами (x, y) выражается через эти базисные векторы по формуле $z = x \cdot 1 + y \cdot i$.



2◇2. Комплексное число $z = x \cdot 1 + y \cdot i$.

Множество всех $\vartheta \in \mathbb{R}$, таких что поворот плоскости $\mathbb{C}$ вокруг точки 0 на угол ϑ совмещает координатный луч OX с лучом, идущим в направлении радиус вектора ненулевой точки $z \in \mathbb{C}$, называется *аргументом* числа z и обозначается $\mathrm{Arg}\,(z)$. Таким образом (ср. с n° 1.6.2),

$$\mathrm{Arg}\,(z) = \{\varphi + 2\pi k \mid k \in \mathbb{Z}\} \subset \mathbb{R}\,,$$

где φ — ориентированная длина дуги[1], идущей по единичной окружности из точки $(1,0)$ в точку $z/|z|$. Выражение радиус вектора z через базисные векторы 1 и i можно переписать как $z = |z| \cdot (\cos\varphi \cdot 1 + \sin\varphi \cdot i)$ с произвольным $\vartheta \in \mathrm{Arg}\,(z)$, поскольку $x = \mathrm{Re}\,(z) = |z| \cdot \cos\varphi$, $y = \mathrm{Im}\,(z) = |z| \cdot \sin\varphi$.

2.3.1. Сложение и умножение. Сложение комплексных чисел определяется как сложение радиус-векторов: $z_1 + z_2$ есть точка, радиус вектор которой равен сумме радиус-векторов точек z_1 и z_2. В координатах это описывается формулой

$$(x_1 \cdot 1 + y_1 \cdot i) + (x_2 \cdot 1 + y_2 \cdot i) = (x_1 + x_2) \cdot 1 + (y_1 + y_2) \cdot i\,.$$

[1] отметим, что таких дуг имеется бесконечно много, но все они отличаются друг от друга на целое число оборотов; эпитет «ориентированная» означает, что длину следует брать со знаком «+», если движение происходит против часовой стрелки, и со знаком «−», если по часовой стрелке

Как мы видели в n° 2.2.1, эта операция удовлетворяет четырём аксиомам абелевой группы.

Произведение комплексных чисел z_1 и z_2 определяется как число, модуль которого равен произведению модулей, а аргумент — сумме аргументов сомножителей:

$$|z_1 z_2| \overset{\text{def}}{=} |z_1| \cdot |z_2|$$

$$\mathrm{Arg}\,(z_1 z_2) \overset{\text{def}}{=} \mathrm{Arg}\,(z_1) + \mathrm{Arg}\,(z_2) = \{\vartheta_1 + \vartheta_2 \mid \vartheta_1 \in \mathrm{Arg}\,(z_1)\,,\ \vartheta_2 \in \mathrm{Arg}\,(z_2)\}$$

Отметим, что $0 \cdot z = 0 \quad \forall\, z \in \mathbb{C}$.

Упражнение 2.4. Проверьте, что вне зависимости от выбора $\varphi_i \in \mathrm{Arg}\,(z_i)$

$$\{\varphi_1 + 2\pi k \mid k \in \mathbb{Z}\} + \{\varphi_2 + 2\pi k \mid k \in \mathbb{Z}\} = \{(\varphi_1 + \varphi_2) + 2\pi k \mid k \in \mathbb{Z}\}\,.$$

Умножение комплексных чисел, очевидно, коммутативно и ассоциативно. Единичным элементом для него является единичный направляющий вектор оси OX, т. е. число $1 \in \mathbb{C}$. Обратным к ненулевому элементу z является число z^{-1} с

$$|z^{-1}| = 1/|z|\,, \quad \mathrm{Arg}\,(z^{-1}) = -\mathrm{Arg}\,(z) \tag{2-14}$$

(см. рис. 2◇2). Таким образом, ненулевые комплексные числа образуют коммутативную группу относительно умножения.

Отображение умножения на фиксированное число $a \in \mathbb{C}$

$$\lambda_a : \mathbb{C} \xrightarrow{z \mapsto az} \mathbb{C}$$

представляет собою *поворотную гомотетию*[1] плоскости $\mathbb{C}$ относительно начала координат на угол $\mathrm{Arg}\,(a)$ с коэффициентом $|a|$. Возникающая таким образом биекция между отличными от нуля точками $a \in \mathbb{C}$ и поворотными гомотетиями относительно начала координат согласована с имеющимися в этих мультипликативных группах умножениями: композиция поворотных гомотетий λ_a и λ_b это в точности поворотная гомотетия λ_{ab} с коэффициентом $|a||b|$ на угол $\mathrm{Arg}\,(a) + \mathrm{Arg}\,(b)$.

Предложение 2.1
Комплексные числа образуют поле.

Доказательство. Из всех свойств поля нам осталось проверить только дистрибутивность (2-9). На геометрическом языке формула $a(b+c) = ab + ac$ переписывается как $\lambda_a(b+c) = \lambda_a(b) + \lambda_a(c)$ и означает, что поворотные гомотетии перестановочны со сложением векторов, или — что то же самое — что любая поворотная гомотетия λ_a переводит параллелограмм в параллелограмм. Но это действительно так, поскольку всякий поворот и всякая гомотетия переводят параллелограмм в параллелограмм. □

[1]напомним, что *поворотной гомотетией* относительно точки O на угол α с коэффициентом $\varrho > 0$ называется композиция поворота на угол α вокруг точки O и растяжения в ϱ раз относительно O (поскольку растяжения коммутируют с поворотами, всё равно, в каком порядке эта композиция выполняется)

2.3.2. Алгебраическое представление комплексных чисел. Прежде всего заметим, что ось OX в поле $\mathbb{C}$ можно отождествить с полем вещественных чисел $\mathbb{R}$ — сложение и умножение комплексных чисел, лежащих на оси OX, в точности совпадает со сложением и умножением чисел вещественной числовой прямой. Поэтому разложение $z = x \cdot 1 + y \cdot i$ радиус-вектора z по базисным векторам $1 = (1,0)$ и $i = (0,1)$ с вещественными коэффициентами $x = \mathrm{Re}\,(z)$ и $y = \mathrm{Im}\,(z)$ является *верным равенством в поле* $\mathbb{C}$ — сложение и умножение в этой формуле могут восприниматься как сложение и умножение комплексных чисел.

Следуя обычной традиции опускать знаки произведений и умножение на единицу, мы будем далее сокращать формулу $z = x \cdot 1 + y \cdot i$ до $z = x + iy$. Пользуясь дистрибутивностью и равенством $i^2 = -1$, получаем следующую формулу для вычисления произведения комплексных чисел $z_1 = x_1 + iy_1$ и $z_2 = x_2 + iy_2$ в координатах:

$$z_1 z_2 = (x_1 + iy_1)(x_2 + iy_2) = (x_1x_2 - y_1y_2) + i(x_1y_2 + x_2y_1)\ . \tag{2-15}$$

Обратное к числу $z = x + iy$ число z^{-1} так же легко выражается через x и y:

$$z^{-1} = \frac{1}{x+iy} = \frac{x-iy}{(x+iy)(x-iy)} = \frac{x-iy}{x^2+y^2} = \frac{x}{|z|^2} - \frac{iy}{|z|^2}\ , \tag{2-16}$$

откуда $\mathrm{Re}\ (z^{-1}) = \mathrm{Re}\,(z)/|z|^2$ и $\mathrm{Im}\ (z^{-1}) = -\mathrm{Im}\,(z)/|z|^2$.

Число $\overline{z} \overset{\text{def}}{=} x - iy$ называется *комплексно сопряжённым* к числу $z = x + iy$. В терминах комплексного сопряжения формулу для обратного числа можно записать в виде $z^{-1} = \overline{z}/|z|^2$. Геометрически, комплексное сопряжение

$$\mathbb{C} \xrightarrow{z \mapsto \overline{z}} \mathbb{C}$$

представляет собою симметрию комплексной плоскости относительно вещественной оси OX. С алгебраической точки зрения сопряжение является инволютивным автоморфизмом поля $\mathbb{C}$, т. е. $\forall\, z \in \mathbb{C}\quad \overline{\overline{z}} = z$ и $\forall\ z_1, z_2 \in \mathbb{C}$ $\overline{z_1 + z_2} = \overline{z}_1 + \overline{z}_2$, $\overline{z_1z_2} = \overline{z}_1\overline{z}_2$.

2.3.3. Пример: тригонометрия. Казуистическое изобилие школьных тригонометрических формул по большей части является лишь изощрённой записью вполне заурядных вычислений с многочленами от комплексной переменной z, в которые подставляются числа, лежащие на единичной окружности.

Рассмотрим, к примеру, произвольные два комплексных числа единичной длины:

$$z_1 = \cos\varphi_1 + i\sin\varphi_1\ , \quad z_2 = \cos\varphi_2 + i\sin\varphi_2\ ,$$

Вычисляя произведение z_1z_2 по определению из n° 2.3.1 и по формуле (2-15), получаем равенство

$$\begin{aligned}\cos(\varphi_1+\varphi_2) + i\sin(\varphi_1+\varphi_2) &= z_1z_2 = \\ &= \Big(\cos\varphi_1\cos\varphi_2 - \sin\varphi_1\sin\varphi_2\Big) + i\Big(\cos\varphi_1\sin\varphi_2 + \sin\varphi_1\cos\varphi_2\Big)\ ,\end{aligned}$$

которое эквивалентно паре равенств на координаты

$$\cos(\varphi_1+\varphi_2)=\cos\varphi_1\cos\varphi_2-\sin\varphi_1\sin\varphi_2$$
$$\sin(\varphi_1+\varphi_2)=\cos\varphi_1\sin\varphi_2+\sin\varphi_1\cos\varphi_2$$

Тем самым, мы *доказали* тригонометрические формулы сложения аргументов.

Вот ещё один пример. Пусть $z=\cos\varphi+i\sin\varphi$. Согласно данному в n° 2.3.1 определению,

$$z^n=\cos(n\varphi)+i\sin(n\varphi)\,.$$

С другой стороны, раскрывая скобки в $(\cos\varphi+i\sin\varphi)^n$ по формуле (1-9) со стр. 10, получаем равенство

$$\begin{gathered}\cos(n\varphi)+i\sin(n\varphi)=(\cos\varphi+i\sin\varphi)^n=\\=\cos^n\varphi+i\binom{n}{1}\cos^{n-1}\varphi\sin\varphi-\binom{n}{2}\cos^{n-2}\varphi\sin^2\varphi-i\binom{n}{3}\cos^{n-3}\varphi\sin^3\varphi+\ \dots=\\=\left(\binom{n}{0}\cos^n\varphi-\binom{n}{2}\cos^{n-2}\varphi\sin^2\varphi+\binom{n}{4}\cos^{n-4}\varphi\sin^4\varphi-\dots\right)+\\+i\cdot\left(\binom{n}{1}\cos^{n-1}\varphi\sin\varphi-\binom{n}{3}\cos^{n-3}\varphi\sin^3\varphi+\binom{n}{5}\cos^{n-5}\varphi\sin^5\varphi-\dots\right)\end{gathered}$$

заключающее в себе сразу *все* мыслимые формулы для кратных углов:

$$\cos(n\varphi)=\binom{n}{0}\cos^n\varphi-\binom{n}{2}\cos^{n-2}\varphi\sin^2\varphi+\binom{n}{4}\cos^{n-4}\varphi\sin^4\varphi-\dots$$
$$\sin(n\varphi)=\binom{n}{1}\cos^{n-1}\varphi\sin\varphi-\binom{n}{3}\cos^{n-3}\varphi\sin^3\varphi+\binom{n}{5}\cos^{n-5}\varphi\sin^5\varphi-\dots$$

Например, $\cos 3\varphi=\cos^3\varphi-3\cos\varphi\cdot\sin^2\varphi=4\cos^3\varphi-3\cos^2\varphi\,.$

Упражнение 2.5. Выразите $\sin(2\pi/5)$ и $\cos(2\pi/5)$ через радикалы от рациональных чисел.

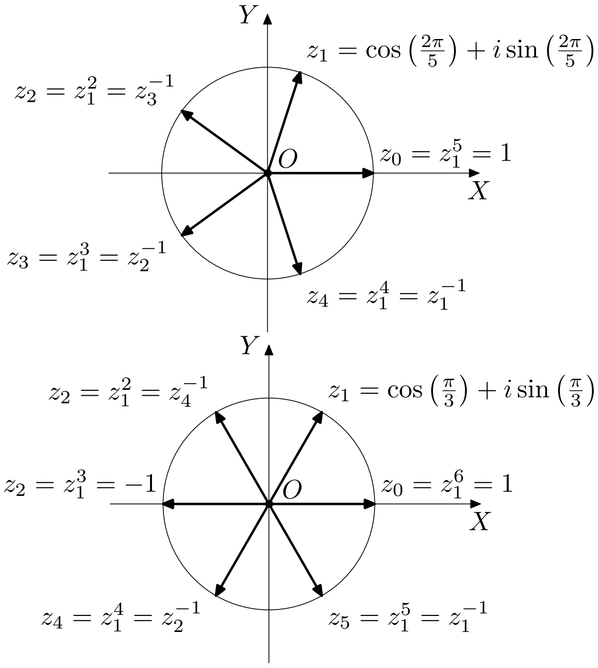
2.3.4. Пример: корни из единицы. Решим в поле $\mathbb{C}$ уравнение $z^n=1$. Сравнивая модули левой и правой части, получаем $|z^n|=|z|^n=1$, откуда $|z|=1$. Сравнивая аргументы левой и правой части уравнения, получаем

$$n\mathrm{Arg}\,(z)=\mathrm{Arg}\,(1)=\{2\pi k\mid k\in\mathbb{Z}\}\,.$$

Поскольку $n\varphi\in\{2\pi k\mid k\in\mathbb{Z}\}\iff\varphi\in\{2\pi k/n\mid k\in\mathbb{Z}\}$, имеется ровно n различных классов эквивалентности вещественных чисел по модулю добавления целых кратных 2π, которые при умножении их представителей на n превращаются в класс $\{2\pi k\mid k\in\mathbb{Z}\}$, — это классы n геометрически различных углов $2\pi k/n$ с $0\leqslant k\leqslant n-1$. Таким образом, уравнение $z^n=1$ имеет ровно n корней

$$\zeta_k=\cos(2\pi k/n)+i\sin(2\pi k/n)\quad(\text{где } k=0,\,1,\,\dots\,,\,(n-1))\,,$$

которые располагаются в вершинах правильного n-угольника, вписанного в единичную окружность так, что вершина ζ_0 находится в точке 1 (см. рис. 2◇3), и образуют абелеву группу относительно операции умножения. Эта группа обозначается $\boldsymbol{\mu}_n$ и называется *группой корней n-той степени из* единицы (фактически мы уже встречались с ней в n° 1.6.2).



2◇3. Корни уравнений $z^5 = 1$ и $z^6 = 1$.

Корень $\zeta \in \boldsymbol{\mu}_n$ называются *первообразным корнем* степени n из единицы, если все остальные элементы группы $\boldsymbol{\mu}_n$ представляются в виде ζ^k с $k \in \mathbb{N}$. Например, корень с наименьшим положительным аргументом

$$\zeta_1 = \cos(2\pi/n) + i\sin(2\pi/n)$$

является первообразным. Но есть и другие: скажем, на рис. 2◇3 все четыре отличных от 1 корня пятой степени из единицы являются первообразными, а в группе $\boldsymbol{\mu}_6$ первообразными являются ζ_1 и $\zeta_5 = \zeta_1^{-1}$ (а все остальные — нет).

Упражнение 2.6. Покажите, что корень $\zeta_1^k = \cos(2\pi k/n) + i\sin(2\pi k/n)$ является первообразным тогда и только тогда, когда $\text{нод}(k, n) = 1$.

Многочлен со старшим коэффициентом единица

$$\varPhi_n(z) = \prod_{\substack{1 \leqslant k < n:\\ \text{нод}(k,n)=1}} (z - z_1^k)\,, \tag{2-17}$$

корнями которого являются первообразные корни n-той степени из 1 и только они, называется n-тым *круговым* (или *циклотомическим*) многочленом. Так, пятый и шестой круговые многочлены равны

$$\Phi_5(z) = (z - z_1)(z - z_2)(z - z_3)(z - z_4) = z^4 + z^3 + z^2 + z + 1$$
$$\Phi_6(z) = (z - z_1)(z - z_4) = z^2 - z + 1 \ .$$

Упражнение 2.7*. Покажите, что все круговые многочлены $\Phi_n(z)$ имеют целые коэффициенты и *неприводимы* над $\mathbb{Q}$ (т. е. не являются произведениями многочленов строго меньшей степени с рациональными коэффициентами).

2.3.5. Пример: уравнение $z^n = a$. Корни уравнения $z^n = a$ это числа $z = |z|\cdot(\cos\varphi + i\sin\varphi)$ с $|z|^n = |a|$, а $n\varphi \in \operatorname{Arg}(a)$. При $a = |a|\cdot(\cos\alpha + i\sin\alpha) \neq 0$ имеется ровно n таких чисел

$$z_k = \sqrt[n]{|a|}\cdot\Big(\cos\big((\alpha+2\pi k)/n\big) + i\cdot\sin\big((\alpha+2\pi k)/n\big)\Big)$$

с $k = 0, 1, \dots, (n-1)$. Они располагаются в вершинах правильного n-угольника, вписанного в окружность радиуса $\sqrt[n]{|a|}$ с центром в нуле так, что радиус-вектор одной из его вершин располагается под углом α/n к оси OX.

2.4. Коммутативные кольца. Множество K с двумя операциями называется *коммутативным кольцом с единицей*, если эти эти операции обладают всеми свойствами из определения поля[1] за исключением свойства (2-8) существования мультипликативно обратного элемента.

Если, кроме существования обратного, из списка аксиом поля исключаются требование существования единицы (2-7) и условие $0 \neq 1$, то множество K с двумя операциями, удовлетворяющими оставшимся аксиомам, называется просто *коммутативным кольцом*.

Примерами отличных от полей колец с единицами являются кольцо целых чисел $\mathbb{Z}$ и кольцо многочленов с коэффициентами в произвольном коммутативном кольце с единицей. Примеры коммутативных колец без единицы доставляют чётные целые числа, многочлены с чётными целыми коэффициентами, многочлены без свободного члена с коэффициентами в любом коммутативном кольце и т. п.

Упражнение 2.8. Убедитесь, что все перечисленные в n° 2.2.3 следствия из аксиом поля остаются в силе в любом коммутативном кольце с единицей.

2.4.1. Пример: гауссовы целые числа. Рассмотрим в $\mathbb{C}$ подкольцо, состоящее из всех чисел с целыми координатами

$$\mathbb{Z}[i] \overset{\text{def}}{=} \{z = x + iy \mid x, y \in \mathbb{Z}\} \ .$$

Оно называется кольцом *гауссовых целых чисел* и часто используется в арифметике. Например, классическая задача о представлении натурального числа в

[1] см. опр. 2.1 на стр. 21

виде суммы двух квадратов целых чисел существенно проясняется расширением кольца $\mathbb{Z}$ до кольца $\mathbb{Z}[i]$. В самом деле, в кольце гауссовых чисел $x^2 + y^2 = (x+iy)(x-iy)$. Таким образом, вопрос о разрешимости в кольце $\mathbb{Z}$ уравнения $x^2 + y^2 = n^2$ на неизвестные $x, y \in \mathbb{Z}$ равносилен вопросу о разрешимости в кольце $\mathbb{Z}[i]$ уравнения $n = z \cdot \overline{z}$ на неизвестную $z \in \mathbb{Z}[i]$. В такой постановке сразу же видно, к примеру, что если числа m_1 и m_2 представляются в виде суммы двух квадратов

$$m_1 = a_1^2 + b_1^2 = (a_1 + ib_1)(a_1 - ib_1) = z_1\overline{z}_1$$
$$m_2 = a_2^2 + b_2^2 = (a_2 + ib_2)(a_2 - ib_2) = z_2\overline{z}_2$$

то их произведение $m = m_1 m_2$ также является суммой двух квадратов:

$$m = z_1 z_2 \cdot \overline{z_1 z_2} = |z_1 z_2|^2 = (a_1 b_1 - a_2 b_2)^2 + (a_1 b_2 + a_2 b_1)^2 .$$

Это наблюдение в сочетании с теоремой о единственности разложения на простые множители в кольце $\mathbb{Z}[i]$ позволяет свести исходную задачу к задаче о представимости простых чисел. Мы ещё вернёмся к этому[1] в n° 6.5.4.

2.5. Делимость. Основным отличием колец от полей является возможное отсутствие для некоторых элементов кольца обратных к ним элементов относительно умножения. Элемент a коммутативного кольца K с единицей называется *обратимым*, если в этом кольце существует такой элемент a^{-1}, что $a^{-1}a = 1$. В противном случае элемент a называется *необратимым*.

Например, в кольце $\mathbb{Z}$ обратимыми элементами являются только 1 и -1. В кольце $\mathbb{Q}[x]$ многочленов с рациональными коэффициентами обратимыми элементами являются ненулевые константы (многочлены степени нуль).

Упражнение 2.9. Покажите, что обратимыми элементами кольца $\mathbb{Z}[i]$ являются четыре числа: ± 1 и $\pm i$.

Между элементами произвольного коммутативного кольца имеется нетривиальное *отношение делимости*. Говорят, что элемент *a делится* на элемент b, если в кольце существует элемент q, такой что $a = bq$. Это записывается как $b|a$ (читается «b делит a») или как $a \,⋮\, b$ (читается «a делится на b»). Отношение делимости тесно связано с решением линейных уравнений.

2.5.1. Пример: уравнение $ax + by = k$ и НОД в кольце $\mathbb{Z}$. Зафиксируем какие-нибудь целые числа a и b и обозначим через

$$(a, b) \stackrel{\text{def}}{=} \{ax + by \mid x, y \in \mathbb{Z}\} \tag{2-18}$$

множество всех целых чисел, представимых в виде $ax + by$ с целыми x, y. Это множество образует в $\mathbb{Z}$ подкольцо, и вместе с каждым своим элементом содержит и все его кратные. Кроме того, все числа из (a, b) нацело делятся на каждый общий делитель чисел a и b, а сами a и b тоже входят в (a, b).

[1] эта задача и множество других изящных вычислений с гауссовыми числами имеются также в книге: *К. Айэрленд, М. Роузен. Классическое введение в современную теорию чисел.* М., «Мир», 1987 (или любое другое издание)

Обозначим через d наименьшее положительное число в (a, b). Остаток от деления любого числа $z \in (a, b)$ на d лежит в кольце (a, b), поскольку он представляется в виде $z - kd$, а z и kd лежат в кольце (a, b). Так как этот остаток строго меньше d, он равен нулю. Следовательно, $(a, b) = (d)$ совпадает с множеством всех чисел, кратных d.

Таким образом, число d является общим делителем чисел $a, b \in (a, b)$, представляется в виде $d = ax + by$ и делится на любой общий делитель чисел a и b, а произвольное число $k \in \mathbb{Z}$ представляется в виде $k = ax + by$ тогда и только тогда, когда оно делится на d. Число d называется *наибольшим общим делителем* чисел $a, b \in \mathbb{Z}$ и обозначается $\text{нод}(a, b)$.

Упражнение 2.10. Обобщите предыдущее рассуждение: для любого конечного набора чисел $a_1, a_2, \dots, a_m$ постройте число d, которое является общим делителем всех a_i, делится на любой общий делитель всех a_i и представляется в виде $d = a_1x_1 + a_2x_2 + \dots + a_mx_m$ с целыми x_i. Покажите, что уравнение $n = a_1x_1 + a_2x_2 + \dots + a_mx_m$ разрешимо относительно x_i в кольце $\mathbb{Z}$ тогда и только тогда, когда n делится на d.

2.5.2. Алгоритм Евклида позволяет явно найти $\text{нод}(a, b)$ и представить его в виде $\text{нод}(a, b) = ax + by$. Работает он так. Пусть $a \geqslant b$. Положим

$$E_0 = a\,,\ E_1 = b\,,\ E_k = \text{остатку от деления } E_{k-2} \text{ на } E_{k-1} \text{ (при } k \geqslant 1). \tag{2-19}$$

Числа E_k строго убывают до тех пор, пока очередное число E_r не разделит нацело предыдущее число E_{r-1}, в результате чего E_{r+1} обратится в нуль. Последний ненулевой элемент E_r последовательности E_k и будет наибольшим общим общим делителем чисел (a, b), причём он автоматически получится представленным в виде $E_r = x \cdot E_0 + y \cdot E_1$, если при вычислении каждого E_k мы будем представлять его в виде $E_k = x \cdot E_0 + y \cdot E_1$.

Упражнение 2.11. Докажите это.

Например, для чисел $n = 10\,203$ и $m = 4\,687$ вычисление состоит из восьми шагов:

$$\begin{aligned}
E_0 &= 10\,203 \\
E_1 &= \ 4\,687 \\
E_2 &= \quad 829 = E_0 - 2\,E_1 = \quad +1\,E_0 \quad -2E_1 \\
E_3 &= \quad 542 = E_1 - 5\,E_2 = \quad -5\,E_0 \quad +11E_1 \\
E_4 &= \quad 287 = E_2 - E_3 = \quad +6\,E_0 \quad -13E_1 \\
E_5 &= \quad 255 = E_3 - E_4 = \quad -11\,E_0 \quad +24E_1 \\
E_6 &= \quad 32 = E_4 - E_5 = \quad +17\,E_0 \quad -37E_1 \\
E_7 &= \quad 31 = E_5 - 7\,E_6 = \quad -130\,E_0 \quad +283E_1 \\
E_8 &= \quad 1 = E_6 - E_7 = \quad +147\,E_0 \quad -320E_1 \\
[E_9 &= \quad 0 = E_7 - 31\,E_8 = -4\,687\,E_0 + 10\,203E_1]
\end{aligned} \tag{2-20}$$

(взятая в скобки последняя строка служит для проверки). Таким образом,

$$\text{нод}(10\,203, 4\,687) = 1 = 147 \cdot 10\,203 - 320 \cdot 4\,687\,.$$

Упражнение 2.12. Докажите, что возникающее на последнем шаге алгоритма Евклида представление нуля в виде $E_{r+1} = q_0 E_0 + q_1 E_1 = 0$ (см. последнюю строку в (2-20)) содержит *наименьшее общее кратное* $\text{нок}(a, b) = |q_0 E_0| = |q_1 E_1|$ (иначе говоря, $\text{нод}(q_0, q_1) = 1$).

Отметим, что с вычислительной точки зрения алгоритм Евклида *несопоставимо* быстрее разложения на простые множители. Читателю предлагается убедиться в этом, попытавшись «вручную» разложить на простые множители числа $n = 10\,203$ и $m = 4\,687$ из абсолютно ручного вычисления (2-20). Найти два очень больших простых числа по заданному их произведению невозможно за разумное время даже на мощном компьютере. Это обстоятельство лежит в основе многих популярных систем шифрования данных.

2.6. Взаимная простота. В произвольном коммутативном кольце K, на элементах которого нет естественного упорядочения, *наибольший общий делитель* элементов $a, b \in K$ определяется как такой элемент $d \in K$, который делит a и b и делится на любой элемент с таким свойством.

Это определение не гарантирует ни существования наибольшего общего делителя, ни его единственность (даже в кольце $\mathbb{Z}$ по этому определению мы получаем два наибольших общих делителя, различающиеся знаком).

Тем не менее, понятие *взаимной простоты* элементов a и b можно определить в любом кольце с единицей так, что многие полезные свойства взаимно простых элементов, справедливые в кольце $\mathbb{Z}$, остаются в силе в любом кольце.

Идея заключается в том, что взаимная простота чисел $a, b \in \mathbb{Z}$ равносильна разрешимости в целых числах уравнения $ax + by = 1$, и именно возможность решать такое уравнение, а не условие $\text{нод}(a, b) = 1$, является наиболее существенным свойством, использующимся в рассуждениях, опирающихся на взаимную простоту.

Определение 2.2

Элементы a и b произвольного коммутативного кольца K с единицей называются *взаимно простыми*, если уравнение

$$ax + by = 1 \tag{2-21}$$

разрешимо относительно x и y в кольце K.

Лемма 2.1

В произвольном коммутативном кольце K для любого $c \in K$ и любых взаимно простых $a, b \in K$ справедливы импликации:

(1) если ac делится на b, то c делится на b

(2) если c делится и на a, и на b, то c делится и на ab.

Кроме того, если $a \in K$ взаимно прост с каждым из элементов $b_1, b_2, \dots, b_n$, то он взаимно прост и с их произведением $b_1 b_2 \ \dots \ b_m$.

Доказательство. Умножая равенство (2-21) на c, получаем равенство

$$c = acx + bcy \ , \tag{2-22}$$

из которого сразу следуют обе импликации (1) и (2). Далее, пусть для каждого i существуют такие $x_i, y_i \in K$, что $ax_i + b_i y_i = 1$. Перемножим все эти равенства и соберём в одно слагаемое все члены, содержащие сомножитель a, который мы вынесем из них за скобку. Получим равенство вида

$$a \cdot X + (b_1 b_2 \cdots b_n) \cdot (y_1 y_2 \cdots y_n) = 1$$

(второе слагаемое — это единственный член, не содержащий a). Оно и означает взаимную простоту a и $b_1 b_2 \cdots b_n$. □

Упражнение 2.13. Пользуясь лем. 2.1, докажите следующую теорему об однозначности разложения на простые множители в кольце $\mathbb{Z}$: всякое целое число z является произведением конечного числа простых чисел[1], причём любые два таких представления $p_1 p_2 \cdots p_k = z = q_1 q_2 \cdots q_m$ имеют одинаковое число сомножителей $k = m$, и эти сомножители можно перенумеровать так, чтобы $\forall\ i$ $p_i = \pm q_i$.

Задачи для самостоятельного решения к §2

Задача 2.1. Найдите вещественную и мнимую часть, модуль, аргумент и по возможности точно нарисуйте комплексные числа

а) $\dfrac{(5+i)(7-6i)}{3+i}$ б) $\dfrac{(1+i)^5}{(1-i)^3}$ в) $\left(\dfrac{\sqrt{3}+i}{1-i}\right)^{30}$

Задача 2.2. Используя только сложение, вычитание, умножение, деление и извлечение квадратных корней из вещественных чисел явно выразите действительные и мнимые части корней квадратного уравнения $z^2 = a$ через действительную и мнимую части числа a.

Задача 2.3. Решите уравнения: а) $z^2 + (2i - 7)z + (13 - i) = 0$ б) $z^3 = i$ в) $(z+1)^n - (z-1)^n = 0$ г) $(z+i)^n + (z-i)^n = 0$ д) $\overline{z} = z^3$.

Задача 2.4. Вычислите $z^m + 1/z^m$, если $z + 1/z = 2\cos\theta$.

Задача 2.5. Выразите $\sin 5\varphi$ через $\sin\varphi$ и получите для $\sin\left(\frac{4\pi}{5}\right)$ и $\cos\left(\frac{2\pi}{5}\right)$ выражения в радикалах от рациональных чисел.

[1] напомним, что целое число называется *простым*, если оно не раскладывается в произведение двух чисел, каждое из которых отлично от ± 1

Задача 2.6 (эйлеровы разложения). Убедитесь, что $\frac{\sin mx}{\sin x}$ является при нечётном $m \in \mathbb{N}$ многочленом от $\sin^2 x$, найдите степень, корни и старший коэффициент этого многочлена, и получите отсюда тождества

а) $\dfrac{\sin(mx)}{\sin x} = (-4)^{\frac{m-1}{2}} \prod\limits_{j=1}^{\frac{m-1}{2}} \left(\sin^2 x - \sin^2\left(\frac{2\pi j}{m}\right)\right)$

б) $(-1)^{\frac{m-1}{2}} \sin(mx) = 2^{m-1} \prod\limits_{j=0}^{m-1} \sin\left(x + \frac{2\pi j}{m}\right)$

Задача 2.7. Вычислите сумму и произведение всех корней, а также s-тых степеней всех корней степени n из единицы (для любого $s \in \mathbb{N}$).

Задача 2.8. Вычислите суммы: а) $\binom{n}{0} + \binom{n}{4} + \binom{n}{8} + \cdots$; б) $\binom{n}{1} + \binom{n}{5} + \binom{n}{9} + \cdots$
в) $\binom{n}{1} - \frac{1}{3}\binom{n}{5} + \frac{1}{9}\binom{n}{9} + \cdots$; г) $\sin x + \sin 2x + \cdots + \sin nx$
д) $\sin^2 x + \sin^2 3x + \cdots + \sin^2(2n-1)$; е) $\cos x + 2\cos 2x + \cdots + n\cos nx$.

Задача 2.9. Покажите, что три различных точки z_1, z_2, $z_3 \in \mathbb{C}$ тогда и только тогда лежат на одной прямой, когда $(z_1 - z_3)/(z_2 - z_3) \in \mathbb{R}$.

Задача 2.10. Покажите, что четыре различных точки z_1, z_2, z_3, $z_4 \in \mathbb{C}$, не лежащие на одной прямой, тогда и только тогда лежат на одной окружности, когда их *двойное отношение* $\frac{(z_1-z_3):(z_2-z_3)}{(z_1-z_4):(z_2-z_4)} \in \mathbb{R}$.

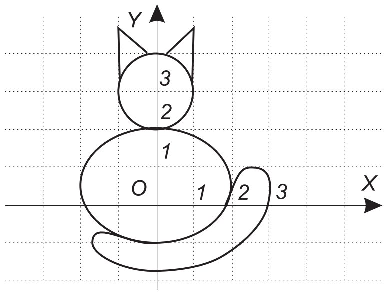


Рис. 2◇4. Комплексная кошечка.

Задача 2.11. Куда переводятся отображениями $z \mapsto z^2$ и $z \mapsto \frac{1}{z}$
а) прямая $y = kx$ б) декартова и полярная координатные сетки
в) окружность $|z + i| = 1$ г) кошечка с рис. рис. 2◇4?

Задача 2.12. Докажите, что отображение $z \longmapsto (az + b)/(cz + d)$ (где $a, b, c, d \in \mathbb{C}$) переводит окружности и прямые или в окружности, или в прямые, сохраняя при этом углы.

Задача 2.13. Покажите, что всякое комплексное число $z \neq -1$ с $|z| = 1$ можно представить в виде $z = (1 + ti)/(1 - ti)$ с $t \in \mathbb{R}$.

Задача 2.14 (топология комплексной плоскости). По определению, *ε-окрестностью* числа $z \in \mathbb{C}$ называется открытый круг радиуса ε с центром в z. Пределы комплексных последовательностей, а также вещественно- и комплексно-значных функций на $\mathbb{C}$, непрерывность таких функций, открытые и замкнутые подмножества в $\mathbb{C}$ и т. п. определяются на языке ε-окрестностей в $\mathbb{C}$ дословно так же, как и в $\mathbb{R}$.

а) Сформулируйте и докажите теоремы о пределе суммы и пределе произведения двух сходящихся комплексных последовательностей.

б) Покажите, что $\lim\limits_{n\to\infty}(x_n + iy_n) = a + ib$ в $\mathbb{C}$ тогда и только тогда, когда в $\mathbb{R}$ существуют оба предела $\lim\limits_{n\to\infty} x_n = a$ и $\lim\limits_{n\to\infty} y_n = b$.

в) Покажите, что в любой ограниченной последовательности можно выделить подпоследовательность, имеющую предел.

г) Покажите, что любая непрерывная функция $f : \mathbb{C} \longrightarrow \mathbb{R}$ на любом ограниченном замкнутом подмножестве $Z \subset \mathbb{C}$ достигает в некоторых точках Z своих минимального и максимального значений на Z.

Задача 2.15 (алгебраическая замкнутость поля $\mathbb{C}$). Пусть $f \in \mathbb{C}[x]$ — произвольный многочлен с $\deg f > 0$. Покажите, что а) $|f|$ непрерывен

б) $\forall M \in \mathbb{R}\ \exists$ замкнутый круг $B \subset \mathbb{C} : |f(z)| > M\ \forall z \notin B$

в) $|f(z)|$ достигает в некоторой точке $z_0 \in \mathbb{C}$ своего минимума

г) вблизи любой точки $z_0 \in \mathbb{C}$, такой что $f(z_0) \neq 0$, найдётся точка z_1, в которой $|f(z_1)| < |f(z_0)|$. А именно, положим $z = z_0 + w$ и перепишем f как многочлен от w, упорядочив мономы по возрастанию степени:

$$f(z) = f(z_0) + a_m w^m + \text{ более старшие степени } w$$

(где $a_m \neq 0$ — самый первый из ненулевых коэффициентов при степенях w). Пусть ϑ — любой из m корней $\sqrt[m]{-f(z_0)/a_m}$ (так что $a_m\vartheta^m = -f(z_0)$). Покажите, что при достаточно малом $t \in \mathbb{R}$ число $z_1(t) = z_0 + t\,\vartheta$ обладает требуемым свойством $|f(z_1)| < |f(z_0)|$.

д) Выведите из предыдущего, что любой отличный от константы многочлен $f \in \mathbb{C}[x]$ имеет корень в $\mathbb{C}$.

§3. Кольца и поля вычетов

3.1. Кольцо вычетов $\mathbb{Z}/(n)$. Напомним (см. n° 1.4.1), что числа $a, b \in \mathbb{Z}$ называются *сравнимыми* по модулю n (что записывается как $a \equiv b \pmod{n}$), если их разность $a - b$ делится на n. Сравнимость по модулю n является отношением эквивалентности (см. n° 1.4) и разбивает множество целых чисел на непересекающиеся классы сравнимых по модулю n чисел. Эти классы называются *классами вычетов по модулю* n, а их совокупность обозначается через $\mathbb{Z}/(n)$. Мы будем писать $[a]_n \in \mathbb{Z}/(n)$ для обозначения класса, содержащего число $a \in \mathbb{Z}$. Такая запись неоднозначна: например, $[-1]_n = [n-1]_n$ обозначают один и тот же класс.

Всего имеется n различных классов: $[0]_n$, $[1]_n$, ... , $[(n-1)]_n$. Сложение и умножение классов вычетов задаётся правилами:

$$[a] + [b] \stackrel{\text{def}}{=} [a + b] \,, \quad [a] \cdot [b] \stackrel{\text{def}}{=} [ab] \,. \tag{3-1}$$

Согласно упр. 1.8 на стр. 13, эти операции определены корректно[1]. Они очевидным образом удовлетворяют аксиомам коммутативного кольца с единицей — формулы (3-1) сводят операции над вычетами к операциям над целыми числами, для которых аксиомы кольца выполняются.

3.1.1. Делители нуля и нильпотенты. В $\mathbb{Z}/(10)$ произведение классов $[2]$ и $[5]$ равно нулю, хотя *каждый* из них отличен от нуля, а в кольце $\mathbb{Z}/(8)$ ненулевой класс $[2]$ имеет нулевой куб $[2]^3 = [8] = [0]$.

В произвольном кольце K элемент $a \in K$ называется *делителем нуля*, если $a \neq 0$ и $ab = 0$ для некоторого ненулевого $b \in K$. Кольцо с единицей без делителей нуля называется *целостным*.

Ненулевой элемент a кольца K называется *нильпотентом*, если $a^n = 0$ для некоторого $n \in \mathbb{N}$. Отметим, что всякий нильпотент автоматически является делителем нуля. Кольцо с единицей без нильпотентов называется *приведённым*. Всякое целостное кольцо автоматически приведено.

Упражнение 3.1. Составьте таблицы сложения и умножения в кольцах $\mathbb{Z}/(n)$ для $n = 3, 4, 5, 6, 7, 8$. Найдите в этих кольцах все делители нуля, все нильпотенты, и все обратимые элементы. Для обратимых элементов составьте таблицу обратных. Какие из этих колец являются полями?

Обратимый элемент a не может быть делителем нуля, поскольку, умножая обе части равенства $ab = 0$, мы получаем $b = 0$. Поэтому кольцо с делителями нуля не может быть полем.

3.1.2. Обратимые элементы кольца вычетов. Обратимость класса $[m]_n \in \mathbb{Z}/(n)$ означает существование такого класса $[x]_n$, что$[m]_n[x]_n = [mx]_n = [1]_n$. Последнее равенство означает существование целых x и y, таких что $mx + ny =$

[1] т. е. не зависят от способа записи классов или, что то же самое — от выбора представителей $a \in [a]$ и $b \in [b]$

1 в кольце $\mathbb{Z}$. Таким образом, класс $[m]_n$ обратим в кольце $\mathbb{Z}/(n)$ тогда и только тогда, когда числа m и n взаимно просты в кольце $\mathbb{Z}$.

Проверить, обратим ли данный класс $[m]_n$, и если да, то явно вычислить обратный класс $[m]_n^{-1}$,можно при помощи алгоритма Евклида из n° 2.5.2. Скажем, вычисление (2-20) на стр. 32 показывает, что класс $[10\,203]$ обратим в $\mathbb{Z}/(4\,687)$ и $[10\,203]^{-1} = [147] \pmod{4\,687}$, а класс $[4\,687]$ обратим в $\mathbb{Z}/(10\,203)$ и $[4\,687]^{-1} = -[320] \pmod{10\,203}$.

Обратимые элементы кольца $\mathbb{Z}/(n)$ образуют абелеву группу относительно умножения. Эта группа называется*группой обратимых вычетов* по модулю n и обозначается $\mathbb{Z}/(n)^*$. Число элементов в ней равно количеству натуральных чисел, меньших n и взаимно простых с n. Оно обозначается через $\varphi(n)$ и называется *функцией Эйлера* от числа $n \in \mathbb{N}$.

3.2. Поле вычетов $\mathbb{F}_p = \mathbb{Z}/(p)$. Из сказанного выше вытекает, что это кольцо вычетов $\mathbb{Z}/(n)$ является полем тогда и только тогда, когда n является *простым числом*. В самом деле, если $n = mk$ составное, ненулевые классы $[m], [k] \in \mathbb{Z}/(n)$ будут делителями нуля и не могут быть обратимы. Напротив, если p простое число, то $\text{нод}(m, p) = 1$ для всех m не кратных p, а значит, каждый ненулевой класс $[m] \in \mathbb{Z}/(p)$ обратим.

Поле $\mathbb{Z}/(p)$, где p простое, принято обозначать $\mathbb{F}_p$.

3.2.1. Пример: бином Ньютона по модулю p. В поле $\mathbb{F}_p = \mathbb{Z}/(p)$ выполняется замечательное равенство

$$\underbrace{1 + 1 + \cdots + 1}_{p \text{ раз}} = 0\,. \tag{3-2}$$

Из него вытекает, что для любых $a, b \in \mathbb{F}_p$ выполняется равенство

$$(a + b)^p = a^p + b^p\,. \tag{3-3}$$

В самом деле, раскрывая скобки в биноме $(a + b)^p$, мы для каждого k получим $\binom{p}{k}$ одночленов $a^k b^{p-k}$, сумма которых равна

$$a^k b^{p-k} \cdot (\underbrace{1 + 1 + \cdots + 1}_{\binom{p}{k} \text{ раз}})\,.$$

При $k \neq 0, p$ заключенная в скобках сумма единиц равна нулю в силу равенства (3-2) и следующего простого замечания.

Лемма 3.1
При простом p и любом k в пределах $1 \leqslant k \leqslant (p-1)$ биномиальный коэффициент $\binom{p}{k}$ делится на p.

Доказательство. Поскольку число p взаимно просто с каждым из чисел в пределах от 1 до $p-1$, оно по лем. 2.1 взаимно просто с произведением $k!(p-k)!$.

Поскольку $p!$ делится на $k!(p-k)!$, мы из того же лем. 2.1 заключаем, что $(p-1)!$ делится на $k!(p-k)!$. Следовательно, $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ делится на p. □

Следствие 3.1 (малая теорема Ферма)
$a^p \equiv a \pmod p$ при любом простом p и любом $a\mathbb{Z}$.

Доказательство. Надо показать, что $[a^p] = [a]$ в поле $\mathbb{F}_p$. Согласно (3-3), имеем

$$[a]^p = (\underbrace{[1] + [1] + \ \cdots \ + [1]}_{a \text{ раз}})^p = \underbrace{[1]^p + [1]^p + \ \cdots \ + [1]^p}_{a \text{ раз}} = \\ = \underbrace{[1] + [1] + \ \cdots \ + [1]}_{a \text{ раз}} = [a]\,.$$

□

Упражнение 3.2. Покажите, что $\binom{mp^n}{p^n} \equiv m \pmod p$ при нод$(m,p) = 1$.

3.2.2. Пример: конечные геометрии. Многие понятия и конструкции из геометрии вещественной координатной плоскости $\mathbb{R}^2$ или вещественного координатного пространства $\mathbb{R}^3$ сохраняют свой смысл после замены поля вещественных чисел $\mathbb{R}$ *произвольным* полем $\mathbb{F}$.

А именно, будем называть *координатной плоскостью* $\mathbb{F}^2$ множество упорядоченных пар элементов поля $\mathbb{F}$:

$$\mathbb{F}^2 \stackrel{\text{def}}{=} \mathbb{F} \times \mathbb{F} = \{(x,y) \mid x, y \in \mathbb{F}\}$$

Пары $(x, y \in \mathbb{F}^2$ мы будем называть *точками*. Кроме точек мы будем рассматривать ещё и *векторы*, также представляющие собою упорядоченные пары чисел $(a_1, a_2) \in \mathbb{F} \times \mathbb{F}$. Подчеркнём, что векторы рассматриваются *отдельно* от точек.

Векторы можно складывать и умножать на числа из поля $\mathbb{F}$: если $a = (a_1, a_2)$, $b = (b_1, b_2)$ и $\lambda \in \mathbb{F}$, то по определению $a + b = (a_1 + a_2, b_1 + b_2)$ и $\lambda \cdot a = (\lambda a_1, \lambda a_2)$. Таким образом, векторы образуют абелеву группу относительно операции сложения. Эту группу можно воспринимать как *группу преобразований сдвига* точечного пространстве $\mathbb{F}^2$ в смысле n° 1.6: каждому вектору $v = (v_1, v_2)$ отвечает *сдвиг на вектор* v

$$\tau_v : \mathbb{F}^2 \xrightarrow{(x,y) \mapsto (x+v_1, y+v_2)} \mathbb{F}_2\,,$$

при этом композиции сдвигов отвечает сложение векторов: $\tau_v \tau_w = \tau_{v+w}$.

Прямую на плоскости $\mathbb{F}^2$ можно *определить* либо как множество точек (x, y), удовлетворяющих линейному уравнению $ax + by = c$, в котором хотя бы один из коэффициентов a, b отличен от нуля, либо как траекторию движения точки $z_0 = (x_0, y_0)$ с ненулевой постоянной скоростью $v = (v_1, v_2)$, т. е. как множество точек вида $z_t = z_0 + tv = (x_0 + tv_1, y_0 + tv_2)$, где «время» t пробегает поле $\mathbb{F}$. Эти два определения эквивалентны в том смысле, что прямая, заданная уравнением $ax + by = c$ представляет собой траекторию любой своей точки, выпущенной со скоростью $(-b, a)$, и наоборот, траектория точки (x_0, y_0), выпущенной со скоростью $v = (v_1, v_2)$, задаётся уравнением $v_2x - v_1y = v_2x_0 - v_1y_0$.

Упражнение 3.3. Проверьте, что на плоскости $\mathbb{F}^2$ над любым полем $\mathbb{F}$ выполняются евклидовы аксиомы инцидентности:

а) имеются три точки, не лежащие на одной прямой;

б) через любые две точки проходит ровно одна прямая;

в) через любую точку, не лежащую на произвольно данной прямой, проходит ровно одна прямая, не пересекающаяся с данной.

Таким образом, все конфигурационные задачи[1] по планиметрии имеют смысл *над любым полем* — например, над конечным полем $\mathbb{F}_p$ из p элементов.

Плоскость $\mathbb{F}_p^2$ над полем $\mathbb{F}_p$ состоит из p^2 точек. Каждая лежащая на ней прямая содержит в точности p из них, поскольку точки $z + t_1v$ и $z + t_2v$ различны при $t_1 \neq t_2$.

Упражнение 3.4. Покажите, что через каждую точку плоскости $\mathbb{F}_p^2$ проходит ровно $(p^2 - 1)/(p - 1) = p + 1$ прямых и что всего на этой плоскости имеется $\binom{p^2}{2}/\binom{p}{2} = p(p+1)$ прямых.

4	3	∞	2	1
2	4	∞	1	3
0	0	+	0	0
3	1	∞	4	2
1	2	∞	3	4

Рис. 3◇1. Шесть проходящих через начало координат прямых на плоскости $\mathbb{F}_5^2$.

На рис. 3◇1 изображены все 25 точек плоскости $\mathbb{F}_5^2$. Начало координат отмечено знаком $+$, точки каждой проходящей через начало координат прямой $y = kx$ (где $k = 0, 1, \dots, \infty$) отмечены соответствующей цифрой k (горизонтальной и вертикальной координатным осям отвечают $k = 0$ и $k = \infty$). Обратите внимание, что четыре точки «3» составляют вместе с точкой «+» одну прямую (также как и четыре точки «2»).

Упражнение 3.5. Нарисуйте на плоскости $\mathbb{F}_5^2$ кривые, заданные уравнениями

$$y = x^2\,, \quad x^2 + y^2 = 1\,, \quad x^2 + y^2 = -1\,.$$

Упражнение 3.6. Сколько прямых и плоскостей имеется в трёхмерном пространстве $\mathbb{F}_p^3$ над полем из p элементов, и сколько из них проходит через начало координат?

3.3. Прямые произведения. Из любого набора абелевых групп

$$A_1, A_2, \dots, A_m$$

[1] т. е. относящиеся к взаимному расположению точек и прямых и не использующие понятий из метрической геометрии, таких как расстояния или величины углов

можно изготовить новую абелеву группу, которая называется *прямым произведением* групп A_ν , обозначается

$$\prod_\nu A_\nu = A_1 \times A_2 \times \cdots \times A_\nu = \{(a_1, a_2, \dots, a_m) \mid a_\nu \in A_\nu \ \forall \nu\} \tag{3-4}$$

и состоит из упорядоченных наборов $(a_1, a_2, \dots, a_m)$ элементов $a_\nu \in A_\nu$, групповая операция на которых определяется покомпонентно:

$$(a_1, a_2, \dots, a_m) \cdot (h_1, h_2, \dots, h_m) = (a_1 \cdot h_1,\ a_2 \cdot h_2,\ \cdots,\ a_m \cdot h_m)\,. \tag{3-5}$$

Упражнение 3.7. Проверьте, что так определённая операция коммутативна и ассоциативна, нулевым элементом для неё является набор нулей $(0, 0, \dots, 0)$, а противоположным к набору $(a_1, a_2, \dots, a_m)$ является набор $(-a_1, -a_2, \dots, -a_m)$.

Если каждая из групп $A_1, A_2, \dots, A_m$ конечна, прямое произведение (3-4) тоже конечно и состоит из $|\prod A_\nu| = \prod |A_\nu|$ элементов.

Отметим, что определение прямого произведения имеет смысл не только для конечных, но и для любых семейств абелевых групп A_ν, занумерованных элементами $\nu \in X$ произвольного множества X. Соответствующее произведение обозначается в этом случае через

$$\prod_{\nu \in X} A_\nu\,.$$

Аналогичным образом, для любого семейства коммутативных колец $\{K_x\}$ (где индекс x пробегает произвольное множество X) определено прямое произведение $\prod K_x$, представляющее собою множество упорядоченных наборов элементов

$$(\dots, a_x, \dots)\,, \quad \text{с} \quad a_x \in K_x$$

и покомпонентным сложением и умножением:

$$\begin{aligned}(\dots, a_x, \dots) + (\dots, b_x, \dots) &\overset{\text{def}}{=} (\dots, a_x + b_x, \dots)\\ (\dots, a_x, \dots)(\dots, b_x, \dots) &\overset{\text{def}}{=} (\dots, a_x b_x, \dots)\,.\end{aligned}$$

Упражнение 3.8. Проверьте, что $\prod K_x$ является кольцом, причём если все K_x были кольцами с единицей, то $\prod K_x$ также будет кольцом с единицей $(1, 1, \dots, 1)$.

Пусть, к примеру, $X = \mathbb{R}$ и все $K_x = \mathbb{R}$, т. е. перемножается континуальное семейство одинаковых экземпляров поля $\mathbb{R}$, занумерованных действительными числами $x \in \mathbb{R}$. В этом случае произведение $\prod\limits_{x \in \mathbb{R}} \mathbb{R}_x$ изоморфно кольцу функций $f : \mathbb{R} \longrightarrow \mathbb{R}$ с обычными операциями поточечного сложения и умножения значений функций: изоморфизм переводит семейство вещественных чисел $(f_x) \in \prod\limits_{x \in \mathbb{R}} \mathbb{R}_x$, занумерованное вещественным числом x, в функцию $f : \mathbb{R} \longrightarrow \mathbb{R}$, значение которой в точке $x \in \mathbb{R}$ равно x-тому элементу семейства f: $f(x) = f_x$.

Прямое произведение $\geqslant 2$ колец всегда имеет делители нуля: любой ненулевой элемент, имеющий хотя бы одну нулевую компоненту, является делителем нуля. Например, $(0, 1, 1, \dots, 1)$ является делителем нуля, поскольку

$$(0, 1, 1, \dots, 1)(1, 0, 0, \dots, 0) = (0, 0, 0, \dots, 0) = 0\,.$$

Таким образом, произведение колец (в частности, произведение полей) никогда не является полем.

Например, если $\mathbb{F}_p$ и $\mathbb{F}_q$ — конечные поля, состоящие соответственно из p и q элементов, то в их произведении $\mathbb{F}_p \times \mathbb{F}_q$ будет ровно $(p-1)(q-1)$ обратимых элементов (a, b), образующих мультипликативную группу $\mathbb{F}_p^* \times \mathbb{F}_q^*$ и $p + q - 2$ делителя нуля, имеющих вид $(a, 0)$ и $(0, b)$ с $a, b \neq 0$.

В общем случае элемент $a = (a_1, a_2, \dots, a_m) \in K_1 \times K_2 \times \cdots \times K_m$ обратим тогда и только тогда, когда каждая его компонента $a_\nu \in K_\nu$ обратима в своём кольце K_ν. Поэтому группа обратимых элементов кольца $\prod K_\nu$ является прямым произведением групп обратимых элементов колец K_ν:

$$\Big(\prod K_\nu\Big)^* = \prod K_\nu^* \tag{3-6}$$

3.4. Гомомрфизмы. Отображение абелевых групп $\varphi : A \longrightarrow B$ называется *гомоморфизмом*, если для любой пары элементов $a_1, a_2 \in A$ в кольце B выполнено соотношение

$$f(a_1 + a_2) = f(a_1) + f(a_2) \tag{3-7}$$

Отметим, что этим условиям, в частности, удовлетворяет *нулевой* (или *тривиальный*) гомоморфизм, отображающий все элементы A в нулевой элемент B.

Упражнение 3.9. Убедитесь, что композиция гомоморфизмов тоже является гомоморфизмом.

Всякий гомоморфизм $\varphi : A \longrightarrow B$ переводит нулевой элемент A в нулевой элемент B, поскольку $\varphi(0) = \varphi(0 + 0) = \varphi(0) + \varphi(0)$, и, вычитая из правой и левой части $\varphi(0)$, получаем $0 = \varphi(0)$. Далее, из равенств

$$\varphi(a) + \varphi(-a) = \varphi(a + (-a)) = \varphi(0) = 0$$

мы заключаем, что $\varphi(-a) = -\varphi(a)$. В частности, образ $\operatorname{im}\varphi = \varphi(A) \subset B$ любого гомоморфизма $\varphi : A \longrightarrow B$ является абелевой подгруппой в B.

3.4.1. Ядро гомоморфизма. Полный прообраз нулевого элемента B при гомоморфизме $\varphi : A \longrightarrow B$ называется *ядром* гомоморфизма φ и обозначается

$$\ker\varphi = \varphi^{-1}(0) = \{a \in A \mid \varphi(a) = 0\}\,.$$

Ядро образует в A подгруппу, поскольку из равенств $\varphi(a_1) = 0$ и $\varphi(a_2) = 0$ вытекает равенство $\varphi(a_1 \pm a_2) = \varphi(a_1) \pm \varphi(a_2) = 0 \pm 0 = 0$.

Два элемента $a_1, a_2 \in A$ тогда и только тогда переходят в один и тот же элемент в B, когда $a_1 - a_2 \in \ker(\varphi)$:

$$\varphi(a_1) = \varphi(a_2) \quad \iff \quad \varphi(a_1 - a_2) = \varphi(a_1) - \varphi(a_2) = 0\,.$$

Мы получили

Предложение 3.1
Слой гомоморфизма абелевых групп $\varphi : A \longrightarrow B$ над произвольной точкой $b \in B$ либо пуст, либо равен

$$\varphi^{-1}(b) = a + \ker\varphi = \{a + a' \mid a' \in \ker\varphi\}\,,$$

где $a \in A$ — какой-нибудь элемент, переходящий в b. В частности, φ инъективен тогда и только тогда, когда $\ker\varphi = \{0\}$. $\square$

3.4.2. Группа гомоморфизмов. Гомоморфизмы $A \longrightarrow B$ образуют абелеву группу относительно операции поточечного сложения значений: по определению, $\varphi_1 + \varphi_2 : a \longmapsto \varphi_1(a) + \varphi_2(a)$. Нулевым элементом этой группы является *нулевой гомоморфизм*, отображающий все элементы A в нулевой элемент B. Мы обозначаем группу гомоморфизмов $A \longrightarrow B$ через $\mathrm{Hom}(A, B)$.

3.4.3. Гомоморфизмы колец. Отображение колец $\varphi : A \longrightarrow B$ называется *гомоморфизмом колец*, если для любой пары элементов $a_1, a_2 \in A$ в кольце B выполнены соотношения:

$$\begin{gathered} f(a_1 + a_2) = f(a_1) + f(a_2) \\ f(a_1 a_2) = f(a_1) f(a_2)\,. \end{gathered} \tag{3-8}$$

Таким образом, любой гомоморфизм колец $\varphi : A \longrightarrow B$ является гомоморфизмом аддитивных абелевых групп, а значит обладает всеми перечисленными выше свойствами, в частности, $\varphi(0) = 0$, $\varphi(-a) = -\varphi(a)$, и все непустые слои φ представляют собою сдвиги слоя над нулём: если $\varphi(a) = b$, то полный прообраз

$$\varphi^{-1}(b) = a + \ker\varphi = \{a + a' \mid a' \in \ker\varphi\}$$

(в частности, φ инъективен тогда и только тогда, когда $\ker\varphi = \{0\}$).

Ядро гомоморфизма колец вместе с каждым $a \in \ker\varphi$ содержит и все его кратные aa', поскольку $\varphi(aa') = \varphi(a)\varphi(a') = 0$. В частности, $\ker\varphi$ является подкольцом в A.

Образ гомоморфизма колец $\varphi : A \longrightarrow B$, очевидно, является подкольцом в B. Отметим, однако, что это подкольцо может не содержать единицы, поскольку $1 \in A$ может не перейти в $1 \in B$. Например, отображение

$$\mathbb{Z} \xrightarrow{\varphi} \mathbb{Z}/(6)\,,$$

переводящее все чётные числа в $[0]_6$, а все нечётные — в $[3]_6$, является гомоморфизмом колец, и $\varphi(1) = [3]_6 \neq [1]_6$.

Тем не менее, для целостного кольца B справедливо

Предложение 3.2
Любой ненулевой гомоморфизм произвольного кольца с единицей в целостное кольцо переводит единицу в единицу.

Доказательство. Так как $\varphi(1) = \varphi(1 \cdot 1) = \varphi(1) \cdot \varphi(1)$, мы имеем равенство $\varphi(1)(\varphi(1) - 1) = 0$, которое в целостном кольце возможно либо при $\varphi(1) = 1$, либо при $\varphi(1) = 0$. Во втором случае $\forall\, a \in A \;\; \varphi(a) = \varphi(1 \cdot a) = \varphi(1)\varphi(a) = 0$. □

3.4.4. Гомоморфизмы полей. Если кольца A и B являются полями, то всякий ненулевой гомоморфизм колец $\varphi : A \longrightarrow B$ является гомоморфизмом мультипликативных групп этих полей. В частности, $\varphi(a/b) = \varphi(a)/\varphi(b)$ для всех a и всех ненулевых b.

Предложение 3.3
Любой ненулевой гомоморфизм из поля в произвольное кольцо является вложением.

Доказательство. Если $\varphi(a) = 0$ для какого-нибудь $a \neq 0$, то $\forall\, b \in A$

$$\varphi(b) = \varphi\left(ba^{-1}a\right) = \varphi\left(ba^{-1}\right)\varphi(a) = 0\,.$$

Поэтому любой ненулевой гомоморфизм из поля имеет нулевое ядро. □

3.5. Китайская теорема об остатках. Пусть число $n \in \mathbb{Z}$ является произведением m попарно взаимно простых сомножителей: $n = n_1 n_2 \cdots n_m$. Покажем, что в этом случае кольцо вычетов $\mathbb{Z}/(n)$ изоморфно прямому произведению колец вычетов $\mathbb{Z}/(n_i)$, т. е. построим такое взаимно однозначное отображение

$$\mathbb{Z}/(n) \xrightarrow{\;\varphi\;} (\mathbb{Z}/(n_1)) \times (\mathbb{Z}/(n_2)) \times \,\cdots\, \times (\mathbb{Z}/(n_m))\,,$$

что $\forall\, a, b \in \mathbb{Z}/(n)$ $\varphi(a+b) = \varphi(a) + \varphi(b)$ и $\varphi(ab) = \varphi(a)\varphi(b)$ в $\prod \mathbb{Z}/(n_i)$. Зададим φ правилом

$$\varphi\left([z]_n\right) \stackrel{\text{def}}{=} \left([z]_{n_1}, [z]_{n_2}, \ldots, [z]_{n_m}\right) \qquad \forall\, z \in \mathbb{Z}\,.$$

Это правило корректно (не зависит от выбора числа $z \in \mathbb{Z}$ в классе $[z]_n \subset \mathbb{Z}$), поскольку равенство $[z_1]_n = [z_2]_n$ означает, что разность $z_1 - z_2$ делится на $n = n_1 n_2 \cdots n_m$, а значит, она делится и на каждое n_i, и стало быть, для каждого i мы будем иметь равенство $[z_1]_{n_i} = [z_2]_{n_i}$. Очевидно, также, что φ является гомоморфизмом:

$$\begin{aligned}
\varphi\left([z]_n + [w]_n\right) = \varphi\left([z+w]_n\right) &= \left([z+w]_{n_1}, [z+w]_{n_2}, \ldots, [z+w]_{n_m}\right) = \\
&= \left([z]_{n_1} + [w]_{n_1}, [z]_{n_2} + [w]_{n_2}, \ldots, [z]_{n_m} + [w]_{n_m}\right) = \\
= \left([z]_{n_1}, [z]_{n_2}, \ldots, [z]_{n_m}\right) &+ \left([w]_{n_1}, [w]_{n_2}, \ldots, [w]_{n_m}\right) = \varphi\left([z]_n\right) + \varphi\left([w]_n\right)
\end{aligned}$$

и ровно то же самое произойдёт с умножением.

Покажем, что φ нулевое ядро. Рассмотрим класс $[z]_n \in \ker(\varphi)$. Поскольку для любого i класс $[z]_{n_i}$ нулевой, z делится на каждое n_i, а так как все n_i попарно взаимно просты, то по лем. 2.1 z делится на их произведение, которое равно n. Тем самым $[z]_n = 0$, что и требовалось.

По предл. 3.1 гомоморфизм с нулевым ядром является вложением. А так как оба кольца $\mathbb{Z}/(n)$ и $\prod \mathbb{Z}/(n_i)$ состоят из одинакового числа элементов $n = \prod n_i$, гомоморфизм φ должен быть биекцией. Этот факт известен как *китайская теорема об остатках*.

На классическом языке китайская теорема об остатках утверждает, что для любого набора остатков $r_1, r_2, \ldots, r_m$ от деления на попарно взаимно простые числа $n_1, n_2, \ldots, n_m$ можно подобрать такое целое число z, которое даёт остаток r_i от деления *на каждое* из n_i, причём любые два числа z_1, z_2, решающие эту задачу, различаются на целое кратное числа $n = n_1 n_2 \cdots n_k$.

Для практического отыскания такого числа z полезно установить сюрьективность гомоморфизма φ непосредственно, не прибегая к предл. 3.1.

Для этого заметим, что из взаимной простоты числа n_i с остальными n_ν вытекает, что n_i взаимно просто и с их произведением $m_i = \prod\limits_{\nu \neq i} n_\nu$ (см. лем. 2.1), т. е. для каждого i найдутся такие $x_i, y_i \in \mathbb{Z}$, что $n_i x_i + m_i y_i = 1$. Число $b_i = m_i y_i$ даёт остаток 1 от деления на n_i и делится на все n_ν с $\nu \neq i$, и мы можем взять

$$z = r_1 b_1 + r_2 b_2 + \cdots + r_m b_m .$$

Для демонстрации эффективности этого алгоритма найдём, к примеру, наименьшее натуральное число, имеющее остатки $r_1 = 2$, $r_2 = 7$ и $r_3 = 43$ от деления, соответственно, на $n_1 = 57$, $n_2 = 91$ и $n_3 = 179$.

Сначала найдём $y_1 \in \mathbb{Z}$, такое что $91 \cdot 179 \cdot y_1 \equiv 1 \pmod{57}$. Поскольку $91 \cdot 179 \equiv 34 \cdot 8 \equiv -13 \pmod{57}$, достаточно применить алгоритм Евклида к $E_0 = 57$ и $E_1 = 13$. В результате получим $22 \cdot 13 - 5 \cdot 57 = 1$. Таким образом,

$$b_1 = -22 \cdot 91 \cdot 179 \quad (\equiv 22 \cdot 13 \pmod{57})$$

даёт при делении на 57, 91 и 179 остатки (1, 0, 0). Аналогичным образом находим числа

$$\begin{aligned} b_2 &= -33 \cdot 57 \cdot 179 \quad && (\equiv 33 \cdot 11 \pmod{91}) \\ b_3 &= -45 \cdot 57 \cdot 91 && (\equiv 45 \cdot 4 \pmod{179}) \end{aligned}$$

дающие при делении на 57, 91 и 179 остатки (0, 1, 0) и (0, 0, 1) соответственно. Тогда требуемые остатки (2, 7, 43) имеет число

$$\begin{aligned} z &= 2\,b_1 + 7\,b_2 + 43\,b_3 = \\ &= -(2 \cdot 22 \cdot 91 \cdot 179 + 7 \cdot 33 \cdot 57 \cdot 179 + 43 \cdot 45 \cdot 57 \cdot 91) = \\ &= -(716\,716 + 2\,356\,893 + 10\,036\,845) = -13\,110\,454 , \end{aligned}$$

а все остальные числа, дающие такие остатки, отличаются от него на целые кратные числа $n = 57 \cdot 91 \cdot 179 = 928\,473$. Наименьшим положительным среди них является $z + 15\,n = 816\,641$.

3.6. Простое подполе и характеристика. Для любого кольца с единицей K имеется канонический гомоморфизм

$$\begin{gathered} \mathbb{Z} \xrightarrow{\varkappa} K \\ \varkappa(\pm n) = \pm(\underbrace{1+1+\,\cdots\,+1}_{n}) \quad \text{для} \quad n \in \mathbb{N}\,. \end{gathered} \tag{3-9}$$

Если $\varkappa$ инъективен, то говорят, что K имеет *характеристику нуль*. В противном случае *характеристикой* называют наименьшее натуральное число p, для которого

$$\underbrace{1+1+\,\cdots\,+1}_{p} = 0\,.$$

Характеристика кольца K обозначается через $\mathrm{char}(K)$.

Предложение 3.4

Характеристика целостного кольца либо равна нулю либо является простым числом.

Доказательство. Сумма любого составного числа единиц является произведением сумм меньших количеств единиц:

$$\underbrace{1+1+\,\cdots\,+1}_{mn} = (\underbrace{1+1+\,\cdots\,+1}_{m})(\underbrace{1+1+\,\cdots\,+1}_{n})\,,$$

и если в K нет делителей нуля, из равенства нулю такого произведения вытекает равенство нулю одного из сомножителей. □

3.6.1. Простое подполе. Пусть $K = \mathbb{F}$ является полем. Наименьшее по включению подполе в $\mathbb{F}$, содержащее 1 и 0, называется *простым подполем* в $\mathbb{F}$.

В силу своего определения простое подполе содержит образ $\mathrm{im}\,(\varkappa)$ гомоморфизма (3-9). Если $\mathrm{char}(\mathbb{F}) = p > 0$, простое подполе совпадает с $\mathrm{im}\,(\varkappa)$ и изоморфно полю $\mathbb{F}_p$. В самом деле, в этом случае $(p) \subset \ker \varkappa$ и отображение $\mathbb{Z}/(p) \longrightarrow \mathbb{F}$, переводящее $a \pmod p$ в $\varkappa(a)$, корректно определено и является сюрьективным гомоморфизмом. По предл. 3.3 этот гомоморфизм инъективен, т. е. является изоморфизмом на образ $\varkappa$. Итак, простым подполем в поле характеристики $p > 0$ является конечное поле $\mathbb{F}_p$.

Если $\mathrm{char}(\mathbb{F}) = 0$, т. е. $\varkappa(q) \neq 0$ при $q \neq 0$, гомоморфизм $\varkappa$ продолжается до гомоморфизма полей

$$\varkappa : \mathbb{Q} \xhookrightarrow{p/q \mapsto \varkappa(p)/\varkappa(q)} \mathbb{F}\,.$$

По предл. 3.3 он инъективен. Тем самым, простое подполе поля характеристики нуль изоморфно полю рациональных чисел $\mathbb{Q}$.

Упражнение 3.10. Покажите, что любой автоморфизм поля оставляет на месте каждый элемент из его простого подполя.

Отметим, что из этого упражнения вытекает, что поле $\mathbb{Q}$ остаётся неподвижным при любом автоморфизме полей $\mathbb{R}$ и $\mathbb{C}$.

Упражнение 3.11. Покажите, что между полями разной характеристики нет ненулевых гомоморфизмов.

3.6.2. Гомоморфизм Фробениуса. Если $\mathrm{char}(\mathbb{F}) = p > 0$, тоже самое вычисление, что и в (n° 3.2), показывает, что

$$\forall\, a, b \in \mathbb{F} \quad (a+b)^p = a^p + \sum_{k=1}^{p-1} (\underbrace{1 + 1 + \dots + 1}_{\binom{p}{k}}) a^k b^{p-k} + b^p = a^p + b^p\,.$$

Тем самым, отображение возведения в p-тую степень

$$F_p : \mathbb{F} \xrightarrow{x \mapsto x^p} \mathbb{F}$$

является гомоморфизмом из поля $\mathbb{F}$ в себя. Он называется *гомоморфизмом Фробениуса*. Согласно малой теореме Ферма (сл. 3.1 на стр. 39) гомоморфизм Фробениуса тождественно действует на простом подполе $\mathbb{F}_p \subset \mathbb{F}$.

Задачи для самостоятельного решения к §3

Задача 3.1. Вычислите нод(a, b) и представьте его в виде $ax + by$ с $x, y \in \mathbb{Z}$ для следующих (a, b): а) $(17,\ 13)$ б) $(44\,863,\ 70\,499)$ в) $(8\,385\,403,\ 2\,442\,778)$.

Задача 3.2. Покажите, что: а) $a^2 + b^2 \,⋮\, 7 \Rightarrow a \,⋮\, 7$ и $b \,⋮\, 7$
б) $a^3 + b^3 + c^3 \,⋮\, 7 \Rightarrow abc \,⋮\, 7$ в) $a^2 + b^2 + c^2 + d^2 + e^2 \,⋮\, 9 \Rightarrow abcde \,⋮\, 9$.

Задача 3.3. Имеет ли уравнение $x^2 + y^2 + z^2 = 2xyz$ ненулевые решения в целых числах?

Задача 3.4. Зафиксируем некоторый класс $a \in \mathbb{Z}/(n)$ и рассмотрим отображение умножения $\alpha : \mathbb{Z}/(n) \xrightarrow{x \mapsto ax} \mathbb{Z}/(n)$ Покажите, что обратимость класса a равносильна каждому из условий: а) a не делитель нуля б) α инъективно в) α сюрьективно г) α биективно.

Задача 3.5 (теорема Эйлера). Пусть в условиях предыдущей задачи a обратим. Изобразим все числа $\mathbb{Z}/(n)$ точками, и проведём из каждой точки x стрелку в точку ax. Покажите, что на этой картинке

а) движение по стрелкам распадается на непересекающиеся циклы

б) всякий цикл, содержащий хоть один обратимый вычет, весь состоит только из обратимых вычетов

в) все циклы, состоящие из обратимых вычетов, имеют одинаковую длину

г) $a^{\varphi(n)} = 1$, где $\varphi(n)$ равно числу обратимых элементов кольца $\mathbb{Z}/(n)$.

Задача 3.6. Делится ли а) $2222^{5555}+5555^{2222}$ на 7? б) $2^{70}+3^{70}$ на 13?

Задача 3.7. Найдите остаток от деления $2007^{2008^{2009}}$ на 11.

Задача 3.8. Вычислите остатки всех степеней десятки от деления на 2, 5, 4, 3, 9, 11, 7, 13 и укажите как можно более простые способы отыскания остатка данного числа от деления на 2, 5, 4, 3, 9, 11, 7, 13 по цифрам его десятичной записи (например: остаток от деления на 3 равен остатку суммы цифр).

Задача 3.9 (первообразные корни в кольце вычетов). Наименьшее $k\in\mathbb{N}$, такое что $b^k=1$ называется *порядком* обратимого вычета a. Вычет $a\in\mathbb{Z}/(n)$ называется *первообразным корнем* по модулю n, если все обратимые элементы кольца $\mathbb{Z}/(n)$ являются его степенями.

а) Докажите, что обратимый вычет тогда и только тогда является первообразным корнем, когда его порядок равен $\varphi(n)$.

б) Пусть порядки $k_1,k_2,\dots,k_n$ вычетов $a_1,a_2,\dots,a_n$ попарно взаимно просты. Чему равен порядок вычета $a=a_1\cdots a_n$?

в) Пусть вычеты порядков k и m существуют. Существует ли вычет порядка $\text{нок}(k,m)$?

г) Докажите, что первообразный корень существует по любому простому модулю.

д) Пусть ϱ — первообразный корень по простому модулю $p>2$. Докажите, что существует $\vartheta\in\mathbb{N}$, такое что $(\varrho+p\vartheta)^{p-1}\equiv 1\,(\operatorname{mod} p)$, но $(\varrho+p\vartheta)^{p-1}\not\equiv 1\,(\operatorname{mod} p^2)$, и что класс $\varrho+p\vartheta$ является первообразным корнем по модулю p^k для всех $k\in\mathbb{N}$.

е) Докажите существование первообразного корня по модулю $2\,p^k$ для всех простых p и всех $k\mathbb{N}$.

ж) Существует ли первообразный корень по модулю 21?

Задача 3.10 (идемпотенты). Вычет $a\in\mathbb{Z}/(n)$ называется *идемпотентом*, если $a^2=a$. Покажите, что а) любой идемпотент является делителем нуля

б) a идемпотент тогда и только тогда, когда $1-a$ идемпотент.

в) При каких n в $\mathbb{Z}/(n)$ имеются идемпотенты?

Задача 3.11. Найдите все идемпотенты в $\mathbb{Z}/(n)$ для а) $n=6$ б) $n=36$ в) $n=p_1p_2\cdots p_n$ г) $n=p_1^{m_1}p_2^{m_2}\cdots p_n^{m_n}$ (где p_i различные простые числа)

Задача 3.12. Найдите *все* целые решения уравнений: а) $28\,x+30\,y+31\,z=365$ б) $1537\,x+1387\,y=1$ в) $5\,x+7\,y=11$ г) $26\,x+32\,y=60$ д) $169\,x+221\,y=26$

Задача 3.13. Чему равно 91-е натуральное число, одновременно дающее остатки:

а) 2 и 7 от деления, соответственно, на 57 и 179?

б) 1, 2, 3 от деления на 2, 3, 5? в) 2, 4, 6, 8 от деления на 5, 9, 11, 14?

Задача 3.14. Сколько решений имеет уравнение $x^2=1$ в $\mathbb{Z}/(n)$ при чётном $n\geqslant 4$?

Задача 3.15. Докажите, что для любого $m\in\mathbb{N}$ существует $n\in\mathbb{N}$, такое что уравнение $x^2=1$ имеет не менее m решений в $\mathbb{Z}/(n)$.

Задача 3.16. Сколько решений имеют уравнения а) $x^3 = 1$ б) $x^2 = 49$ в кольце вычетов $\mathbb{Z}/(360)$?

Задача 3.17. Напишите приведённый многочлен $x^m + a_1x^{m-1} + \cdots + a_{m-1}x + a_m$ минимальной возможной степени с коэффициентами $a_i \in \mathbb{Z}/(n)$, имеющий в $\mathbb{Z}/(n)$ ровно n различных корней для а) $n = 101$ б) $n = 111$ в) $n = 121$

Задача 3.18 (функция Эйлера). Функция $f : \mathbb{Z} \longrightarrow \mathbb{C}$ называется *мультипликативным характером*, если $f(mn) = f(m)f(n)$ при взаимно простых m, n.
а) Покажите, что $\varphi(n)$ является мультипликативным характером
б) Покажите, что для $n = p_1^{k_1} \cdots p_n^{k_n}$ (где все p_i просты и различны)

$$\varphi(n) = n \cdot \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_n}\right) .$$

в) Найдите все n с $\varphi(n) = 10$.

Задача 3.19 (функция Мёбиуса). Функция Мёбиуса $\mu(n)$ сопоставляет каждому $n \in \mathbb{N}$ нуль, если n делится на квадрат простого числа, и $(-1)^s$, где s — число всех натуральных простых делителей n, если n не делится на квадраты простых чисел; кроме того, $\mu(1) = 1$. Покажите, что
а) $\mu(n)$ является мультипликативным характером числа n
б) $\sum\limits_{d|n} \mu(d) = \begin{cases} 1 \text{ при } n = 1 \\ 0 \text{ при } n > 1 \end{cases}$

Задача 3.20 (обращение Мёбиуса). Пусть для функции $\mathbb{N} \xrightarrow{g} \mathbb{C}$ при каждом $n \in \mathbb{N}$ известно значение суммы $\sigma(n) = \sum\limits_{d|n} g(d)$. Покажите, что функция g восстанавливается по функции σ по формуле $g(n) = \sum\limits_{d|n} \sigma(d) \cdot \mu(n/d)$.

Задача 3.21. Для произвольного $m \in \mathbb{N}$ вычислите $\sum\limits_{d|m} \varphi(d)$.

Задача 3.22. Решите в $\mathbb{F}_p$ уравнение $x^2 = 1$ и вычислите произведение всех ненулевых элементов поля $\mathbb{F}_p$.

Задача 3.23 (теорема Вильсона). Покажите, что натуральное число $p \geqslant 2$ просто тогда и только тогда, когда $(p-1)! + 1$ делится на p.

Задача 3.24. Покажите, что мультипликативная группа ненулевых элементов поля $\mathbb{F}_p$ циклическая[1].

Задача 3.25. Какие значения принимают многочлены $x^p - x$, x^{p-1} и $x^{\frac{p-1}{2}}$ на $\mathbb{F}_p$ и на множестве квадратов из $\mathbb{F}_p$?

Задача 3.26. Выясните, сколько в поле $\mathbb{F}_p$ имеется ненулевых квадратов, и покажите, что уравнение $x^2 + y^2 = -1$ разрешимо в $\mathbb{F}_p$ при любом p.

[1] т. е. все элементы этой группы являются степенями какого-нибудь одного элемента

Задача 3.27 (лемма Гаусса). Выпишем элементы поля $\mathbb{F}_p$ в строку вида:

$$-[(p-1)/2]\,,\ \dots\ ,\ -[1]\,,\ [0]\,,\ [1]\,,\ \dots\ ,\ [(p-1)/2]\,.$$

Докажите, что $a \in \mathbb{F}_p$ тогда и только тогда является квадратом, когда число «положительных» чисел этой записи, становящихся «отрицательными» от умножения на a, чётно.

Задача 3.28. При каких p в $\mathbb{F}_p$ разрешимы уравнения а) $x^2 = -1$ б) $x^2 = 2$

Задача 3.29. При каком простом p есть ненулевой гомоморфизм $\mathbb{Z}[i] \longrightarrow \mathbb{F}_p$?

Задача 3.30 (квадратичная взаимность). Пусть p — простое число. Сопоставим каждому $n \in \mathbb{Z}$ *символ Лежандра – Якоби*

$$\left(\frac{n}{p}\right) \stackrel{\text{def}}{=} \begin{cases} 0\,, \text{ если } n \text{ делится на } p \\ 1\,, \text{ если } n \text{ является ненулевым квадратом по модулю } p \\ -1\,, \text{ если } n \text{ не является квадратом по модулю } p \end{cases}$$

а) Покажите, что при фиксированном p символ $\left(\frac{n}{p}\right)$ является мультипликативным характером числа n (см. зад. 3.18).

б) Вычислите $\displaystyle\sum_{n=1}^{p-1}\left(\frac{n}{p}\right)$

в) Сравните знак $\left(\frac{m}{p}\right)$ со знаком произведения $\displaystyle\prod_{j=1}^{\frac{p-1}{2}} \frac{\sin\left(\frac{2\pi m}{p}\cdot j\right)}{\sin\left(\frac{2\pi}{p}\cdot j\right)}$.

г) Разложив все отношения синусов в предыдущем равенстве по формулам из зад. 2.6, докажите для любых простых чисел $p, q \in \mathbb{N}$ *квадратичный закон взаимности* Гаусса

$$\left(\frac{p}{q}\right)\cdot\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\,.$$

д) Найдите $\left(\frac{43}{109}\right)$.

Задача 3.31. Докажите эквивалентность друг другу следующих свойств простого числа $p \in \mathbb{N}$: а) -1 является квадратом в $\mathbb{F}_p$ б) $p \not\equiv 3 \pmod 4$

в) p перестаёт быть простым[1] в кольце гауссовых чисел $\mathbb{Z}[i]$

г) p является суммой двух квадратов натуральных чисел

Задача 3.32 (разложение в сумму двух квадратов). В предположении, что в кольце гауссовых чисел $\mathbb{Z}[i]$ справедлива теорема об однозначности разложения на простые[2] множители, докажите, что натуральное число тогда и только тогда не является ни квадратом ни суммой двух квадратов, когда в его разложение на простые множители входит нечётная степень простого числа вида $4k+3$.

---

[1] т. е. распадается в произведение чисел со строго меньшим модулем

[2] т. е. неразложимые в произведение двух необратимых сомножителей; мы докажем эту теорему в §6

§4. Многочлены и алгебраические числа

Всюду в этом параграфе мы обозначаем через K произвольное коммутативное кольцо с единицей, а через $\Bbbk$ — произвольное поле.

4.1. Ряды и многочлены. Бесконечное выражение вида

$$A(t) = \sum_{\nu \geqslant 0} a_\nu t^\nu = a_0 + a_1 t + a_2 t^2 + \cdots \quad \text{с} \quad a_i \in K \tag{4-1}$$

называется *формальным степенным рядом* от переменной t с коэффициентами в кольце K. Два формальных степенных ряда

$$\begin{aligned} A(t) &= a_0 + a_1 t + a_2 t^2 + \cdots \\ B(t) &= b_0 + b_1 t + b_2 t^2 + \cdots \end{aligned} \tag{4-2}$$

равны, если $a_i = b_i$ для всех i. Рад (4-1), у которого все коэффициенты кроме a_0 нулевые, называется *константой*.

Сложение и умножение рядов (4-2) определяется стандартными правилами раскрытия скобок и приведения подобных слагаемых: коэффициенты при t^m у суммы и произведения

$$\begin{aligned} S(t) = A(t) + B(t) = s_0 + s_1 t + s_2 t^2 + \cdots \\ P(t) = A(t) B(t) = p_0 + p_1 t + p_2 t^2 + \cdots \end{aligned}$$

вычисляются по правилам[1]

$$\begin{aligned} s_\nu &= a_\nu + b_\nu \\ p_\nu &= \sum_{\alpha + \beta = \nu} a_\alpha b_\beta = a_0 b_\nu + a_1 b_{\nu-1} + \cdots + a_0 b_\nu \end{aligned} \tag{4-3}$$

Упражнение 4.1. Убедитесь, что операции (4-3) удовлетворяют аксиомам коммутативного кольца с единицей.

Кольцо формальных степенных рядов от переменной t с коэффициентами в кольце K обозначается через $K[[t]]$. Начальный коэффициент a_0 ряда (4-1) называется *свободным членом* этого ряда. Первый ненулевой коэффициент ряда A называется *младшим* коэффициентом.

Если в кольце K нет делителей нуля, младший коэффициент произведения двух рядов равен произведению младших коэффициентов сомножителей. Поэтому кольцо формальных степенных рядов с коэффициентами из целостного кольца само является целостным.

[1] формально говоря, эти правила задают операции над *последовательностями* (a_ν) и (b_ν) элементов кольца K, и буква t используется лишь для облегчения восприятия этих правил

Кольцо $K[[x_1, x_2, \ldots, x_n]]$ формальных степенных рядов от n переменных $x_1, x_2, \ldots, x_n$ определяется по индукции:

$$K[[x_1, x_2, \ldots, x_n]] = K[[x_1, x_2, \ldots, x_{n-1}]]\,[[x_n]]$$

и представляет собой множество формальных сумм вида

$$F(t) = a_0 + \sum_{\nu_1,\ldots,\nu_n \in \mathbb{N}} a_{\nu_1 \ldots \nu_n} x_1^{\nu_1} x_2^{\nu_2} \cdots x_n^{\nu_n}\,.$$

Ряды с конечным числом ненулевых коэффициентов называются *многочленами*. Многочлены от переменных $x_1, x_2, \ldots, x_n$ с коэффициентами в кольце K образуют в кольце всех формальных степенных рядов подкольцо, которое обозначается

$$K[x_1, x_2, \ldots, x_n] \subset K[[x_1, x_2, \ldots, x_n]]$$

Таким образом, многочлен от одной переменной t представляет собой формальное выражение вида

$$f(t) = a_0 + a_1 t + \cdots + a_n t^n\,.$$

Последний ненулевой коэффициент этого выражения называется *старшим* коэффициентом многочлена f, а его номер называется *степенью* многочлена f и обозначается $\deg f$.

Упражнение 4.2. Убедитесь, что старший коэффициент произведения двух многочленов с коэффициентами из целостного кольца равен произведению старших коэффициентов сомножителей.

Из этого упражнения вытекает, что для многочленов с коэффициентами из целостного кольца справедливо равенство

$$\deg(f_1 f_2) = \deg(f_1) + \deg(f_2)\,.$$

В частности, обратимыми элементами кольца многочленов являются только обратимые константы.

4.2. Деление с остатком. Будем говорить, что многочлен $f(x) \in K[x]$ *приведён*, если его старший коэффициент равен единице.

Предложение 4.1 (деление многочленов с остатком)
Для любого многочлена f и любого приведённого многочлена u с коэффициентами из произвольного кольца K с единицей существуют многочлены $q \in K[x]$ (*неполное частное* от деления f на u) и $r \in K[x]$(*остаток* от деления f на u), такие что $f(x) = u(x) \cdot q(x) + r(x)$ и либо $\deg(r) < \deg(u)$, либо $r = 0$. Если кольцо K целостное, то такие q и r определяются по f однозначно.

Доказательство. Существование устанавливается при помощи обычного деления «уголком». А именно, полагаем $r_0 = f$, $q_0 = 0$ и далее для каждого $k = 1, 2, \ldots$ пока $\deg(r_{k-1}) \geqslant \deg(u)$ строим многочлены

$$\begin{aligned} q_k(x) &= (\text{старший коэффициент } r_{k-1}) \cdot x^{\deg(r_{k-1})-\deg(u)} \\ r_k(x) &= r_{k-1}(x) - q_k(x) \cdot u(x)\,. \end{aligned}$$

На каждом шагу мы имеем равенство $f = (q_1 + q_2 + \cdots + q_k) \cdot u + r_k$, и степени многочленов q_k и r_k с каждым шагом строго уменьшаются. В конце концов мы получим равенство $f = (q_1 + q_2 + \cdots + q_\ell) \cdot u + r_\ell$ с $\deg(r_\ell) < \deg(u)$.

Пусть теперь кольцо K целостное, а p, s — другая пара многочленов, таких что $\deg(s) < \deg(u)$ и $up+s = f = uq+r$. Тогда $u(q-p) = r-s$, и если $p-q \neq 0$, то $\deg(u(q-p)) = \deg(u) + \deg(q-p) \geqslant \deg(u) > \deg(r-s)$. Следовательно, $p - q = 0$, откуда и $r - s = 0$. □

Следствие 4.1

Для любых многочленов f, g с коэффициентами в произвольном поле $\Bbbk$ существует единственная пара многочленов $q, r \in \Bbbk[x]$, таких что $f = g \cdot q + r$ и либо $\deg(r) < \deg(g)$, либо $r = 0$.

Доказательство. Запишем g в виде $g = a \cdot u$, где $a \in \Bbbk$ — старший коэффициент многочлена g, а $u \in \Bbbk[x]$ приведёнен. Тогда представление f в виде $f = g \cdot q + r$ равносильно представлению f в виде $f = u \cdot \widetilde{q} + r$, в котором $\widetilde{q} = aq$. □

4.2.1. Пример: вычисление значения многочлена в точке. Остаток от деления многочлена

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

на линейный двучлен $u(x) = x - \alpha$ — это константа, равная значению $f(\alpha)$ многочлена f при $x = \alpha$, в чём легко убедиться, подставляя $x = \alpha$ в равенство

$$f(x) = (x - \alpha) \cdot q(x) + r$$

(в котором $\deg r = 0$).

Поучительно, однако, вычислить этот остаток непосредственным делением «уголком». Следуя алгоритму из доказательства предл. 4.1, находим:

$$\begin{aligned} r_1(x) &= (a_{n-1} + \alpha a_n)x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1 x + a_0 \\ r_2(x) &= \big(a_{n-2} + \alpha(a_{n-1} + \alpha a_n)\big)x^{n-2} + a_{n-3}x^{n-3} + \cdots + a_1 x + a_0 \\ r_3(x) &= \Big(a_{n-3} + \alpha\big(a_{n-2} + \alpha(a_{n-1} + \alpha a_n)\big)\Big)x^{n-2} + a_{n-4}x^{n-4} + \cdots + a_1 x + a_0 \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \end{aligned}$$

$$r_n = a_0 + \alpha \cdot \Bigg(a_1 + \alpha \cdot \Bigg(a_2 + \cdots + \alpha \cdot \big(a_{n-2} + \alpha \cdot (a_{n-1} + \alpha \cdot a_n)\big) \cdots \Bigg)\Bigg)$$

В результате мы получаем для вычисления значения $f(\alpha)$ так называемую *схему Горнера*:

$$f(\alpha) = a_0 + \alpha \cdot \Big(a_1 + \alpha \cdot \Big(a_2 + \ \cdots\ + \alpha \cdot \big(a_{n-2} + \alpha \cdot (a_{n-1} + \alpha \cdot a_n)\big) \cdots \Big)\Big)$$

Это вычисление требует значительно меньшего количества арифметических операций, чем непосредственная подстановка $f(\alpha) = a_0 + a_1\alpha + \cdots + a_n\alpha^n$.

Упражнение 4.3. Найдите в кольце $\mathbb{Z}[x, y] = \mathbb{Z}[x][y]$ частное от деления многочлена $y^n - x^n$ на линейный двучлен $(y - x)$.

Предложение 4.2
Пусть $\Bbbk$ — произвольное поле. Для любого набора многочленов

$$f_1, f_2, \dots, f_n \in \Bbbk[x]$$

существует единственный приведённый многочлен $d \in \Bbbk[x]$, который делит каждый из многочленов f_i и делится на любой многочлен, делящий каждый из многочленов f_i. Многочлен d представляется в виде

$$f_1h_1 + f_2h_2 + \ \cdots\ + f_nh_n \quad \text{с} \quad h_i \in \Bbbk[x] \tag{4-4}$$

Произвольно взятый многочлен $g \in \Bbbk[x]$ представим в виде (4-4) тогда и только тогда, когда он делится на d.

Доказательство. Единственность многочлена d очевидна: два многочлена, каждый из которых делится на другой, имеют одинаковую степень и, тем самым, могут различаться лишь постоянным множителем, который равен единице, поскольку оба многочлена приведены.

Доказательство существования и остальных свойств многочлена d полностью аналогично рассуждению из n° 3.1.2. А именно, обозначим через

$$(f_1, f_2, \dots, f_n) = \{f_1h_1 + f_2h_2 + \ \cdots\ + f_nh_n \mid h_i \in \Bbbk[x]\} \tag{4-5}$$

множество всех многочленов $g \in \Bbbk[x]$, представимых в виде (4-4). Оно является подкольцом в $\Bbbk[x]$ и вместе с каждым входящим в него многочленом g содержит также и все кратные ему многочлены hg (с любым $h \in \Bbbk[x]$). Кроме того, $(f_1, f_2, \dots, f_n)$ содержит каждый из многочленов f_i, и все многочлены из $(f_1, f_2, \dots, f_n)$ делятся на любой общий делитель всех многочленов f_i.

Возьмём в качестве d любой приведённый многочлен из $(f_1, f_2, \dots, f_n)$ наименьшей встречающейся среди ненулевых многочленов из $(f_1, f_2, \dots, f_n)$ степени. Остаток r от деления произвольного многочлена $g \in (f_1, f_2, \dots, f_n)$ на d представляется в виде $r = g - qd$ и, значит, лежит в кольце $(f_1, f_2, \dots, f_n)$. Поскольку $\deg r$ не может быть строго меньше, чем $\deg d$, мы заключаем, что $r = 0$, т. е. что все многочлены в $(f_1, f_2, \dots, f_n)$ делятся на d. $\square$

4.2.2. НОД и взаимная простота. Многочлен d из предл. 4.2 называется *наибольшим общим делителем* многочленов f_i и обозначается

$$\text{нод}(f_1, f_2, \dots, f_n)\,.$$

Из предл. 4.2 вытекает, что в кольце $\Bbbk[x]$ многочленов с коэффициентами в поле, как и в кольце $\mathbb{Z}$, *взаимная простота* многочленов $f_1, f_2, \dots, f_m$, т. е. возможность представить единицу в виде

$$1 = h_1 f_1 + h_2 f_2 + \cdots + h_n f_n\,,$$

равносильна условию $\text{нод}(f_1, f_2, \dots, f_n) = 1$, т. е. отсутствию у многочленов $f_1, f_2, \dots, f_n$ общих делителей положительной степени.

Определение 4.1
Многочлен $f \in K[x]$ называется *неприводимым*, если из равенства $f = gh$ вытекает, что g или h является обратимой константой.

Упражнение 4.4. Пусть $\Bbbk$ — любое поле. Пользуясь лем. 2.1, докажите следующую теорему об однозначности разложения на простые множители в кольце $\Bbbk[x]$: любой многочлен f является произведением конечного числа неприводимых многочленов, причём любые два таких представления $p_1 p_2 \cdots p_k = f = q_1 q_2 \cdots q_m$ имеют одинаковое число сомножителей $k = m$, и эти сомножители можно перенумеровать так, чтобы $\forall\ i\ p_i = \lambda_i q_i$, где $\lambda_i \in \Bbbk$ — некоторые ненулевые константы.

4.2.3. Алгоритм Евклида из n° 2.5.2 дословно переносится в кольцо многочленов $\Bbbk[x]$ с коэффициентами в произвольном поле $\Bbbk$. А именно, для пары многочленов $f_1(x)$ и $f_2(x)$ с $\deg(f_1) \geqslant \deg(f_2)$ положим $E_0 = f_1$, $E_1 = f_2$, и E_k = остатку от деления E_{k-2} на E_{k-1} при $k \geqslant 1$. Степени многочленов E_k будут строго убывать до тех пор, пока какой-то E_r не разделит нацело предыдущий E_{r-1}, в результате чего E_{r+1} обратится в нуль. Последний ненулевой многочлен E_r будет равен $\text{нод}(f_1, f_2)$, причём если при вычислении каждого E_k мы будем представлять его в виде $E_k = h_1^{(k)} f_1 + h_2^{(k)} f_2$, то $E_r = \text{нод}(f_1, f_2)$ и $E_{r+1} = 0$ тоже получатся представленными в таком виде, а в выражении $E_{r+1} = 0 = h_1^{(r+1)} f_1 + h_2^{(r+1)} f_2$ многочлены $h_1^{(r+1)}$ и $h_2^{(r+1)}$ будут взаимно простыми множителями, дополняющими, соответственно, f_1 и f_2 до их наименьшего общего кратного $\text{нок}(f_1, f_2) = h_1^{(r+1)} f_1 = -h_2^{(r+1)} f_2$.

Упражнение 4.5. Докажите все эти утверждения.

Например, для многочленов

$$\begin{aligned} f_1 &= x^7 + 3\,x^6 + 4\,x^5 + x^4 + 5\,x^2 + 3\,x^3 + 3\,x + 4 \\ f_2 &= x^5 + 5\,x^4 + 11\,x^3 + 12\,x^2 + 7\,x + 4 \end{aligned}$$

первый шаг алгоритма Евклида приводит к

$$\begin{aligned} E_0 &= x^7 + 3\,x^6 + 4\,x^5 + x^4 + 5\,x^2 + 3\,x^3 + 3\,x + 4 \\ E_1 &= x^5 + 5\,x^4 + 11\,x^3 + 12\,x^2 + 7\,x + 4 \\ E_2 &= -4\,x^4 - 13\,x^3 - 21\,x^2 - 10\,x - 8 = E_0 - \bigl(x^2 - 2\,x + 3\bigr)\,E_1 \end{aligned}$$

дальше делить на E_2 удобнее не E_1, а $16E_1$, а потом поделить результат на 16

$$\begin{aligned} E_3 &= \frac{1}{16}\left(x^3+5\,x^2+10\,x+8\right) = \frac{1}{16}\left(16E_1+(4\,x+7)\;E_2\right) = \\ &= \frac{4\,x+7}{16}\,E_0 - \frac{4\,x^3-x^2-2\,x+5}{16}\,E_1 \end{aligned}$$

следующий шаг уже даёт наибольший общий делитель

$$\begin{aligned} E_4 &= -16\,(x^2+3\,x+4) = E_2 + 16\;(4\,x-7)\;E_3 = \\ &= 16\left(x^2-3\right)\,E_0 - 16\left(x^4-2\,x^3+2\,x-2\right)\,E_1 \end{aligned}$$

поскольку

$$\begin{aligned} E_5 &= E_3 + \frac{x+2}{256}\,E_4 = \\ &= \frac{x^3+2\,x^2+x+1}{16}\,E_0 - \frac{x^5+x^2+1}{16}\,E_1 = 0\,. \end{aligned}$$

Таким образом,

$$\begin{aligned} \text{нод}(f_1,f_2) &= x^2+3\,x+4 = -\left(x^2-3\right)\,f_1(x) + \left(x^4-2\,x^3+2\,x-2\right)\,f_2(x) \\ \text{нок}(f_1,f_2) &= \left(x^3+2\,x^2+x+1\right)\,f_1(x) = \left(x^5+x^2+1\right)\,f_2(x)\,. \end{aligned}$$

4.3. Корни многочленов. Элемент $\alpha \in K$, называется *корнем* многочлена $f \in K[x]$, если $f(\alpha) = 0$. Как мы видели в n° 4.2.1, это условие равносильно тому, что $f(x)$ делится в $K[x]$ на $(x-\alpha)$.

Предложение 4.3

Если в K нет делителей нуля, то всякий многочлен $f \in K[x]$, имеющий корнями различные числа $\alpha_1, \alpha_2, \dots, \alpha_s \in K$, делится в $K[x]$ на произведение

$$\prod_{i=1}^{s}(x-\alpha_i)\,.$$

В частности, если $f \neq 0$, то $\deg(f) \geqslant s$.

Доказательство. Запишем f в виде $f(x) = (x-\alpha_1)\cdot f_1(x)$. Поскольку в K нет делителей нуля, и $(\alpha_i - \alpha_1) \neq 0$ при $i \neq 1$, подставляя в предыдущее равенство значения $x = \alpha_2,\ \alpha_3,\ \dots\ ,\ \alpha_s$, убеждаемся, что $\alpha_2,\ \alpha_3,\ \dots\ ,\ \alpha_s$ являются корнями многочлена $f_1(x)$, и можем повторить рассуждение. □

Следствие 4.2

Ненулевой многочлен f с коэффициентами из целостного кольца не может иметь в этом кольце более $\deg(f)$ различных корней.

Упражнение 4.6 (формула Лагранжа). Пусть $\Bbbk$ — поле, и $a_0, a_1, \dots, a_n \in \Bbbk$ — любые $n+1$ различных его элементов. Покажите, что для произвольного набора значений $b_0, b_1, \dots, b_n \in \Bbbk$ существует единственный многочлен $f(x) \in \Bbbk[x]$ степени $\leqslant n$, такой что $f(a_i) = b_i$ при всех $i = 0, 1, \dots\ n$.

Следствие 4.3
Пусть кольцо K целостное, и $f, g \in K[x]$ имеют степени, не превосходящие n. Если $f(\alpha_i) = g(\alpha_i)$ для более, чем n попарно разных $\alpha_i \in K$, то $f = g$ в $K[x]$.

Доказательство. Многочлен $f - g$ нулевой, поскольку имеет степень $\leqslant n$ и больше, чем n корней. □

Упражнение 4.7. Пусть $\Bbbk$ — поле. Проверьте, что многочлен степени $\leqslant 3$ неприводим в $\Bbbk[x]$ тогда и только тогда, когда у него нет корней в поле $\Bbbk$.

4.3.1. Общие корни нескольких многочленов. Пусть $\Bbbk$ — поле. Число α тогда и только тогда является общим корнем многочленов $f_1, f_2, \dots, f_m \in \Bbbk[x]$, когда α является корнем их наибольшего общего делителя. В самом деле, если $(x-\alpha)$ делит каждый из f_i, то по предл. 4.2 $(x-\alpha)$ делит $\text{нод}(f_1, f_2, \dots, f_m)$, и наоборот. Таким образом, отыскание общих корней набора многочленов сводится к отысканию корней их наибольшего общего делителя, что часто бывает проще, чем отыскание корней любого из f_i в отдельности, т. к. $\deg \text{нод}(f_1, f_2, \dots, f_m)$ часто бывает меньше $\min\bigl(\deg(f_i)\bigr)$.

Если многочлены $f_1, f_2, \dots, f_m \in \Bbbk[x]$ взаимно просты, то они не имеют общих корней не только в поле $\Bbbk$, но и ни в каком большем кольце $K \supset \Bbbk$. В самом деле, поскольку существуют многочлены $h_i \in \Bbbk[x]$, такие что

$$f_1 h_1 + f_2 h_2 + \dots + f_m h_m = 1\,,$$

многочлены f_i не обращаются одновременно в нуль ни при каком значении x.

4.4. Кольцо вычетов $\Bbbk[x]/(f)$ определяется аналогично кольцу $\mathbb{Z}/(n)$. Зафиксируем произвольный отличный от константы многочлен $f \in \Bbbk[x]$ и обозначим через

$$(f) = \{fh \mid h \in \Bbbk[x]\}$$

подкольцо всех многочленов, делящихся на f. Отношение $g_1 \equiv g_2 \pmod f$, по определению означающее, что $g_1 - g_2 \in (f)$, является отношением эквивалентности и разбивает $\Bbbk[x]$ в объединение непересекающихся классов

$$[g]_f = g + (f) = \{g + fh \mid h \in \Bbbk[x]\}\,, \tag{4-6}$$

которые называются *классами вычетов* по модулю f. Сложение и умножение этих классов задаётся формулами

$$[g] + [h] \overset{\text{def}}{=} [g+h]\,, \quad [g] \cdot [h] \overset{\text{def}}{=} [gh]\,. \tag{4-7}$$

Упражнение 4.8. Проверьте корректность этого определения (независимость классов $[g+h]$ и $[gh]$ от выбора представителей $g \in [g]$ и $h \in [h]$), а также выполнение в $\Bbbk[x]/(f)$ всех аксиом коммутативного кольца с единицей.

Нулевым элементом кольца $\Bbbk[x]/(f)$ является класс $[0]_f = (f)$, единицей является класс $[1]_f = 1 + (f)$. Поскольку никакая константа не может делиться на многочлен положительной степени, классы всех констант $c \in \Bbbk$ различны по модулю f. Иначе говоря, поле $\Bbbk$ гомоморфно вкладывается в кольцо $\Bbbk[x]/(f)$ в качестве подполя, образованного классами констант. Поэтому для классов чисел $c \in \Bbbk$ мы всюду далее пишем c вместо $[c]_f$.

Упражнение 4.9. Покажите, что поле $\Bbbk[x]/(x-\alpha)$ изоморфно полю $\Bbbk$.

Так как любой многочлен $g \in \Bbbk[x]$ единственным образом записывается в виде $g = fh + r$, где $\deg(r) < \deg(f)$, в каждом классе $[g]_f$ имеется единственный представитель $r \in [g]_f$ степени $\deg(r) < \deg(f)$.

Таким образом, каждый класс из $\Bbbk[x]/(f)$ *единственным образом* записывается в виде $[a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}]_f = a_0 + a_1\vartheta + \cdots + a_{n-1}\vartheta^{n-1}$, где $\vartheta = [x]_f$, а $a_i \in \Bbbk$.

Упражнение 4.10. Покажите, что многочлен $f \in \Bbbk[x]$ (где $\Bbbk$ — поле) неприводим тогда и только тогда, когда в кольце вычетов $\Bbbk[x]/(f)$ нет делителей нуля.

Заметим, что класс $\vartheta = [x]_f$ удовлетворяет в кольце $\Bbbk[x]/(f)$ уравнению $f(\vartheta) = 0$, т. к. $f(\vartheta) = f\left([x]_f\right) = [f(x)]_f = [0]_f$. Поэтому сложение и умножение классов по правилам (4-7) можно интерпретировать как формальное сложение и умножение записей

$$a_0 + a_1\vartheta + \ \cdots \ + a_{n-1}\vartheta^{n-1}\,, \tag{4-8}$$

по стандартным правилам раскрытия скобок и приведения подобных, но с учётом того, что символ ϑ удовлетворяет соотношению $f(\vartheta) = 0$.

По этой причине кольцо $\Bbbk[x]/(f)$ часто обозначают через $\Bbbk[\vartheta] : f(\vartheta) = 0$ и называют *расширением* поля $\Bbbk$ засчёт *присоединения* к нему корня ϑ многочлена $f \in \Bbbk[x]$. Выражения (4-8) в таком контексте называются *алгебраическими числами*[1].

Например, кольцо $\mathbb{Q}[x]/(x^2-2)$ можно воспринимать как множество формальных записей вида $a + b\sqrt{2}$, где символ $\sqrt{2} \in \mathbb{Q}[x]/(x^2-2)$ обозначает класс $x \pmod{x^2-2}$. Сложение и умножение таких записей происходит по стандартным правилам раскрытия скобок с учётом того, что $\left(\sqrt{2}\right)^2 = 2$:

$$\begin{aligned}(a + b\sqrt{2}) + (c + d\sqrt{2}) &= (a+c) + (b+d)\sqrt{2}\\ (a + b\sqrt{2})(c + d\sqrt{2}) &= (ac + 2\,bd) + (cb + ad)\sqrt{2}\end{aligned}$$

[1] в классической терминологии *алгебраическим числом* называется элемент поля $\mathbb{Q}[x]/(f)$, где $f \in \mathbb{Q}[x]$ — неприводимый многочлен (см. предложение (предл. 4.4) ниже); обсуждаемая нами ситуация отличается от классической тем, что во-первых, вместо $\mathbb{Q}$ мы рассматриваем произвольное поле $\Bbbk$, а во-вторых, не требуем, чтобы соотношение на ϑ было неприводимо

Упражнение 4.11. Проверьте, что $\mathbb{Q}[\sqrt{2}]$ является полем, и выясните, являются ли полями кольца $\mathbb{Q}[\vartheta]$, в которых ϑ удовлетворяет соотношению:
а) $\vartheta^3+1=0$ б) $\vartheta^3+2=0$.

4.4.1. Пример: чисто алгебраическое определение поля $\mathbb{C}$. Поле комплексных чисел можно *определить* как расширение поля $\mathbb{R}$ при помощи корня квадратного уравнения $x^2+1=0$, т. е. как кольцо

$$\mathbb{R}[x]/(x^2+1)=\mathbb{R}\left[\sqrt{-1}\right]:\left(\sqrt{-1}\right)^2=-1\,,$$

состоящее из чисел вида $a+b\sqrt{-1}$, где $a,b\in\mathbb{R}$, а символ $\sqrt{-1}$ обозначает класс одночлена x по модулю (x^2+1). Сложение и умножение таких чисел происходит по правилам

$$(a+b\sqrt{-1})+(c+d\sqrt{-1})=(a+c)+(b+d)\sqrt{-1}$$
$$(a+b\sqrt{-1})(c+d\sqrt{-1})=(ac-bd)+(cb+ad)\sqrt{-1}\,.$$

Кольцо $\mathbb{R}\left[\sqrt{-1}\right]$ является полем, поскольку каждый ненулевой класс $a+b\sqrt{-1}$ обладает обратным

$$\frac{1}{a+b\sqrt{-1}}=\frac{a}{a^2+b^2}-\frac{b}{a^2+b^2}\sqrt{-1}\,.$$

Упражнение 4.12. Сопоставим числу $a+b\sqrt{-1}\in\mathbb{R}\left[\sqrt{-1}\right]$ вектор $a+bi$ из поля $\mathbb{C}$, определённого нами геометрически в n° 2.3. Проверьте, что это изоморфизм полей.

Предложение 4.4
Пусть $\Bbbk$ — произвольное поле. Кольцо $\Bbbk[x]/(f)$ является полем тогда и только тогда, когда многочлен f неприводим в $\Bbbk[x]$.

Доказательство. Если $f=gh$, где оба многочлена f,g имеют строго меньшую, чем f, степень, то ненулевые классы $[g],[h]$ будут делителями нуля в $\Bbbk[x]/(f)$, что невозможно в поле. Если же f неприводим, то он будет взаимно прост с любым многочленом $g\notin(f)$, т. е. для некоторых $h,q\in\Bbbk[x]$ будет выполняться равенство $fh+gq=1$, и стало быть $[q]\cdot[g]=[1]$ в $\Bbbk[x]/(f)$, т. е. любой ненулевой класс $[g]_f\in\Bbbk[x]/(f)$ будет обратим. □

Упражнение 4.13. Напишите явную формулу для вычисления обратного элемента к числу $a_0+a_1\vartheta$ в поле $\mathbb{Q}(\vartheta)$ с $\vartheta^2+\vartheta+1=0$.

4.4.2. Конечные поля $\mathbb{F}_p[\vartheta]$. Если взять в качестве $\Bbbk$ конечное поле

$$\mathbb{F}_p=\mathbb{Z}/(p)$$

из p элементов, а в качестве $f\in\mathbb{F}_p[x]$ неприводимый многочлен степени n, то кольцо вычетов $\mathbb{F}_p[x]/(f)$ будет конечным полем из p^n элементов вида

$$a_0+a_1\vartheta+\dots+a_{n-1}\vartheta^{n-1}$$

со произвольными $a_i \in \mathbb{F}_p$ и соотношением $f(\vartheta) = 0$.

Например, $x^2 + x + 1 \in \mathbb{F}_2[x]$ неприводим, поскольку не имеет корней в $\mathbb{F}_2$. Соответствующее поле $\mathbb{F}_4 = \mathbb{F}_2[x]/(x^2 + x + 1) = \mathbb{F}_2[\omega] : \omega^2 + \omega + 1 = 0$ состоит из четырёх элементов[1]: 0, 1, $\omega = x \pmod{(x^2 + x + 1)}$ и $1 + \omega = \omega^2 = \omega^{-1}$.

Упражнение 4.14. Убедитесь, что мультипликативная группа $\mathbb{F}_4^*$ поля $\mathbb{F}_4$ изоморфна циклической группе $\boldsymbol{\mu}_3$.

Расширение $\mathbb{F}_2 \subset \mathbb{F}_4$ в некотором смысле аналогично расширению

$$\mathbb{R} \subset \mathbb{C} \simeq \mathbb{R}[\omega] : \omega^2 + \omega + 1 = 0\,,$$

получающемуся присоединением к полю $\mathbb{R}$ комплексного первообразного кубического корня из единицы[2]. Аналогом комплексного сопряжения (переводящего ω в $\overline{\omega} = \omega^2$) в поле $\mathbb{F}_4$ является гомоморфизм Фробениуса (см. n° 3.6.2)

$$F_2 : \mathbb{F}_4 \xrightarrow{a \mapsto a^2} \mathbb{F}_4\,,$$

который тождественно действует на простом подполе $\mathbb{F}_2 = \{0, 1\}$ и переводит корни многочлена $x^2 + x + 1$ друг в друга.

Рассмотрим другой пример. Многочлен $x^2 + 1 \in \mathbb{F}_3[x]$ не имеет корней в $\mathbb{F}_3$, и значит, неприводим. Соответствующее поле $\mathbb{F}_9 = \mathbb{F}_3\left[\sqrt{-1}\right]$ состоит из девяти элементов $a + b\sqrt{-1}$ где $a, b \in \{-1, 0, 1\} = \mathbb{F}_3$.

Упражнение 4.15. Составьте для поля $\mathbb{F}_9$ таблицу умножения, таблицу обратных элементов, таблицу квадратов, таблицу кубов и опишите действие гомоморфизма Фробениуса $F_3 : a \mapsto a^3$. Изоморфна ли мультипликативная группа $\mathbb{F}_9^*$ группе $\boldsymbol{\mu}_8$?

На самом деле, для каждого $n \in \mathbb{N}$ и любого простого $p \in \mathbb{N}$ существует единственное с точностью до изоморфизма поле $\mathbb{F}_q$, состоящее из $q = p^n$ элементов, и всякое конечное поле изоморфно одному из этих полей $\mathbb{F}_q$. Доказательство этого факта содержатся в задачах для самостоятельного решения к этому параграфу. При решении этих задач весьма полезным является тот факт, что мультипликативная группа конечного поля, состоящего из q элементов, изоморфна группе $\boldsymbol{\mu}_{q-1}$ и, тем самым, зависит только от числа q, а не от конструкции самого поля. Это следует из предл. 4.5, которое мы докажем в следующем пункте.

4.4.3. Конечные мультипликативные подгруппы в поле. Рассмотрим абелеву группу A, операцию в которой будем записывать мультипликативно.

Группа A называется *циклической* если в ней имеется элемент $a \in A$, такой что все элементы группы A представляются в виде a^n с некоторым $n \in \mathbb{Z}$. Всякий элемент $a \in A$, обладающий этим свойством, называется *образующей* циклической группы A.

[1] отметим, что в силу равенства $-1 = 1$ в поле $\mathbb{F}_2$ можно обходиться без «минусов»

[2] т.е. комплексного корня того же самого многочлена $x^2 + x + 1$

Например, группа комплексных корней из единицы $\boldsymbol{\mu}_n \subset \mathbb{C}$, рассматривавшаяся нами в n° 2.3.4, является циклической, а её образующими являются первообразные корни.

Если группа A конечна, то среди степеней любого элемента $a \in A$ будут встречаться одинаковые, скажем $a^k = a^m$ с $k > m$. Домножая обе части этого равенства на a^{-m}, получаем равенство $a^{k-m} = 1$. Таким образом, для каждого элемента существует показатель $m \in \mathbb{N}$, такой что $a^m = 1$. Наименьший такой показатель называется *порядком* элемента a и обозначается $\operatorname{ord} a$.

Если $\operatorname{ord} a = n$, то первые n степеней $a^0 = 1$, $a^1 = a$, a^2 , ... , a^{n-1} являются попарно различными элементами группы A, и любая целая степень a^m совпадает с одной из них — той, что равна остатку от деления m на n .

Предложение 4.5
Любая конечная подгруппа в мультипликативной группе произвольного поля $\Bbbk$ является циклической.

Доказательство. Пусть подгруппа $A \subset \Bbbk^*$ состоит из n элементов. Обозначим через m максимальный из порядков элементов группы A. Мы должны показать, что $m \geqslant n$. Для этого достаточно убедиться, что порядок любого элемента группы A является делителем числа m: если это верно, то все n элементов группы A будут корнями многочлена $x^m - 1 = 0$, а значит, их не может быть больше, чем m.

Чтобы увидеть, что порядки всех элементов группы являются делителями максимального порядка, достаточно для любых двух элементов $b_1, b_2 \in A$, имеющих порядки m_1, m_2, построить элемент $b \in A$, порядок которого равен $\text{НОК}(m_1, m_2)$.

Упражнение 4.16. Покажите, что при $\text{НОД}(m_1, m_2) = 1$ в качестве такого элемента подойдёт $b = b_1 b_2$.

Если m_1 и m_2 не взаимно просты, то, раскладывая их согласно упр. 2.13 в произведение простых чисел, мы можем представить $\text{НОК}(m_1, m_2)$ в виде произведения $\ell_1 \ell_2$ так, что $m_1 = k_1 \ell_1$, $m_2 = k_2 \ell_2$ и $\text{НОД}(\ell_1, \ell_2) = 1$ (для этого надо отправить в ℓ_1 все простые делители m_1, которые входят в m_1 в бо́льшей степени, чем в m_2). Тогда элементы $b_1' = b_1^{k_1}$ и $b_2' = b_2^{k_2}$ будут иметь взаимно простые порядки ℓ_1 и ℓ_2, а их произведение $b_1' b_2'$ по упр. 4.16 будет иметь порядок $\ell_1 \ell_2 = \text{НОК}(n_1, n_2)$. □

4.4.4. Пример: квадратичные вычеты. Зафиксируем целое простое $p > 2$. Ненулевые элементы поля $\mathbb{F}_p$, являющиеся квадратами, называются *квадратичными вычетами* по модулю p. Они образуют мультипликативную подгруппу в $\mathbb{F}_p^*$. Эта подгруппа является образом отображения возведения в квадрат $\mathbb{F}_p^* \xrightarrow{x \mapsto x^2} \mathbb{F}_p^*$. которое является гомоморфизмом мультипликативных групп. Так как ядро этого гомоморфизма состоит из двух элементов[1] ± 1, квадратич-

[1] уравнение $x^2 = 1$ имеет ровно два корня в любом целостном кольце с единицей

ных вычетов имеется ровно $(p-1)/2$.

Судить о том, является ли данный элемент $a \in \mathbb{F}_p^*$ квадратом или нет, можно при помощи малой теоремы Ферма (сл. 3.1), из которой вытекает, что $a^{p-1} = 1$ для любого ненулевого $a \in \mathbb{F}_p$. Если $b = a^2$, то $b^{(p-1)/2} = a^{p-1} = 1$. Возведение в степень $(p-1)/2$

$$\mathbb{F}_p^* \xrightarrow{x \mapsto x^{(p-1)/2}} \mathbb{F}_p^* \tag{4-9}$$

также является гомоморфизмом мультипликативных групп, причём его образ содержится среди корней всё того же уравнения $x^2 = 1$. Отметим, что -1 лежит в этом образе, поскольку $\mathbb{F}_p^*$ — это циклическая группа, и в ней есть элемент порядка $(p-1) > (p-1)/2$. Тем самым, ядро гомоморфизма (4-9) совпадает с подгруппой квадратичных вычетов.

Следовательно, $a \in \mathbb{F}_p^*$ является квадратом тогда и только тогда, когда $a^{\frac{p-1}{2}} = 1$. Например, -1 является квадратом в $\mathbb{F}_p$ в точности тогда, когда $(p-1)/2$ чётно.

4.5. Поле частных целостного кольца. Приведённая в n° 1.4.4 и n° 2.1.2 конструкция поля $\mathbb{Q}$ позволяет изготовить аналогичное поле Q_K из любого целостного кольца K. Элементами поля Q_K являются формальные дроби a/b, определяемые как классы эквивалентности упорядоченных пар $(a,b) \in K \times K$ с $b \neq 0$ по отношению

$$(a_1, b_1) \sim (a_2, b_2) \quad \text{при} \quad a_1 b_2 = a_2 b_1\,, \tag{4-10}$$

которое является минимальной эквивалентностью, содержащей всевозможные отождествления

$$(a,b) \sim (ac, bc)\ \forall\, c \neq 0\,. \tag{4-11}$$

Сложение и умножение дробей определяется формулами

$$\frac{a_1}{b_1} + \frac{a_2}{b_2} \overset{\text{def}}{=} \frac{a_1 b_2 + a_2 b_1}{b_1 b_2} \qquad \frac{a_1}{b_1} \cdot \frac{a_2}{b_2} \overset{\text{def}}{=} \frac{a_1 a_2}{b_1 b_2} \tag{4-12}$$

Дословно те же рассуждения, которые использовались в решении упр. 1.9 из n° 1.4.4 и упр. 2.3 из n° 2.1.2 показывают, что (4-10) действительно является отношением эквивалентности[1], операции (4-11) определены корректно[2] и удовлетворяют всем аксиомам поля из опр. 2.1 на стр. 21.

Поле Q_K называется *полем частных* целостного кольца K. Кольцо K вкладывается в поле Q_K посредством инъективного гомоморфизма

$$\iota : K \xhookrightarrow{a \mapsto a/1} Q_K\,, \tag{4-13}$$

[1]целостность кольца K существенна при проверке транзитивности отношения (4-10), см. указания к решению упр. 1.9

[2]достаточно убедиться, что формулы (4-12) корректно ведут себя по отношению к отождествлениям (4-11), что очевидно

который обладает следующим *свойством универсальности*:

$$\text{для любого вложения } K \overset{\varphi}{\hookrightarrow} \mathbb{F} \text{ в произвольное поле } \mathbb{F} \text{ существует единственное вложение полей } \mathbb{Q}_F \xrightarrow{\widetilde{\varphi}} \mathbb{F}, \text{ такое что } \varphi = \widetilde{\varphi} \circ \iota \tag{4-14}$$

В самом деле, чтобы продолжить произвольно заданное вложение

$$\varphi : K \hookrightarrow \mathbb{F}$$

до гомоморфизма $\widetilde{\varphi} : Q_K \longrightarrow \mathbb{F}$, у нас нет иного выбора, как положить

$$\widetilde{\varphi}(a/b) = \widetilde{\varphi}(a)/\widetilde{\varphi}(b) = \varphi(a)/\varphi(b)\,.$$

С другой стороны, это правило действительно корректно определяет гомоморфизм: эквивалентность $\frac{a_1}{b_1} \sim \frac{a_2}{b_2}$ влечёт за собой эквивалентность[1] $\frac{\varphi(a_1)}{\varphi(b_1)} \sim \frac{\varphi(a_2)}{\varphi(b_2)}$, а суммы и произведения дробей перейдут в суммы и произведения, поскольку сложение и умножение отношений a/b в любом поле $\mathbb{F}$ происходит именно по формулам (4-12).

Упражнение 4.17. Покажите, что поле Q_K и вложение (4-13) однозначно определяются универсальным свойством (4-14) в том смысле, что для любого другого вложения $K \xrightarrow{\iota'} Q'_K$, обладающего универсальным свойством (4-14), существует единственный изоморфизм $\psi : Q_K \xrightarrow{\sim} Q'_K$, такой что $\iota' = \psi \circ \iota$.

Для кольца $K = \mathbb{Z}$ описанная конструкция приводит к полю $Q_{\mathbb{Z}} = \mathbb{Q}$, а универсальное свойство (4-14) превращается в утверждение о том, что $\mathbb{Q}$ канонически вкладывается в любое поле характеристики нуль в качестве простого подполя (ср. с n° 3.6.1).

4.6. Поле рациональных функций $\Bbbk(x)$. Поле частных целостного кольца $\Bbbk[x]$ обозначается через $\Bbbk(x)$ и называется *полем рациональных функций* от одной переменной. Элементы этого поля представляют собой отношения многочленов $p(x)/q(x)$ с коэффициентами в поле $\Bbbk$.

Запись $p(x)/q(x)$ называется *несократимым представлением* соответствующей дроби, если $\text{нод}(p, q) = 1$. Каждая дробь имеет несократимую запись, для получения которой следует поделить числитель и знаменатель произвольной записи p/q на $\text{нод}(p, q)$.

Упражнение 4.18. Покажите, что несократимая запись любой дроби единственна с точностью до умножения числителя и знаменателя на ненулевую константу (в частности, имеется ровно одна несократимая запись с приведённым знаменателем).

При вычислениях с рациональными функциями весьма полезен следующий результат, являющийся прямым аналогом китайской теоремы об остатках из n° 3.5.

[1] применяя φ к равенству $a_1 b_2 = a_2 b_1$, получаем равенство $\varphi(a_1)\varphi(b_2) = \varphi(a_2)\varphi(b_1)$

Предложение 4.6 (китайская теорема об остатках)
Пусть $\Bbbk$ — произвольное поле, и многочлен $f \in \Bbbk[x]$ является произведением m сомножителей: $f = f_1 f_2 \cdots f_m$, таких что нод$(f_i, f_j) = 1\ \forall\, i, j$. Отображение

$$\Bbbk[x]/(f) \xrightarrow{\varphi} (\Bbbk[x]/(f_1)) \times (\Bbbk[x]/(f_2)) \times \cdots \times (\Bbbk[x]/(f_m))$$
$$\varphi : [g]_f \longmapsto ([g]_{f_1}, [g]_{f_2}, \ldots , [g]_{f_m})$$

является корректно определённым изоморфизмом колец.

Доказательство. Проверки того, что φ корректно определён[1], является гомоморфизмом и имеет нулевое ядро, дословно повторяют рассуждения из n° 3.5, и мы оставляем их читателю. Покажем, что φ сюрьективен. Для этого, как и в n° 3.5, построим для любого заданного набора классов $[r_i]_{f_i} \in \Bbbk[x]/(f)$ многочлен $g \in \Bbbk[x]$, такой что $g \equiv r_i \pmod{f_i}$ при всех i. Для каждого i обозначим произведение всех сомножителей f_ν кроме f_i через

$$F_i = \prod_{\nu \neq i} f_\nu \, .$$

Поскольку f_i взаимно прост со всеми f_ν с $\nu \neq i$, он, согласно лем. 2.1, взаимно прост и с F_i, а значит, существует многочлен[2] $h_i \in \Bbbk[x]$, такой что

$$F_i \cdot h_i \equiv 1 \pmod{f_i} \, .$$

Итак, многочлен $g_i = F_i \cdot h_i \equiv 1 \pmod{f_i}$ и делится на все f_ν с $\nu \neq i$. Следовательно, $g = r_1 g_1 + r_2 g_2 + \cdots + r_m g_m \equiv r_i \pmod{f_i}$ при всех i . □

Предложение 4.7
Если знаменатель несократимой записи f/g является произведением попарно взаимно простых многочленов $g = g_1 g_2 \ldots g_m$, то дробь f/g *единственным образом* представляется в виде суммы

$$\frac{f}{g} = h + \frac{f_1}{g_1} + \frac{f_2}{g_2} + \cdots + \frac{f_m}{g_m} \, , \tag{4-15}$$

в которой $\deg h = \deg f - \deg g$ и $\deg f_i < \deg g_i$.

Доказательство. Пусть у нас имеется какое-то равенство вида (4-15). Умножая обе его части на g, получаем в $\Bbbk[x]$ равенство вида

$$f = hg + f_1 Q_1 + f_2 Q_2 + \cdots + f_m Q_m \, , \tag{4-16}$$

[1] т. е. $\varphi([g]_f)$ не зависит от выбора представителя $g \in \Bbbk[x]$ в классе $[g]_f \subset \Bbbk[x]$

[2] чтобы найти его явно, можно, например, взять остаток R_i от деления F_i на f_i и применить к паре $E_0 = f_i$, $E_1 = R_i$ алгоритм Евклида

в котором $Q_i = \prod\limits_{\nu \neq i} g_\nu$ и $\deg(\sum f_\nu Q_\nu) < \deg Q$. Отсюда мы заключаем, что многочлен h является неполным частным от деления f на g, многочлен $r = \sum f_\nu Q_\nu$ — остатком от этого деления, а каждый f_i есть единственный многочлен степени $< \deg g_i$, представляющий в кольце вычетов $\Bbbk[x]/(g_i)$ класс

$$r^{-1} \pmod{g_i} \equiv f\, Q_i^{-1} \pmod{g_i}\,.$$

Таким образом, все ингредиенты формулы (4-15) однозначно определяются многочленами f и g, и если взять их такими, как сказано выше, то мы как раз и получим равенство (4-16), а с ним и равенство (4-15). □

Предложение 4.8
Любую дробь вида f/g^m, в которой $\deg f < \deg(g^m) = m \deg g$, можно *единственным образом* представить в виде суммы

$$\frac{f}{g^m} = \frac{f_1}{g} + \frac{f_2}{g^2} + \cdots + \frac{f_m}{g^m}\,, \tag{4-17}$$

в которой степени всех числителей строго меньше $\deg g$.

Доказательство. Представление (4-17) равносильно представлению многочлена f в виде

$$f = f_1 g^{m-1} + f_2 g^{m-2} + \cdots + f_{m-1} g + f_m\,, \tag{4-18}$$

которое аналогично представлению целого числа f в g-ичной позиционной системе исчисления: f_m равен остатку от деления на g самого многочлена f, f_{m-1} — остатку от деления на g частного $(f - f_m)/g$ (которое по построению f_m является многочленом), f_{m-2} — остатку от деления на g частного $((f - f_m)/g - f_{m-1})\,/g$ и т. д. □

Из предыдущих двух лемм вытекает, что любая дробь $f/g \in \Bbbk[x]$ допускает *единственное* представление в виде суммы многочлена степени $\deg f - \deg g$ (неполного частного от деления f на g) и вида p/q^m, где q пробегает множество неприводимых делителей знаменателя, m меняется от 1 до кратности вхождения q в разложение знаменателя на неприводимые множители, и каждый числитель имеет степень $\deg p < \deg q$. Такое представление называется *разложением f/g на простейшие дроби* и часто оказывается полезным при дифференцировании и интегрировании рациальных функций, а также при их разложении в степенные ряды (мы ещё вернёмся к этому в n° 5.3).

Задачи для самостоятельного решения к §4

Задача 4.1. Найдите все кратные (комплексные) корни многочлена

$$x^7 + 7\,x^5 - 36\,x^4 + 15\,x^3 - 216\,x^2 + 9\,x - 324\,.$$

Задача 4.2. Найдите первообразную и 1000-ю производную от $x^4/(1+x^2)$.

Задача 4.3. Найдите остатки от деления многочлена $x^{179} + x^{57} + x^2 + 1$ в кольце $\mathbb{Z}[x]$ на многочлены а) $x^2 - 1$ б) $x^2 + 1$ в) $x^2 + x + 1$.

Задача 4.4. Покажите, что всякий многочлен $f \in \mathbb{R}[x]$ раскладывается в произведение линейных двучленов и квадратных трёхчленов с отрицательным дискриминантом. Разложите на неприводимые множители в $\mathbb{R}[x]$ многочлен $x^8 + 128$.

Задача 4.5 (формулы Виета). Выразите коэффициенты a_k приведённого многочлена $f(x) = x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n = (x-\alpha_1)(x-\alpha_2)\,\cdots\,(x-\alpha_n)$ через его корни α_ν и найдите линейную подстановку $x = t - a$ (где a должно быть явно выражено через a_k), в результате которой у многочлена $f(t-\alpha)$ сократится моном с t^{n-1}.

Задача 4.6 (дискриминант). Число $D_f = \prod\limits_{i<j}(\alpha_i - \alpha_j)^2$ называется *дискриминантом* приведённого многочлена $f(x) = \prod(x - \alpha_j)$. Выразите через p и q дискриминанты трёхчленов а) $x^2 + px + q$ б) $x^3 + px + q$.

Задача 4.7. Докажите, что кубический трёхчлен $f(x) = x^3 + px + q \in \mathbb{R}$ имеет три различных вещественных корня если, и только если его дискриминант D_f (см. зад. 4.6) положителен, и в этом случае подходящая замена $t = \lambda x$ приводит уравнение $f(x) = 0$ к виду $4\,t^3 - t\,x = a$, где $a \in \mathbb{R}$ и $|a| \leqslant 1$. Пользуясь формулой для косинуса тройного угла (см. стр. 28) выразите корни последнего уравнения через тригонометрические функции.

Задача 4.8. Решите в тригонометрических функциях (см. предыдущую задачу) уравнения: а) $x^3 - 3\,x + 1 = 0$, б) $x^3 + x^2 - 2\,x - 1 = 0$.

Задача 4.9. Придумайте квадратное уравнение, корни z_1, z_2 которого таковы, что среди (комплексных) чисел $\sqrt[3]{z_1} + \sqrt[3]{z_2}$ содержатся все корни кубического трёхчлена $f(x) = x^3 + px + q$. При каких знаках дискриминанта D_f числа z_1, z_2
а) вещественны и различны б) комплексно сопряжены?

Задача 4.10. Найдите вещественные корни многочленов:
а) $x^3 - x + 1$; б) $x^3 + 2\,x^2 + x + 1$.

Задача 4.11. Вычислите в радикалах: а) $\cos(\pi/9)$, б) $\cos(\pi/12)$, в) $\cos(\pi/7)$.

Задача 4.12. Обозначим через $\zeta \in \mathbb{C}$ какой-нибудь первообразный корень степени k из единицы. Покажите, что а) $\forall\, a \in \mathbb{C}\ \prod\limits_{\nu=0}^{k-1}(\zeta^\nu x - a) = (-1)^{k+1}(x^k - a^k)$

б) $\forall\, f \in \mathbb{C}[x]\ \ \exists\, h \in \mathbb{C}[x] : \ \prod\limits_{\nu=0}^{k-1} f(\zeta^\nu x) = h(x^k)$, причём корнями h являются в точности k-тые степени корней f

Задача 4.13. Напишите многочлен f, корнями которого являются в точности
а) квадраты комплексных корней многочлена $x^4 + 2x^3 - x + 3$
б) кубы комплексных корней многочлена $x^4 - x - 1$

Задача 4.14. Является ли кольцо $\mathbb{R}[x]/(f)$ полем при
а) $f = x^4 + 1$ б) $f = x^3 + 1$ в) $f = x^2 + 3$?

Задача 4.15 (минимальный многочлен). Пусть $\Bbbk \subset \mathbb{F}$ два поля. Элемент $\alpha \in \mathbb{F}$ называется *алгебраическим* над $\Bbbk$, если $f(\alpha) = 0$ для некоторого многочлена $f(a) \in \Bbbk[x]$, и приведённый многочлен наименьшей степени с таким свойством называется *минимальным многочленом* элемента α над полем $\Bbbk$. Докажите, что минимальный многочлен неприводим в $\Bbbk[x]$ и делит в $\Bbbk[x]$ все многочлены, для которых α является корнем.

Задача 4.16. Найдите минимальный многочлен числа а) $2 - 3i$ над $\mathbb{R}$
б) $\sqrt{2} + \sqrt{3}$ над $\mathbb{Q}$ в) $\sqrt[3]{2}$ над[1] $\mathbb{Q}[\sqrt{2} + \sqrt{3}]$ г) $\sqrt[105]{9}$ над $\mathbb{Q}$.

Задача 4.17. Если ли среди полей $\mathbb{Q}[\sqrt{2}]$, $\mathbb{Q}[\sqrt{3}]$ и $\mathbb{Q}[\sqrt[3]{2}]$ изоморфные между собой?

Задача 4.18. Опишите все автоморфизмы полей
а) $\mathbb{Q}[\sqrt{2}]$ б) $\mathbb{Q}[\sqrt{2}, \sqrt{3}] = \mathbb{Q}[\sqrt{2}][\sqrt{3}]$ в) $\mathbb{Q}[\sqrt[4]{2}]$ г) $\mathbb{Q}[1 + i]$

Задача 4.19. Пусть A — произвольное коммутативное кольцо с единицей, и $f \in A[x]$ имеет обратимый старший коэффициент. Покажите, что для любого $g \in A[x]$ существуют $q, r \in A[x]$, такие что $g = fq + r$ и либо $\deg r < \deg f$, либо $r = 0$. Выведите отсюда, что для любого приведённого[2] $f \in A[x]$ существует расширение $A \subset B$, такое что f полностью разлагается в $B[x]$ на линейные множители.

Задача 4.20. Пусть $\Bbbk$ — любое поле, $f \in \Bbbk[x]$ неприводимый многочлен, и $\mathbb{F} = \Bbbk[x]/(f)$. Для любого поля $K \supset \Bbbk$ постройте биекцию между множеством гомоморфизмов $\mathbb{F} \hookrightarrow K$, тождественно действующих на элементы подполя $\Bbbk$, и множеством корней многочлена f в поле K.

Задача 4.21 (поле разложения). В условиях предыдущей задачи постройте поле $\mathbb{F}_f \supset \Bbbk$, такое что: (1) f полностью разлагается в $\mathbb{F}_f[x]$ на линейные множители (2) для любого поля $K \supset \Bbbk$, над которым f полностью разлагается на линейные множители, существует гомоморфизм $\mathbb{F}_f \hookrightarrow K$, тождественно действующий на все элементы подполя $\Bbbk$. Покажите, что поле $\mathbb{F}_f$ с такими свойствами единственно с точностью до изоморфизма, тождественного на подполе $\Bbbk$ (оно называется *полем разложения* многочлена f).

Задача 4.22 (круговые многочлены). Напомним (см. n° 2.3.4), что n-тый *круговой* многочлен Φ_n — это приведённый многочлен, корнями которого являются

[1] через $\mathbb{Q}[\sqrt{2}+\sqrt{3}]$ обозначено поле $\mathbb{Q}[x]/(f)$, где $f \in \mathbb{Q}[x]$ — минимальный многочлен числа $\sqrt{2} + \sqrt{3}$ над $\mathbb{Q}$

[2] напомним, что мы называем *приведёнными* многочлены со старшим коэффициентом единица

комплексные первообразные корни n-той степени из 1 и только они. Покажите, что а) $\Phi_{2n}(x)=\Phi_n(-x)$ при нечётном n б) $x^n-1=\prod\limits_{d|n}\Phi_d(x)$
в) $\Phi_n(x)=\prod\limits_{d|n}(x^{n/d}-1)^{\mu(d)}$ (используйте предыдущую задачу и подходящую модификацию обращения Мёбиуса — ср. с зад. 3.20 и зад. 9.20)
г) $\Phi_p(x)=x^{p-1}+\dots+x+1$ и $\Phi_{p^k}(x)=\Phi_p\left(x^{p^{k-1}}\right)$ при простом p
д) $\Phi_{pm}(x)=\Phi_m\left(x^p\right)/\Phi_m(x)$ при простом $p\not| m$
е) $\Phi_{p_1^{k_1}\cdots p_n^{k_n}}(x)=\Phi_{p_1p_2\cdots p_n}\left(x^{p_1^{k_1-1}\cdots p_n^{k_n-1}}\right)$ для попарно разных простых p_i
ж) Φ_n неприводим над $\mathbb{Q}$, имеет целые коэффициенты и найдите $\deg\Phi_n$

Задача 4.23. Пусть $\mathbb{F}_q$ — конечное поле из q элементов. Покажите, что любая функция $\mathbb{F}\longrightarrow\mathbb{F}$ является многочленом и приведите пример двух разных многочленов, задающих одинаковые функции.

Задача 4.24. Разложите над полем $\mathbb{F}_p$ рациональную функцию $1/(x^p-x)$ в сумму простейших дробей.

Задача 4.25. Найдите все неприводимые многочлены степени $\leqslant 5$ над $\mathbb{F}_2$ и все неприводимые многочлены степени $\leqslant 3$ над $\mathbb{F}_3$.

Задача 4.26. Сколько в $\mathbb{F}_3[x]$ неприводимых многочленов степени а) 3 б) 4 ?

Задача 4.27. Покажите что над любым (в том числе конечным) полем имеется
а) бесконечно много неприводимых многочленов
б) неприводимый многочлен любой степени.

Задача 4.28. Используя подходящую модификацию обращения Мёбиуса, докажите, что число неприводимых многочленов степени n в $\mathbb{F}_p[x]$ равно

$$\frac{1}{n}\sum_{d|n}p^d\mu(n/d)$$

(см. зад. 4.22 (в), зад. 3.20, зад. 9.20, а также зад. 5.11).

Задача 4.29. Пусть $\Bbbk$ — поле характеристики p и $a\in\Bbbk$. Покажите, что многочлен x^p-a либо неприводим в $\Bbbk[x]$, либо имеет p-кратный корень в $\Bbbk$.

Задача 4.30. Пусть многочлен $f(x)=x^p-x-a\in\mathbb{F}_p$ имеет в неком расширении $\mathbb{F}\supset\mathbb{F}_p$ корень ζ . Явно укажите в $\mathbb{F}$ ещё $p-1$ корней многочлена f и покажите, что в $\mathbb{F}_p[x]$ многочлен f либо неприводим, либо полностью разлагается на линейные множители.

Задача 4.31. Пусть $\mathbb{F}$ — конечное поле из q элементов и $\mathbb{F}_p\subset\mathbb{F}$ — его простое подполе. Покажите, что а) все элементы $\mathbb{F}$ алгебраичны над $\mathbb{F}_p$ (см. зад. 4.15)
б) $q=p^n$ для некоторого n .
в) порядок любого элемента в мультипликативной группе $\mathbb{F}^*$ делит $q-1$.
г) Пользуясь обращением Мёбиуса из зад. 3.20, напишите формулу для числа элементов d-того порядка

д) Выясните, сколько в $\mathbb{F}^*$ элементов $(q-1)$-го порядка и какова степень минимального многочлена (см. зад. 4.15) такого элемента.

Задача 4.32. Докажите, что корни многочлена $x^{p^k} - x$, лежащие в произвольном поле характеристики p, образуют в нём подполе.

Задача 4.33. Какова максимальная степень неприводимых делителей многочлена $x^{p^k} - x$ над полем $\mathbb{F}_p$?

Задача 4.34. Докажите, что для любого простого p и натурального n поле $\mathbb{F}_q$ из $q = p^n$ элементов существует и единственно с точностью до изоморфизма.

Задача 4.35. При каких q_1, q_2 существует ненулевой гомоморфизм $\mathbb{F}_{q_1} \longrightarrow \mathbb{F}_{q_2}$?

Задача 4.36. Опишите все автоморфизмы поля $\mathbb{F}_q$.

§5. Формальные степенные ряды

5.1. Алгебраические операции над формальными рядами. Напомним (см. n° 4.1), что кольцо формальных степенных рядов $K[[x]]$ с коэффициентами в коммутативном кольце K с единицей образовано бесконечными формальными суммами вида

$$f(x) = \sum_{\nu \geqslant 0} a_\nu x^\nu = a_0 + a_1 x + a_2 x^2 + \cdots \,, \quad a_i \in K \,,$$

которые складываются и умножаются по стандартным правилам раскрытия скобок и приведения подобных слагаемых.

Будем называть *n-арной алгебраической операцией* всякое правило, сопоставляющее рядам $f_1, f_2, \ldots, f_n \in K[[x]]$ новый ряд $g \in K[[x]]$ так, что каждый коэффициент ряда g вычисляется конечным числом арифметических действий над конечным числом коэффициентов рядов $f_1, f_2, \ldots, f_n$.

Например, сложение и умножение рядов — это алгебраические операции, а подстановка вместо x численного значения $\alpha \in K$ алгебраической операцией обычно не является[1]. Напротив, подстановка в ряд $f(x)$ вместо x любого ряда без свободного члена $g(x) = b_1 x + b_2 x^2 + \cdots$ — это алгебраическая операция, дающая ряд

$$\begin{aligned} f(g(x)) = \sum a_k (b_1 x + b_2 x^2 + \cdots)^k = \\ a_0 + a_1(b_1 x + b_2 x^2 + \cdots) + a_2(b_1 x + b_2 x^2 + \cdots)^2 + a_3(b_1 x + b_2 x^2 + \cdots)^3 + \cdots \\ = a_0 + (a_1 b_1) \cdot x + (a_1 b_2 + a_2 b_1^2) \cdot x^2 + (a_1 b_3 + 2\, a_2 b_1 b_2 + a_3 b_1^3) \cdot x^3 + \cdots \,, \end{aligned}$$

в котором на коэффициент при x^m влияют лишь начальные члены первых m слагаемых. Ещё одним примером алгебраической операции является обращение рядов.

Предложение 5.1

Ряд $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots \in K[[x]]$ тогда и только тогда обратим в $K[[x]]$, когда его свободный член a_0 обратим в K. Если обратный ряд существует, то операция обращения $f \mapsto f^{-1}$ является алгебраической.

Доказательство. Если существует ряд $f^{-1}(x) = b_0 + b_1 x + b_2 x^2 + \cdots$, такой что $f(x) \cdot f^{-1}(x) = 1$, то $a_0 b_0 = 1$, откуда a_0 обратим. Наоборот, допустим, что $a_0 \in K$ обратим. Приравнивая коэффициенты при одинаковых степенях x в

[1] очевидным исключением из этого правила служит вычисление значения ряда $f(x)$ при $x = 0$, дающее в качестве результата свободный член этого ряда; похожий эффект иногда возникает при вычислении значений некоторых очень специальных рядов в некоторых очень специальных точках α; но при произвольных α и f вычисление $f(\alpha)$ требует, вообще говоря, выполнения бесконечно большого количества сложений

правой и левой части равенства $f(x)\cdot f^{-1}(x) = 1$, мы получаем на коэффициенты b_i бесконечную систему уравнений

$$\begin{aligned} a_0b_0 &= 1 \\ a_0b_1 + a_1b_0 &= 0 \\ a_0b_2 + a_1b_1 + a_2b_0 &= 0 \\ \cdots\cdots\cdots&\cdots\cdots\cdots \end{aligned} \tag{5-1}$$

из которой $b_k = -a_0^{-1}(a_1b_{k-1} + a_2b_{k-2} + \cdots + a_kb_0)$ при $k \geqslant 1$, а $b_0 = a_0^{-1}$. Это позволяет рекурсивно вычислить все коэффициенты. □

5.1.1. Пример: геометрическая прогрессия. Непосредственная проверка показывает, что обратным элементом к линейному двучлену $1 - x$ является формальный ряд

$$\frac{1}{1-x} = 1 + x + x^2 + x^3 + \ \cdots \ = \sum_{k\geqslant 0} x^k \ , \tag{5-2}$$

который называется *геометрической прогрессией*.

Упражнение 5.1. Явно выпишите все коэффициенты рядов
а) $1/(1+x)$ б) $1/(1\pm x^m)$ в) $1/(1+x+x^2)$

5.2. Дифференциальное исчисление.

Подставим в степенной ряд

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots$$

вместо x сумму $x + t$, где t — ещё одна переменная. Получится ряд

$$f(x+t) = a_0 + a_1(x+t) + a_2(x+t)^2 + \cdots \in K[[x,t]]\,.$$

Раскроем в нём все скобки и сгруппируем слагаемые по степеням переменной t, обозначив через $f_m(x) \in K[[x]]$ ряд, возникающий как коэффициент при t^m :

$$f(x+t) = f_0(x) + f_1(x)\cdot t + f_2(x)\cdot t^2 + f_3(x)\cdot t^3 + \ \cdots \ = \sum_{i\geqslant 0} f_m(x)\cdot t^m\,. \tag{5-3}$$

Упражнение 5.2. Убедитесь, что $f_0(x) = f(x)$ совпадает с исходным рядом f .

Ряд $f_1(x)$ называется *производной* от исходного ряда f и обозначается $f'(x)$ или $\frac{d}{dx}f$. Он однозначно определяется равенством

$$f(x+t) = f(x) + f'(x)\cdot t + (\text{члены, делящиеся на } t^2)$$

и может быть вычислен как значение при $t = 0$ ряда

$$\begin{aligned} &\frac{f(x+t)-f(x)}{t} = \\ &\qquad = a_1\cdot\frac{(x+t)-t}{t} + a_2\cdot\frac{(x+t)^2-t^2}{t} + a_3\cdot\frac{(x+t)^3-t^3}{t} + \ \cdots = \\ &\qquad\qquad = \sum_{k\geqslant 1} a_k\cdot\left((x+t)^{k-1} + (x+t)^{k-2}x + (x+t)^{k-3}x^2 + \ \cdots + \ x^{k-1}\right)\,. \end{aligned}$$

Полагая $t = 0$, получаем

$$f'(x) = \sum_{k\geqslant 1} k\, a_k x^{k-1} = a_1 + 2\, a_2 x + 3\, a_3 x^2 + \ \cdots \tag{5-4}$$

5.2.1. Ряды с нулевой производной. Из формулы (5-4) вытекает, что производная от константы равна нулю.

Если $\mathrm{char} K = 0$, то верно и обратное: $f' = 0$ тогда и только тогда, когда $f = \mathrm{const}$.

Если же кольцо K имеет положительную характеристику, то производная от всех мономов x^m, показатель которых делится на характеристику, обратится в нуль, поскольку согласно проделанному выше вычислению коэффициент m в формуле

$$\frac{d}{dx}\, x^m = \underbrace{x^{m-1} + \ \cdots \ + x^{m-1}}_{m} = m \cdot x^{m-1}$$

представляет собою сумму m единиц кольца. В частности, над полем $\Bbbk$ характеристики $p > 0$ производная от ряда $f(x)$ равна нулю тогда и только тогда, когда $f(x) = g(x^p)$ для некоторого $g \in \Bbbk[[x]]$.

Предложение 5.2 (правила дифференцирования)
Для любого $\alpha \in K$ и любых $f, g \in K[[x]]$ справедливы равенства

$$(\alpha f)' = \alpha \cdot f'\,, \quad (f+g)' = f' + g'\,, \quad (fg)' = f' \cdot g + f \cdot g'\,. \tag{5-5}$$

Кроме того, если ряд g не имеет свободного члена, то

$$(f(g(x)))' = g'(x) \cdot f'(g(x))\,, \tag{5-6}$$

а если ряд f обратим, то

$$(1/f)' = -\frac{f'}{f^2}\,. \tag{5-7}$$

Доказательство. Первые два равенства в (5-5) вытекают прямо из формулы (5-4). Для доказательства третьего перемножим ряды

$$\begin{aligned} f(x+t) &= f(x) + t \cdot f'(x) + (\text{члены, делящиеся на } t^2) \\ g(x+t) &= g(x) + t \cdot g'(x) + (\text{члены, делящиеся на } t^2)\,. \end{aligned}$$

С точностью до членов, делящихся на t^2, получим

$$f(x+t)g(x+t) = f(x)g(x) + t \cdot (f'(x)g(x) + f(x)g'(x)) + (\text{члены, делящиеся на } t^2)\,,$$

откуда $(fg)' = f' \cdot g + f \cdot g'$. Формула (5-6) доказывается похожим образом. Подставим в $f(x)$ вместо x ряд $g(x+t)$: $f(g(x+t)) = f\big(g(x) + t \cdot g'(x) +$

(члены, делящиеся на t^2)$\big)$ и обозначая ряд, который прибавляется к $g(x)$ в аргументе f, через $\tau(x,t) = t\cdot g'(x) + $ (члены, делящиеся на t^2) . Получаем

$$\begin{aligned} f(g(x+t)) = f\big(g(x) + \tau(x,t)\big) = \\ = f(g(x)) + \tau(x,t)\cdot f'(g(x)) + (\text{члены, делящиеся на } \tau(x,t)^2) = \\ = f(g(x)) + t\cdot g'(x)\cdot f'(g(x)) + (\text{члены, делящиеся на } t^2)\ , \end{aligned}$$

откуда $(f(g(x))' = g'(x)\cdot f'(g(x))$. Для доказательства последней формулы продифференцируем обе части равенства $f\cdot f^{-1} = 1$. Получим $f'\cdot f^{-1} + f\cdot (f^{-1})' = 0$, откуда $(f^{-1})' = -f'/f^2$. □

Упражнение 5.3. Покажите, что в разложении (5-3) $f_m(x) = \frac{1}{m!}\frac{d^m}{dx^m}f(x)$ (здесь и далее через $\frac{d^m}{dx^m} = \left(\frac{d}{dx}\right)^m$ обозначается m-тая производная, т. е. результат m-кратного применения операции $\frac{d}{dx}$).

5.2.2. Пример: дифференцирование степеней. Применяя правило Лейбница к произведению $f^m = f\cdot f\cdot\dots\cdot f$ получаем для любого ряда f формулу

$$(f^m)' = m\cdot f^{m-1}\cdot f'\ . \tag{5-8}$$

В частности, производная от ряда $1/(1-x)^m$ равна $m/(1-x)^{m+1}$, откуда по индукции заключаем, что m-тая производная от геометрической прогрессии $(1-x)^{-1}$ равна $m!/(1-x)^{m+1}$. Дифференцируя $(m-1)$ раз обе части разложения

$$(1-x)^{-1} = 1 + x + x^2 + x^3 + x^4 + \ \cdots\ ,$$

получаем формулу Ньютона для бинома с отрицательным показателем

$$\begin{aligned} \frac{1}{(1-x)^m} = \sum_{k\geqslant 0}\frac{(k+m-1)(k+m-2)\ \cdots\ (k+1)}{(m-1)!}\cdot x^k = \\ = \sum_{k\geqslant 0}\binom{k+m-1}{k}\cdot x^k\ . \end{aligned} \tag{5-9}$$

5.2.3. Пример: кратные корни многочленов. Пусть $\Bbbk$ — произвольное поле. Число $\alpha\in\Bbbk$ называется m-кратным корнем многочлена $f\in\Bbbk[x]$, если $f(x) = (x-\alpha)^m\cdot g(x)$, где $g(\alpha)\neq 0$. Корни кратности $m\geqslant 2$ называются *кратными*.

Предложение 5.3
Пусть $\Bbbk$ — любое поле. Для того, чтобы $\alpha\in\Bbbk$ был кратным корнем $f\in\Bbbk[x]$ необходимо и достаточно, чтобы $f(\alpha) = f'(\alpha) = 0$.

Доказательство. Если α — кратный корень многочлена f, то

$$f(x) = (x-\alpha)^2 g(x)\ .$$

Дифференцируя, получаем $f'(x) = (x-\alpha)(2 + (x-\alpha)g(x))$, откуда $f'(\alpha) = 0$.

Если α не является кратным корнем, то $f(x) = (x-\alpha)g(x)$, где $g(x)\neq 0$. Тогда $f'(x) = (x-\alpha)g'(x) + g(x)$ и $f'(\alpha) = g(\alpha)\neq 0$. □

Предложение 5.4
Над полем нулевой характеристики α является m-кратным корнем многочлена f тогда и только тогда, когда α является корнем f и первых $(m-1)$ производных от f, но не является корнем m-той производной.

Доказательство. Если $f(x) = (x-\alpha)^m \cdot g(x)$, где $g(\alpha) \neq 0$, то

$$f'(x) = (x-\alpha)^{m-1} \cdot (m + (x-\alpha) \cdot g(x))\ .$$

Второй сомножитель в этом равенстве отличен от нуля при $x = \alpha$. Поэтому α является m-кратным корнем f тогда и только тогда, когда α является $(m-1)$-кратным корнем f'. □

Предложение 5.5
Если $\mathrm{char}(\Bbbk) = p > 0$, то $f' = 0$ тогда и только тогда, когда $f = g^p$ для некоторого $g \in \Bbbk[x]$.

Доказательство. Согласно n° 5.2.1, равенство $f' = 0$ равносильно тому, что $f(x) = g(x^p)$ для некоторого $g \in \Bbbk[x]$. Поскольку в характеристике p возведение в p-тую степень является гомоморфизмом (см. n° 3.2.1), $g(x^p) = g(x)^p$. □

Следствие 5.1
Для произвольного поля $\Bbbk$ неприводимый многочлен $f \in \Bbbk[x]$ не имеет кратных корней ни в самом поле $\Bbbk$, ни в каком кольце $K \supset \Bbbk$.

Доказательство. Согласно предл. 5.5 производная неприводимого многочлена отлична от нуля над любым полем. Поскольку f неприводим, он взаимно прост с f'. Согласно n° 4.3.1 взаимно простые многочлены не могут иметь общих корней ни в каком кольце $K \supset \Bbbk$. □

5.3. . Пусть $K = \mathbb{C}$. Формула (5-9) позволяет разложить в ряд любую рациональную функцию $f/g \in \mathbb{C}(x)$, если известно разложение на множители её знаменателя. А именно, пусть

$$g(x) = 1 + a_1x + a_2x^2 + \cdots + a_nx^n = \prod (1-\alpha_i x)^{m_i}\ , \tag{5-10}$$

где все числа $\alpha_i \in \mathbb{C}$ попарно различны.

Упражнение 5.4. Убедитесь, что при $a_n \neq 0$ числа α_i из разложения (5-10) суть корни приведённого многочлена $t^n + a_1t^{n-1} + \cdots + a_{n-1}t + a_n = \prod (t-\alpha_i)^{m_i}$.

Тогда по предл. 4.7 и предл. 4.8 рациональная функция f/g является суммой простейших дробей вида

$$\frac{\beta}{(1-\alpha_i x)^m} = \beta \sum_{k \geqslant 0} \alpha_i^k \binom{k+m-1}{m-1} \cdot x^k \tag{5-11}$$

где k лежит в пределах $1 \leqslant k \leqslant m_i$, а $\beta = \beta(i,k) \in \mathbb{C}$ — константы, зависящие от i, k, f и g.

Если если знаменатель g не имеет кратных корней, вычисление получается особенно простым. В этом случае при $\deg f < \deg g$ рациональная функция f/g имеет по предл. 4.7 разложение

$$\frac{f(x)}{(1-\alpha_1 x)(1-\alpha_2 x)\cdots(1-\alpha_n x)} = \frac{\beta_1}{1-\alpha_1 x} + \frac{\beta_2}{1-\alpha_2 x} + \ \cdots \ + \frac{\beta_n}{1-\alpha_n x} \tag{5-12}$$

и представляет собою сумму геометрических прогрессий

$$\frac{1}{f(x)} = \sum \left(\beta_1 \alpha_1^k + \beta_2 \alpha_2^k + \ \cdots \ + \beta_n \alpha_n^k\right) \cdot x^k \,.$$

Чтобы определить константы $\beta_i \in \mathbb{C}$, умножим левую и правую части (5-12) на общий знаменатель и подставим в полученное равенство значение $x = \alpha_i^{-1}$. Все слагаемые в правой части кроме i-того обратятся в нуль, и мы получим

$$\beta_i = \prod_{\nu \neq i} \frac{g(\alpha_i^{-1})}{(1-(\alpha_\nu/\alpha_i))} = \frac{\alpha_i^{n-1} g(\alpha_i^{-1})}{\prod\limits_{\nu \neq i}(\alpha_i - \alpha_\nu)} \,. \tag{5-13}$$

5.3.1. Решение линейных рекуррентных уравнений. Предыдущие вычисления можно использовать для отыскания «формулы k-того члена» последовательности z_k, заданной *линейным рекуррентным уравнением n-того порядка*:

$$z_k + a_1 z_{k-1} + a_2 z_{k-2} + \ \cdots \ + a_n z_{k-n} = 0 \,, \tag{5-14}$$

где коэффициенты $a_1, a_2, \ldots, a_n \in \mathbb{C}$ — некоторые фиксированные заданные числа. В самом деле, уравнение (5-14) — это уравнение, которому должны удовлетворять при $k \geqslant n$ коэффициенты z_k степенного ряда

$$\frac{b_0 + b_1 x + \cdots + b_{n-1} x^{n-1}}{1 + a_1 x + a_2 x^2 + \ \cdots \ + a_n x^k} = z_0 + z_1 x + z_2 x^2 + \cdots$$

Если подобрать $b_0, b_1, \ldots, b_{n-1} \in \mathbb{C}$ в числителе левой части так, чтобы первые n коэффициентов справа совпадали с начальным куском последовательности (5-14), и разложить полученную рациональную функцию в ряд описанным выше способом, то мы получим явные выражения элементов последовательности z_k через k.

Найдём, к примеру, явное выражение через k для *чисел Фиббоначчи* z_k, которые определяются условиями

$$z_0 = 0 \,, \quad z_1 = 1 \,, \quad z_k = z_{k-1} + z_{k-2} \quad \text{при} \quad k \geqslant 2 \,,$$

т. е. решают рекуррентное уравнение $z_k - z_{k-1} - z_{k-2} = 0$ на коэффициенты ряда

$$\frac{b_0 + b_1 x}{1 - x - x^2} = x + z_2 x^2 + z_3 x^3 + \ \cdots \tag{5-15}$$

(мы подставили в правую часть данные по условию $z_0 = 0$ и $z_1 = 1$).

Умножая обе части (5-15) на общий знаменатель и сравнивая коэффициенты при x^0 и x^1, получаем $b_0 = 0$ и $b_1 = 1$. Тем самым, числа Фиббоначчи являются коэффициентами ряда

$$z(x) = \frac{x}{1 - x - x^2} = \frac{\beta_+}{1 - \alpha_+ x} + \frac{\beta_-}{1 - \alpha_- x}\,,$$

где $\alpha_\pm = (1 \pm \sqrt{5})/2$ суть корни многочлена $t^2 - t - 1$, а числа $\beta_\pm$ находятся по формуле (5-13) с учётом равенств $\alpha_+\alpha_- = -1$, $\alpha_+ + \alpha_- = 1$, и $\alpha_+ - \alpha_- = \sqrt{5}$:

$$\beta_+ = -\beta_- = \frac{1}{\alpha_+ - \alpha_-} = \frac{1}{\sqrt{5}}\,.$$

Таким образом,

$$\frac{x}{1 - x - x^2} = \frac{1}{\sqrt{5}}\left(\frac{1}{1 - \alpha_+ x} - \frac{1}{1 - \alpha_- x}\right) = \sum_{k \geqslant 0} \frac{\alpha_+^k - \alpha_-^k}{\sqrt{5}} \cdot x^k\,,$$

т. е. k-тое число Фиббоначчи имеет вид

$$z_k = \frac{(1 + \sqrt{5})^k - (1 - \sqrt{5})^k}{2^k \sqrt{5}}\,.$$

В общем случае решение рекуррентного уравнения (5-14) описывает

Предложение 5.6

Всякая последовательность z_k, удовлетворяющая при $k \geqslant n$ линейному рекуррентному уравнению n-того порядка

$$z_k + a_1 z_{k-1} + a_2 z_{k-2} + \;\cdots\; + a_n z_{k-n} = 0\,, \tag{5-16}$$

с постоянными коэффициентами $a_i \in \mathbb{C}$, имеет вид

$$z_k = \alpha_1^k \cdot \varphi_1(k) + \alpha_2^k \cdot \varphi_2(k) + \;\cdots\; + \alpha_r^k \cdot \varphi_r(k)\,,$$

где $\alpha_1, \alpha_2, \dots, \alpha_r$ суть все различные корни многочлена[1]

$$t^n + a_1 t^{n-1} + \dots + a_{n-1} t + a_n\,, \tag{5-17}$$

а каждая из функций $\varphi_i \in \mathbb{C}[x]$ представляет собою многочлен степени на единицу меньшей, чем кратность соответствующего корня α_i.

Доказательство. Ряд $\sum z_k x^k \in \mathbb{C}[[x]]$, коэффициенты которого решают уравнение (5-16), является суммой дробей вида $\beta \cdot (1 - \alpha x)^{-m}$, где α пробегает различные корни многочлена (5-17), показатель степени m может принимать любое значение от 1 до кратности соответствующего корня α, а $\beta = \beta(\alpha, m)$ — комплексное число, однозначно вычисляемое по α, m и первым n коэффициентам последовательности z_k. Согласно формуле (5-11) k-тый член разложения такой дроби имеет вид $\alpha^k \varphi(k)$, где $\varphi(k) = \binom{k+m-1}{m-1}$ есть многочлен от k степени $m - 1$. □

[1] он называется *характеристическим многочленом* рекуррентного уравнения (5-14)

5.4. Логарифм и экспонента. Начиная с этого места и до конца параграфа мы будем по умолчанию предполагать, что область коэффициентов $K = \mathbb{F}$ является полем характеристики нуль.

В этом случае из формулы (5-4) для производной вытекает, что для любого ряда $f(x) = a_0 + a_1x + a_2x^2 + \cdots$ существует единственный ряд без свободного члена, производная от которого равна $f(x)$. Этот ряд называется *первообразным рядом* или *интегралом* от f и обозначается

$$\int f(x)\,dx \stackrel{\text{def}}{=} a_0x + \frac{a_1}{2}\,x^2 + \frac{a_2}{3}\,x^3 + \cdots = \sum_{k\geqslant 1}\frac{a_{k-1}}{k}\,x^k\,. \tag{5-18}$$

5.4.1. Логарифмирование. Первообразный ряд от знакопеременной геометрической прогрессии называется *логарифмом* и обозначается

$$\begin{aligned}\ln(1+x) \stackrel{\text{def}}{=} \int \frac{dx}{1+x} = \int \left(1 - x + x^2 - x^3 + \cdots\right)\,dx = \\ = x - \frac{x^2}{2} + \frac{x^3}{3} - \frac{x^4}{4} + \frac{x^5}{5} - \cdots = \sum_{k\geqslant 1}\frac{(-1)^{k-1}}{k}x^k\,.\end{aligned} \tag{5-19}$$

Вместо $1+x$ в логарифм можно подставить любой ряд $u(x)$ с единичным свободным членом — ряд $\ln(u(x))$ получается подстановкой в правую часть (5-19) вместо x ряда $u(x)-1$ без свободного члена, что является алгебраической операцией (см. n° 5.1).

Упражнение 5.5 (логарифмическая производная). Покажите, что $(\ln u)' = u'/u$ для любого ряда u с единичным свободным.

Обозначим через $N \subset \mathbb{F}[[x]]$ аддитивную абелеву группу всех рядов без свободного члена, а через $U \subset \mathbb{F}[[x]]$ — мультипликативную абелеву группу всех рядов с единичным свободным членом.

Операция *логарифмирования*, переводящая ряд $u(x) \in U$ в ряд $\ln(u(x)) \in N$, является алгебраической и задаёт отображение

$$\log : U \xrightarrow{u\mapsto \ln u} N\,. \tag{5-20}$$

Лемма 5.1

Для рядов $u, w \in U$ равенства $u = w$, $u' = w'$, $\ln(u) = \ln(w)$ и $\ln'(u) = \ln'(w)$ попарно эквивалентны друг другу.

Доказательство. Первое равенство влечёт за собой все остальные. Два ряда из U (соотв. два ряда из N) совпадают тогда и только тогда, когда совпадают их производные. Поэтому первые два равенства (соотв. последние два равенства) равносильны друг другу. Остаётся показать, что из последнего равенства следует первое. Для этого, пользуясь упр. 5.5, перепишем последнее равенство в виде $u'/u = w'/w$ и перенесём всё в одну часть:

$$\frac{u'}{u} - \frac{w'}{w} = \frac{u'w - w'u}{uw} = (u/w)\cdot(u/w)' = 0\,.$$

Отсюда $u/w = \text{const} = 1$. $\square$

Упражнение 5.6. Покажите, что $\forall u \in U \ \ln(1/u) = -u$.

5.4.2. Экспоненцирование. Ряд

$$e^x \stackrel{\text{def}}{=} \sum_{k\geqslant 0} \frac{x^k}{k!} = 1 + x + \frac{x^2}{2} + \frac{x^3}{6} + \frac{x^4}{24} + \frac{x^5}{120} + \cdots \tag{5-21}$$

называется *экспонентой*. Это единственный ряд со свободным членом единица, удовлетворяющий дифференциальному уравнению $f'(x) = f(x)$.

Подставляя в (5-21) вместо x любой ряд $\tau(x)$ без свободного члена, мы получаем ряд $e^{\tau(x)}$ со свободным членом 1, который называется *экспонентой* ряда $\tau(x)$. Таким образом, возникает экспоненциальное отображение

$$\exp : N \xrightarrow{\tau \mapsto e^\tau} U \ . \tag{5-22}$$

Теорема 5.1
Экспоненциальное и логарифмическое отображения (5-22) и (5-20) являются взаимно обратными изоморфизмами абелевых групп. В частности, для любых рядов $u, u_1, u_2 \in U$ и $\tau, \tau_1, \tau_2 \in N$ выполняются тождества:

$$\ln e^\tau = \tau \ , \quad e^{\ln u} = u \ , \quad \ln(u_1 u_2) = \ln(u_1) + \ln(u_2) \ , \quad e^{\tau_1 + \tau_2} = e^{\tau_1} e^{\tau_2} \, .$$

Доказательство. Равенство $\ln e^\tau = \tau$ проверяется взятием производной от обеих частей (оба ряда имеют нулевой свободный член и обязаны совпадать, коль скоро совпадают их производные). Аналогично, $\forall\, u_1, u_2 \in U$ ряды $\ln(u_1 u_2)$ и $\ln u_1 + \ln u_2$ лежат в N и имеют равные производные:

$$\begin{aligned}(\ln(u_1u_2))' = \frac{(u_1u_2)'}{u_1u_2} = \frac{u_1'u_2 + u_1u_2'}{u_1u_2} &= \\ = \frac{u_1'}{u_1} + \frac{u_2'}{u_2} &= (\ln u_1)' + (\ln u_2)' = (\ln u_1 + \ln u_2)' \ .\end{aligned}$$

Поэтому $\ln(u_1u_2) = \ln u_1 + \ln u_2$, т. е. логарифмирование является гомоморфизмом. Равенство $e^{\ln u} = u$ проверяется логарифмированием обеих частей с использованием уже доказанного равенства $\ln e^\tau = \tau$ и лем. 5.1. Из равенств $e^{\ln u} = u$ и $\ln e^\tau = \tau$ вытекает, что экспоненцирование и логарифмирование являются взаимно обратными биекциями. Поэтому экспоненцирование — тоже гомоморфизм. $\square$

Упражнение 5.7. Покажите непосредственным сравнением коэффициентов рядов, что $e^{x+y} = e^x e^y$ в $\mathbb{F}[x, y]$.

5.5. Бином Ньютона. Для любого числа $\alpha \in \mathbb{F}$ определим *биномиальный ряд* с показателем α формулой

$$(1+x)^\alpha \stackrel{\text{def}}{=} e^{\alpha \ln(1+x)}.$$

Подставляя вместо $1+x$ произвольные ряды $u \in U$, мы для любого числа $\alpha \in \mathbb{F}$ получаем алгебраическую операцию *возведения в α-тую степень*

$$U \xrightarrow{u \mapsto u^\alpha} U\,,$$

обладающую всеми интуитивно ожидаемыми от степенной функции свойствами: для любых рядов $u, v \in U$ и чисел $\alpha, \beta \in \mathbb{F}$ выполняются равенства

$$u^\alpha \cdot u^\beta = e^{\alpha \ln u} \cdot e^{\beta \ln u} = e^{\alpha \ln u + \beta \ln u} = e^{(\alpha+\beta)\ln u} = u^{\alpha+\beta} \tag{5-23}$$

$$(u^\alpha)^\beta = e^{\beta \ln(u^\alpha)} = e^{\beta \ln\left(e^{\alpha \ln u}\right)} = e^{\alpha\beta \ln u} = u^{\alpha\beta} \tag{5-24}$$

$$(uv)^\alpha = e^{\alpha \ln(uv)} = e^{\alpha(\ln u + \ln v)} = e^{\alpha \ln u + \alpha \ln v} = e^{\alpha \ln u} \cdot e^{\alpha \ln v} = u^\alpha v^\alpha \tag{5-25}$$

В частности, для любого ряда u с единичным свободным членом $u^{1/n} = \sqrt[n]{u}$ в том смысле, что $\left(u^{1/n}\right)^n = u$.

Для явного отыскания коэффициентов a_i биномиального ряда

$$(1+x)^\alpha = a_0 + a_1 x + a_2 x^2 + \cdots$$

вычислим его логарифмическую производную:

$$\frac{((1+x)^\alpha)'}{(1+x)^\alpha} = (\ln(1+x)^\alpha)' = \left(\ln e^{\alpha \ln(1+x)}\right)' = \left(\alpha \ln(1+x)\right)' = \frac{\alpha}{1+x}\,.$$

Приводя левую и правую часть к общему знаменателю, получаем соотношение

$$\left(a_1 + 2a_2 x + 3a_3 x^2 + \ \cdots\ \right) \cdot (1+x) = \alpha \cdot (1 + a_1 x + a_2 x^2 + a_3 x^3 + \ \cdots\ )\,.$$

Сравнивая коэффициенты при x^{k-1} в правой и левой части, приходим к рекуррентному соотношению $k a_k + (k-1) a_{k-1} = \alpha a_{k-1}$, из которого

$$a_k = \frac{\alpha - (k-1)}{k} \cdot a_{k-1} = \frac{(\alpha-(k-1))(\alpha-(k-2))}{k(k-1)} \cdot a_{k-2} = \ \cdots$$

$$\cdots\ = \frac{(\alpha-(k-1))(\alpha-(k-2))\cdots(\alpha-1)\alpha}{k!}\,.$$

Стоящая в правой части дробь имеет и в числителе и в знаменателе по k множителей, представляющих собою последовательно уменьшающиеся на единицу числа: в знаменателе — от k до 1, в числителе — от α до $(\alpha-k+1)$. Эта дробь называется *биномиальным коэффициентом* и обозначается

$$\binom{\alpha}{k} \stackrel{\text{def}}{=} \frac{\alpha(\alpha-1)\cdots(\alpha-k+1)}{k!} \tag{5-26}$$

Нами доказано

Предложение 5.7 (формула Ньютона)
Для любого числа $\alpha \in \mathbb{F}$ имеется разложение

$$(1+x)^\alpha = \sum_{k\geqslant 0}\binom{\alpha}{k}x^k = 1+\alpha x+\frac{\alpha(\alpha-1)}{2}x^2+\frac{\alpha(\alpha-1)(\alpha-2)}{6}x^3+\cdots .$$

5.5.1. Пример: бином с рациональными показателями. При натуральном значении показателя $\alpha = n \in \mathbb{N}$ имеется лишь конечное число ненулевых биномиальных коэффициентов, поскольку при $k > n$ в числителе (5-26) образуется нулевой сомножитель. Поэтому разложение бинома в этом случае конечно:

$$(1+x)^n = 1+n\,x+\frac{n(n-1)}{2}\,x^2+\cdots+x^n = \sum_{k=0}^{n}\binom{n}{k}\cdot x^k .$$

При целом отрицательном $\alpha = -m$, $m \in \mathbb{N}$, мы снова получаем разложение (5-9) из n° 5.2.2

$$(1+x)^{-m} = 1-m\,x+\frac{m(m+1)}{2}\,x^2-\frac{m(m+1)(m+2)}{6}\,x^3+\cdots = \\ = \sum_{k\geqslant 0}(-1)^k\binom{k+m-1}{k}\cdot x^k .$$

При $\alpha = 1/n$, $n \in \mathbb{N}$ формула Ньютона разворачивает в степенной ряд радикал

$$\sqrt[n]{1+x} = 1+\frac{1}{n}\,x+\frac{\frac{1}{n}\left(\frac{1}{n}-1\right)}{2}\,x^2+\frac{\frac{1}{n}\left(\frac{1}{n}-1\right)\left(\frac{1}{n}-2\right)}{6}\,x^3+\cdots = \\ = 1+\frac{x}{n}-\frac{n-1}{2}\cdot\frac{x^2}{n^2}+\frac{(n-1)(2n-1)}{2\cdot 3}\cdot\frac{x^3}{n^3}-\frac{(n-1)(2n-1)(3n-1)}{2\cdot 3\cdot 4}\cdot\frac{x^4}{n^4}+\cdots$$

Например, при $n = 2$ в качестве коэффициента при x^k мы получаем дробь вида

$$(-1)^{k-1}\cdot\frac{1\cdot 3\cdot 5\cdot\cdots\cdot(2k-3)}{2\cdot 4\cdot 6\cdot\cdots\cdot(2k)} = \frac{(-1)^{k-1}}{2k-1}\cdot\frac{(2k)!}{(2\cdot 4\cdot 6\cdot\cdots\cdot(2k))^2} = \\ = \frac{(-1)^{k-1}}{(2k-1)\cdot 4^k}\cdot\binom{2k}{k}.$$

Таким образом,

$$\sqrt{1+x} = \sum_{k\geqslant 0}\frac{(-1)^{k-1}}{2k-1}\cdot\binom{2k}{k}\cdot\frac{x^k}{4^k} . \tag{5-27}$$

5.5.2. Пример: числа Каталана. Воспользуемся разложением (5-27) для получения явной формулы для *чисел Каталана*, часто возникающих в различных комбинаторных задачах. Пусть при вычислении суммы $(n+1)$ слагаемых

$$a_0+a_1+a_2+\cdots+a_n \qquad \text{(всего } n \text{ плюсов)} \tag{5-28}$$

в каждый момент времени разрешается делать не более одного сложения. Такое вычисление разбивается на n последовательных шагов, на каждом из которых выполняется некоторое конкретное сложение, в результате чего все знаки «+» оказываются занумерованными в том порядке, в котором они выполняются. Количество всех возникающих таким способом нумераций n плюсов называется n-ым *числом Каталана* c_n. Удобно также по определению положить $c_0 = 1$.

Подчеркнём, что рассматриваемые нами нумерации плюсов далеко не произвольны.

Упражнение 5.8. Убедитесь, что $c_1 = 1$, $c_2 = 2$, $c_3 = 5$, $c_4 = 14$ (и, тем самым, $c_n \neq n!$).

Количество способов вычислить сумму (5-28) так, чтобы последним выполняется i-тый слева плюс, равно $c_{i-1}c_{n-i}$ — мы можем независимо посчитать сумму i чисел, стоящих слева от i-того плюса, и $n-i+1$ чисел, стоящих от него справа, для чего у нас имеется, соответственно, c_{i-1} и c_{n-i} способов.

Таким образом, числа Каталана c_n удовлетворяют соотношению

$$c_n = c_0c_{n-1} + c_1c_{n-2} + \cdots + c_{n-2}c_1 + c_{n-1}c_0 \ , \tag{5-29}$$

i-тое слагаемое которого учитывает все вычисления, в которых последним выполняется i-тый слева плюс записи (5-28).

Чтобы выразить c_n через n явно, рассмотрим степенной ряд

$$c(x) = \sum_{k\geqslant 0} c_k x^k = 1 + c_1x + c_2x^2 + c_3x^3 + \cdots \ .$$

Равенство (5-29) означает, что этот ряд удовлетворяет соотношению

$$\frac{c(x)-1}{x} = c(x)^2 \, .$$

Иначе говоря, $t = c(x)$ является решением квадратного уравнения

$$x\cdot t^2 - t - 1 = 0$$

на неизвестную t. Решая его[1], получаем $c(x) = \left(1-\sqrt{1-4x}\right)/(2x)$. По (5-27)

$$\sqrt{1-4x} = -\sum_{k\geqslant 0}\frac{1}{2k-1}\cdot\binom{2k}{k}\cdot x^k \, ,$$

откуда

$$c_k = \frac{1}{2}\cdot\frac{1}{2k+1}\cdot\binom{2k+2}{k+1} = \frac{1}{k+1}\cdot\binom{2k}{k} \, .$$

[1]обратите внимание, что ряд $1-\sqrt{1-4x}$ не имеет свободного члена и потому делится в $\mathbb{Q}[[x]]$ на $2x$, причём частное имеет свободный член $c_0 = 1$, как нам и требуется; второе решение $\dfrac{1+\sqrt{1-4x}}{2x}$ не является «целым» степенным рядом: знаменатель не обратим, а числитель, имея ненулевой свободный член, на него не делится

Отметим, что с первого взгляда даже не очевидно, что это число — целое.

Задачи для самостоятельного решения к §5

Задача 5.1. Выпишите явное выражение через n для коэффициента при t^n у формального степенного ряда а) $(2\,t^2-3\,t+1)^{-1}$ б) $(t^4+2\,t^3-7\,t^2-20\,t-12)^{-1}$ в) $\sqrt[3]{1+2t}$ г) $1/\sqrt{1-3t}$ д) $\mathrm{ch}(t)\overset{\text{def}}{=}(e^t+e^{-t})/2$ е) $\mathrm{sh}(t)\overset{\text{def}}{=}(e^t-e^{-t})/2$ ж) $\cos(t)\overset{\text{def}}{=}(e^{it}+e^{-it})/2$ з) $\sin(t)\overset{\text{def}}{=}(e^{it}-e^{-it})/2i$

Задача 5.2. Напишите явную формулу для k-того члена последовательности a_k, такой что $a_0=1$, $a_1=-1$ и $a_k=2a_{k-1}-a_{k-2}$ при $k\geqslant 2$.

Задача 5.3. Пусть $g(x)=\prod(x-\alpha_i)$, где все α_i попарно различны. Покажите, что для любого $f\in\Bbbk[x]$ с $\deg f<\deg g$ разложение рациональной функции f/g в сумму простейших дробей из предл. 4.7 имеет вид:

$$\frac{f}{g}=\sum\frac{f(\alpha_i)/g'(\alpha_i)}{(x-\alpha_i)}$$

где g' — производная от g.

Задача 5.4 (формула Тейлора). Покажите, что над любым полем $\Bbbk$ характеристики нуль для произвольно заданного набора из $n+1$ значений $b_0,b_1,\dots,b_n\in\Bbbk$ и произвольно заданной точки $a\in\Bbbk$ существует единственный многочлен f степени $\leqslant n$, такой, что $f(a)=b_0$ и $(d/dx)^i f(a)=b_i$ при всех $i=1,\dots,n$. Напишите для такого многочлена явную формулу.

Задача 5.5. Покажите, что все коэффициенты ряда $\mathrm{tg}(x)=\sin(x)/\cos(x)$ положительны.

Задача 5.6. Покажите, ряд e^x не является рациональной функцией (т. е. не равен частному двух многочленов).

Задача 5.7. Напишите не являющийся рациональной функцией ряд, коэффициенты которого только нули единицы.

Задача 5.8. Обозначим через $p_m(n)$ число диаграмм Юнга веса n из $\leqslant m$ строк и положим $p(0)\overset{\text{def}}{=}1$. Выразите $p_m(n)$ через $p_{m-1}(n)$ и $p_m(n-m)$ и покажите, что производящая функция $P_m(t)=\sum\limits_{n\geqslant 0}p_m(n)\,t^n\in\mathbb{Q}[[t]]$ рациональна.

Задача 5.9 (теорема Эйлера о пятиугольных числах). Обозначим через $p(n)$ число всех диаграмм Юнга веса[1] n, положим $p(0)\overset{\text{def}}{=}1$ и образуем производящую функцию $P(t)=\sum\limits_{n\geqslant 0}p(n)t^n\in\mathbb{Q}[[t]]$. Покажите, что а) $P(t)=\prod\limits_{k\geqslant 1}(1-t^k)^{-1}$

[1] число $p(n)$ также называется *числом разбиений* числа n

б) $1/P(t) = 1 + \sum\limits_{n\geqslant 1} (\widehat{p}_{\text{ч}}(n) - \widehat{p}_{\text{н}}(n))\cdot t^n$, где через $\widehat{p}_{\text{ч}}(n)$ и $\widehat{p}_{\text{н}}(n)$ обозначены количества диаграмм Юнга веса n с попарно разными длинами строк, состоящих, соответственно, из чётного и нечётного количества строк

в) $p(n) = \sum\limits_{k\geqslant 1} (-1)^{k+1} \left(p\left(n - \frac{3k^2-k}{2}\right) + p\left(n - \frac{3k^2+k}{2}\right)\right) =$
$= p(n-1)+p(n-2)-p(n-5)-p(n-6)+p(n-12)+p(n-15)-\cdots$.

г) Вычислите $p(10)$.

Задача 5.10. В выпуклом n угольнике проводят максимально возможное число диагоналей так, чтобы они не пересекались нигде, кроме вершин. Сколькими способами это можно сделать?

Задача 5.11. Обозначим через i_m число всех неприводимых приведённых многочленов степени m в $\mathbb{F}_p[x]$ (см. зад. 4.28). Покажите, что в $\mathbb{Q}[[t]]$ выполняется равенство $(1-pt)^{-1} = \prod\limits_{m\in\mathbb{N}} (1-t^m)^{-i_m}$.

Задача 5.12 (действие $\mathbb{Q}[[d/dx]]$ на $\mathbb{Q}[x]$). Для каждого ряда

$$F(t) = \sum_{k\geqslant 0} a_k t^k \in \mathbb{Q}[[t]]$$

рассмотрим дифференциальный оператор

$$\widetilde{F} = F\left(\frac{d}{dx}\right) : \mathbb{Q}[x] \longrightarrow \mathbb{Q}[x]\,,$$

который переводит каждый многочлен $g \in \mathbb{Q}[x]$ в сумму

$$\widetilde{F}g = \sum_{k\geqslant 0} a_k (d/dx)^k g = a_0 g + a_1 g' + a_2 g'' + a_3 g''' + \cdots\,,$$

а) Убедитесь, что отображение $\widetilde{F} : \mathbb{Q}[x] \longrightarrow \mathbb{Q}[x]$ корректно определено[1] и $\mathbb{Q}$-*линейно*, т. е. $\widetilde{F}(\lambda f + \mu g) = \lambda \widetilde{F} f + \mu \widetilde{F} g\ \forall\, \lambda, \mu \in \mathbb{Q}$ и $\forall\, f, g \in \mathbb{Q}[x]$.

б) Выразите коэффициенты многочлена $F_m(x) \overset{\text{def}}{=} \widetilde{F} x^m$ через коэффициенты ряда F и покажите, что ряд F однозначно восстанавливается по набору многочленов F_m (они называются *многочленами Аппеля* ряда F).

в) Выясните, как действует на $\mathbb{Q}[x]$ оператор $e^{\alpha \frac{d}{dx}}$, где $\alpha \in \mathbb{Q}$.

г) Покажите, что $\mathbb{Q}$-линейное отображение $\varPhi : \mathbb{Q}[x] \longrightarrow \mathbb{Q}[x]$ тогда и только тогда представляется в виде $\varPhi = \widetilde{F}$ для некоторого $F \in \mathbb{Q}[[t]]$, когда оно перестановочно со всеми операторами сдвига $T_\alpha : f(x) \mapsto f(x+\alpha)$ (где $\alpha \in \mathbb{Q}$).

д) Выясните, какими рядами задаются *разностные операторы*:

$$\nabla : f(x) \longmapsto f(x) - f(x-1) \tag{5-30}$$
$$\Delta : f(x) \longmapsto f(x+1) - f(x) \tag{5-31}$$

[1] т. е. является алгебраической операцией на множестве всех многочленов

Задача 5.13 (ряд Тодда и числа Бернулли). Ряд

$$\mathrm{td}(t) \stackrel{\mathrm{def}}{=} t/(1-e^{-t}) = \sum_{k\geqslant 0} \frac{a_k}{k!}\, t^k \in \mathbb{Q}[[t]]$$

называется *рядом Тодда*. Числа b_k, равные числам a_k из этой формулы при $k \neq 1$, и $b_1 = -a_1$ называются *числами Бернулли*.

а) Найдите в явном виде функцию $\big((B(t) - B(-t)\big)/2$ и все числа a_{2k+1}.

б) Найдите первую дюжину чисел Бернулли.

в) Докажите для $k \geqslant 2$ рекурсивную формулу[1] $1 + \sum\limits_{\nu=1}^{k-1} \binom{k}{\nu} b_\nu = 0$.

г) Покажите, что числа b_{2k} (с чётными номерами) образуют знакопеременную последовательность.

Задача 5.14 (суммирование степеней). Обозначим через $S_m(x)$ первообразную с нулевым свободным членом от m-того многочлена Аппеля ряда Тодда, т.е. такой многочлен $S_m(x) \in \mathbb{Q}[x]$ без свободного члена, что

$$\frac{d}{dx} S_m(x) = \mathrm{td}\left(\frac{d}{dx}\right) x^m$$

Покажите, что при всех целых неотрицательных n

$$0^m + 1^m + 2^m + \cdots + n^m = S_m(n)\,,$$

и напишите явные формулы для суммирования k-тых степеней первых n натуральных числе для каждого k от 1 до 6. (Указание: подействуйте на сумму степеней разностным оператором ∇ из зад. 5.12 (д))

[1] эту формулу часто изображают мнемоническим равенством $\check{b}^k = (1+\check{b})^k$, где значёк $\check{b}$ указывает на то, что показатели при букве b следует воспринимать не как степени, а как номера чисел Бернулли, т.е. писать не верхними индексами, а нижними

§6. Фактор кольца и идеалы

6.1. Идеалы. Подкольцо I коммутативного кольца K называется *идеалом*, если вместе с каждым своим элементом оно содержит и все его кратные.

В n° 3.4.3 мы видели, что этими свойствами обладает ядро любого гомоморфизма колец. Примерами идеалов являются также подмножества вида

$$(a) = \{ka \mid k \in K\}\,, \tag{6-1}$$

состоящие из всех элементов, кратных фиксированному элементу $a \in K$. Идеалы вида (6-1) называются *главными*. Мы встречались с ними при построении колец вычетов $\mathbb{Z}/(n)$ и $\Bbbk[x]/(f)$, где они возникали как ядра гомоморфизмов

$$\mathbb{Z} \xrightarrow{m \mapsto [m]_n} \mathbb{Z}/(n)\,, \quad \Bbbk[x] \xrightarrow{g \mapsto [g]_f} \Bbbk[x]/(f)$$

сопоставляющих целому числу (соотв. многочлену) класс его вычета.

Более общим образом, для любого набора элементов $a_1, a_2, \dots, a_m \in K$ множество всех элементов, представимых в виде $k_1a_1 + k_2a_2 + \dots + k_ma_m$ с произвольными $k_1, k_2, \dots, k_m \in K$ тоже является идеалом. Он обозначается через

$$(a_1, a_2, \dots, a_m) \stackrel{\text{def}}{=} \{k_1a_1 + k_2a_2 + \dots + k_ma_m \mid k_1, k_2, \dots, k_m \in K\} \tag{6-2}$$

и называется *идеалом, порождённым* $a_1, a_2, \dots, a_m$. Мы встречались с такими идеалами, когда доказывали существование наибольшего общего делителя в кольцах целых чисел и многочленов с коэффициентами в поле.

Кроме того, в любом кольце K имеются *тривиальные* идеалы $(0) = \{0\}$ и $(1) = K$.

Упражнение 6.1. Покажите, что следующие условия на идеал I в коммутативном кольце K с единицей попарно равносильны:
а) $I = K$ б) $1 \in I$ в) I содержит обратимый элемент.

Предложение 6.1
Коммутативное кольцо K с единицей тогда и только тогда является полем, когда в нём нет нетривиальных идеалов.

Доказательство. Из упр. 6.1 вытекает, что ни в каком поле нетривиальных идеалов нет. Наоборот, если в кольце нет нетривиальных идеалов, то главный идеал (b), порождённый любым ненулевым элементом b, совпадает со всем кольцом и, в частности, содержит единицу, т. е. $1 = ab$ для некоторого a. Тем самым, любой ненулевой элемент обратим. $\square$

6.2. Факторизация. Пусть произвольное коммутативное кольцо K разбито в объединение непустых непересекающихся подмножеств, занумерованных элементами некоторого множества X

$$K = \bigsqcup_{x \in X} K_x \,. \tag{6-3}$$

Иначе можно сказать, что имеется сюрьективное отображение множеств

$$K \xrightarrow{x} X \,, \tag{6-4}$$

сопоставляющее каждому элементу $a \in K$ номер $x(a)$ того подмножества разбиения (6-3), где лежит a. Или же можно сказать, что на K задано отношение эквивалентности, и множество классов эквивалентности обозначено через X, так что отображение 6-4 переводит каждый класс эквивалентности $[a]$ в $x(a)$.

Мы хотим задать на множестве X структуру коммутативного кольца так, чтобы отображение 6-4 стало гомоморфизмом колец, или — что то же самое — так, чтобы сложение и умножение классов разбиения (6-3) задавалось формулами

$$[a] + [b] = [a+b] \,, \quad [a] \cdot [b] = [ab] \,. \tag{6-5}$$

Из установленных нами в n° 3.4.3 свойств гомоморфизмов колец вытекает, что для этого *необходимо*, чтобы содержащий нулевой элемент класс $[0]$ разбиения (6-3) (который будет ядром гомоморфизма (6-4)), был идеалом кольца K, а все остальные слои были аддитивными сдвигами ядра на элементы кольца K, т. е. чтобы $\forall\, a \in K$ выполнялось равенство

$$[a] = a + [0] = \{a + b \mid b \in [0]\} \,.$$

Оказывается, что этих условий и достаточно: для любого идеала $I \subset K$ множество классов

$$[a]_I = a + I \stackrel{\text{def}}{=} \{a + b \mid b \in I\} \tag{6-6}$$

образует разбиение кольца K, и правила (6-5) корректно определяют на нём структуру коммутативного кольца с единицей $[1]_I$ и нулём $[0]_I = I$.

Упражнение 6.2. Убедитесь, что отношение сравнимости по модулю идеала

$$a_1 \equiv a_2 \pmod{I} \,,$$

означающее, что $a_1 - a_2 \in I$, является отношением эквивалентности, разбивающим K в точности на классы (6-6), и проверьте, что формулы (6-5) корректно определены на этих классах.

Определение 6.1

Классы эквивалентности (6-6) называются *классами вычетов* (или *смежными классами*) по модулю идеала I. Множество этих классов с операциями (6-5) называется *фактор кольцом* кольца K по идеалу I и обозначается K/I. Эпиморфизм

$$K \xrightarrow{a\mapsto[a]_I} K/I\,, \tag{6-7}$$

сопоставляющий каждому элементу кольца его класс вычетов, называется *гомоморфизмом факторизации*

6.2.1. Пример: кольца вычетов $\mathbb{Z}/(n)$ и $\Bbbk[x]/(f)$ суть фактор кольца кольца целых числел и кольца многочленов по главным идеалам $(n)\subset\mathbb{Z}$ и $(f)\subset\Bbbk[x]$ соответственно.

6.2.2. Пример: образ гомоморфизма. Согласно n° 3.4.3, образ любого гомоморфизма коммутативных колец $K_1\xrightarrow{\varphi}K_2$ канонически изоморфен фактор кольцу $K_1/\ker(\varphi)$. При этом изоморфизме элементу $b=\varphi(a)\in\operatorname{im}\varphi\subset K_2$ отвечает класс вычетов $[a]_{\ker\varphi}=\varphi^{-1}(b)$.

6.3. Кольца главных идеалов. Целостное кольцо K с единицей называется *кольцом главных идеалов*, если каждый идеал $I\subset K$ является *главным*, т. е. имеет вид $I=(d)=\{ad\mid a\in K\}$.

Параллелизм между кольцами $\mathbb{Z}$ и $\Bbbk[x]$, где $\Bbbk$ — поле, который мы наблюдали выше, объясняется тем, что оба эти кольца являются кольцами главных идеалов. Мы фактически доказали это, когда строили в этих кольцах наибольший общий делитель. Ниже мы воспроизведём это доказательство ещё раз таким образом, чтобы оно годилось для чуть более широкого класса колец, допускающих *деление с остатком.*

6.3.1. Пример: евклидовы кольца. Целостное кольцо K с единицей называется *евклидовым*, если существует *функция высоты* (или *евклидова норма*)

$$K\setminus\{0\}\xrightarrow{\nu}\mathbb{N}\cup\{0\}\,,$$

сопоставляющая каждому ненулевому элементу $a\in K$ целое неотрицательное число $\nu(a)$ так, что $\forall\, a,b\in K\setminus\{0\}$ выполняются два свойства:

$$\nu(ab)\geqslant\nu(a) \tag{6-8}$$

$$\exists\, q,r\in K\ :\ a=bq+r\ \text{ и либо } \nu(r)<\nu(b)\,,\text{ либо } r=0\,. \tag{6-9}$$

Элементы q и r из (6-9), называются, соответственно, *неполным частным* и *остатком* от деления a на b. Подчеркнём, что их единственности (для данных a и b) не предполагается.

Например, в кольце целых чисел $\mathbb{Z}$ функцией высоты является абсолютная величина, а в кольце многочленов $\Bbbk[x]$ с коэффициентами в поле $\Bbbk$ высотой служит степень многочлена.

Упражнение 6.3. Покажите, что кольца

а) $\mathbb{Z}[i]\overset{\text{def}}{=}\{\,a+bi\in\ \mid a,b\in\mathbb{Z}\,,\ i^2=-1\}$

б) $\mathbb{Z}[\omega]\overset{\text{def}}{=}\{a+b\omega\in\mathbb{C}\mid a,b\in\mathbb{Z}\,,\,\omega^2+\omega+1=0\,\}$

являются евклидовыми относительно высоты $\nu(z)=|z|^2$.

Предложение 6.2
Любое евклидово кольцо является кольцом главных идеалов[1].

Доказательство. В любом идеале $I \subset K$ имеется ненулевой элемент $d \in I$ наименьшей высоты. Покажем, что каждый элемент $a \in I$ делится на d, что даст равенство $I = (d)$. Деля a на d с остатком, получаем $a = dq + r$. Тогда $r = a - dq \in I$, поскольку $a, d \in I$. Поскольку строгое неравенство $\nu(r) < \nu(d)$ невозможно по выбору d, мы заключаем, что $r = 0$. □

Следствие 6.1
Кольца $\mathbb{Z}$, $\Bbbk[x]$ (где $\Bbbk$ — поле), $\mathbb{Z}[i]$ и $\mathbb{Z}[\omega]$ (см. упр. 6.3) являются кольцами главных идеалов.

Упражнение 6.4. Покажите, что в любом евклидовом кольце равенство $\nu(ab) = \nu(a)$ в свойстве (6-8) равносильно тому, что элемент b обратим

6.3.2. НОД и взаимная простота. В кольце главных идеалов K у любого набора элементов $a_1, a_2, \dots, a_n$ есть наибольший общий делитель — такой $d = \text{нод}(a_1, a_2, \dots, a_n)$ — такой элемент кольца, который делит каждый из элементов a_i и делится на любой элемент с таким свойством. Это простая переформулировка того, что идеал, порождённый элементами $a_1, a_2, \dots, a_n$, является главным. В самом деле, поскольку

$$(a_1, a_2, \dots, a_n) = \{x_1a_1 + x_2a_2 + \cdots + x_na_n \mid x_i \in K\} = (d)$$

для некоторого $d \in K$, элемент d, как и все элементы $(a_1, a_2, \dots, a_n)$, имеет вид $d = \sum x_\nu a_\nu$, и значит, делится на любой общий делитель чисел a_i. С другой стороны, все элементы $(a_1, a_2, \dots, a_n) = (d)$, включая сами a_i, делятся на d.

Отметим, что наибольший общий делитель d определён не однозначно, а с точностью до умножения на произвольный обратимый элемент кольца.

Упражнение 6.5. В любом целостном коммутативном кольце K равенство ненулевых главных идеалов $(a) = (b)$ равносильно тому, что $a = sb$, где $s \in K$ обратим.

Несмотря на эту неоднозначность, наибольший общий делитель элементов a_i (понимаемый как класс элемента с точностью до умножения на обратимую константу) по-прежнему принято обозначать через $\text{нод}(a_1, a_2, \dots, a_n)$, если это не ведёт к недоразумениям. Из наличия представления

$$\text{нод}(a_1, a_2, \dots, a_n) = x_1a_1 + x_2a_2 + \cdots + x_na_n$$

[1]отметим, что обратное неверно, но контрпримеры приходят из достаточно продвинутой арифметики и геометрии, и для их содержательного обсуждения требуется техника, которой мы пока ещё не владеем; впрочем, заинтересовавшийся читатель может обратиться к замечанию 3 на стр. 365 книги *Э. Б. Винберг. Курс алгебры*. М. «Факториал» (1999)

вытекает, что в любом кольце главных идеалов отсутствие необратимых общих делителей у элементов $a_1, a_2, \dots, a_n$ равносильно *взаимной простоте* этих элементов, т. е. возможности представить единицу кольца в виде

$$1 = x_1 a_1 + x_2 a_2 + \cdots + x_n a_n \quad \text{с некоторыми } x_i \in K$$

(иначе взаимную простоту $a_1, a_2, \dots, a_n$ можно охарактеризовать как равенство $(a_1, a_2, \dots, a_n) = K$)

Упражнение 6.6. Докажите, что в любом кольце главных идеалов K справедлива *китайская теорема об остатках*: если $a_1, a_2, \dots, a_m \in K$ таковы, что $\forall\ i \neq j$ $\text{нод}(a_i, a_j) = 1$, то $K/(a_1 \cdot a_2 \cdot \cdots \cdot a_m) \simeq (K/(a_1)) \times (K/(a_2)) \times \cdots (K/(a_m))$.

Предложение 6.3
В любом кольце главных идеалов K следующие свойства элемента $p \in K$ попарно эквивалентны друг другу:
(1) фактор кольцо $K/(p)$ является полем;
(2) в фактор кольце $K/(p)$ нет делителей нуля;
(3) p неприводим, т. е. $p = ab \Rightarrow a$ или b обратим в K.

Доказательство. Импликация (1) $\Rightarrow$ (2) уже была доказана нами для любого поля в n° 3.1.1. Покажем, что в любом целостном кольце K (не обязательно являющемся кольцом главных идеалов) имеет место импликация (2) $\Rightarrow$ (3). Из $p = ab$ следует, что $[a][b] = 0$ в $K/(p)$, и если в $K/(p)$ нет делителей нуля, то один из сомножителей, скажем $[a]$, равен $[0]$. Тогда $a = ps = abs$ для некоторого $s \in K$, и значит, $a(1 - bs) = 0$. Поскольку в K нет делителей нуля, $bs = 1$, т. е. b обратим. Покажем теперь, что в кольце главных идеалов (3) $\Rightarrow$ (1). Если p неприводим, то $\forall\ b \notin (p)$ $\text{нод}(p, b) = 1$, а значит, $\exists\ x, y \in K : px + by = 1$, откуда $[b][y] = 1$ в $K/(p)$. Тем самым, любой класс $[b] \neq [0]$ обратим в $K/(p)$, т. е. $K/(p)$ — поле. $\square$

Упражнение 6.7. Проверьте, что идеалы $(x, y) \subset \mathbb{Q}[x, y]$ и $(2, x) \in \mathbb{Z}[x]$ не являются главными.

6.4. Нётеровы кольца. Любое множество элементов $\{a_\nu\}$ коммутативного кольца K порождает идеал $(a_\nu) \subset K$, состоящий из всевозможных *конечных* линейных комбинаций $b_1 a_{\nu_1} + b_2 a_{\nu_2} + \cdots + b_m a_{\nu_m}$ элементов $a_\nu \in A$ с произвольными коэффициентами $b_i \in K$. Очевидно, что всякий идеал можно описать таким образом, взяв достаточно большое множество порождающих a_ν (например, все элементы идеала). Во многих задачах алгебры, геометрии и анализа ключевую роль играет следующее условие конечности.

Определение 6.2
Кольцо K называется *нётеровым*, если каждый идеал $I \subset K$ может быть порождён конечным набором элементов.

Упражнение 6.8. Покажите, что фактор кольцо нётерова кольца тоже нётерово.

Условие нётеровости можно переформулировать несколькими эквивалентными способами, которыми мы часто будем пользоваться в дальнейшем.

Лемма 6.1
Следующие свойства коммутативного кольца K попарно эквивалентны:

1) любое множество элементов $\{a_\nu\}$ содержит некоторое конечное подмножество, которое порождает тот же идеал, что и само множество;

2) любой идеал допускает конечное множество порождающих;

3) для любой бесконечной цепочки вложенных идеалов $I_1 \subset I_2 \subset I_3 \subset \cdots$ существует такое $n \in \mathbb{N}$, что $I_\nu = I_n$ для всех $\nu \geqslant n$.

Доказательство. Ясно, что (1) $\Rightarrow$ (2). Чтобы из (2) вывести (3), заметим, что $I = \bigcup I_\nu$ тоже является идеалом, а значит, порождён конечным набором элементов. Все они принадлежат некоторому I_n, и тогда $I_n = I = I_\nu$ при $\nu \geqslant n$. Чтобы вывести (1) из (3) будем по индукции строить цепочку идеалов $I_n = (a_1, a_2, \dots, a_n)$, начав с произвольного элемента a_1 из данного множества $\{a_\nu\}$ и добавляя на k-том шагу очередную образующую a_k так, чтобы $a_k \notin (a_1, a_2, \dots, a_{k-1})$. Так как $I_{k-1} \subsetneq I_k$, этот процесс не может продолжаться бесконечно, и на каком-то шагу мы получим идеал, содержащий все a_ν. □

Теорема 6.1 (теорема Гильберта о базисе)
Если кольцо K нётерово, то кольцо многочленов $K[x]$ тоже нётерово.

Доказательство. Рассмотрим произвольный идеал $I \subset K[x]$, обозначим через $L_d \subset K$ множество старших коэффициентов всех многочленов степени $\leqslant d$ в I и положим $L_\infty = \bigcup\limits_d L_d$.

Упражнение 6.9. Убедитесь, что все L_d и L_∞ являются идеалами в K.

Поскольку K нётерово, все эти идеалы конечно порождены. Пусть L_∞ порождается старшими коэффициентами $a_1, a_2, \dots, a_s \in K$ многочленов

$$f_1^{(\infty)}, f_2^{(\infty)}, \dots, f_{s_\infty}^{(\infty)} \in I \tag{6-10}$$

и пусть $\max_\nu(\deg f_\nu) = m$. Аналогично, для каждого $0 \leqslant k \leqslant m-1$ обозначим через $f_1^{(k)}, f_2^{(k)}, \dots, f_{s_k}^{(k)}$ те многочлены, старшие коэффициенты которых порождают идеал $L_k \subset K$.

Покажем, что идеал I порождается $s_0 + \dots + s_{m-1} + s_\infty$ многочленами $f_\nu^{(\mu)}$.

Для этого заметим, что любой многочлен $f \in I$ сравним по модулю многочленов (6-10) с многочленом степени $\leqslant (m-1)$. В самом деле, представим старший коэффициент a многочлена f в виде $a = b_1a_1 + b_2a_2 + \dots + b_sa_s$. Если $\deg f \geqslant m$, то многочлен $f - \sum b_i f_i^{(\infty)} \cdot x^{\deg f - \deg f_i^{(\infty)}}$ имеет строго меньшую степень, чем f. Повторно применяя к нему это же рассуждение, мы после нескольких итераций придём к многочлену степени $\leqslant (m-1)$.

Получившийся многочлен степени $m-1$ по тем же самым причинам сравним по модулю многочленов $f_1^{(m-1)}, f_2^{(m-1)}, \ldots, f_{s_{m-1}}^{(m-1)}$ с многочленом степени, не превышающей $m-2$, и т. д. □

Следствие 6.2
Кольцо $K[x_1, x_2, \ldots, x_n]$ нётерово, если K нётерово.

Упражнение 6.10. Покажите, что кольцо формальных степенных рядов над нётеровым кольцом нётерово.

Определение 6.3
Пусть K — произвольное коммутативное кольцо с единицей. Всякое кольцо вида $A = K[x_1, x_2, \ldots, x_n]/I$, где $I \subset K[x_1, x_2, \ldots, x_n]$ — произвольный идеал, называется *конечно порождённой K-алгеброй*[1]. Классы $a_i = x_i \,(\mathrm{mod}\, I)$ называются *образующими* K-алгебры A, а многочлены $f \in I$ — *соотношениями* между этими образующими.

Говоря неформально, K-алгебра состоит из всевозможных выражений, которые можно составить из элементов кольца K и коммутирующих букв

$$a_1, a_2, \ldots, a_n$$

при помощи сложения и умножения с учётом полиномиальных соотношений $f(a_1, a_2, \ldots, a_n) = 0$, где f пробегает I.

Следствие 6.3
Всякая конечно порождённая коммутативная алгебра над нётеровым кольцом нётерова.

6.4.1. Примеры ненётеровых колец. Кольцо многочленов от бесконечного числа переменных $\mathbb{Q}[x_1, x_2, x_3, \ldots]$, элементами которого, по определению, являются всевозможные конечные суммы взятых с рациональными коэффициентами мономов вида $x_{\nu_1}^{m_1} x_{\nu_2}^{m_2} \cdots x_{\nu_s}^{m_s}$ (произведение конечного числа переменных x_ν в некоторых степенях), не является нётеровым, поскольку, например, идеал $(x_1, x_2, \ldots)$, состоящий из всех многочленов без свободного члена, не является конечно порождённым.

Упражнение 6.11. Докажите это и выясните, является ли конечно порождённым идеал, образованный в кольце бесконечно гладких функций $\mathbb{R} \longrightarrow \mathbb{R}$ всеми функциями, обращающимися в нуле в нуль вместе со всеми своими производными.

[1] или,, более торжественно, *конечно порождённой коммутативной алгеброй* над кольцом K

6.5. Разложение на множители. Всюду в этом пункте мы по умолчанию считаем, что K — это *целостное* (т. е. без делителей нуля) коммутативное кольцо с единицей.

6.5.1. Ассоциированные элементы. Ненулевые элементы $a, b \in K$ называются *ассоциированными*, если b делится на a, и a делится на b. Из равенств $a = mb$ и $b = na = nmb$ вытекает равенство $b(1 - nm) = 0$, откуда $mn = 1$. Таким образом, ассоциированность элементов означает, что они получаются друг из друга умножением на обратимый элемент кольца. Например, в кольце целых чисел $\mathbb{Z}$ числа a и b ассоциированы тогда и только тогда, когда $a = \pm b$.

6.5.2. Неприводимые элементы. Элемент $q \in K$ называется *неприводимым*, если он не обратим, и из равенства $q = mn$ вытекает, что m или n обратим. Другими словами, неприводимость элемента q означает, главный идеал q не содержится строго ни в каком другом главном идеале. Например, неприводимыми элементами кольца целых чисел являются простые числа.

Поскольку $(p), (q) \subset (p, q)$, в кольце главных идеалов, где $(p, q) = (d)$ для некоторого $d = \text{нод}(p, q)$, любые два неприводимых элемента p, q либо взаимно просты (что отвечает равенству $d = 1$), либо ассоциированы (что отвечает равенству $(p, q) = (p) = (q)$).

В произвольном кольце два неассоциированных неприводимых элемента могут не быть взаимно простыми в смысле опр. 2.2 на стр. 33. Например, в $\mathbb{Q}[x, y]$ элементы x и y не взаимно просты и не ассоциированы.

Предложение 6.4
В нётеровом кольце всякий элемент является произведением конечного числа неприводимых.

Доказательство. Если элемент a неприводим, доказывать нечего. Пусть a приводим. Запишем его в виде произведения необратимых элементов. Каждый приводимый сомножитель этого произведения снова запишем в виде произведения необратимых элементов и т. д. Эта процедура закончится, когда все сомножители станут неприводимы, что и требуется. Если же она никогда не закончится, мы сможем образовать бесконечную последовательность строго вложенных друг в друга главных идеалов $(a_1) \subset (a_2) \subset (a_3) \subset \cdots$, что невозможно. □

6.5.3. Простые элементы. Необратимый элемент p произвольного кольца K называется *простым*, если для любых $a, b \in K$ из того, что произведение ab делится на p, вытекает, что a или b делится на p. Иначе можно сказать, что простота элемента p означает, что в кольце $K/(p)$ нет делителей нуля.

В целостном кольце любой простой элемент p автоматически неприводим: если $p = xy$, то один из сомножителей, скажем x, делится на p, и тогда $p = pyz$, откуда $yz = 1$ и y обратим.

В кольце главных идеалов верно и обратное: по предл. 6.3 все неприводимые элементы кольца главных идеалов просты.

В произвольно взятом кольце простота элемента может оказаться строго более сильным свойством, чем неприводимость. Например, в кольце

$$\mathbb{Z}[\sqrt{5}] = \mathbb{Z}[x]/(x^2-5)$$

число 2 неприводимо, но не просто, поскольку в фактор кольце

$$\mathbb{Z}[\sqrt{5}]/(2) \simeq \mathbb{Z}[x]/(2, x^2-5) \simeq \\ \simeq \mathbb{Z}[x]/(2, x^2+1) \simeq \mathbb{F}_2[x]/(x^2+1) \simeq \mathbb{F}_2[x]/\big((x+1)^2\big)$$

есть делитель нуля $(x+1) \pmod{(2, x^2+1)}$. На языке алгебраических чисел проделанное вычисление означает, что число $1+\sqrt{5}$ не делится на 2 в $\mathbb{Z}[\sqrt{5}]$, а его квадрат $(1+\sqrt{5})^2 = 6+2\sqrt{5}$ — делится, несмотря на то, что 2 является *неприводимым* элементом кольца $\mathbb{Z}[\sqrt{5}]$.

Упражнение 6.12. Убедитесь, что 2, $\sqrt{5}+1$, $\sqrt{5}-1$ неприводимы и попарно неассоциированы в кольце $\mathbb{Z}[\sqrt{5}]$. Из этого вытекает, в частности, что 4 имеет в $\mathbb{Z}[\sqrt{5}]$ два *различных* разложения на неприводимые множители:

$$2\cdot 2 = 4 = \left(\sqrt{5}+1\right)\cdot\left(\sqrt{5}-1\right)\,.$$

Определение 6.4

Целостное кольцо называется *факториальным*, если каждый его необратимый элемент является произведением конечного числа неприводимых элементов, причём любые два таких разложения $p_1p_2\ \cdots\ p_m = q_1q_2\ \cdots\ q_k$ состоят из одинакового числа сомножителей $k=m$, и после надлежащей их перенумерации найдутся такие обратимые элементы s_ν, что $q_\nu = p_\nu s_\nu$ при всех ν.

Предложение 6.5

Целостное кольцо K, в котором каждый элемент является произведением конечного числа неприводимых, факториально тогда и только тогда, когда все его неприводимые элементы просты.

Доказательство. Покажем, что если K факториально, то любой неприводимый элемент $q\in K$ прост. Пусть произведение ab делится на q. Таким образом, разложение ab на неприводимые множители содержит множитель, ассоциированный с q. В силу единственности, разложение произведения ab является произведением разложений a и b. Поэтому q ассоциирован с одним из неприводимых делителей a или b, т. е. a или b делится на q, что и требовалось.

Пусть все неприводимые элементы K просты. Покажем, что равенство

$$p_1p_2\cdots p_k = q_1q_2\cdots q_m\,, \tag{6-11}$$

в котором все сомножители просты, возможно только если $k=m$ и каждый p_i ассоциирован с q_i (может быть, после надлежащей перенумерации). Поскольку произведение в правой части (6-11) делится на p_1, из простоты p_1 вытекает, что один из сомножителей этого произведения делится на p_1. Будем считать, что это $q_1 = sp_1$. Поскольку q_1 неприводим, элемент s обратим. Пользуясь целостностью кольца K, сокращаем равенство (6-11) на p_1 и получаем более короткое равенство $p_2p_3 \cdots p_k = (sq_2)q_3 \cdots q_m$, к которому применимы те же рассуждения. □

Следствие 6.4
Нётерово кольцо факториально тогда и только тогда, когда все его неприводимые элементы просты.

Следствие 6.5
Всякое кольцо главных идеалов факториально.

Упражнение 6.13 (китайская теорема об остатках). Докажите, что в любом кольце главных идеалов K справедлива такая версия китайской теоремы об остатках: если $n = p_1^{m_1}p_2^{m_2}\dots p_r^{m_r}$, то $k/(n) \simeq K/\left(p_1^{m_1}\right)\oplus K/\left(p_1^{m_1}\right)\oplus\cdots\oplus K/\left(p_r^{m_r}\right)$.

6.5.4. Пример: гауссовы целые числа. Согласно упр. 6.3, кольцо гауссовых чисел $\mathbb{Z}[i] \subset \mathbb{C}$ является кольцом главных идеалов, а потому в нём справедлива теорема об однозначности разложения на неприводимые множители.

Выясним, какие целые простые числа $p \in \mathbb{Z}$ остаются неприводимыми в кольце гауссовых чисел. Для этого заметим, что разложение любого целого вещественного $n \in \mathbb{Z}$, будучи инвариантным относительно комплексного сопряжения, должно вместе с каждым неприводимым множителем $a + ib \in \mathbb{C} \setminus \mathbb{R}$ содержать и сопряжённый ему множитель $a - ib$. В частности, если простое $p \in \mathbb{Z}$ перестаёт быть неприводимым в $\mathbb{Z}[i]$, то оно представляется в виде $p = (a + ib)(a - ib) = a^2 + b^2$ с ненулевыми $a, b \in \mathbb{Z}$. Таким образом, простое $p \in \mathbb{Z}$ тогда и только тогда приводимо в $\mathbb{Z}[i]$, когда p является суммой двух квадратов.

Чтобы явно описать все такие p, вспомним, что неприводимость $p \in \mathbb{Z}[i]$ равносильна тому, что фактор кольцо $\mathbb{Z}[i]/(p)$ является полем[1], и посмотрим на это фактор кольцо как на фактор кольца многочленов $\mathbb{Z}[x]$:

$$\mathbb{Z}[i]/(p) \simeq \mathbb{Z}[x]/(p, x^2 + 1) \simeq \mathbb{F}_p[x]/(x^2 + 1) .$$

Правое кольцо является полем тогда и только тогда, когда многочлен $x^2 + 1$ неприводим над $\mathbb{F}_p$, что равносильно отсутствию у него корней в $\mathbb{F}_p$. Таким образом, простое $p \in \mathbb{Z}$ является суммой двух квадратов, если и только если -1 квадратичный вычет по модулю p. Как мы видели в n° 4.4.4, это происходит в точности тогда, когда $(p - 1)/2$ чётно, т. е. для простых $p = 4k + 1$ и $p = 2$.

[1] см. предложение (предл. 6.3)

6.5.5. НОД в факториальном кольце. В факториальном кольце K у любого набора элементов $a_1, a_2, \dots, a_m \in K$ существует наибольший общий делитель. А именно, для каждого класса ассоциированных неприводимых элементов $q \in K$ обозначим через m_q максимальное целое число, такое что q^{m_q} делит каждое из чисел a_i. Поскольку каждое a_i является произведением конечного числа неприводимых элементов, числа m_q будут отличны от нуля лишь для конечного числа классов q. Таким образом, корректно определён класс числа

$$\text{нод}(a_1, a_2, \dots, a_m) = \prod_q q^{m_q}$$

с точностью до умножения на обратимые константы. Очевидно, что это число делится на любой общий делитель чисел a_i, поскольку такой делитель, в силу факториальности кольца K, должен делиться на q^{m_q} для каждого неприводимого q.

6.5.6. Многочлены над факториальным кольцом. Пусть K — факториальное кольцо. Назовём *содержанием* многочлена

$$f = a_0x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n \in K[x]$$

наибольший общий делитель его коэффициентов $\operatorname{cont}(f) \stackrel{\text{def}}{=} \text{нод}(a_0, a_1, \dots, a_n)$.

Лемма 6.2
$\operatorname{cont}(fg) = \operatorname{cont}(f) \cdot \operatorname{cont}(g)$ для любых $f, g \in K[x]$.

Доказательство. Достаточно для каждого неприводимого $q \in K$ показать, что q делит левую часть равенства $\operatorname{cont}(fg) = \operatorname{cont}(f) \cdot \operatorname{cont}(g)$ если и только если он делит правую. Для этого применим к этому равенству гомоморфизм редукции по модулю q

$$K[x] \xrightarrow{f \mapsto [f]_q} (K/(q))[x],$$

заменяющий коэффициенты многочленов на их классы вычетов по модулю q. Поскольку неприводимые элементы факториального кольца просты, кольцо $K/(q)$ целостное. Поэтому кольцо многочленов $(K/(q))[x]$ тоже целостное. Тем самым, произведение $[fg]_q = [f]_q[g]_q$ обращается в нуль, если и только если один из сомножителей $[f]_q$, $[g]_q$ равен нулю, что и требуется. □

Обозначим через Q_K поле частных факториального кольца K. Кольцо многочленов $K[x]$ является подкольцом в кольце многочленов $Q_K[x]$.

Лемма 6.3
Каждый многочлен $f(x) \in Q_K[x]$ можно записать в виде

$$f(x) = \frac{a}{b} \cdot \widetilde{f}(x), \tag{6-12}$$

где $\widetilde{f}(x) \in K[x]$ и $\operatorname{cont}(f) = \text{нод}(a, b) = 1$. При этом a, b и $\widetilde{f}$ определяются по f однозначно с точностью до умножения на обратимые элементы кольца K.

Доказательство. Для получения такой записи надо вынести из коэффициентов f их общий знаменатель. Получится многочлен с коэффициентами в K, умноженный на число вида $1/c \in Q_K$. Потом вынести из всех коэффициентов полученного многочлена их наибольший общий делитель d. Получится многочлен содержания 1, умноженный на $d/c \in Q_K$. Остаётся записать c/d несократимой дробью a/b. Докажем единственность. Если $(a/b) \cdot \widetilde{f}(x) = (c/d) \cdot \widetilde{g}(x)$ в $Q_K[x]$, то $ad \cdot \widetilde{f}(x) = bc \cdot \widetilde{g}(x)$ в $K[x]$. Сравнивая содержание обеих частей, получаем $ad = bc$, что в силу отсутствия общих неприводимых множителей у a и b, а также у c и d, возможно только если a ассоциирован с c, а b — с d. Но тогда и $\widetilde{f}(x) = \widetilde{g}(x)$ с точностью до умножения на обратимую константу. □

Следствие 6.6 (лемма Гаусса)
Многочлен $f \in K[x]$ содержания 1 неприводим в кольце $Q_K[x]$ тогда и только тогда, когда он неприводим в $K[x]$.

Доказательство. Пусть $f(x) = g(x) \cdot h(x)$ в $Q_K[x]$. Записывая многочлены g и h виде (6-12), приходим к равенству

$$f(x) = \frac{a}{b} \cdot \widetilde{g}(x) \cdot \widetilde{h}(x)\,,$$

где $\widetilde{g}, \widetilde{h} \in K[x]$, $c, d \in K$, и $\operatorname{cont}(\widetilde{g}) = \operatorname{cont}(\widetilde{h}) = \text{нод}(a, b) = 1$. По лем. 6.2 $\operatorname{cont}(\widetilde{g}\widetilde{h}) = 1$. Поэтому, в силу единственности представления (6-12), элементы a и b обратимы в K, а $f(x) = \widetilde{g}(x) \cdot \widetilde{h}(x)$ с точностью до умножения на обратимую константу. □

Теорема 6.2
Кольцо многочленов над факториальным кольцом факториально.

Доказательство. Область главных идеалов $Q_K[x]$ факториальна. Поэтому всякий многочлен $f \in K[x]$ раскладывается в $Q_K[x]$ на неприводимые множители. Записывая их в виде (6-12), получаем равенство

$$\operatorname{cont}(f)\widetilde{f}(x) = f(x) = \frac{a}{b} \prod \widetilde{f}_\nu\,,$$

где $\widetilde{f}_\nu \in K[x]$ неприводимые в $Q_K[x]$ (а тем более в $K[x]$) многочлены из $K[x]$ содержания 1 и $\text{нод}(a, b) = 1$. По лем. 6.2 $\operatorname{cont}(\prod \widetilde{f}_\nu) = 1$, и в силу единственности представления (6-12) мы получаем (с точностью до умножения на обратимые константы из K) равенства $b = 1$ и $f = a \prod \widetilde{f}_\nu$. Раскладывая $a \in K$ в произведение неприводимых констант, получаем разложение f в произведение неприводимых множителей в кольце $K[x]$.

Докажем единственность такого разложения. Пусть в $K[x]$ выполняется равенство $a_1 a_2 \cdots a_k \cdot p_1 p_2 \cdots p_s = b_1 b_2 \cdots b_m \cdot q_1 q_2 \cdots q_r$ где $a_\alpha, b_\beta \in K$ — неприводимые константы, а $p_\mu, q_\nu \in K[x]$ неприводимые многочлены, автоматически имеющие содержание 1. Сравнивая содержание обеих частей с учётом лем. 6.2, получаем равенство $a_1 a_2 \cdots a_k = b_1 b_2 \cdots b_m$ в K. В силу факториальности K, имеем $k = m$ и (после надлежащей перенумерации сомножителей) $a_i = s_i b_i$, где s_i обратимы. Следовательно, с точностью до обратимой константы из K в $K[x]$ выполняется равенство $p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_r$. В силу факториальности $Q_K[x]$ и неприводимости p_i и q_i также и в $Q_K[x]$, мы заключаем, что $r = s$ и (после надлежащей перенумерации сомножителей) $p_i = q_i$ с точностью до постоянного множителя из Q_K. Из единственности представления (6-12) вытекает, что эти постоянные множители являются обратимыми константами из K. □

Следствие 6.7
Если K — факториальное кольцо (например, область главных идеалов или поле), то кольцо многочленов $K[x_1, x_2, \ldots, x_n]$ от любого числа переменных факториально. □

6.5.7. Разложение многочленов в $\mathbb{Q}[x]$ и $\mathbb{Z}[x]$. Всякий многочлен с рациональными коэффициентами пропорционален в $\mathbb{Q}[x]$ многочлену с целыми коэффициентами. Разложение многочлена $f \in \mathbb{Z}[x]$ на множители в $\mathbb{Q}[x]$ разумно начать с отыскания его рациональных корней, что делается за конечное число проб.

Упражнение 6.14. Покажите, что несократимая дробь $a = p/q \in \mathbb{Q}$ может быть корнем многочлена $f(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n \in \mathbb{Z}[x]$, только если p делит a_0, а q делит a_n.

Знание комплексных корней f тоже весьма полезно.

Упражнение 6.15. Разложите $x^4 + 4$ в произведение двух квадратных трёхчленов из $\mathbb{Z}[x]$.

После того, как упомянутые выше простые соображения исчерпаны, можно воспользоваться довольно трудоёмким, но вполне эффективным (если под рукой есть компьютер) *алгоритмом Кронекера*, который позволяет либо явно найти разложение заданного многочлена с целыми коэффициентами в кольце $\mathbb{Z}[x]$, либо убедиться, что его нет, откуда, по лемме Гаусса, будет следовать, что его нет и в $\mathbb{Q}[x]$. Состоит алгоритм в следующем

В любом нетривиальном разложении $f = gh$ в $\mathbb{Z}[x]$ степень одного из делителей, скажем h, не превосходит целой части $(\deg f)/2$, которую мы обозначим через n. Чтобы выяснить, делится f в $\mathbb{Z}[x]$ на какой-нибудь многочлен степени $\leqslant n$, или нет, достаточно подставить в f произвольные $n+1$ различных чисел $z_0, z_1, \ldots, z_n \in \mathbb{Z}$ и рассмотреть все возможные наборы чисел $d_0, d_1, \ldots, d_n$, в которых d_i делит $f(z_i)$. Таких наборов имеется конечное число, и набор значений $h(z_i)$ многочлена h (буде такой многочлен существует) является одним из этих наборов d_i. По упр. 4.6 в $\mathbb{Q}[x]$ есть ровно один многочлен степени $\leqslant n$ принимающий значения d_i в точках z_i. Это *интерполяционный многочлен Лагранжа*

$$f_d(x) = \sum_{i=0}^{n} d_i \cdot \prod_{\nu \neq i} \frac{(x - z_\nu)}{(z_i - z_\nu)} \tag{6-13}$$

Таким образом, если h существует, то находится среди тех из многочленов (6-13), что имеют целые коэффициенты. Остаётся явно разделить f на все эти многочлены и либо убедиться, что они не делят f, либо найти среди них делитель f.

Быстро и «в уме» прикинуть, существует ли в $\mathbb{Z}[x]$ разложение $f = gh$, иногда возможно при помощи редукции многочлена f по простому модулю, как в доказательстве лем. 6.2. А именно, отображение

$$\mathbb{Z}[x] \xrightarrow{f \mapsto [f]_n = f \,(\mathrm{mod}\, n)} \big(\mathbb{Z}/(n)\big)[x]\,, \tag{6-14}$$

которое приводит все коэффициенты многочлена по модулю[1] n, является гомоморфизмом колец, и равенство $f = gh$ в $\mathbb{Z}[x]$ влечёт за собой равенства $[f]_n = [g]_n \cdot [h]_n$ во всех кольцах $\big(\mathbb{Z}/(n)\big)[x]$.

При простом $n = p$ кольцо коэффициентов $\mathbb{Z}/(n) = \mathbb{F}_p$ является полем, и при анализе разложимости $[f]_p$ в $\mathbb{F}_p[x]$ можно использовать факториальность кольца $\mathbb{F}_p[x]$ и потенциальную возможностью перебрать все неприводимые делители любого многочлена (ср. с зад. 4.25). Проиллюстрируем это несколькими примерами.

Покажем, что многочлен $f(x) = x^5 + x^2 + 1$ неприводим в кольце $\mathbb{Z}[x]$. Для этого достаточно рассмотреть его редукцию по модулю 2. Поскольку у f нет целых корней, нетривиальное разложение $f = gh$ в $\mathbb{Z}[x]$ возможно только с $\deg(g) = 2$ и $\deg(h) = 3$. Так как у $[f]_2 = x^5 + x^2 + 1$ нет корней и в $\mathbb{F}_2$, оба многочлена $[g]_2$, $[h]_2$ неприводимы в $\mathbb{F}_2[x]$. Но единственный неприводимый многочлен второй степени в $\mathbb{F}_2[x]$ это x^2+x+1, и x^5+x^2+1 на него не делится.

Ещё один пример: покажем, что при простом p круговой многочлен

$$\varPhi_p(x) = x^{p-1} + x^{p-2} + \dots + x + 1 = (x^p - 1)/(x-1)$$

неприводим в $\mathbb{Z}[x]$. Для этого перепишем его как многочлен от переменной $t = x - 1$:

$$f(t) = \varPhi_p(t+1) = \frac{(t+1)^p - 1}{t} = t^p + \binom{p}{1} t^{p-1} + \dots + \binom{p}{p-1} t\,.$$

При редукции по модулю p от многочлена $f(t)$ остаётся только старший моном $[f(t)]_p = t^n$. Если $f(t) = g(t)h(t)$ в $\mathbb{Z}[t]$, то в силу единственности разложения на простые множители в $\mathbb{F}_p[t]$ оба сомножителя g, h тоже должны редуцироваться в многочлены вида t^k, т. е. все их коэффициенты кроме старшего, должны делиться на p. Но тогда младший коэффициент f, будучи произведением младших коэффициентов g, h, должен делиться на p^2, что не так. Следовательно, f неприводим в $\mathbb{Z}[t]$.

[1] т. е. переводит полином $a_m x^m + a_{m-1}x^{m-1} + \dots + a_1 x + a_0$ с целыми коэффициентами в полином $[a_m]_n x^m + [a_{m-1}]_n x^{m-1} + \dots + [a_1]_n x + [a_0]_n$ с коэффициентами в кольце вычетов $\mathbb{Z}/(n)$

Упражнение 6.16 (критерий Эйзенштейна). Пусть все коэффициенты приведённого многочлена $f \in \mathbb{Z}[x]$ делятся на простое число $p \in \mathbb{N}$, а младший коэффициент, делясь на p, не делится при этом на p^2. Покажите, что f неприводим в $\mathbb{Z}[x]$.

6.6. Гомоморфизмы подъёма и вычисления. Пусть K — коммутативное кольцо, а X — произвольное множество. Множество всех функций $X \longrightarrow K$ обозначается K^X и образует кольцо относительно операций поточечного сложения и умножения значений функций:

$$f + g : x \mapsto f(x) + g(x) \qquad fg : x \mapsto f(x)g(x) \; .$$

Тождественно нулевая функция является в K^X нулём, а тождественно единичная (если в K есть единица) — единицей.

С каждым отображением множеств $X \xrightarrow{\varphi} Y$ связан гомоморфизм *подъёма*[1] вдоль φ

$$\varphi^* \; : \; K^Y \xrightarrow{f \mapsto f \circ \varphi} K^X \; ,$$

который переводит функции на Y в их композиции с φ. На языке некоммутативной алгебры подъём есть не что иное, как правое умножение всех отображений из $\mathrm{Hom}(Y, K)$ на отображение $\varphi \in \mathrm{Hom}(X, Y)$:

$$\mathrm{Hom}(Y, K) \xrightarrow{f \mapsto f\varphi} \mathrm{Hom}(X, K)$$

Отметим, что хотя кольца функций и не являются целостными, гомоморфизм подъёма всегда переводит единицу кольца K^Y в единицу кольца K^X.

Упражнение 6.17. Из каких функций состоит ядро гомоморфизма подъёма?

В геометрии и анализе обычно изучаются множества X и Y, наделённые той или иной дополнительной структурой: мерой, топологией, локальными координатами и т. п. Соответственно и функции на таких множествах рассматриваются не любые, а согласованные с этой структурой: интегрируемые, непрерывные, гладкие и т. п. Эти специальные функции образуют в кольце всех функций подкольцо, которое в алгебре принято обозначать $K[X] \subset K^X$ и называть *структурным кольцом* (или *кольцом регулярных функций*) соответствующей геометрической или аналитической теории.

Отображения между множествами с дополнительной структурой тоже рассматриваются не произвольные, а согласованные со структурой: измеримые, непрерывные, дифференцируемые и т. п. В алгебре такие отображения называются *регулярными*. Как только теория зафиксирована, т. е. в кольце функций каждого рассматриваемого в этой теории множества X выделено подкольцо регулярных функций $K[X]$, так сразу же становится возможным чисто алгебраическое описание регулярных отображений в этой теории.

[1]по-английски *pull back* (по-русски подъёмы тоже иногда называют *обратными образами*

А именно, назовём отображение $X \xrightarrow{\varphi} Y$ *регулярным*, если отвечающий этому отображению гомоморфизм подъёма $K^Y \xrightarrow{\varphi^*} K^X$ переводит регулярные функции на Y в регулярные функции на X, т. е. является гомоморфизмом подколец $K[Y] \xrightarrow{\varphi^*} K[X]$.

Упражнение 6.18. Обозначим через $C \subset \mathbb{R}^{[0,1]}$ подкольцо непрерывных функций на $[0,1]$. Покажите, что

а) отображение $[0,1] \xrightarrow{\varphi} [0,1]$ непрерывно, если и только если $\varphi^*(C) \subset C$;

б) сюрьективность непрерывного отображения $\varphi : [0,1] \longrightarrow [0,1]$ равносильна инъективности гомоморфизма подъёма $\varphi^* : C \longrightarrow C$.

6.6.1. Гомоморфизмы вычисления. В случае, когда $X = \{*\}$ состоит из одной точки, гомоморфизм поднятия, отвечающий её вложению $\{*\} \overset{y}{\hookrightarrow} Y$ в какое-нибудь множество Y в качестве некой точки $y \in Y$, переводит функцию $f \in Y^K$ в число $f(y) \in K^{\{*\}} = K$, и тем самым, представляет собою *гомоморфизм вычисления*[1] значений функций на Y в точке $y \in Y$:

$$\mathrm{ev}_y \;:\; K^Y \xrightarrow{f \mapsto f(y)} K$$

Этот гомоморфизм эпиморфен, а его ядро состоит из всех функций, которые обращающихся в нуль в точке y.

Используя гомоморфизмы вычисления, можно для любого абстрактно заданного кольца с единицей R, содержащего основное кольцо K в качестве подкольца, построить множество $X[R]$, для которого R можно будет естественным образом отождествить с некоторым подкольцом в $K^{X[R]}$ и, тем самым, рассматривать как «кольцо регулярных функций» некоторой «геометрической теории».

А именно, назовём K-*точкой* кольца R любой гомоморфизм

$$R \xrightarrow{p} K\,,$$

тождественно действующий на подкольце $K \subset R$, и возьмём в качестве $X[R]$ множество всех K-точек кольца R. Каждый элемент $f \in R$ может восприниматься как функция на $X[R] \xrightarrow{f} K$, значение которой на K-точке $R \xrightarrow{p} K$, по определению, равно $p(f) \in K$. Подкольцо $K \subset R$ при этом превращается в множество постоянных функций.

Упражнение 6.19. Постройте биекцию между точками отрезка $[0,1]$ и $\mathbb{R}$-точками кольца непрерывных функций $C = \{f : [0,1] \longrightarrow \mathbb{R}\}$.

Тем самым, как только зафиксировано кольцо констант K, например $K = \mathbb{R}$, и выбран некоторый класс колец R, содержащих K в качестве подкольца, так сразу же возникает геометрическая теория, пространствами в которой будут множества $X[R]$, описанные выше, а кольцами регулярных функций на этих

[1] по-английски: *evaluation map*

пространствах будут подкольца $R \subset K^{X[R]}$, вложенные в $K^{X[R]}$ так, как это объяснялось выше. Замечательно, что всякий гомоморфизм колец

$$R_1 \xrightarrow{\varphi} R_2 ,$$

тождественно действующий на кольце констант K, может восприниматься при этом как гомоморфизм подъёма для некоторого отображения пространств, ассоциированных с этими кольцами, а именно, для отображения подъёма

$$\varphi^* : X[R_2] \xrightarrow{p \mapsto p\circ\varphi} X[R_1] ,$$

переводящего K-точку $R_2 \xrightarrow{p} K$ в её подъём $R_1 \xrightarrow{\varphi} R_2 \xrightarrow{p} K$ вдоль гомоморфизма φ.

Упражнение 6.20. Убедитесь, что $(\varphi^*)^* = \varphi$.

В результате между точками и функциями возникает замечательная симметрия, играющая фундаментальную роль во всей математике. Причина её кроется в том, что выражение $f(x)$ в действительности абсолютно симметрично по x и f — можно считать, что f вычисляется на x, а можно считать, что x вычисляется на f — и нет никакого естественного способа сделать этот выбор *a priori*. Точки точно также являются же функциями на пространстве функций, как функции — на пространстве точек.

Если в качестве кольца констант взять некоторое поле $\Bbbk$, а в качестве колец регулярных функций — конечные прямые произведения $\Bbbk^n$ (с произвольными $n \in \mathbb{N}$), то описанный выше механизм сопоставления кольцам пространств выдаст в качестве результата геометрическую теорию, известную как *конечномерная линейная алгебра*, с которой начнём знакомиться в следующем параграфе.

Если взять более сложный класс колец — конечно порождённые алгебры над полем, то мы получим теорию, известную как *аффинная алгебраическая геометрия*, которую мы тоже обсудим на втором курсе.

Задачи для самостоятельного решения к §6

Задача 6.1. Найдите все натуральные числа, делящиеся на 30 и имеющие ровно 30 различных натуральных делителей.

Задача 6.2. Конечно ли фактор кольцо $\mathbb{Z}[x]/(f, g)$, если все общие делители многочленов $f, g \in \mathbb{Z}[x]$ исчерпываются ± 1?

Задача 6.3 (суммы, произведения и пересечения идеалов). Для любых двух идеалов I, J проверьте, что пересечение $I \cap J$,

$$\text{\textit{произведение}} \qquad IJ \overset{\text{def}}{=} \{x_1y_1 + x_2y_2 + \cdots + x_ny_n \mid x_i \in I\,,\ y_i \in J\,,\ n \in \mathbb{N}\} \quad \text{и}$$

$$\text{\textit{сумма}} \quad I + J \overset{\text{def}}{=} \{x + y \mid x \in I\,,\ y \in J\}$$

тоже являются идеалами, причём $IJ \subset I \cap J$. Приведите пример, когда $IJ \neq I \cap J$.

Задача 6.4 (радикал идеала). Пусть K — коммутативное кольцо с единицей. Покажите, что для любого идеала $I \subset K$ его *радикал*

$$\sqrt{I} = \{a \in K \mid \exists\, n \in \mathbb{N} : a^n \in I\}$$

тоже является идеалом и что $\sqrt{IJ} = \sqrt{I \cap J}$ для любых идеалов $I, J \subset K$.

Задача 6.5 (нильрадикал). Множество всех нильпотентных элементов коммутативного кольца K с 1 называется *нильрадикалом* кольца K и обозначается $\mathfrak{n} = \mathfrak{n}(K)$. Убедитесь, что $\mathfrak{n} = \sqrt{(0)}$ является идеалом и докажите, что $\mathfrak{n}(K)$ является пересечением всех простых идеалов кольца K.

Задача 6.6 (взаимно простые идеалы). Два идеала I, J произвольного коммутативного кольца K с единицей называются *взаимно простыми*, если существуют $x \in I$ и $y \in J$, такие что $x + y = 1$ (это условие равносильно тому, что $I + J = K$, см. зад. 6.3). Покажите, что если идеал I взаимно прост с каждым из идеалов $J_1, J_2, \dots, J_n$, то он взаимно прост и с их пересечением.

Задача 6.7 (китайская теорема об остатках). Пусть идеалы $I_1, I_2, \dots, I_n$ попарно взаимно просты. Покажите, что для любого набора из n классов

$$[a_\nu] \in K/I_\nu \qquad (\text{где } \nu = 1,\, 2,\, \dots,\, n)$$

существует элемент $a \in K$, такой что $[a_\nu] = a \,(\mathrm{mod}\ I_\nu)$ одновременно для всех ν, и что любые два элемента a', a'' с этим свойством сравнимы по модулю пересечения всех идеалов I_ν (иными словами, отображение

$$\varphi : K \longrightarrow (K/I_1) \times (K/I_2) \times \cdots \times (K/I_n)\,,$$

переводящее $a \in K$ в набор классов $(a \,(\mathrm{mod}\ I_1),\, a \,(\mathrm{mod}\ I_2),\, \dots,\, a \,(\mathrm{mod}\ I_n))$, является эпиморфизмом колец с ядром $\bigcap\limits_{\nu} I_\nu$)

Задача 6.8. Приводимы ли в $\mathbb{Q}[x]$ многочлены: а) $x^4 - 8x^3 + 12x^2 - 6x + 2$ б) $x^5 - 12x^3 + 36x - 12$

Задача 6.9. Убедитесь, что каждый гомоморфизм колец $K \xrightarrow{\varphi} L$ индуцирует гомоморфизм колец многочленов $K[x] \xrightarrow{\widehat{\varphi}} L[x]$, состоящий в применении φ ко всем коэффициентам. Пусть оба кольца K, L целостные и многочлен $f \in K[x]$ переводится гомоморфизмом $\widehat{\varphi}$ в неприводимый над полем частных Q_L многочлен той же степени, что и f. Покажите, что f неприводим в $K[x]$.

Задача 6.10. В кольце $\mathbb{Z}[x]$ разложите на неприводимые множители или докажите неприводимость многочленов: а) x^4+x+1 б) $x^5+x^4+x^2+x+2$ в) x^6+x^3+1 г) $x^{105}-9$ д) $(x-a_1)(x-a_2)\dots(x-a_n)-1$ (все числа $a_1,\dots,a_n\in\mathbb{Z}$ различны).

Задача 6.11 (максимальные идеалы). Пусть K — произвольное коммутативное кольцо с 1. Собственный[1] идеал $\mathfrak{m}\subset K$ называется *максимальным*, если он не содержится ни в каком строго большем собственном идеале. Докажите, что
а) идеал $\mathfrak{m}\subset K$ максимален, если и только если $K/\mathfrak{m}$ — поле
б) всякий максимальный идеал прост
в) любой собственный идеал содержится в некотором максимальном[2].

Задача 6.12. Перечислите все идеалы в кольце степенных рядов $\Bbbk[[t]]$ над произвольным полем $\Bbbk$. Много ли среди них максимальных?

Задача 6.13. Найдите непростой неприводимый элемент в кольце $\mathbb{Z}[\sqrt{13}]$.

Задача 6.14 (алгебраические элементы). Пусть $\Bbbk$ — любое поле, и $K\supset\Bbbk$ — любое целостное кольцо. Для произвольного элемента $\xi\in K$ рассмотрим *гомоморфизм вычисления* $\mathrm{ev}_\xi:\Bbbk[x]\longrightarrow K$, переводящий многочлен

$$f(x)=a_0x^n+a_1x^{n-1}+\dots+a_{n-1}x+a_n\in\Bbbk[x]$$

в его значение $f(\xi)=a_0\xi^n+a_1\xi^{n-1}+\dots+a_{n-1}\xi+a_n\in K$ на элементе ξ. Убедитесь, что $\mathrm{im}\,(\mathrm{ev}_\xi)$ это наименьшее по включению подкольцо в K, содержащее $\Bbbk$ и ξ, и докажите, что $\mathrm{im}\,(\mathrm{ev}_\xi)$ поле тогда и только тогда, когда $\ker\mathrm{ev}_\xi\neq0$ (такой ξ называется *алгебраическим* над $\Bbbk$, а приведённая образующая f главного идеала $(f)=\ker\mathrm{ev}_\xi$ называется *минимальным многочленом* элемента ξ над $\Bbbk$, ср. с зад. 4.15).

Задача 6.15. Есть ли среди фактор колец кольца $\mathbb{Z}[i]$ поле
а) характеристики 2 б) характеристики 3 ?
в) Если да, то сколько элементов может быть в этом поле?

---

[1] т. е. отличный от нуля и всего кольца

[2] в общем случае для этого потребуется *лемма Цорна* (см. зад. 1.19); в нётеровом кольце можно обойтись без неё

Раздел III
Векторы и матрицы

§7. Векторы

7.1. Векторные пространства. Формальное определение векторного пространства, представленное ниже, аксиоматизирует свойства алгебраических операций над геометрическими векторами — сложение векторов и умножение векторов на числа. Хотя векторные пространства бывают самой разной природы (от расширений полей и пространств функций до пространств решений уравнений и пространств подмножеств) интуитивное представление абстрактных векторов в виде направленных отрезков, которые складываются и умножаются на числа так, как этому учили в школе, является весьма продуктивным.

Определение 7.1
Аддитивная абелева группа V называется *векторным пространством* (а её элементы — *векторами*) над полем $\Bbbk$, если задана операция *умножения векторов на числа*

$$\Bbbk \times V \longrightarrow V \;:\; (\lambda, v) \mapsto \lambda \cdot v = \lambda v\,,$$

которая обладает следующими свойствами:

$$\lambda(\mu v) = (\lambda\mu)v \qquad \forall\,\lambda,\mu \in \Bbbk\,,\ \forall\, v \in V \tag{7-1}$$
$$(\lambda + \mu)v = \lambda v + \mu v \qquad \forall\,\lambda,\mu \in \Bbbk\,,\ \forall\, v \in V \tag{7-2}$$
$$\lambda(v + w) = \lambda v + \lambda w \qquad \forall\, v, w \in V\,,\ \forall\,\lambda \in \Bbbk \tag{7-3}$$
$$1 \cdot v = v \qquad \forall\,\lambda,\mu \in \Bbbk\,,\ \forall\, v \in V \tag{7-4}$$

Групповая операция в векторном пространстве V называется *сложением векторов*. Нейтральный элемент 0 группы V называется *нулевым вектором*, а векторы v и $-v$ — *противоположными* векторами. Подмножество $U \subset V$, являющееся векторным пространством относительно имеющихся в V операций, называется *подпространством* в V.

Упражнение 7.1. Выведите из свойств (7-1)–(7-3), что для всех $v \in V$ и $\lambda \in \Bbbk$ выполняются равенства $0 \cdot v = 0$ и $\lambda \cdot 0 = 0$, а также, что результатом умножения произвольного вектора v на число $-1 \in \Bbbk$ является противоположный к v вектор, т.е. $(-1) \cdot v = -v$.

Замечание 7.1. В зависимости от ситуации, произведение вектора $v \in V$ на число $\lambda \in \Bbbk$ бывает удобно записывать либо как λv, либо как $v\lambda$. По определению, мы считаем обе записи λv и $v\lambda$ равноправными и означающими одно и то же — результат умножения вектора $v \in V$ на число $\lambda \in \Bbbk$ согласно имеющейся на V структуре векторного пространства.

Определение 7.2

Отображение $\varphi : V \longrightarrow W$ между векторными пространствами над полем $\Bbbk$ называется *линейным*, если $\varphi(\lambda_1 v_1 + \lambda_2 v_2) = \lambda_1\varphi(v_1) + \lambda_2\varphi(v_2)$ для любых $\lambda_1, \lambda_2 \in \Bbbk$ и $v_1, v_2 \in V$. Линейные отображения также называют *линейными операторами* или *гомоморфизмами векторных пространств*. Биективные линейные отображения называются *изоморфизмами*.

7.1.1. Пример: поле $\Bbbk$. Простейшим нетривиальным примером векторного пространства является само поле $\Bbbk$. Линейное отображение $\Bbbk \xrightarrow{\varphi} \Bbbk$ однозначно определяется тем, куда оно переводит единицу, поскольку

$$\varphi(x) = \varphi(x \cdot 1) = x \cdot \varphi(1)\,.$$

Таким образом, линейные отображения $\Bbbk \xrightarrow{\varphi} \Bbbk$ — это растяжения $\varphi : x \mapsto ax$ с произвольными $a = \varphi(1) \in \Bbbk$. Подчеркнём, что отображение $x \mapsto ax + b$ с $b \neq 0$ линейным *не* является.

7.1.2. Пример: координатное пространство $\Bbbk^n$ является n-мерным обобщением одномерного пространства $\Bbbk$. А именно, прямое произведение аддитивных абелевых групп

$$\Bbbk^n = \underbrace{\Bbbk \times \Bbbk \times \cdots \times \Bbbk}_{n \text{ раз}}$$

элементами которого являются строки $v = (x_1, x_2, \dots, x_n)$ с $x_i \in \Bbbk$, которые складываются и умножаются на числа покомпонентно:

$$(x_1, x_2, \dots, x_n) + (y_1, y_2, \dots, y_n) = (x_1 + y_1\,,\ x_2 + y_2\,,\ \dots\,,\ x_n + y_n\,)$$
$$\lambda \cdot (x_1, x_2, \dots, x_n) = (\lambda x_1, \lambda x_2, \dots, \lambda x_n)\,,$$

называется *n-мерным координатным пространством* над полем $\Bbbk$.

Упражнение 7.2. Проверьте выполнение в пространстве $\Bbbk^n$ свойств (7-1)–(7-3) (ср. с упр. 3.7 и упр. 3.8)

Векторы $e_1, e_2, \dots, e_n \in \Bbbk^n$, такие что единственная ненулевая координата e_i стоит на i-том месте и равна единице:

$$e_i = (0, \dots, 0, 1, 0, \dots, 0)\,, \tag{7-5}$$

называются *стандартными базисными векторами*. Произвольный вектор

$$v = (x_1, x_2, \dots, x_n) \in \Bbbk^n$$

единственным способом линейно выражается через них

$$v = x_1e_1 + x_2e_2 + \cdots + x_ne_n\,. \tag{7-6}$$

Линейное отображение $F : \Bbbk^n \longrightarrow \Bbbk^m$ между координатными пространствами однозначно определяется тем, куда оно переводит базисные векторы e_i : образ произвольного вектора (7-6) выражается через образы базисных векторов как

$$F(v) = F\left(x_1v_1 + x_2v_2 + \cdots + x_nv_n\right) = x_1F(e_1) + x_2F(e_2) + \cdots + x_nF(e_n)\,.$$

Если записать координаты векторов $F(e_i) \in \Bbbk^m$ в виде столбцов высоты m, то мы получим прямоугольную таблицу размера $m \times n$ (m строк и n столбцов)

$$(f_{ij}) = \begin{pmatrix} f_{11} & f_{12} & \dots & f_{1n} \\ f_{21} & f_{22} & \dots & f_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ f_{m1} & f_{m2} & \dots & f_{mn} \end{pmatrix} \tag{7-7}$$

которая называется *матрицей* оператора F. Обозначая стандартные базисные векторы пространства $\Bbbk^m$ через $\varepsilon_1, \varepsilon_2, \dots, \varepsilon_m$, мы можем описать j-тый столбец матрицы (7-7) как столбец коэффициентов линейного выражения вектора $F(e_j)$ через базисные векторы ε_i :

$$F(e_j) = \varepsilon_1 f_{1j} + \varepsilon_2 f_{2j} + \cdots + \varepsilon_m f_{mj} = \sum_i \varepsilon_i f_{ij}$$

(мы написали числовые множители справа от векторов, чтобы индексы, по которым происходит суммирование, стояли рядом).

Применяя оператор F к произвольному вектору $v = \sum\limits_j e_jx_j \in \Bbbk^n$, мы получим вектор $F(v) \in \Bbbk^m$ со столбцом координат

$$F(v) = \sum_j F(e_j)x_j = \begin{pmatrix} f_{11}x_1 + f_{12}x_2 + \cdots + f_{1n}x_n \\ f_{21}x_1 + f_{22}x_2 + \cdots + f_{2n}x_n \\ f_{31}x_1 + f_{32}x_2 + \cdots + f_{3n}x_n \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ f_{m1}x_1 + f_{m2}x_2 + \cdots + f_{mn}x_n \end{pmatrix} \tag{7-8}$$

7.1.3. Решения системы однородных линейных уравнений. Множество U всех векторов $u = (x_1, x_2, \dots, x_n) \in \Bbbk^n$, удовлетворяющих линейному однородному уравнению

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = 0\,, \tag{7-9}$$

где $a_i \in \Bbbk$ — заданные числа, образует векторное подпространство в координатном пространстве $\Bbbk^n$. Если уравнение (7-9) нетривиально[1], подпространство

[1] т. е. среди коэффициентов a_i есть ненулевые

U решений уравнения (7-9) называется *гиперплоскостью* в $\Bbbk^n$. Пересечение нескольких гиперплоскостей, т. е. множество всех решений системы однородных линейных уравнений

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = 0 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = 0 \\ a_{31}x_1 + a_{32}x_2 + \cdots + a_{3n}x_n = 0 \\ \cdots\cdots\cdots\cdots\cdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = 0 \end{cases} \tag{7-10}$$

также является векторным подпространством в $\Bbbk^n$. Согласно (7-8) его можно иначе описать как *ядро* линейного отображения $A : \Bbbk^n \longrightarrow \Bbbk^m$ с матрицей

$$(a_{ij}) = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}$$

т. е. как множество векторов $v \in \Bbbk^n$, таких что $A(v) = 0$.

7.1.4. Пример: пространство матриц. Матрицы размера $m \times n$ (m строк и n столбцов) образуют векторное пространство относительно операций поэлементного сложения матриц и умножения всех элементов матрицы на число. Это пространство обозначается $\mathrm{Mat}_{m\times n}(\Bbbk)$. Оно изоморфно координатному пространству $\Bbbk^{mn}$ — формальная разница между этими двумя пространствами заключается только в том, что координаты векторов в $\mathrm{Mat}_{m\times n}(\Bbbk)$ организуются не в строки или столбцы, а в прямоугольную таблицу.

Матрицы E_{ij}, имеющие единицу в пересечении i-той строки и j-того столбца и нули во всех остальных местах, называются *стандартными базисными матрицами* или *матричными единицами*. Произвольная матрица $A = (a_{ij})$ единственным образом линейно выражается через матричные единицы как $A = \sum\limits_{ij} a_{ij}E_{ij}$.

7.1.5. Пример: пространство функций. Пусть X — произвольное множество. Функции $X \xrightarrow{f} \Bbbk$ образует векторное пространство относительно поточечного сложения значений и умножения на константы:

$$[f_1 + f_2](x) = f_1(x) + f_2(x), \quad [\lambda f](x) = \lambda \cdot f(x).$$

Если множество X конечно и состоит из n элементов

$$X = \{1, 2, \dots, n\},$$

пространство функций $X \longrightarrow \Bbbk$ изоморфно координатному пространству $\Bbbk^n$: отображение, сопоставляющее функции f набор её значений во всех точках X

$$(f_1, f_2, \dots, f_n) = \big(f(1), f(2), \dots, f(n)\big)$$

линейно и биективно.

Функции, обращающиеся в нуль в заданной точке $x \in X$ составляют в пространстве функций гиперплоскость, задаваемую линейным по f уравнением $f(x) = 0$.

Если взять в качестве $\Bbbk$ поле $\mathbb{F}_2$, состоящее из двух элементов, то возникает биекция между функциями $X \longrightarrow \mathbb{F}_2$ и подмножествами $Z \subset X$, сопоставляющая каждому подмножеству Z его *характеристическую функцию* $\chi_Z : X \longrightarrow \mathbb{F}_2$, равную 1 на Z и 0 на $X \smallsetminus Z$. Эта биекция наделяет множество подмножеств структурой векторного пространства над полем $\mathbb{F}_2$, изоморфного пространству функций $X \longrightarrow \mathbb{F}_2$ (см. зад. 7.10).

7.1.6. Пример: пространство многочленов. Кольцо многочленов $\Bbbk[x]$ с коэффициентами в поле $\Bbbk$ образует векторное пространство над $\Bbbk$ относительно операций сложения многочленов и умножения их на константы.

Многочлены степени не выше n образуют в $\Bbbk[x]$ векторное подпространство, которое мы будем обозначать $\Bbbk[x]_{\leqslant n}$. Это подпространство изоморфно координатному пространству $\Bbbk^{n+1}$: отображение, сопоставляющее многочлену

$$f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$$

набор его коэффициентов $(a_0, a_1, \ldots, a_n)$ линейно и биективно.

Для каждого $\alpha \in \Bbbk$ отображение вычисления $\mathrm{ev}_\alpha : \Bbbk[x] \longrightarrow \Bbbk$, сопоставляющее многочлену $f(x) \in \Bbbk[x]$ его значение $f(\alpha) \in \Bbbk$ в точке $x = \alpha$ линейно. Его ядро состоит из многочленов h, имеющих корень в заданной точке $\alpha \in \Bbbk$. Таким образом, многочлены h с заданным корнем $\alpha \in \Bbbk$ образует в пространстве многочленов гиперплоскость, задаваемую одним линейным уравнением $h(\alpha) = 0$ на многочлен h.

7.2. Базисы. Говорят, что вектор $w \in V$ *линейно выражается*, через векторы $v_1, v_2, \ldots, v_n$, если

$$w = \lambda_1v_1 + \lambda_2v_2 + \cdots + \lambda_nv_n$$

для некоторых $\lambda_i \in \Bbbk$. Выражение, стоящее в правой части этой формулы, называется *линейной комбинацией* векторов $v_i \in V$ с коэффициентами $\lambda_i \in \Bbbk$.

Семейство векторов $\{v_\nu\} \subset V$ (возможно, бесконечное) называется *порождающим* векторное пространство V, если каждый вектор $w \in V$ линейно выражается через *конечный* набор векторов из семейства $\{v_\nu\}$ (этот конечный набор может быть разным для разных $w \in V$).

Порождающий набор векторов $\{v_\nu\} \subset V$ называется *базисом* векторного пространства пространства V, если любой вектор $w \in V$ имеет *единственное* представление в виде линейной комбинации конечного числа базисных векторов, т. е. если из равенства

$$\sum x_ie_i = \sum y_ie_i$$

вытекает, что $x_i = y_i$ для всех i. Коэффициенты x_i единственного линейного выражения $w = \sum x_i v_i$ вектора w через базисные векторы v_ν называются *координатами* вектора w в базисе $\{v_\nu\}$.

Например, стандартные базисные векторы (7-5) образуют базис координатного пространства $\Bbbk^n$, и координатами вектора $v = (x_1, x_2, \dots, x_n) \in \Bbbk^n$ в этом базисе являются числа x_i.

Упражнение 7.3. Пусть векторы $v_1, v_2, \dots, v_n$ составляют базис векторного пространства V. Покажите, что отображение *взятия координат* $V \longrightarrow \Bbbk^n$, сопоставляющее вектору $w = \sum x_i v_i$ строку его координат $(x_1, x_2, \dots, x_n) \in \Bbbk^n$ в базисе $v_1, v_2, \dots, v_n$ является изоморфизмом векторных пространств.

7.2.1. Пример: базис пространства многочленов. Счётный набор мономов $1,\ x,\ x^2, \dots$ является базисом векторного пространства многочленов $\Bbbk[x]$, поскольку каждый многочлен, по определению, представляет собою конечную линейную комбинацию таких мономов, и равенство двух многочленов, по определению, означает равенство их коэффициентов.

По той же причине первые $n+1$ мономов $1,\ x,\ x^2, \dots, x^n$ составляют базис пространства $\Bbbk[x]_{\leqslant n}$ многочленов степени не выше n.

Упражнение 7.4. Покажите, что любой набор многочленов $f_0, f_1, \dots, f_n \in \Bbbk[x]$, в котором $\deg f_m = m$ и каждый $f_m = a_0 x^m + a_1 x^{m-1} + \dots + a_{m-1} x + a_m$ имеет ненулевой старший коэффициент a_0, является базисом векторного пространства $\Bbbk[x]_{\leqslant n}$ многочленов степени не выше n.

Отметим, что в пространстве формальных степенных рядов $\Bbbk[[x]]$ счётный набор мономов $1,\ x,\ x^2, \dots$ базисом *не является*, поскольку ряд с бесконечным числом ненулевых коэффициентов не является *конечной* линейной комбинацией мономов.

Упражнение 7.5. Покажите, что в $\Bbbk[[x]]$ нет счётного базиса.

7.2.2. Пример: базис пространства функций. В пространстве функций на конечном множестве $X = \{1,\ 2, \dots, n\}$ со значениями в поле $\Bbbk$ имеется базис, образованный *δ-функциями* $\{\delta_1, \delta_2, \dots, \delta_n\}$, которые задаются формулами

$$\delta_i(x) = \begin{cases} 1, & \text{при } x = i\,, \\ 0, & \text{при } x \neq i\,. \end{cases}$$

В самом деле, произвольная функция $X \xrightarrow{f} \Bbbk$ имеет единственное линейное выражение через δ-функции — коэффициентами этого являются значения функции f в соответствующих точках множества X

$$f(x) = \sum_{i=1}^{n} f(i) \cdot \delta_i(x)\,. \tag{7-11}$$

Если взять в качестве X какие-нибудь $n+1$ различных точек поля $\Bbbk$

$$X = \{a_0, a_1, \dots, a_n\} \subset \Bbbk\,,$$

каждая δ-функция на нём реализуется многочленом n-той степени

$$f_i(x) = \prod_{\nu \neq i} \frac{x - a_\nu}{a_i - a_\nu} = \frac{(x-a_0)\cdots(x-a_{i-1})(x-a_{i+1})\cdots(x-a_n)}{(a_i-a_0)\cdots(a_i-a_{i-1})(a_i-a_{i+1})\cdots(a_i-a_n)} \,. \tag{7-12}$$

Упражнение 7.6. Покажите, что многочлены (7-12) составляют базис пространства $\Bbbk[x]_{\leqslant n}$ и координатами многочлена $g \in \Bbbk[x]_{\leqslant n}$ в этом базисе являются значения $g(a_i)$.

7.2.3. Линейная зависимость. Векторы $v_1, v_2, \ldots, v_m$ называются *линейно независимыми*, если из равенства $\sum \lambda_i v_i = 0$ вытекает, что все $\lambda_i = 0$. Наоборот, если существует конечная линейная комбинация

$$\lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_m v_m = 0 \,, \tag{7-13}$$

в которой имеются ненулевые коэффициенты λ_i, то векторы $v_1, v_2, \ldots, v_m$ называются *линейно зависимыми*.

Линейная зависимость векторов означает, что любой входящий в неё с ненулевым коэффициентом вектор линейно выражается через остальные. Например, если $\lambda_m \neq 0$, то

$$v_m = -\frac{\lambda_1}{\lambda_m} v_1 - \frac{\lambda_2}{\lambda_m} v_2 - \cdots - \frac{\lambda_{m-1}}{\lambda_m} v_{m-1} \,.$$

Наоборот, любое линейное выражение вида $v_m = \mu_1 v_1 + \mu_2 v_2 + \cdots + \mu_{m-1} v_{m-1}$ можно записать в виде линейной зависимости

$$\mu_1 v_1 + \mu_2 v_2 + \cdots + \mu_{m-1} v_{m-1} - v_m = 0 \,.$$

Лемма 7.1
Набор векторов $\{e_\nu\}$, порождающий векторное пространство V, тогда и только тогда является базисом, когда он линейно независим.

Доказательство. Если $\sum \lambda_i e_i = 0$ и не все λ_i нулевые, то любой вектор $v = \sum x_i e_i$ допускает *другое* выражение $v = \sum (x_i + \lambda_i) e_i$ через векторы e_i. Наоборот, если $v = \sum x_i e_i = \sum y_i e_i$ — два различных представления одного вектора, то перенося правую часть в середину, получаем линейную зависимость $\sum (x_i - y_i) v_i = 0$. □

Лемма 7.2
Если векторы $v_1, v_2, \ldots, v_m$ порождают V, а векторы $e_1, e_2, \ldots, e_k$ линейно независимы, то $m \geqslant k$ и некоторые k из векторов v_i можно заменить на векторы $e_1, e_2, \ldots, e_k$ так, что полученный набор векторов останется порождающим.

Доказательство. Пусть $e_1 = \sum x_i v_i$. Перенумеруем v_i так, чтобы $x_1 \neq 0$. Тогда вектор v_1 линейно выражается через e_1 и $v_2, \ldots, v_m$. Поэтому после замены

v_1 на e_1 набор останется порождающим. Теперь, по индукции, предположим, что $e_1, \dots, e_j, v_{j+1}, \dots, v_m$ порождают V и $j < k$. Поскольку векторы e_i линейно независимы, в разложение e_{j+1} через $e_1, \dots, e_j, v_{j+1}, \dots, v_m$ должен с ненулевым коэффициентом входить хоть один из векторов v_i. Перенумеруем v_i так, чтобы это был v_{j+1}. Тогда v_{j+1} линейно выражается через $e_1, e_2, \dots, e_{j+1}$ и $v_{j+2}, \dots, v_m$, и после его замены на e_{j+1} набор останется порождающим. □

Теорема 7.1 (теорема о базисе)
Любой порождающий набор векторов содержит в себе некоторый базис. Любые два базиса одного пространства равномощны. Любой линейно независимый набор векторов можно дополнить до базиса.

Доказательство. Предположим сначала, что пространство V порождается конечным набором векторов $v_1, v_2, \dots, v_m$. По очереди выкидывая из него те векторы, которые линейно выражаются через остальные, мы в конце концов получим линейно независимый порождающий набор векторов, который по лем. 7.1 является базисом. Второе утверждение следует из лем. 7.2, согласно которой число векторов в любом линейно независимом наборе не больше, чем в любом порождающем, и стало быть, все линейно независимые порождающие наборы состоят из одного и того же числа векторов. Третье утверждение вытекает из того, что добавляя к линейно независимому набору вектор, который не выражается через него линейно, мы снова получаем линейно независимый набор. Согласно лем. 7.2, повторив эту процедуру не более m раз, мы придём к линейно независимому набору, порождающему всё пространство, т. е. получим базис.

Если не предполагать, что пространство V линейно порождается конечным набором векторов, в предыдущем рассуждении следует заменить обычную индукцию трансфинитной. А именно, множество всех линейно независимых наборов векторов в V, частично упорядоченное отношением включения, является *полным*[1] ЧУМ*ом*, т. е. для каждой (в том числе и бесконечной) цепочки линейно независимых наборов векторов, в которой про любые два набора известно, что один из них является подмножеством другого, существует линейно независимый набор векторов, содержащий в себе в качестве подмножеств все наборы из рассматриваемой цепочки.

Упражнение 7.7. Убедитесь, что в качестве такого мажорирующего набора можно взять объединение всех наборов цепочки.

Поэтому, согласно *лемме Цорна*[2], любой линейно независимый набор векторов содержится в некотором *максимальном* линейно независимом наборе $\{e_\nu\}$ — таком, который сам уже не содержится в качестве собственного подмножества ни в каком большем линейно независимом наборе.

Максимальный линейно независимый набор $\{e_\nu\}$ является порождающим, поскольку при добавлении к нему любого вектора v получающийся строго боль-

[1] см. зад. 1.18 на стр. 20

[2] см. зад. 1.19 там же

ший набор должен оказаться линейно зависим, т. е. некоторая конечная линейная комбинация векторов v и e_i обратится в нуль. В силу линейной независимости векторов e_ν вектор v будет входить в эту комбинацию с ненулевым коэффициентом, а значит, будет линейно выражаться через e_i.

Таким образом, любой линейно независимый набор векторов *любого* векторного пространства содержится в некотором базисе.

Если в проделанном только что рассуждении ограничиться рассмотрением линейно независимых наборов векторов, содержащихся в произвольно заданном множестве векторов $\mathscr{G} \subset V$, порождающем пространство V, мы получим базис пространства V, являющийся подмножеством в $\mathscr{G}$.

Доказательство того, что любые два базиса равномощны, требует трансфинитного расширения лем. 7.2.

Упражнение 7.8. Пусть множество векторов $\mathscr{G} \subset V$ порождает V, а множество векторов $\mathscr{E} \subset V$ линейно независимо. Покажите, что в $\mathscr{G}$ имеется равномощное $\mathscr{E}$ подмножество, такое что после замены векторов этого подмножества множеством векторов $\mathscr{E}$ полученный набор векторов останется порождающим.

Из этого упражнения вытекает, любая линейно независимая система векторов равномощна некоторому подмножеству в любой порождающей системы. Отсюда по теореме Кантора – Бернштейна[1] мы заключаем, что любые два базиса равномощны. □

Определение 7.3
Пространство V, обладающее конечным базисом, называется *конечномерным*. Число векторов в базисе называется *размерностью* пространства V и обозначается $\dim V$.

7.2.4. Пример: конечные поля. Любое конечное поле $\mathbb{F}$ является конечномерным векторным пространством над своим простым подполем $\mathbb{F}_p \subset \mathbb{F}$. Если размерность $\mathbb{F}$ как векторного пространства над $\mathbb{F}_p$ равна n, то $\mathbb{F}$ по упр. 7.3 изоморфно (как векторное пространство) координатному пространству $\mathbb{F}_p^n$. В частности, $|\mathbb{F}| = p^n$.

Упражнение 7.9. Может ли поле из 27 элементов содержать подполе из 9 элементов?

7.2.5. Пример: пространство операторов. Линейные операторы

$$U \xrightarrow{F} W$$

между двумя векторными пространствами U и W над полем $\Bbbk$ образуют векторное пространство относительно операций поточечного сложения значений

[1] напомним, что *теорема Кантора – Бернштейна* утверждает, что если множество A инъективно отображается в множество B, а множество B инъективно отображается в множество A, то между множествами A и B существует биекция

и умножения их на числа

$$F + G : v \longmapsto F(v) + G(v) \quad \text{и} \quad \lambda F : v \longmapsto \lambda \cdot F(v)\,.$$

Пространство операторов обозначается через $\mathrm{Hom}(U, W)$.

Если пространства U и W конечномерны, то выбирая в них базисы

$$u_1, u_2, \dots, u_n \in U \quad \text{и} \quad w_1, w_2, \dots, w_m \in W\,,$$

мы, точно также, как в n° 7.1.2, можем сопоставить любому оператору

$$F : U \longrightarrow W$$

матрицу $F_{wu} \subset \mathrm{Mat}_{m\times n}$, в j-том столбце которой будут стоять коэффициенты f_{ij} разложения

$$F(u_j) = \sum_{i=1}^{m} w_i \cdot f_{ij} \in W \tag{7-14}$$

образа базисного вектора $u_j \in U$ по базису $w_1, w_2, \dots, w_m \in W$. Получающаяся таким образом матрица

$$F_{wu} = (f_{ij}) = \begin{pmatrix} f_{11} & f_{12} & \dots & f_{1n} \\ f_{21} & f_{22} & \dots & f_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ f_{m1} & f_{m2} & \dots & f_{mn} \end{pmatrix} \tag{7-15}$$

называется *матрицей оператора* F *в базисах*

$$u = (u_1, u_2, \dots, u_n) \quad \text{и} \quad w = (w_1, w_2, \dots, w_m)\,.$$

Действие оператора на произвольный вектор $v = \sum u_j x_j$ однозначно определяется его матрицей по формуле

$$F(v) = F\Big(\sum_{j=1}^{n} u_j x_j\Big) = \sum_{j=1}^{n} F(u_j) x_j = \sum_{j=1}^{n}\sum_{i=1}^{m} w_i f_{ij} x_j \tag{7-16}$$

Таким образом, сопоставление оператору матрицы устанавливает изоморфизм между пространством линейных операторов $\mathrm{Hom}(U, V)$ и пространством матриц $\mathrm{Mat}_{m\times n}(\Bbbk)$.

Упражнение 7.10. Убедитесь, что сложение операторов и умножение операторов на числа в точности соответствует сложению и умножению на числа их матриц.

Подчеркнём, что этот изоморфизм зависит от выбора базисов u и w.

Предложение 7.1
Для конечномерных векторных пространств U, W

$$\dim \operatorname{Hom}(U,W) = \dim U \cdot \dim W$$

и если $u_1, u_2, \dots, u_n \in U$ и $w_1, w_2, \dots, w_m \in W$ — некоторые базисы, то mn отображений $E_{w_i u_j}$, действующих на базисные векторы пространства U по правилам

$$E_{w_i u_j} : u_k \longmapsto \begin{cases} w_i & \text{при } k = j \\ 0 & \text{при } k \neq j \end{cases}$$

(где $1 \leqslant i \leqslant m$ и $1 \leqslant k, j \leqslant n$), составляют базис пространства $\operatorname{Hom}(U,W)$.

Доказательство. Операторам $E_{w_i u_j}$ отвечают в описанном выше изоморфизме стандартные базисные векторы E_{ij} пространства $\operatorname{Mat}_{m\times n}(\Bbbk) \simeq \Bbbk^{mn}$. □

7.3. Подпространства. Пересечение любого семейства подпространств U_ν произвольного векторного пространства V тоже является подпространством в V. Пересечение всех подпространств, содержащих заданное множество векторов $M \subset V$, называется *линейной оболочкой* множества M и обозначается $\operatorname{span}(M)$. Это наименьшее по включению векторное подпространство в V, содержащее M. Иначе его можно описать как множество всех конечных линейных комбинаций векторов из M. В самом деле, такие линейные комбинации составляют векторное подпространство в V, которое содержатся в любом подпространстве, содержащем M .

Объединение подпространств, как правило, подпространством не является. Например многочлены вида ax^2 и многочлены вида bx образуют два одномерных подпространства в пространстве многочленов, но сумма $x^2 + x$ не лежит в их объединении.

Упражнение 7.11. Покажите, что объединение двух подпространств является подпространством только когда одно из подпространств содержится в другом.

Линейная оболочка объединения подпространств U_ν называется их *суммой* и обозначается $\sum U_\nu$. Сумма подпространств состоит из всевозможных конечных сумм векторов, принадлежащих этим подпространствам:

$$\sum U_\nu = \operatorname{span}\Bigl(\bigcup_\nu U_\nu\Bigr) = \{u_{i_1} + u_{i_2} + \dots + u_{i_s} \mid u_\nu \in U_\nu\}$$

7.3.1. Размерность суммы и пересечения. Из теоремы о базисе вытекает, что базис любого подпространства $U \subset V$ можно дополнить до базиса во всём пространстве, откуда, в частности, следует неравенство $\dim U \leqslant \dim V$.

Предложение 7.2
Для любых двух конечномерных подпространств U_1, U_2 произвольного векторного пространства V $\dim(U_1) + \dim(U_2) = \dim(U_1 \cap U_2) + \dim(U_1 + U_2)$.

Доказательство. Выберем какой-нибудь базис $u_1, u_2, \dots, u_k$ в $U_1 \cap U_2$ и дополним его векторами $v_1, v_2, \dots, v_r$ и $w_1, w_2, \dots, w_s$ до базисов в подпространствах U_1 и U_2 соответственно. Достаточно показать, что векторы

$$u_1, u_2, \dots, u_k,\ v_1, v_2, \dots, v_r,\ w_1, w_2, \dots, w_s$$

образуют базис пространства U_1+U_2. Ясно, что они его порождают. Допустим, что они линейно зависимы. Поскольку каждый из наборов $u_1, \dots, u_k, v_1, \dots, v_r$ и $u_1, \dots, u_k, w_1, \dots, w_s$ в отдельности линейно независим, в линейной зависимости

$$\lambda_1 u_1 + \lambda_2 u_2 + \dots + \lambda_k u_k + \mu_1 v_1 + \mu_2 v_2 + \dots + \mu_r v_r + \eta_1 w_1 + \eta_2 w_2 + \dots + \eta_s w_s = 0$$

присутствуют как векторы v_i, так и векторы w_j. Перенося в одну часть все векторы $u_1, u_2, \dots, u_k,\ v_1, v_2, \dots, v_r$, а в другую — все векторы $w_1, w_2, \dots, w_s$, получаем равенство между вектором из U_1 и вектором из U_2, означающее, что этот вектор лежит в пересечении $U_1 \cap U_2$. Но тогда в его разложении по базисам пространств U_1 и U_2 нет векторов v_i и w_j — противоречие. □

Следствие 7.1
Для любых подпространств U_1, U_2 конечномерного векторного пространства V выполняется неравенство $\dim(U_1 \cap U_2) \geqslant \dim(U_1) + \dim(U_2) - \dim(V)$. В частности, $U_1 \cap U_2 \neq 0$ при $\dim(U_1) + \dim(U_2) > \dim V$.

Доказательство. Это вытекает из неравенства $\dim(U_1 + U_2) \leqslant \dim V$ и предыдущего предл. 7.2. □

7.3.2. Прямые суммы подпространств. Подпространства $U_1, U_2 \subset V$ называются *трансверсальными*, если их пересечение нулевое: $U_1 \cap U_2 = 0$. В этом случае каждый вектор $w \in U_1 + U_2$ имеет *единственное* представление в виде $w = u_1 + u_2$ с $u_1 \in U_1$ и $u_2 \in U_2$, поскольку из равенства $u_1 + u_2 = u_1' + u_2'$ вытекает, что $u_1 - u_1' = u_2 - u_2' \in U_1 \cap U_2 = 0$. Сумма двух трансверсальных подпространств называется *прямой* и обозначается $U_1 \oplus U_2$.

Более общим образом, сумма подпространств $U_1, U_2, \dots, U_n \subset V$ называется *прямой* и обозначается $U_1 \oplus U_2 \oplus \dots \oplus U_n$, если каждый вектор

$$w \in U_1 + U_2 + \dots + U_n$$

имеет единственное представление в виде

$$w = u_1 + u_2 + + \dots + u_n \quad \text{с } u_i \in U_i\,.$$

Например, если векторы $\{e_i\}$ образуют базис пространства V, то V является прямой суммой одномерных подпространств, порождённых векторами e_i.

Упражнение 7.12. Покажите, что для того, чтобы сумма подпространств U_i была прямой, необходимо и достаточно, чтобы каждое из подпространств U_i было трансверсально сумме остальных подпространств.

Иначе можно сказать, что сумма подпространств $U_1, U_2, \ldots, U_m \subset V$ является прямой тогда и только тогда, когда любой набор ненулевых векторов $u_1, u_2, \ldots, u_m$, в котором $u_i \in U_i$, линейно независим.

Трансверсальные подпространства $U, W \subset V$, такие что $U \oplus W = V$, называются *дополнительными.*

7.3.3. Прямые суммы и прямые произведения пространств. Для любого семейства векторных пространств V_ν (индекс ν пробегает произвольное фиксированное множество X) прямое произведение абелевых групп

$$\prod_{\nu \in X} V_\nu \,,$$

элементами которого являются занумерованные индексом ν семейства векторов (v_ν), в которых $v_\nu \in V_\nu \;\; \forall\, \nu \in X$ (см. n° 3.3), имеет естественную структуру векторного пространства с покомпонентными операциями

$$\lambda \cdot (v_\nu) + \mu \cdot (w_\nu) = (\lambda v_\nu + \mu w_\nu) \;.$$

Оно называется *прямым произведением* пространств V_ν.

Подпространство прямого произведения, состоящее из семейств (v_ν), содержащих лишь конечное число ненулевых векторов, называется *прямой суммой* векторных пространств V_ν и обозначается $\bigoplus\limits_\nu V_\nu$. Если набор пространств

$$V_1, V_2, \ldots, V_n$$

конечен, то прямая сумма совпадает с прямым произведением

$$V_1 \oplus V_2 \oplus \cdots \oplus V_n = V_1 \times V_2 \times \cdots \times V_n \,.$$

Упражнение 7.13. Пусть векторное пространство V является прямой суммой своих подпространств $U_1, U_2, \ldots, U_m \subset V$ в смысле n° 7.3.2. Покажите, что V изоморфно прямой сумме пространств U_i, рассматриваемых как абстрактные векторные пространства.

Если набор подпространств бесконечен, прямое произведение строго мощнее прямой суммы. Например, прямая сумма счётного семейства одномерных пространств изоморфна пространству многочленов $\Bbbk[x]$, а прямое произведение счётного семейства одномерных пространств изоморфно пространству степенных рядов $\Bbbk[[x]]$ (см. замечание перед упр. 7.5 на стр. 109).

7.4. Линейные операторы. Поскольку всякое линейное отображение векторных пространств $F : V \longrightarrow W$ является гомоморфизмом абелевых групп, для него выполняются все свойства, отмеченные нами в n° 3.4.

Так, *образ* $\operatorname{im} F = F(V) \subset W$ является подпространством в V, причём $F(0) = 0$ и $F(-v) = -F(v)$ для всех $v \in V$, а *ядро*

$$\ker F = F^{-1}(0) = \{v \in V \mid F(v) = 0\}$$

является подпространством в V, и слой отображения F над каждым вектором $w \in \operatorname{im} F$ представляет собой сдвиг ядра на любой вектор из этого слоя, т. е. если $F(v) = w$, то $F^{-1}(w) = v + \ker F$, поскольку

$$F(v_1) = F(v_2) \iff v_1 - v_2 \in \ker F\,.$$

В частности, линейное отображение инъективно тогда и только тогда, когда его ядро — нулевое. Уточнением этого факта является

Предложение 7.3
Для любого линейного оператора $F : V \longrightarrow W$, действующего из конечномерного векторного пространства V, выполнено равенство

$$\dim \ker F + \dim \operatorname{im} F = \dim V\,. \tag{7-17}$$

Доказательство. Выберем базис $u_1, u_2, \dots, u_k$ в $\ker F$ и дополним его векторами $e_1, e_2, \dots, e_m$ до базиса всего пространства V. Достаточно показать, что векторы $F(e_1)$, $F(e_2)$, ... , $F(e_m)$ составляют базис в $\operatorname{im} F$. Они порождают образ, поскольку для любого $v = \sum y_i u_i + \sum x_j e_j$ имеем

$$F(v) = \sum y_i F(u_i) + \sum x_j F(e_j) = \sum x_j F(e_j)\,.$$

Они линейно независимы, поскольку из равенства $0 = \sum \lambda_i F(e_i) = F(\sum \lambda_i e_i)$ вытекает, что $\sum \lambda_i e_i \in \ker F$ является линейной комбинацией векторов u_i, что возможно только если все $\lambda_i = 0$. □

Следствие 7.2
Следующие свойства линейного оператора $F : V \longrightarrow V$ эквивалентны:
(1) F изоморфизм (2) $\ker F = 0$ (3) $\operatorname{im} F = V$

Доказательство. Свойства (2) и (3) равносильны друг другу по предл. 7.3, а их одновременное выполнение равносильно (1). □

7.4.1. Пример: структурная теория линейных уравнений. Всякая система линейных уравнений

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = b_2 \\ a_{31}x_1 + a_{32}x_2 + \cdots + a_{3n}x_n = b_3 \\ \qquad\cdots\cdots\cdots\cdots\cdots \\ a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nn}x_n = b_n \end{cases} \tag{7-18}$$

констатирует тот факт, что вектор $b \in \Bbbk^m$, столбец координат которого стоит в правой части системы, является образом неизвестного вектора

$$v = (x_1, x_2, \dots, x_n) \in \Bbbk^n$$

под действием линейного оператора $A : \Bbbk^n \longrightarrow \Bbbk^m$, переводящего стандартные базисные векторы координатного пространства $\Bbbk^n$. Таким образом, речь идёт об одном уравнении $F(v) = b$ на вектор v. Качественное устройство решений такого уравнения мы уже много раз описывали: если $b \notin \operatorname{im} A$, то множество решений пусто, а если $b \in \operatorname{im} A$, множество решений является параллельным сдвигом подпространства $\ker A$ на любой вектор v, являющийся решением.

Иначе говоря, разность любых двух решений v и v' является решением однородной системы линейных уравнений, получающейся из (7-18), если положить все $b_i = 0$. Из предл. 7.3 и сл. 7.2 вытекают

Следствие 7.3
Размерность пространства решений системы из m однородных линейных уравнений от n переменных не меньше, чем $n - m$. В частности, любая система однородных линейных уравнений, в которой число переменных строго больше числа уравнений, всегда обладает ненулевым решением.

Следствие 7.4 (альтернатива Фредгольма)
Если в системе (7-18) число уравнений равно числу неизвестных, то либо она имеет единственное решение при любых значениях правых частей, либо система однородных уравнений, возникающих, когда все $b_i = 0$, обладает ненулевым решением.

Доказательство. Это перевод сл. 7.2 на язык линейных уравнений. □

Задачи для самостоятельного решения к §7

Задача 7.1. Покажите, что два векторных пространства изоморфны тогда и только тогда, когда они имеют одинаковую размерность
а) в предположении, что эти пространства конечномерны
б) без этого предположения (равенство размерностей понимается в этом случае как равномощность базисов).

Задача 7.2. Покажите, что свойство набора векторов $B = \{e_1, e_2, \dots, e_n\}$ быть базисом конечномерного векторного пространства V равносильно любому из следующих эквивалентных друг другу свойств: а) B порождает V, и $n = \dim V$
б) B линейно независим, и $n = \dim V$
в) B линейно независим, и это свойство теряется при добавлении к B любого вектора
г) B порождает V, и это свойство теряется при удалении из B любого вектора
д) B линейно независим, и в V нет линейно независимых наборов из большего числа векторов
е) B порождает V, и V нельзя породить меньшим числом векторов.

Задача 7.3. Пусть $u_1, u_2, \dots, u_k$ линейно независимы, а $e_1, e_2, \dots, e_n$ составляют базис. Известно, что если один из векторов e_i заменить вектором u_i с тем же номером, то тоже получится базис (для любого $i = 1,\, 2,\, \dots,\, k$). Верно ли, что тогда все наборы $u_1,\, \dots,\, u_i,\, e_{i+1},\, \dots,\, e_n$ являются базисами?

Задача 7.4. Приведите пример конечномерного пространства W и трёх попарно трансверсальных подпространств $U, V, T \subset W$, таких что

$$\dim U + \dim V + \dim T = \dim W\,, \text{ но } \quad W \neq U \oplus V \oplus T\,.$$

Задача 7.5. Пусть $\dim(U + V) = \dim(U \cap V) + 1$ для некоторых подпространств $U, V \subset V$. Обязательно ли $U + V$ равно одному из подпространств U, V, а $U \cap V$ — другому?

Задача 7.6. Пусть k-мерные подпространства $W_1, W_2, \dots, W_m \subset V$ таковы, что $\dim W_i \cap W_j = k - 1$ для любых $i \neq j$. Покажите, что существует либо $(k-1)$-мерное подпространство $U \subset V$, содержащееся во всех W_i, либо $(k+1)$-мерное подпространство $W \subset V$, содержащее все W_i.

Задача 7.7. Образуют ли многочлены а) $(x-k)^n$ б) $\binom{x}{k}$ (где $0 \leqslant k \leqslant n$) базис в пространстве $\mathbb{Q}[x]_{\leqslant n}$ многочленов степени не выше n с рациональными коэффициентами?

Задача 7.8. Найдите размерность пространства
а) многочленов степени $\leqslant n$ от m переменных
б) однородных многочленов степени d от m переменных
в) однородных симметрических[1] многочленов степени 10 от 4 переменных
г) симметрических многочленов степени $\leqslant 3$ от 4 переменных.

Задача 7.9. Какова размерность пространства многочленов $f \in \mathbb{R}[x]$ степени $\leqslant n$, обращающихся в нуль в точке $(3-2i) \in \mathbb{C}$?

Задача 7.10 (пространство подмножеств). Обозначим через $\mathscr{S}(M)$ множество всех подмножеств данного множества M. Покажите, что $\mathscr{S}(M)$ является векторным пространством над полем $\mathbb{F}_2$ относительно операций $X + Y \overset{\text{def}}{=} (X \cup Y) \smallsetminus (X \cap Y)$, $1 \cdot X \overset{\text{def}}{=} X$, и $0 \cdot X \overset{\text{def}}{=} \varnothing$. Для m-элементного множества M найдите $\dim \mathscr{S}(M)$ и укажите в $\mathscr{S}(M)$ какой-нибудь базис.

Задача 7.11 (конечные пространства). Сколько всего имеется в d-мерном векторном пространстве над конечным полем из q элементов а) векторов
б) упорядоченных наборов из k линейно независимых векторов
в) k-мерных векторных подпространств?

[1]многочлен от m переменных $_1, _2, \dots, _m$ называется *симметрическим*, если он не меняется при любой перестановке номеров переменных; например, многочлен $(x_1-x_2)^2(x_1-x_3)^2(x_2-x_3)^2 \in \Bbbk[x_1,x_2,x_3]$ симметрический, а многочлен $(x_1-x_2)(x_1-x_3)(x_2-x_3)$ — нет

Задача 7.12 (гауссовы биномиальные коэффициенты). Обозначим через $\binom{d}{k}_q$ ответ к зад. 7.11 (в), рассматриваемый как рациональная функция от переменной q, и разрешим переменной q принимать вещественные значения. Найдите

$$\lim_{q\to 1}\binom{d}{k}_q .$$

Задача 7.13. В условиях предл. 7.1 зафиксируем какие-нибудь подпространства

$$U_0\subset U \quad \text{и} \quad W_0\subset W$$

размерностей n_0 и m_0 соответственно. Покажите, что линейные отображения $U\xrightarrow{F} W$ с $\ker F\subset U_0$ и $\operatorname{im} F\subset W_0$ образуют в $\operatorname{Hom}(U,W)$ векторное подпространство, и найдите его размерность.

Задача 7.14. Установите для любых двух линейных операторов $F,G: V\longrightarrow V$ включения а) $\ker(FG)\subset\ker(G)$ б) $\operatorname{im}(FG)\subset\operatorname{im}(F)$ и приведите (конечномерные) примеры операторов, для которых оба эти включения строгие.

Задача 7.15. Докажите для любого линейного оператора F на конечномерном векторном пространстве V импликации:
а) $\ker(F^k)=\ker(F^{k+1})\Rightarrow\ \forall n\in\mathbb{N}\ \ker(F^k)=\ker(F^{k+n})$
б) $\operatorname{im}(F^k)=\operatorname{im}(F^{k+1})\Rightarrow\ \forall n\in\mathbb{N}\ \operatorname{im}(F^k)=\operatorname{im}(F^{k+n})$

Задача 7.16 (собственные векторы). Пусть $F: V\longrightarrow V$ — линейный оператор на произвольном векторном пространстве V. Вектор $v\in V$ называется *собственным вектором* оператора F, если $F(v)=\lambda v$ для некоторого $\lambda\in\Bbbk$ (λ называется в этом случае *собственным значением* или *собственным числом* оператора F на векторе v). Покажите что: а) $V_\lambda\cap V_\mu=0$ при $\lambda\neq\mu$
б) множество всех собственных векторов с данным собственным числом $\lambda\in\Bbbk$

$$V_\lambda=\{v\in V\mid F(v)=\lambda v\}=\ker(F-\lambda\cdot\mathrm{Id}_V)$$

образует векторное подпространство в V (оно называется *собственным подпространством* оператора F с собственным числом λ)
в) всякий набор собственных векторов $v_1,v_2,\dots,v_m$ с попарно разными собственными значениями $\lambda_1,\lambda_2,\dots,\lambda_m$ линейно независим
г) если все векторы пространства V являются собственными для F, то

$$F=\lambda\cdot\mathrm{Id}_V .$$

Задача 7.17. Докажите линейную независимость над $\mathbb{R}$ следующих наборов функций $\mathbb{R}\longrightarrow\mathbb{R}$ а) $1,\ \sin x,\ \cos x,\ \dots,\ \sin nx,\ \cos nx$
б) $1,\ \sin x,\ \sin^2 x,\ \cdots,\ \sin^m x$
в) $e^{\lambda_1 x},\ \dots,\ e^{\lambda_m x}$ г) $x^{\lambda_1},\ \dots,\ x^{\lambda_m}$ ($\lambda_1,\lambda_2,\dots,\lambda_m\in\mathbb{R}$ различны)

Задача 7.18. Являются ли наборы функций а) $x,\ x^2,\ \dots,\ x^{p+1}$ б) $x^p, x^{p^2},\ \cdots,\ x^{p^p}$ линейно независимыми в пространстве функций $\mathbb{F}_p\longrightarrow\mathbb{F}_p$ над полем $\mathbb{F}_p$?

Задача 7.19 (нильпотентные операторы). Линейный оператор $F : V \longrightarrow V$ называется *нильпотентным*, если $F^n = 0$ для некоторого n. Покажите, что каждый нильпотентный оператор F имеет нулевое ядро и не имеет ненулевых собственных значений, а также что $F^{\dim V} = 0$.

Задача 7.20 (инволютивные операторы). Пусть оператор $F : V \longrightarrow V$ на векторном пространстве V таков, что $F^2 = \mathrm{Id}_V$. Положим

$$V_+ = \{v \in V \mid Fv = v\} = \ker(F - \mathrm{Id}_V)$$
$$V_- = \{v \in V \mid Fv = -v\} = \ker(F + \mathrm{Id}_V)$$

Покажите, что а) $V_- = \mathrm{im}\,(F - \mathrm{Id}_V)$ б) $V_+ = \mathrm{im}\,(F + \mathrm{Id}_V)$
в) либо одно из пространств $V_\pm$ нулевое, а второе совпадает со всем V, либо $V = V_+ \oplus V_-$ (иными словами, $V_+ \cap V_- = 0$ и $V_+ + V_- = V$)

Задача 7.21 (проекторы). Пусть нетождественный ненулевой линейный оператор $F : V \longrightarrow V$ таков, что $F^2 = F$. Положим $V_0 = \ker F$ и

$$V_1 = \{v \in V \mid Fv = v\} = \ker(F - \mathrm{Id}_V)\,.$$

Покажите, что $V = V_0 \oplus V_1$ и оператор F проектирует V на V_1 вдоль V_0, т. е. отображает каждый вектор $w = v_0 + v_1 \in V$ в v_1.

Задача 7.22 (полупростые операторы). Линейный оператор $F : V \longrightarrow V$ называется *полупростым*, если в пространстве V имеется базис из собственных векторов оператора F. Пусть полупростой оператор F переводит в себя некоторое подпространство $U \subset V$. Покажите что ограничение $F|_U : U \longrightarrow U$ тоже является полупростым оператором.

Задача 7.23. Покажите, что оператор умножения на t в фактор кольце $\Bbbk[t]/(t^n)$ не полупростой при $n \geqslant 2$.

Задача 7.24. Пусть $\mathrm{char}(\Bbbk) = 0$. Обозначим через $D : \Bbbk[[x]] \longrightarrow \Bbbk[[x]]$ оператор дифференцирования $D : f(x) \longmapsto f'(x)$. Покажите, что для каждого $\lambda \in \Bbbk$ собственное подпространство V_λ оператора D одномерно, и укажите в нём какой-нибудь базисный вектор.

Задача 7.25. В условиях предыдущей задачи найдите все собственные значения и собственные подпространства оператора D^2.

Задача 7.26. Покажите что ограничение оператора дифференцирования D на подпространство многочленов степени $\leqslant n$ не полупростое.

Задача 7.27. Пусть $\Bbbk \subset \mathbb{F}$ — два поля, причём $\mathbb{F}$ конечномерно как векторное пространство над $\Bbbk$. Покажите, что любой элемент поля $\mathbb{F}$ является корнем некоторого многочлена из $\Bbbk[x]$.

Задача 7.28. Пусть в условиях предыдущей задачи $f \in \Bbbk[x]$ неприводим, $\deg f = n$, $\alpha \in \mathbb{F}$ — корень f, и $\Bbbk(\alpha) \subset \mathbb{F}$ — наименьшее по включению подполе, содержащее $\Bbbk$ и α. Найдите $\dim \Bbbk(\alpha)$ как векторного пространства над полем $\Bbbk$.

Задача 7.29. Конечномерно ли $\mathbb{R}$ как векторное пространство над $\mathbb{Q}$?

Задача 7.30. Докажите линейную независимость над $\mathbb{Q}$ следующих наборов вещественных чисел: а) $\sqrt{2}$, $\sqrt{3}$ и $\sqrt{5}$ б*) $\sqrt[n_1]{p_1^{m_1}}$, $\sqrt[n_2]{p_2^{m_2}}$, … , $\sqrt[n_s]{p_s^{m_s}}$ (где $p_i, n_i, m_i \in \mathbb{N}$, p_i различны и просты, и нод$(n_i, m_i) = 1$ при всех i).

Задача 7.31 (минимальный многочлен оператора). Покажите, что для любого линейного оператора $V \xrightarrow{F} V$ на n-мерном векторном пространстве V
а) существует ненулевой многочлен

$$f(x) = a_0x^m + a_1x^{m-1} + \dots + a_{m-1}x + a_m \in \Bbbk[x]\,,$$

такой что $f(F) = a_0F^m + a_1F^{m-1} + \dots + a_{m-1}F + a_m\mathrm{Id}_V = 0$ в $\mathrm{End}(V)$
б) все такие многочлены образуют (вместе с нулевым многочленом) главный идеал в $\Bbbk[x]$ (приведённая образующая этого идеала называется *минимальным многочленом* оператора F и обозначается $\mu_F(x) \in \Bbbk[x]$)
в) минимальный многочлен $\mu_F(x)$ делится в $\Bbbk[x]$ на $\prod(x - \lambda)$, где произведение берётся по всем различным собственным числам (см. зад. 7.16) оператора F.

Задача 7.32. Пусть $\Bbbk$ — поле, $q(x) \in \Bbbk[x]$ — произвольный многочлен, $V = \Bbbk[x]/(q)$.
а) Покажите, что $e_\nu = x^\nu \pmod{q}$ (где $0 \leqslant \nu \leqslant \deg q - 1$) образуют базис V
б) Напишите в этом базисе матрицу оператора умножения $F : V \xrightarrow{[f]\mapsto[xf]} V$ на класс $x \pmod{q}$ и найдите минимальный многочлен оператора F, когда:
в) q неприводим г) $q = p^m$, где p неприводим
д) $q = p_1^{m_1} p_2^{m_2} \cdots p_s^{m_s}$, где p_ν различные неприводимые
е) Пусть $q(x) = (x - \lambda)^n$, где $\lambda \in \Bbbk$. Постройте в V базис, в котором матрица F имеет вид

$$\begin{pmatrix} \lambda & 1 & & & 0 \\ & \lambda & 1 & & \\ & & \lambda & \ddots & \\ & & & \ddots & 1 \\ 0 & & & & \lambda \end{pmatrix}$$

Задача 7.33. Опишите ядра, образы и найдите минимальные многочлены *верхнего* и *нижнего разностных операторов*

$$\Delta : f(x) \mapsto f(x+1) - f(x)$$
$$\nabla : f(x) \mapsto f(x) - f(x-1)$$

на векторном пространстве $\Bbbk[x]_{\leqslant n}$ многочленов степени не выше n, и напишите матрицы этих операторов в базисах а) x^ν (где $0 \leqslant \nu \leqslant n$)
б) $\gamma_k(x) = (x+1)(x+2)\cdots(x+k)/k!$ (где $0 \leqslant \nu \leqslant n$ и $\gamma_0 = 1$)
в) $\gamma_n(x)$, $\gamma_n(x+1)$, … , $\gamma_n(x+n)$.

§8. Двойственность

8.1. Двойственное пространство. Пусть V — векторное пространство над полем $\Bbbk$. Линейные отображения $V \xrightarrow{\varphi} \Bbbk$ называются *линейными функционалами* (или *линейными формами*) на пространстве V. Линейные формы образуют векторное подпространство в пространстве всех функций $V \longrightarrow \Bbbk$. Оно называется *двойственным* (или *сопряжённым*) к пространству V и обозначается

$$V^* = \mathrm{Hom}(V, \Bbbk)\,.$$

Как и всякое линейное отображение, любая линейная форма однозначно определяется своими значениями на векторах произвольного базиса $\{e_\nu\}_{\nu \in X}$ пространства V: для любого набора значений $\alpha_\nu \in \Bbbk$ существует единственная форма $\varphi \in V^*$, такая что $\varphi(e_\nu) = \alpha_\nu$ при всех ν. Значение этой формы на произвольном векторе $v = \sum e_\nu x_\nu$ равно

$$\varphi(v) = \varphi\left(\sum e_\nu x_\nu\right) = \sum \varphi\left(e_\nu\right) x_\nu = \sum \alpha_\nu x_\nu\,.$$

Отметим, что даже если базис бесконечен, в (единственном) разложении любого вектора v по базису имеется лишь конечное число ненулевых коэффициентов x_ν, так что написанное выражение корректно задаёт форму φ. Мы получаем

Предложение 8.1

Фиксация в пространстве V базиса $\mathscr{E} = \{e_\nu\}_{\nu \in X}$ устанавливает изоморфизм пространства V^* с пространством $\Bbbk^{\mathscr{E}}$ всех функций $\mathscr{E} \xrightarrow{\varphi} \Bbbk$ (или, что то же самое, с прямым произведением одномерных пространств $\Bbbk$ в количестве, равном количеству базисных векторов пространства V). Этот изоморфизм переводит $\varphi \in V^*$ в ограничение φ на множество базисных векторов. □

8.1.1. Координатные функционалы. С каждым базисом $\{e_\nu\}$ пространства V связан набор *координатных функционалов* $\{e_\nu^*\} \subset V^*$, которые действуют на базисные векторы пространства V по правилу

$$e_i^* \,:\, e_\nu \longmapsto \begin{cases} 1 & \text{при } \nu = i \\ 0 & \text{при } \nu = i \end{cases} \tag{8-1}$$

Иначе можно сказать, что i-тый координатный функционал e_i^* сопоставляет каждому вектору $v \in V$ его координату вдоль базисного вектора e_i, т. е. коэффициент x_i разложения $v = \sum e_\nu x_\nu$.

Предложение 8.2

Координатные функционалы любого базиса пространства V линейно независимы в V^*.

Доказательство. Пусть $\sum \lambda_j e_j^* = 0$ в V^*, где сумма слева может содержать лишь конечное число ненулевых коэффициентов. Вычисляя обе части на базисном векторе e_i, получаем, что $\lambda_i = 0$ при любом i. □

Замечание 8.1. Если пространство V бесконечномерно, линейная оболочка координатных функционалов любого базиса в V строго меньше всего пространства V^*.

8.1.2. Пример: пространство, двойственное к многочленам. Применительно к пространству многочленов $V = \Bbbk[x]$, изоморфизм из предл. 8.1, построенный по стандартному базису из мономов, отождествляет $\Bbbk[x]^*$ с прямым произведением счётного семейства одномерных подпространств, которое можно в свою очередь отождествить с пространством формальных степенных от другой переменной t, обозначая базисный вектор i-того одномерного подпространства через t^i. Мы получаем изоморфизм $\Bbbk[x]^* \longrightarrow \Bbbk[[t]]$, переводящий функционал $\varphi \in \Bbbk[x]^*$ в производящую функцию для его значений на мономах от x

$$\varphi \longmapsto \sum_{k \geqslant 0} \varphi(x^k)\, t^k \in \Bbbk[[t]]\,. \tag{8-2}$$

Координатные функционалы мономиального базиса x^i переходят при этом в мономы t^i, которые не порождают всего пространства $\Bbbk[t]$. Например, с каждой точкой $a \in \Bbbk$ связан *функционал вычисления*

$$\mathrm{ev}_a : \Bbbk[x] \xrightarrow{f \mapsto f(a)} \Bbbk\,,$$

сопоставляющий многочленам их значения в точке a. Изоморфизм (8-2) переводит его в геометрическую прогрессию $\gamma_a(t) = (1 - at)^{-1}$, которая при $a \neq 0$ не лежит в линейной оболочке мономов t^i.

Упражнение 8.1. Покажите, что при разных $a_1, a_2, \dots, a_m \in \Bbbk$ геометрические прогрессии $\gamma_{a_1}, \gamma_{a_2}, \dots, \gamma_{a_m} \in \Bbbk[[t]]$ линейно независимы (в частности, над $\Bbbk = \mathbb{R}$ мы получаем континуальное линейно независимое семейство форм на $\Bbbk[t]$).

8.1.3. Двойственные базисы и изоморфизм $V \simeq V^{**}$. Если пространство V конечномерно, пространство V^* тоже конечномерно и координатные функционалы e_i^* любого базиса $e = (e_1, e_2, \dots, e_n)$ пространства V образуют базис пространства V^*. В самом деле, каждый функционал $\varphi \in V^*$ единственным образом выражается через них по формуле

$$\varphi = \varphi(e_1)\, e_1^* + \varphi(e_2)\, e_2^* + \cdots + \varphi(e_n)\, e_n^*$$

(чтобы убедиться в этом, достаточно вычислить обе части на базисных векторах $e_i \in V$). Базисы $(e_1, e_2, \dots, e_n) \in V$ и $(e_1^*, e_2^*, \dots, e_n^*) \in V^*$ называются *двойственными*.

В конечномерном мире пространства V и V^* играют совершенно симметричную роль по отношению друг к другу. А именно, каждый вектор $v \in V$ может рассматриваться как *функционал вычисления* на пространстве V^*

$$\mathrm{ev}_v : V^* \xrightarrow{\varphi \mapsto \varphi(v)} \Bbbk$$

переводящий линейные формы в их значения на векторе v. Поскольку число $\varphi(v) \in \Bbbk$ линейно зависит как от v, так и от φ, сопоставление вектору v функционала вычисления ev_v корректно задаёт линейный оператор

$$\mathrm{ev} : V \xrightarrow{v \mapsto \mathrm{ev}_v} V^{**} \tag{8-3}$$

Этот оператор переводит любой базис $e_1, e_2, \dots, e_n \in V$ в двойственный к базису $e_1^*, e_2^*, \dots, e_n^* \in V^*$ базис пространства V^{**} и, тем самым, является изоморфизмом. Нами установлена фундаментальная

Теорема 8.1
Сопоставление вектору $v \in V$ формы вычисления $V^* \xrightarrow{\mathrm{ev}_v} \Bbbk$ канонически отождествляет конечномерное пространство пространство V с V^{**}. □

Эта теорема означает, что каждая форма на пространстве V^* является функционалом вычисления на вполне определённом векторе $v \in V$, а любой базис $\xi_1, \xi_2, \dots, \xi_n$ пространства V^* является набором координатных форм для единственного базиса $e_1, e_2, \dots, e_n \in V$ (двойственного к $\xi_1, \xi_2, \dots, \xi_n$ базиса в $V^{**} = V$).

Упражнение 8.2. Пусть $\dim V = n$ и наборы векторов $v_1, v_2, \dots, v_n \in V$ и форм $\xi_1, \xi_2, \dots, \xi_n \in V^*$ таковы, что $\xi_i(v_i) = 1$ и $\xi_i(v_j) = 0$ при $i = j$. Покажите, что
а) оба они являются базисами
б) любой вектор v выражается через векторы v_i с коэффициентами $\xi_i(v)$.

8.1.4. Пример: формула Тейлора. Пусть $\mathrm{char}(\Bbbk) = 0$. Рассмотрим в пространстве $\Bbbk[x]_{\leqslant n}$ многочленов степени не выше n функционалы

$$\delta_a^{(0)},\ \delta_a^{(1)},\ \dots,\ \delta_a^{(n)},$$

сопоставляющие многочлену f значения его производных в точке $a \in \Bbbk$:

$$f(a),\ f'(a),\ \dots,\ f^{(n)}(a)\,.$$

Многочлены $(x-a)^k/k!$ (где $k = 0,\,1,\,\dots,\,n$) и формы $\delta_a^{(i)}$ удовлетворяют условию упр. 8.2 и, тем самым, являются двойственными друг другу базисами. В частности, произвольный многочлен $g(x)$ степени не выше n обладает разложением $g(x) = g(a)\cdot 1 + g'(a)\cdot(x-a) + g''(a)\cdot(x-a)^2/2 + \cdots + g^{(n)}(a)\cdot(x-a)^n/n!\,.$

Замечание 8.2. Для бесконечномерного пространства V линейный оператор (8-3) задаёт вложение пространства V в пространство V^{**}. Чтобы убедиться в этом, выберем в V какой-нибудь базис $\{e_\nu\}$. Ядро $\ker \mathrm{ev}$ состоит из таких векторов $v = \sum x_\nu e_\nu$ (сумма конечна), что функционал $\sum x_\nu \mathrm{ev}_{e_\nu} \in V^{**}$ зануляется на любой форме $\varphi \in V^*$. Так как значение этого функционала на координатной форме $e_i^* \in V^*$ равно x_i, все $x_i = 0$. Однако вложение (8-3) в бесконечномерном случае неэпиморфно, поскольку мощность пространства V^{**} ещё больше, чем у V^* (уже более мощного, чем V).

Далее до конца этого параграфа мы по умолчанию предполагаем, что все пространства, о которых идёт речь, конечномерны.

8.1.5. Свёртка. Будем называть *свёрткой* (или *спариванием*) между векторными пространствами V и W отображение

$$V \times W \xrightarrow{v,w \mapsto \langle v,w\rangle} \Bbbk \tag{8-4}$$

сопоставляющее каждой паре векторов $v \in V$, $w \in W$ число $\langle v, w\rangle \in \Bbbk$, которое линейно зависит от v при фиксированном w и линейно зависит от w при фиксированном v, т. е. для любых векторов $v_1, v_2 \in V$, $w_1, w_2 \in W$ и любых чисел $\lambda_1, \lambda_2, \mu_1, \mu_2 \in \Bbbk$ выполняется равенство

$$\begin{aligned}\langle \lambda_1 v_1 + \lambda_2 v_2, \mu_1 w_1 + \mu_2 w_2\rangle &= \\ &= \lambda_1\mu_1\langle v_1, w_1\rangle + \lambda_1\mu_2\langle v_1, w_2\rangle + \lambda_2\mu_1\langle v_2, w_1\rangle + \lambda_2\mu_2\langle v_2, w_2\rangle\,.\end{aligned}$$

Спаривание называется *невырожденным*, если оно удовлетворяет условиям следующей леммы:

Лемма 8.1
Следующие свойства свёртки (8-4) равносильны друг другу:

1) для каждого ненулевого $v \in V$ найдётся $w \in W$, а для каждого ненулевого $w \in W$ найдётся $v \in V$, такие что $\langle v, w\rangle \neq 0$.
2) отображение $V \longrightarrow W^*$, сопоставляющее вектору v линейную форму $w \mapsto \langle v, w\rangle$ на W, является изоморфизмом
3) отображение $W \longrightarrow V^*$, сопоставляющее вектору w линейную форму $v \mapsto \langle v, w\rangle$ на V, является изоморфизмом

Доказательство. В силу линейности $\langle v, w\rangle$ по v и по w, оба отображения, о которых идёт речь в (2) и (3), корректно определены и линейны. Условие (1) утверждает, что оба они инъективны. Поэтому из (1) вытекают неравенства $\dim V \leqslant \dim W^*$ и $\dim W \leqslant \dim V^*$. Так как $\dim V = \dim V^*$ и $\dim W = \dim W^*$, оба эти неравенства являются равенствами, а вложения (2) и (3) — изоморфизмы. Таким образом, из (1) вытекают (2) и (3). Наоборот, если выполняется одно из условий (2) или (3), то автоматически выполняется и второе[1], а значит, и условие (1). $\square$

[1]это переформулировка канонического отождествления $W \simeq W^{**}$: если V изоморфно W^*, то и W изоморфно $V^* = W^{**}$

8.1.6. Пример: спаривание между $\Bbbk[D]/\left((D)^{n+1}\right)$ и $\Bbbk[x]_{\leqslant n}$. Обозначим через $D = d/dx$ оператор дифференцирования $D : f \mapsto Df = f'$ на пространстве $\Bbbk[x]_{\leqslant n}$ многочленов степени не выше n. Для любого ряда

$$g(t) = a_0 + a_1 t + a_2 t^2 + \cdots \in \Bbbk[[t]]$$

обозначим через $g(D) = \sum\limits_{k\geqslant 0} a_k D^k \in \operatorname{End}(\Bbbk[x]_{\leqslant n})$ линейный оператор, переводящий многочлен $f \in \Bbbk[x]$ в многочлен

$$g(D)f = a_0 f + a_1 Df + a_2 D^2 f + \cdots + a_{\deg f} D^{\deg f} f$$

Упражнение 8.3. Покажите, что операторы вида $g(D) \in \operatorname{End}(\Bbbk[x]_{\leqslant n})$ образуют коммутативное кольцо, изоморфное кольцу вычетов $\Bbbk[D]/\left(D^{n+1}\right)$.

Будем называть фактор кольцо $\Bbbk[D]/\left(D^{n+1}\right)$ кольцом *обрезанных дифференциальных операторов*. Зададим между пространствами $\Bbbk[D]/\left(D^{n+1}\right)$ и $\Bbbk[x]_{\leqslant n}$ спаривание правилом

$$\langle g(D), f(x)\rangle = g(D)f(0) \tag{8-5}$$

(применяем к f дифференциальный оператор $g(D)$ и вычисляем значение получившегося многочлена $g(D)f$ в нуле). Это спаривание удовлетворяет условию (1) из лем. 8.1. В самом деле, если младший член $g(D)$ имеет вид $a_k D^k$, где $k \leqslant n$ и $a_k \neq 0$, то $\langle g, x^k\rangle = a_k k! \neq 0$. Аналогично, если старший член f имеет вид $b_m D^m$, где $m \leqslant n$ и $a_m \neq 0$, то $\langle D^m, f\rangle = a_m m! \neq 0$.

Таким образом, пространства $\Bbbk[D]/\left(D^{n+1}\right)$ и $\Bbbk[x]_{\leqslant n}$ двойственны друг другу посредством свёртки (8-5).

Упражнение 8.4. Убедитесь, что двойственный к базису их мономов x^k базис пространства $\Bbbk[D]/\left(D^{n+1}\right)$ состоит из классов $D^k/k! \pmod{D^{n+1}}$.

8.2. Аннуляторы.

8.2. Аннуляторы. Чтобы подчеркнуть симметрию между пространствами V и V^* мы иногда будем называть элементы пространства V^* *ковекторами* и использовать вместо $\varphi(v)$ более симметричное обозначение

$$\langle \varphi, v\rangle \overset{\text{def}}{=} \varphi(v)\,,$$

как в n° 8.1.5. Если выбрать в пространствах V и V^* двойственные базисы

$$(e_1, e_2, \dots, e_n) \in V \quad \text{и} \quad (e_1^*, e_2^*, \dots, e_n^*) \in V^*$$

то результатом свёртки ковектора $\varphi = a_1 e_1^* + a_2 e_2^* + \cdots + a_n e_n^* \in V^*$ с вектором $v = e_1 x_1 + e_2 x_2 + \cdots + e_n x_n \in V$ будет число

$$\left\langle \sum_j a_j e_j^*, \sum_i x_i e_i \right\rangle = \sum_{ij} a_i \langle e_i^*, e_j\rangle x_j = a_1 x_1 + a_2 x_2 + \cdots + a_n x_n \in \Bbbk\,.$$

Таким образом, любое однородное линейное уравнение

$$a_1 x_1 + a_2 x_2 + \cdots + a_n x_n = 0$$

на переменные $(x_1, x_2, \dots, x_n)$ есть не что иное, как привязанная к некоторому конкретному выбору двойственных базисов координатная запись соотношения

$$\langle \varphi, v \rangle = 0\,,$$

о котором при заданном $\varphi \in V^*$ можно думать как о линейном уравнении на вектор $v \in V$, а при заданном $v \in V$ — как о линейном уравнении на ковектор $\varphi \in V^*$. Иными словами, V^* можно воспринимать как пространство однородных линейных уравнений на векторы из V, а V — двойственным образом — как пространство однородных линейных уравнений на ковекторы из V^*.

Определение 8.1
Для произвольных подмножеств $M \subset V^*$ и $N \subset M$ подпространства

$$\begin{aligned}\operatorname{Ann}(M) &= \{v \in V \mid \langle \varphi, v \rangle = 0 \ \forall \varphi \in M\ \} \subset V\\ \operatorname{Ann}(N) &= \{\varphi \in V \mid \langle \varphi, v \rangle = 0 \ \forall v \in N\ \} \subset V^*\end{aligned}$$

называются *аннуляторами* множеств M и N.

Упражнение 8.5. Убедитесь, что аннулятор любого множества (ко) векторов всегда является векторным подпространством двойственного пространства.

Если воспринимать множество M как систему однородных линейных уравнений на V, то $\operatorname{Ann}(M)$ — это пространство всех решений этой системы. С другой стороны, если смотреть на V как на пространство линейных уравнений на V^*, то $\operatorname{Ann}(M)$ — это совокупность всех однородных линейных уравнений, для которых все векторы из множества M являются решениями. Дословно такие же две интерпретации имеются и у аннулятора $\operatorname{Ann}(N)$.

Упражнение 8.6. Покажите, что аннулятор множества совпадает с аннулятором его линейной оболочки: $\operatorname{Ann}(M) = \operatorname{Ann}(\operatorname{span}(M))$.

Предложение 8.3
Для любого подпространства $U \subset V \quad \dim U + \dim \operatorname{Ann} U = \dim V$.

Доказательство. Выберем базис $u_1, u_2, \dots, u_k \in U$ и дополним его векторами $w_1, w_2, \dots, w_m$ до базиса в V (таким образом, $\dim V = k + m$). Обозначим через

$$u_1^*, u_2^*, \dots, u_k^*,\ w_1^*, w_2^*, \dots, w_m^* \in V^*$$

двойственный базис. Тогда $w_1^*, w_2^*, \dots, w_m^* \in \operatorname{Ann} U$, поскольку для любого

$$v = \sum x_i u_i \in U$$

свёртка $\langle w_\nu^*, v \rangle = \langle w_\nu^*, \sum x_i u_i \rangle = \sum x_i \langle w_\nu^*, u_i \rangle = 0$. Если ковектор

$$\varphi = \sum y_i u_i^* + \sum z_j w_j^* \in \operatorname{Ann}(U)\,,$$

то все его координаты $y_i = \langle \varphi, u_i \rangle = 0$. Поэтому $w_1^*, w_2^*, \dots, w_m^*$ линейно порождают $\operatorname{Ann}(U)$. Так как они линейно независимы, они составляют в $\operatorname{Ann}(U)$ базис. Тем самым, $\dim \operatorname{Ann}(U) = m = \dim V - \dim U$. $\square$

Следствие 8.1
Для любого подпространства $U \subset V$ $\quad \operatorname{Ann}\operatorname{Ann}(U) = U$.

Доказательство. $U \subset \operatorname{Ann}\operatorname{Ann}(U)$ и по предл. 8.3 $\dim \operatorname{Ann}\operatorname{Ann} U = \dim U$. □

Теорема 8.2
Соответствие $U \longleftrightarrow \operatorname{Ann}(U)$ устанавливает биекцию между подпространствами двойственных пространств V и V^*. Эта биекция оборачивает включения (т. е. $U \subset W \Leftrightarrow \operatorname{Ann} U \supset \operatorname{Ann} W$) и переводит суммы подпространств в пересечения, а пересечения — в суммы.

Доказательство. Обозначим через $\mathscr{S}(V)$ множество всех подпространств векторного пространства V. Равенство $\operatorname{Ann}\operatorname{Ann}(U) = U$ означает, что два отображения, сопоставление подпространству его аннулятор в двойственном пространстве:

$$\mathscr{S}(V) \underset{\operatorname{Ann} W \leftarrow W}{\overset{U \to \operatorname{Ann} U}{\rightleftarrows}} \mathscr{S}(V^*)$$

обратны друг другу, и следовательно, биективны. Далее, очевидно, что

$$U \subset W \quad \Rightarrow \quad \operatorname{Ann} U \supset \operatorname{Ann} W\,.$$

В силу равенств $U = \operatorname{Ann}\operatorname{Ann} U$ и $W = \operatorname{Ann}\operatorname{Ann} W$, обратная импликация вытекает из доказанной импликации, применённой к пространствам $\operatorname{Ann} U$ и $\operatorname{Ann} W$ в роли U и W. Наконец, равенство $\bigcap\limits_\nu \operatorname{Ann}(U_\nu) = \operatorname{Ann}\left(\sum\limits_\nu U_\nu\right)$ вытекает из того, что любая линейная форма, зануляющаяся на каждом из подпространств U_ν, зануляется и на их линейной оболочке, а форма, зануляющаяся на сумме подпространств, зануляется и на каждом из них в отдельности. Беря в этом равенстве аннуляторы обеих частей и записывая U_ν как $\operatorname{Ann} W_\nu$, получаем равенство $\operatorname{Ann}\left(\bigcap\limits_\nu W_\nu\right) = \sum\limits_\nu \operatorname{Ann}(W_\nu)\,.$ □

8.3. Двойственные операторы. Как мы видели в n° 6.6, с каждым отображением $F : U \longrightarrow W$ связан *гомоморфизм подъёма* функций $W \xrightarrow{\varphi} \Bbbk$ до функций $U \xrightarrow{\varphi\circ F} \Bbbk$. В силу того, что композиция линейных отображений является линейным отображением, линейные формы $\varphi \in W^*$ поднимаются вдоль линейного отображения F до линейных форм $\varphi\circ F \in V^*$, а так как $\varphi\circ F$ линейно зависит от φ, отображение $F^* : W^* \longrightarrow V^*$, переводящее φ в $\varphi\circ F$, является линейным оператором из W^* в U^*. Он называется *двойственным* (или *сопряжённым* к оператору F.

Поскольку $\varphi\circ F$ линейно зависит также и от F, *сопряжение операторов*

$$\operatorname{Hom}(U, V) \xrightarrow{F \mapsto F^*} \operatorname{Hom}(W^*, U^*) \tag{8-6}$$

само по себе является линейным оператором.

Согласно определению, действие F на векторы $u \in U$ и действие F^* на ковекторы $\xi \in W^*$ однозначно определяются друг другом по формуле

$$\langle F^*\xi, v\rangle = \langle \xi, Fv\rangle \quad \forall\, \xi \in W^*,\, v \in V\,. \tag{8-7}$$

Поэтому каноническое отождествление V^{**} с V задаёт каноническое отождествление F^{**} с F. Таким образом, сопряжения $F \mapsto F^*$ и $F^* \mapsto F^{**} = F$ обратны друг другу, т. е. оператор сопряжения (8-6) является изоморфизмом.

Упражнение 8.7. Докажите, что $\Big(F \circ G\Big)^* = G^* \circ F^*$.

Предложение 8.4
Имеют место равенства $\ker F^* = \operatorname{Ann}\operatorname{im} F$ и $\operatorname{im} F^* = \operatorname{Ann}\,\ker F$.

Доказательство. Первое равенство очевидно из формулы (8-7):

$$\xi \in \operatorname{Ann}\operatorname{im} F \iff \langle \xi, Fv\rangle = 0\ \forall\, v{\in}V \iff \langle F^*\xi, v\rangle = 0\ \forall\, v{\in}V \iff F^*\xi = 0\,.$$

Второе получается взятием аннуляторов от обеих частей первого равенства, написанного для оператора F^*. □

Следствие 8.2
Инъективность F равносильна сюрьективности F^*. Двойственным образом, сюрьективность F равносильна инъективности F^*.

8.3.1. Пример: оператор, двойственный дифференцированию. В обозначениях примера из n° 8.1.6 на стр. 127 рассмотрим линейный оператор

$$D^* : \Bbbk[D]/\left(D^{n+1}\right) \longrightarrow \Bbbk[D]/\left(D^{n+1}\right)$$

на пространстве обрезанных дифференциальных операторов, двойственный к оператору дифференцирования

$$D : \Bbbk[x]_{\leqslant n} \xrightarrow{f \mapsto f'} \Bbbk[x]_{\leqslant n}$$

на пространстве $\Bbbk[x]_{\leqslant n}$ многочленов степени не выше n относительно невырожденного спаривания между этими пространствами, заданного формулой

$$\langle g(D), f(x)\rangle = g(D)f(0)\,.$$

В силу равенства $\langle D^{k+1}, f\rangle = D^{k+1}f(0) = \langle D^k, Df\rangle$ оператор D^* действует на базис D^k пространства $\Bbbk[D]/\left(D^{n+1}\right)$ по правилу $D^*(D^k) = D^{k+1}$. Следовательно, D^* является оператором умножения на D в фактор кольце $\Bbbk[D]/\left(D^{n+1}\right)$.

Ядро $\ker D^*$ представляет собою одномерное пространство операторов, пропорциональных D^n и является аннулятором образа оператора дифференцирования $\Bbbk[x]_{\leqslant n} \xrightarrow{D} \Bbbk[x]_{\leqslant n}$, представляющего собою подпространство многочленов степени $\leqslant (n-1)$. Аналогично, ядро оператора дифференцирования на

$\Bbbk[x]_{\leqslant n} \xrightarrow{D} \Bbbk[x]_{\leqslant n}$, состоящее из констант, является аннулятором образа умножения на D в $\Bbbk[D]/\left(D^{n+1}\right)$.

Упражнение 8.8. Опишите операторы ∇^* и Δ^* на пространстве $\Bbbk[D]/\left(D^{n+1}\right)$, двойственные разностным операторам

$$\nabla : f(x) \mapsto f(x) - f(x-1) \quad \text{и} \quad \Delta : f(x) \mapsto f(x+1) - f(x)$$

на пространстве $\Bbbk[x]_{\leqslant n}$.

8.3.2. Матрица двойственного оператора. Выберем в U и U^* двойственные базисы $\{u_j\}$ и $\{u_j^*\}$, а в W и W^* — двойственные базисы $\{w_i\}$ и $\{w_i^*\}$, и сопоставим оператору $F : U \longrightarrow W$ его матрицу $F_{wu} = (f_{ij})$ в базисах u и w. Напомним[1], что в j-том столбце матрицы F_{wu} стоят координаты f_{ij} (где $1 \leqslant i \leqslant m$) образа j-того базисного вектора u_j в базисе w, т. е. коэффициенты разложения $F(u_j) = f_{1j}w_1 + f_{2j}w_2 + \dots + f_{mj}w_m$, или свёртки

$$f_{ij} = \langle w_i^*, Fu_j \rangle = \langle F^* w_i^*, u_j \rangle .$$

Эта же свёртка является одновременно j-той координатой ковектора $F^*(w_i)$ в базисе u^*, т. е. (j,i)-тым элементом f_{ji}^* матрицы $F_{u^*w^*}^* = \left(f_{ij}^*\right)$ двойственного оператора F^* в двойственных базисах. Иначе говоря, i-тая строка матрицы F_{wu} является i-тым столбцом матрицы $F_{u^*w^*}^*$, а j-тый столбец матрицы F_{wu} является i-той строкой матрицы $F_{u^*w^*}^*$.

Матрица A^t по строкам которой записаны сверху вниз прочитанные слева направо столбцы[2] матрицы A называется *транспонированной* к матрице A. Если $A = (a_{ij}) \in \mathrm{Mat}_{m\times n}(\Bbbk)$, то $A^t = \left(a_{ij}^t\right) \in \mathrm{Mat}_{m\times n}(\Bbbk)$ и $a_{ij}^t = a_{ji}$.

Итак, матрицы двойственных операторов в двойственных базисах получаются друг из друга транспонированием: $F_{u^*w^*}^* = F_{wu}^t$.

Следствие 8.3 (теорема о ранге матрицы)
У любой матрицы $A \in \mathrm{Mat}_{m\times n}(\Bbbk)$ размерность линейной оболочки её строк в $\Bbbk^n$ и размерность линейной оболочки её столбцов в $\Bbbk^m$ равны друг другу. Это число называется *рангом* матрицы A и обозначается $\mathrm{rk}\, A$.

Доказательство. Обозначим через $F : \Bbbk^n \longrightarrow \Bbbk^m$ линейный оператор, матрица которого в стандартных базисах этих двух координатных пространств равна A. Тогда размерность линейной оболочки столбцов матрицы A равна $\dim \mathrm{im}\, F$, а размерность линейной оболочки строк матрицы A равна $\dim \mathrm{im}\, F^*$, где $F^* : \Bbbk^{m*} \longrightarrow \Bbbk^{n*}$ — двойственный к F оператор. По (предл. 8.4) и предл. 7.3

$$\dim \mathrm{im}\, F^* = \dim \mathrm{Ann}\, \ker F = n - \dim \ker F = \dim \mathrm{im}\, F .$$

$\square$

[1] ср. с формулой (7-15) на стр. 113

[2] по-другому можно сказать, что матрица A^t получается из матрицы A отражением относительно биссектрисы левого верхнего угла — прямой $i = j$

Следствие 8.4 (теорема Кронекера – Капелли)
Система (неоднородных) линейных уравнений

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = b_2 \\ a_{31}x_1 + a_{32}x_2 + \cdots + a_{3n}x_n = b_3 \\ \cdots\cdots\cdots\cdots\cdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = b_m \end{cases}$$

имеет решение тогда и только тогда, когда

$$\operatorname{rk}\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} = \operatorname{rk}\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} & b_1 \\ a_{21} & a_{22} & \dots & a_{2n} & b_2 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} & b_m \end{pmatrix}$$

Доказательство. Наличие у системы решения означает, что столбец правых частей b лежит в линейной оболочке столбцов матрицы $A = (a_{ij})$. Это равносильно тому, что при добавлении к матрице A столбца b размерность линейной оболочки столбцов не меняется. $\square$

Следствие 8.5
Размерность пространства решений системы однородных линейных уравнений на n переменных с матрицей коэффициентов A равна $n - \operatorname{rk} A$.

Доказательство. $\dim\ker = n - \dim\operatorname{im} A = n - \operatorname{rk} A$. $\square$

8.4. Фактор пространства. Со всяким подпространством $U \subset V$ связано разбиение пространства V на *смежные классы* подпространства U

$$[v]_U = v \,(\mathrm{mod}\, U) = v + U = \{w \in V \mid w - v \in U\}$$

которые представляют собой классы эквивалентности по отношению $v \sim w$, означающему, что $w - v \in U$. Сложение классов и их умножение на числа определяются обычными формулами

$$[v] + [w] = [v + w]$$
$$\lambda[v] = [\lambda v]$$

Упражнение 8.9. Проверьте, что эти операции корректно определены и задают на множестве классов структуру векторного пространства над полем $\Bbbk$.

Пространство смежных классов подпространства U обозначается V/U и называется *фактор пространством* пространства V по подпространству U. Отображение факторизации $V \longrightarrow V/U$, переводящее каждый вектор $v \in V$ в его класс $v \,(\mathrm{mod}\, U)$, линейно и сюрьективно.

Замечание 8.3. Иначе смежный класс вектора $v \in V$ по подпространству $U \subset V$ можно воспринимать как параллельный сдвиг $v+U$ подпространства U на вектор v. В таком контексте он называется *аффинным*[1] подпространством, параллельным U и проходящим через v. Размерность $\dim U$ называется размерностью аффинного подпространства $v+U$.

8.4.1. Пример: фактор по ядру. Для любого линейного оператора

$$F : V \longrightarrow W$$

имеется канонический изоморфизм $V/\ker F \simeq \operatorname{im} F$, сопоставляющий классу $[v] \in V/\ker F$ вектор $F(v) \in \operatorname{im} F$. Это переформулировка того, что

$$F(v) = F(w) \iff v - w \in \ker F$$

Следствие 8.6

Если векторы $v_1, v_2, \dots, v_k$ дополняют некоторый базис $u_1, u_2, \dots, u_m$ подпространства $U \subset V$ до базиса во всём пространстве V, то их классы

$$[v_1],\ [v_2],\ \dots\ ,\ [v_k]$$

образуют базис фактор пространства V/U. В частности,

$$\dim U + \dim V/U = \dim V\,.$$

Доказательство. Это частный случай предл. 7.3 (и его доказательства), относящийся к отображению факторизации $V \twoheadrightarrow V/U$. □

Следствие 8.7

Для любого подпространства $U \subset V$ имеются канонические изоморфизмы

$$(V/U)^* \simeq \operatorname{Ann}(U) \quad \text{и} \quad U^* \simeq V^*/\operatorname{Ann}(U)\,.$$

Доказательство. Если форма $\varphi \in \operatorname{Ann} U$, то для любых $u \in U$ и $v \in V$ выполняются равенства $\varphi(v+u) = \varphi(v) + \varphi(u) = \varphi(v)$. Поэтому правило $\widetilde{\varphi}([v]) = \varphi(v)$ корректно задаёт линейную форму $\widetilde{\varphi}$ на факторе V/U. Отображение

$$\operatorname{Ann}(U) \xrightarrow{\varphi \mapsto \widetilde{\varphi}} (V/U)^*$$

линейно и имеет нулевое ядро. Так как размерности пространств одинаковы, это изоморфизм. Для доказательства второго изоморфизма рассмотрим оператор $V^* \longrightarrow U^*$, переводящий линейную форму на V в её ограничение на $U \subset V$. Поскольку ядро этого гомоморфизма — это $\operatorname{Ann} U$, его образ изоморфен $V^*/\operatorname{Ann}(U) \subset U^*$. Так как размерности обоих пространств одинаковы, вложение является равенством. □

[1]подробнее об аффинных пространствах речь пойдёт в n° 14.6

8.4.2. Пример: линейная оболочка как фактор. Пусть даны векторы

$$w_1, w_2, \dots, w_n \in \Bbbk^m = V\,.$$

Их линейная оболочка $W = \operatorname{span}(w_1, w_2, \dots, w_n) \subset \Bbbk^m$ является образом линейного оператора $F : \Bbbk^n \longrightarrow \Bbbk^m$, переводящего стандартный базисный вектор $e_i \in \Bbbk^n$ в вектор $w_i \in W$. Ядро этого оператора $U = \ker F \subset \Bbbk^n$ представляет собою *пространство линейных соотношений* между векторами w_i в $\Bbbk^m$ в том смысле, что вектор $u = (\lambda_1, \lambda_2, \dots, \lambda_n) = \lambda_1 e_1 + \lambda_2 e_2 + \cdots + \lambda_n e_n \in \Bbbk^n$ лежит в U тогда и только тогда, когда $\lambda_1 w_1 + \lambda_2 w_2 + \cdots + \lambda_n w_n = 0$ в W.

Изоморфизм $W = \operatorname{im} F \simeq \Bbbk^n/U$ означает в этом случае, что векторы $w \in W$ есть классы эквивалентностей линейных комбинаций $x_1w_1+x_2w_2+\cdots+x_nw_n$ по модулю тех комбинаций, которые являются линейными зависимостями между векторами w_i.

В следующем разделе мы покажем, что в пространстве W всегда можно выбрать базис, состоящий из классов $F(e_j) = e_j \pmod U$ некоторых *стандартных* базисных векторов e_j координатного пространства $\Bbbk^n$.

Говоря точнее, мы укажем алгоритм, разбивающий стандартные базисные векторы $e_1, e_2, \dots, e_n$ координатного пространства $\Bbbk^n$ на две группы

$$\{e_1, e_2, \dots, e_n\} = \{e_{i_1}, e_{i_2}, \dots, e_{i_r}\} \sqcup \{e_{j_1}, e_{j_2}, \dots, e_{j_{n-r}}\} \tag{8-8}$$

так, что дополнительные друг другу координатные подпространства

$$E_I = \operatorname{span}(e_{i_1}, e_{i_2}, \dots, e_{i_r}) \simeq \Bbbk^r \quad \text{и} \quad E_J = \operatorname{span}(e_{j_1}, e_{j_2}, \dots, e_{j_{n-r}}) \simeq \Bbbk^{n-r},$$

натянутые на векторы этого разбиения, удовлетворяют такой лемме:

Лемма 8.2
Следующие условия на r-мерное подпространство $U \subset \Bbbk^n$ эквивалентны:
(1) $U \cap E_J = 0$
(2) факторизация $\Bbbk^n \twoheadrightarrow \Bbbk^n/U$ изоморфно отображает E_J на $\Bbbk^n/U$
(3) проекция $c_I : \Bbbk^n \twoheadrightarrow E_I$ вдоль E_J изоморфно отображает U на E_I.
(4) в U найдётся r векторов $u_1, u_2, \dots, u_r$ вида $u_\nu = e_{i_\nu} + w_\nu$, где $w_\nu \in E_J$.
При выполнении этих условий векторы, о котором идёт речь в (4), единственны и составляют базис в U.

Доказательство. Из (1) следует, что пространство U имеет нулевое пересечение с ядром проекции $c_I : \Bbbk^n \twoheadrightarrow E_J$, а пространство E_J — с ядром отображения факторизации $\Bbbk^n \twoheadrightarrow V/U$. Поэтому ограничение факторизации по U на подпространство E_J и ограничение проекции вдоль E_J на подпространство U инъективны и, по соображениям размерности, являются изоморфизмами . Наоборот, каждое из условий (2), (3) влечёт трансверсальность соответствующего пространства ядру рассматриваемого отображения, т. е. условие (1). Условие (4) говорит, что $c_I(u_\nu) = e_{i_\nu}$. Если это так, то c_I изоморфизм. Наоборот, если

c_I изоморфизм, то векторы $u_\nu \in U$, проектирующиеся в базисные векторы e_{i_ν} пространства E_I существуют, единственны и образуют базис в U. □

Упражнение 8.10. Пусть $e_1^*, e_2^*, \dots, e_n^*$ обозначают стандартный базис[1] в $\Bbbk^{n*}$, и $E_J^* = \operatorname{span}\big(e_{j_1}^*, e_{j_2}^*, \dots, e_{j_{n-r}}^*\big)$, $E_I^* = \operatorname{span}\big(e_{i_1}^*, e_{i_2}^*, \dots, e_{i_r}^*\big)$. Покажите, что если подпространство $U \subset \Bbbk^n$ удовлетворяет условиям из лем. 8.2, то его аннулятор $\operatorname{Ann} U \subset \Bbbk^{n*}$ обладает следующими эквивалентными друг другу свойствами:

а) $\operatorname{Ann} U \cap E_I^* = 0$ б) E_I^* изоморфно отображается на $\Bbbk^{n*}/\operatorname{Ann} U$

в) проекция $c_J : \Bbbk^{n*} \twoheadrightarrow E_J^*$ вдоль E_I^* изоморфно отображает U на E_J^*

г) в $\operatorname{Ann} U$ есть $(n-r)$ ковекторов вида $u_\mu^\perp = e_{j_\mu}^* + \tau_\mu$, где $\tau_\mu \in E_J^*$.

При этом векторы, о которых идёт речь в (г), единственны, образуют базис в $\operatorname{Ann} U$ и связаны с векторами $u_\nu = e_{i_\nu} + w_\nu \in U$ из условия (4) в лем. 8.2 формулой

$$\tau_\mu = -\langle e_{j_\mu}^*, w_1\rangle \cdot e_{i_1}^* - \langle e_{j_\mu}^*, w_2\rangle \cdot e_{i_2}^* - \cdots - \langle e_{j_\mu}^*, w_r\rangle \cdot e_{i_r}^* . \tag{8-9}$$

8.5. Метод Гаусса. Пусть подпространство $U \subset \Bbbk^n$ задано как линейная оболочка k векторов

$$\begin{aligned} w_1 &= (w_{11},\, w_{12},\, \dots,\, w_{1n}) \\ w_2 &= (w_{21},\, w_{22},\, \dots,\, w_{2n}) \\ &\dots\dots\dots\dots\dots\dots \\ w_k &= (w_{k1},\, w_{k2},\, \dots,\, w_{kn}), \end{aligned} \tag{8-10}$$

Мы собираемся построить в U базис $u_1, u_2, \dots, u_r$, удовлетворяющий условию (4) из лем. 8.2. На языке матриц это условие означает, что в матрице, по строкам которой записаны координаты векторов u_i, как в (8-10), в r столбцах с номерами $I = (i_1, i_2, \dots, i_r)$ находится *единичная подматрица*

$$E = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & 1 \end{pmatrix}$$

размера $r \times r$. Идея построения состоит в том, чтобы обнулять координаты в столбцах матрицы (8-10), последовательно заменяя подходящие пары векторов w_i, w_j их линейными комбинациями $w_i' = aw_i + bw_j$ и $w_j' = cw_i + dw_j$ так, чтобы линейная оболочка этой пары не менялась. Таковы, к примеру, замены следующих трёх типов:

$$\begin{array}{lll} 1)\quad w_i' = w_i + \lambda w_j & w_j' = w_j & (\text{с любым } \lambda \in \Bbbk \text{ любое}) \\ 2)\quad w_i' = w_j & w_j' = w_i & \\ 3)\quad w_i' = \varrho w_i & w_j' = w_j & (\text{с ненулевым } \varrho \in \Bbbk) \end{array} \tag{8-11}$$

[1] двойственный к стандартному базису $e_1, e_2, \dots, e_n$ пространства $\Bbbk^n$

Исходные векторы линейно выражаются в них через преобразованные как

$$\begin{array}{ll} w_i = w_i' - \lambda w_j' & w_j = w_j' \\ w_i = w_j' & w_j = w_i' \\ w_i = \varrho^{-1} w_i' & w_j = w_j' \,. \end{array}$$

При заменах (8-11) матрица (w_{ij}), по строкам которой стоят координаты векторов (8-10), испытывает следующие *элементарные преобразования строк*:

1) к одной из строк прибавляется другая, умноженная на любое число[1]

2) какие-нибудь две строки матрицы меняются местами

3) одна из строк умножается на ненулевое число.

Лемма 8.3 (о приведении к строгому ступенчатому виду)
Всякая матрица $A \in \mathrm{Mat}_{m\times n}(\Bbbk)$ элементарными преобразованиями строк приводится к виду, в котором самый левый ненулевой элемент каждой строки равен 1, располагается строго правее, чем в предыдущей строке, и является единственным ненулевым элементом своего столбца.

Доказательство. Удобно разбить процесс на n последовательных шагов (по количеству столбцов). Будем предполагать, что после выполнения $(k-1)$-го шага та часть матрицы, что находится слева от k-ого столбца, имеет нужный вид (при $k=1$ это ничего не означает). Пусть в этой части имеется s ненулевых строк. По нашему предположению $0 \leqslant s \leqslant k-1$ и эти строки являются верхними. Очередной k-тый шаг вычисления состоит из следующих действий.

Выберем в k-том столбце в строках строго ниже s-той какой-нибудь ненулевой элемент a (если его нет, можно перейти к $(k+1)$-му шагу). Умножим строку, где он стоит, на a^{-1}. Потом поменяем эту строку местами с $(s+1)$-ой строкой. Это не изменит левые $(k-1)$ столбцов матрицы, а $(s+1)$-ую строку приведёт к виду

$$\underbrace{0\,0\,\ldots\,0\,0}_{k-1}\,1\,\underbrace{*\,*\,\ldots\,*\,*}_{n-k}\,.$$

Теперь для каждого $i \neq s+1$ вычтем из i-той строки $(s+1)$-ую строку, умноженную на элемент, стоящий в пересечении i-той строки и k-того столбца. Это не изменит левые $(k-1)$ столбцов матрицы и занулит все элементы k-того столбца за исключением стоящей $(s+1)$-ой строке единицы. В результате мы попадаем в исходное положение для $(k+1)$-го шага. $\square$

[1] подчеркнём, что все остальные строки (в том числе та, что прибавлялась) остаются без изменения

8.5.1. Пример: базисы линейной оболочки и фактора. Поскольку линейная оболочка строк матрицы не меняется при элементарных преобразованиях, ненулевые строки $u_1, u_2, \dots, u_r$ итоговой строгой ступенчатой матрицы порождают то же самое подпространство U, что и строки $w_1, w_2, \dots, w_k$ исходной матрицы (8-10), но при этом удовлетворяют условию (4) из лем. 8.2, в которой в качестве $I = (i_1, i_2, \dots, i_r)$ следует взять набор номеров тех столбцов, где стоят самые левые единицы строк строгой ступенчатой матрицы. Тем самым, строки ступенчатой матрицы составляют базис в U, а классы базисных векторов $e_j \in \Bbbk^n$ с $j \notin I$, образуют базис в $\Bbbk^n/U$.

В частности, мы получаем обещанное перед формулировкой лем. 8.2

Следствие 8.8

Для каждого r-мерного подпространства $U \subset \Bbbk^n$ существует хотя бы одно разбиение $\Bbbk^n = E_I \oplus E_J$ в сумму дополнительных r-мерного и $(n-r)$-мерного координатных подпространств, удовлетворяющее условиям лем. 8.2.

Для иллюстрации всего сказанного найдём базис в линейной оболочке U четырёх векторов координатного пространства $\mathbb{Q}^5$, строки которых образуют матрицу:

$$\begin{pmatrix} 2 & -4 & -8 & 2 & -4 \\ -1 & 1 & 3 & 0 & 1 \\ -1 & -1 & 1 & 2 & -1 \\ -1 & 0 & 2 & 1 & 1 \end{pmatrix} \tag{8-12}$$

умножим последнюю строку на -1 и поменяем местами с первой

$$\begin{pmatrix} 1 & 0 & -2 & -1 & -1 \\ -1 & 1 & 3 & 0 & 1 \\ -1 & -1 & 1 & 2 & -1 \\ 2 & -4 & -8 & 2 & -4 \end{pmatrix}$$

зануляем первый столбец под первой строкой, добавляя ко всем строкам подходящие кратности первой:

$$\begin{pmatrix} 1 & 0 & -2 & -1 & -1 \\ 0 & 1 & 1 & -1 & 0 \\ 0 & -1 & -1 & 1 & -2 \\ 0 & -4 & -4 & 4 & -2 \end{pmatrix}$$

теперь зануляем второй столбец под второй строкой, добавляя подходящие её кратности к последним двум строкам:

$$\begin{pmatrix} 1 & 0 & -2 & -1 & -1 \\ 0 & 1 & 1 & -1 & 0 \\ 0 & 0 & 0 & 0 & -2 \\ 0 & 0 & 0 & 0 & -2 \end{pmatrix}$$

делим третью строку на -2 и зануляем последний столбец вне третьей строки, добавляя к первой и четвёртой строкам подходящие кратности третьей

$$\begin{pmatrix} 1 & 0 & -2 & -1 & 0 \\ 0 & 1 & 1 & -1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \tag{8-13}$$

Получилась строгая ступенчатая матрица. Её строки составляют базис в линейной оболочке строк исходной матрицы (8-12). Таким образом, $\dim U = 3$ и U изоморфно проектируется на трёхмерное координатное подпространство

$$E_{(1,2,5)} = \operatorname{span}(e_1,\, e_2,\, e_5)$$

вдоль дополнительного к нему двумерного координатного подпространства

$$E_{(3,4)} = \operatorname{span}(e_3,\, e_4)$$

так что строки матрицы (8-13) переходят при такой проекции в точности в стандартные базисные векторы e_1, e_2, e_3. Тем самым, подпространство U имеет нулевое пересечение с ядром этой проекции, т. е. $U \cap E_{(3,4)} = 0$. Поэтому координатное подпространство $E_{(3,4)}$ изоморфно проектируется на фактор $\mathbb{Q}^5/U$, и классы $e_3 \pmod U$ и $e_4 \pmod U$ образуют в нём базис.

Замечание 8.4. Приведение матрицы к строгому ступенчатому виду указывает лишь одно из возможных координатных подпространств E_I, на которое подпространство U изоморфно проектируется вдоль дополнительного координатного подпространства E_J. Вообще говоря, таких таких координатных подпространств E_I может быть много. Более того, над бесконечным полем $\Bbbk$ случайно взятое подпространство $U \subset \Bbbk^n$ почти наверняка изоморфно проектируется *на каждое* из $\binom{n}{r}$ r-мерных координатных подпространств E_I.

Упражнение 8.11. Покажите, что r-мерное пространство U, заданное координатами каких-нибудь $m \geqslant r$ порождающих векторов (8-10), изоморфно проектируется на координатное подпространство E_I тогда и только тогда, когда в матрице (8-10), по строкам которой написаны координаты этих векторов, в столбцах с номерами $i_1, i_2, \dots, i_r$ находится $m \times r$ подматрица ранга r.

8.5.2. Пример: решение системы линейных уравнений. На двойственном языке вычисление (8-12)–(8-13) выглядит как решение системы линейных уравнений. А именно, аннулятор $\operatorname{Ann} U \subset \mathbb{Q}^{5*}$ подпространства $U \subset \mathbb{Q}^5$, порождённого строками матрицы

$$\begin{pmatrix} 2 & -4 & -8 & 2 & -4 \\ -1 & 1 & 3 & 0 & 1 \\ -1 & -1 & 1 & 2 & -1 \\ -1 & 0 & 2 & 1 & 1 \end{pmatrix} \tag{8-14}$$

есть пространство решений системы однородных линейных уравнений

$$\begin{cases} 2\,x_1 - 4\,x_2 - 8\,x_3 + 2\,x_4 - 4\,x_5 = 0 \\ -x_1 + x_2 + 3\,x_3 + x_5 = 0 \\ -x_1 - x_2 + x_3 + 2\,x_4 - x_5 = 0 \\ -x_1 + 2\,x_3 + x_4 + x_5 = 0 \end{cases} \tag{8-15}$$

матрица коэффициентов которой есть матрица (8-14). Приведя её к строгому ступенчатому виду (8-13)

$$\begin{pmatrix} 1 & 0 & -2 & -1 & 0 \\ 0 & 1 & 1 & -1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

мы выбрали в пространстве уравнений U базис, состоящий из уравнений

$$\begin{cases} x_1 - 2\,x_3 - x_4 = 0 \\ x_2 + x_3 - x_4 = 0 \\ x_5 = 0 \end{cases}$$

которые эквивалентны исходным уравнениям (8-15), но допускают явное выражение переменных x_1, x_2, x_5 через переменные x_3 и x_4

$$\begin{cases} x_1 = 2\,x_3 + x_4 \\ x_2 = -x_3 + x_4 \\ x_5 = 0 \end{cases} \tag{8-16}$$

Переменные x_3 и x_4 называются в этой ситуации *свободными* (им можно придавать любые значения), а переменные x_1, x_2 и x_5 — *связанными* (они однозначно определяются из (8-16) как только заданы какие-нибудь значения свободных переменных). На геометрическом языке это означает, что двумерное пространство $\mathrm{Ann}\,(U) \simeq (\mathbb{Q}^5/U)^*$ изоморфно проектируется в $\mathbb{Q}^{5^*}$ на координатное подпространство $E^*_{3,4} = \mathrm{span}(e^*_3,\, e^*_4)$ вдоль дополнительного координатного подпространства $E^*_{1,2,5} = \mathrm{span}(e^*_1,\, e^*_2,\, e^*_5)$. В частности, в пространстве $\mathrm{Ann}\,(U) \simeq (\mathbb{Q}^5/U)^*$ решений системы (8-15) есть базис из ковекторов вида[1] $u_1^\perp = (\,*\,,\,*\,,\,1\,,\,0\,,\,*\,)$, $u_2^\perp = (\,*\,,\,*\,,\,0\,,\,1\,,\,*\,)$. Отмеченные звёздочками координаты легко находятся из (8-16) и равны $(\,2\,,\,-1\,,\,1\,,\,0\,,\,0\,)$ и $(\,1\,,\,1\,,\,0\,,\,1\,,\,0\,)$.

[1]эти ковекторы являются прообразами стандартных базисных ковекторов e^*_3, e^*_4 относительно проекции $\mathrm{Ann}\,(U) \twoheadrightarrow E^*_{(3,4)}$ вдоль $E_{(1,2,5)}$ и образуют базис в $\left(\mathbb{Q}^5/U\right)^* \simeq \mathrm{Ann}\,(U)$, двойственный к обсуждавшемуся выше базису $e_3\,(\mathrm{mod}\,U)$, $e_4\,(\mathrm{mod}\,U)$ в факторе $\mathbb{Q}^5/U$

Пространство решений произвольной системы линейных однородных уравнений

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = 0 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = 0 \\ a_{31}x_1 + a_{32}x_2 + \cdots + a_{3n}x_n = 0 \\ \cdots\cdots\cdots\cdots\cdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = 0 \end{cases} \tag{8-17}$$

описывается аналогично. Обозначим через $U \subset \Bbbk^n$ линейную оболочку строк матрицы $A = (a_{ij})$. Тогда пространство решений системы (8-17) представляет собой аннулятор $\operatorname{Ann}(U) \simeq (\Bbbk^n/U)^*$. Если выбрать в пространстве уравнений U базис вида

$$\begin{aligned} u_1 &= e_{i_1} + \alpha_{1j_1}e_{j_1} + \alpha_{1j_2}e_{j_2} + \cdots + \alpha_{1j_{n-r}}e_{j_{n-r}} \\ u_2 &= e_{i_2} + \alpha_{2j_1}e_{j_1} + \alpha_{2j_2}e_{j_2} + \cdots + \alpha_{2j_{n-r}}e_{j_{n-r}} \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ u_r &= e_{i_r} + \alpha_{rj_1}e_{j_1} + \alpha_{rj_2}e_{j_2} + \cdots + \alpha_{rj_{n-r}}e_{j_{n-r}} \end{aligned} \tag{8-18}$$

(удовлетворяющий условию (4) из лем. 8.2), то матрица (α_{ij}) соответствующей ему системы уравнений будет содержать единичную подматрицу размера $r \times r$ в столбцах с номерами $i_1, i_2, \dots, i_r$. Согласно упр. 8.10 ковекторы

$$\begin{aligned} u_1^{\perp} &= e_{j_1}^* - \alpha_{1j_1}e_{i_1}^* - \alpha_{2j_1}e_{i_2}^* - \cdots - \alpha_{rj_1}e_{i_r}^* \\ u_2^{\perp} &= e_{j_1}^* - \alpha_{1j_2}e_{i_1}^* - \alpha_{2j_2}e_{i_2}^* + \cdots - \alpha_{rj_2}e_{i_r}^* \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ u_{n-r}^{\perp} &= e_{j_{n-r}}^* - \alpha_{1j_{n-r}}e_{i_1}^* - \alpha_{2j_{n-r}}e_{i_2}^* - \cdots - \alpha_{rj_{n-r}}e_{i_r}^* \end{aligned} \tag{8-19}$$

составляют базис пространства $\operatorname{Ann}(U) \subset \Bbbk^{n*}$ решений системы (8-17).

Упражнение 8.12. Проверьте это независимо от упр. 8.10.

Иначе можно сказать, что базисные решения $u_j^{\perp}$ получаются приданием одной из свободных переменных $x_{j_1}, x_{j_2}, \dots, x_{j_{n-r}}$ значения 1, остальным свободным переменным — значения нуль, а каждой связанной переменной x_{i_ν} — того значения, которое получается из единственного содержащего x_{i_ν} уравнения.

8.6. Расположение подпространства относительно базиса. Покажем, что с точностью до добавления нулевых строк результат приведения к строгому ступенчатому виду матрицы координат любого набора векторов порождающих данное подпространство $U \subset \Bbbk^n$ не зависит ни от выбора этих векторов, ни от способа приведения.

Для этого рассмотрим убывающую цепочку координатных подпространств

$$V = V^0 \supset V_1 \supset V_2 \supset \cdots \supset V_{n-1} \supset V_n = 0\,, \tag{8-20}$$

в которой $V^i = \operatorname{span}(e_{i+1}, e_{i+2}, \dots, e_n)$, и обозначим через $\pi_i : V \twoheadrightarrow V/V^i$ отображение факторизации[1]. Цепочка (8-20) называется *полным флагом*.

Сопоставим каждому r-мерному подпространству $U \subset V$ набор неотрицательных целых чисел $d_i = \dim \pi_i(U) = r - \dim U \cap V^i \quad (i = 0, 1, \dots, n)$.

Числа $d_0, d_1, \dots, d_n$ образуют неубывающую последовательность, которая начинается с $d_0 = 0$, заканчивается на $d_n = r$ и прирастает не более, чем на единицу за один шаг: $d_i - d_{i-1} \leqslant 1$.

Упражнение 8.13. Докажите это.

Например, для подпространства $U \subset \mathbb{Q}^5$, порождённого строками матрицы (8-13), получаем последовательность $(d_0, d_1, \dots, d_5) = (0, 1, 2, 2, 2, 3)$.

Набор $I = (i_1, i_2, \dots, i_r)$ тех номеров, в которых происходят ненулевые приращения $d_{i_\nu} - d_{i_\nu - 1} = 1$, зависит только от подпространства U и флага (8-20). Мы будем называть его *комбинаторным типом* U относительно полного координатного флага (8-20). Так, подпространство $U \subset \mathbb{Q}^5$, порождённое строками матрицы (8-13) имеет комбинаторный тип $I = (1, 2, 5)$.

Упражнение 8.14. Убедитесь, что комбинаторный тип подпространства, порождённого строками строгой ступенчатой матрицы, всегда представляет собою набор номеров тех столбцов, где стоят самые левые единицы строк.

Таким образом, форма ступенчатой матрицы, однозначно определяется флагом (8-20) и подпространством U. Поскольку базис $u_{i_1}, u_{i_2}, \dots, u_{i_r} \in U$, проектирующийся в стандартные базисные векторы $e_{i_1}, e_{i_2}, \dots, e_{i_r}$ вдоль дополнительного координатного подпространства E_J тоже единственен (см. лем. 8.2), ненулевые строки строки строгой ступенчатой матрицы, которая получится при применении метода Гаусса к матрице координат любой системы порождающих векторов пространства U, зависит только от самого подпространства U и зафиксированного нами с самого начала стандартного базиса в $\Bbbk^n$, в котором записываются координаты всех векторов. Мы доказали

Следствие 8.9

В каждом подпространстве $U \subset \Bbbk^n$ существует единственный базис со строгой ступенчатой матрицей координат M_U, и сопоставление подпространству U матрицы M_U устанавливает биекцию между строгими ступенчатыми матрицами с r ненулевыми строками и r-мерными подпространствами в $\Bbbk^n$. $\square$

Упражнение 8.15. Покажите, что строгие ступенчатые матрицы комбинаторного типа $(i_1, i_2, \dots, i_r)$ образуют в $\operatorname{Mat}_{r\times n}(\Bbbk)$ аффинное подпространство[2] размерности $r(n-r) - \sum\limits_{\nu=1}^{r}(i_\nu - \nu + 1)$.

[1] отождествляя фактор пространство V/V^i с координатным подпространством $W_i = \operatorname{span}(e_1, e_2, \dots, e_i)$, можно считать, что π_i проектирует $\Bbbk^n$ на W_i вдоль V^i, т. е. просто забывает последние $(n-i)$ координат

[2] см. зам. 8.3. на стр. 133

8.6.1. Грассманиан $\mathrm{Gr}(k,n)$. Множество всех k-мерных подпространств координатного пространства $\Bbbk^n$ называется *грассманианом* $\mathrm{Gr}(k,n)$.

Если подпространство $U \in \mathrm{Gr}(k,n)$ изоморфно проектируется на некоторое координатное подпространство $E_I = \mathrm{span}(e_{i_1}, e_{i_2}, \dots, e_{i_k})$ вдоль дополнительного координатного подпространства E_J, то и все близкие[1] к U подпространства U' также будут изоморфно проектироваться на E_I вдоль E_J. Согласно сл. 8.8 все такие подпространства U' взаимно однозначно соответствуют матрицам размера $k \times n$, содержащим в r столбцах с номерами из I единичную подматрицу размера $k \times k$. Множество всех таких матриц образует $k(n-k)$-мерное аффинное подпространство в $\mathrm{Mat}_{k\times n}$ (смежный класс векторного подпространства матриц с нулями в столбцах I и произвольными элементами в остальных $k(n-k)$ клетках).

Таким образом, грассманиан $\mathrm{Gr}(k,n)$ «покрывается» $\binom{n}{k}$ аффинными пространствами размерности $k(n-k)$ в том смысле, что в окрестности каждой своей точки он выглядит в точности как такое аффинное пространство. Эти аффинные пространства называются стандартными *аффинными картами* на $\mathrm{Gr}(k,n)$. Поскольку одно и то же пространство U обычно можно изоморфно спроектировать на несколько k-мерных координатных подпространств E_I, стандартные аффинные карты имеют большие пересечения друг с другом[2].

Из сл. 8.9 вытекает, что грассманиан $\mathrm{Gr}(k,n)$ разбивается в дизъюнктное объединение подмножеств $S_I \subset \mathrm{Gr}(k,n)$, каждое из которых состоит из всех подпространств U заданного комбинаторного типа I, где I пробегает всевозможные наборы из k строго возрастающих номеров

$$1 \leqslant i_1 < i_2 < \cdots < i_k \leqslant n\,. \tag{8-21}$$

Подмножества S_I называются *клетками Шуберта*. Например, подпространство $U \subset \mathbb{Q}^5$, порождённое строками матрицы (8-13), находится в клетке с индексом $I = (1,2,5)$.

Вместо наборов I из возрастающих номеров (8-21) для индексирования клеток Шуберта чаще используют диаграммы Юнга λ, полагая $i_\nu - \nu = \lambda_{k+1-\nu}$, так что строго возрастающая последовательность $i_1, i_2, \dots, i_k$ переписывается как $\lambda_k + 1,\ \lambda_{k-1} + 2,\ \lambda_{k-2} + 3,\ \dots,\ \lambda_1 + k$. При этом наборы (8-21) оказываются в биективном соответствии с диаграммами Юнга $\lambda = (\lambda_1, \lambda_2, \dots, \lambda_k)$, лежащими в прямоугольнике $k \times (n-k)$, т. е. удовлетворяющими условиям $(n-k) \geqslant \lambda_1 \geqslant \lambda_2 \geqslant \cdots \geqslant \lambda_k \geqslant 0$.

[1] в любом разумном смысле — например, полученные малым шевелением коэффициентов базисных векторов, если дело происходит над полем $\mathbb{R}$; в §10 мы увидим, что «близость» в данном контексте означает принадлежность, вместе с U, некоторому всюду плотному открытому подмножеству в пространстве матриц, дополнительному к множеству решений некоторой системы полиномиальных уравнений на матричные элементы (ср. с зам. 8.4. на стр. 138

[2] на самом деле пересечение всех $\binom{n}{k}$ стандартных карт изображается в каждой из карт дополнением к решению системы полиномиальных уравнений и поэтому всюду плотно в грассманиане

Так, клетке грассманиана $\mathrm{Gr}(3,5)$, содержащей подпространство, порождённое строками матрицы (8-13), и имеющей индекс $I = (1,2,5)$, отвечает

$$\lambda = (2,0,0) = \ydiagram{2}$$

Эта клетка состоит из подпространств, порождённых строками матриц вида

$$\begin{pmatrix} 1 & 0 & * & * & 0 \\ 0 & 1 & * & * & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

и является 4-мерным аффинным подпространством пространства матриц. Ещё несколько клеток Шуберта грассманиана $\mathrm{Gr}(3,5)$ и ступенчатых матриц, из которых они состоят, представлены в таблице (8-22).

Некоторые клетки Шуберта грассманиана $\mathrm{Gr}(3,5)$

диаграмма λ	вид ступенчатой матрицы	$\dim S_\lambda$
$(0,0,0) = \varnothing$	$\begin{pmatrix} 1 & 0 & 0 & * & * \\ 0 & 1 & 0 & * & * \\ 0 & 0 & 1 & * & * \end{pmatrix}$	6
$(1,0,0) = \ydiagram{1}$	$\begin{pmatrix} 1 & 0 & * & 0 & * \\ 0 & 1 & * & 0 & * \\ 0 & 0 & 0 & 1 & * \end{pmatrix}$	5
$(1,1,0) = \ydiagram{1,1}$	$\begin{pmatrix} 1 & * & 0 & 0 & * \\ 0 & 0 & 1 & 0 & * \\ 0 & 0 & 0 & 1 & * \end{pmatrix}$	4
$(2,1,0) = \ydiagram{2,1}$	$\begin{pmatrix} 1 & * & 0 & * & 0 \\ 0 & 0 & 1 & * & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$	3
$(2,1,1) = \ydiagram{2,1,1}$	$\begin{pmatrix} 0 & 1 & 0 & * & 0 \\ 0 & 0 & 1 & * & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$	2
$(2,2,1) = \ydiagram{2,2,1}$	$\begin{pmatrix} 0 & 1 & * & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$	1
$(2,2,2) = \ydiagram{2,2,2}$	$\begin{pmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$	0

(8-22)

Каждая клетка S_λ является аффинным пространством пространства матриц и согласно упр. 8.15 имеет размерность $k(n-k) - |\lambda|$ (где $|\lambda|$, как обычно, обозначает общее количество клеток в диаграмме λ).

Отметим, что над конечным полем из q элементов это даёт соотношение

$$\binom{n}{k}_q = q^{k(n-k)} \sum_\lambda q^{-|\lambda|} \tag{8-23}$$

(сумма по всем диаграммам, лежащим в прямоугольнике $k\times(n-k)$), где

$$\binom{n}{k}_q \overset{\text{def}}{=} |\mathrm{Gr}(k,n)| = \frac{q^n(q^n-q)\cdots(q^n-q^{k-1})}{q^k(q^k-q)\cdots(q^k-q^{k-1})} = \\ = q^{n-k}\cdot\frac{(q^{n-1}-1)(q^{n-2}-1)\cdots(q^{n-k+1}-1)}{(q^{k-1}-1)(q^{k-2}-1)\cdots(q-1)} \qquad (8\text{-}24)$$

есть количество k-мерных подпространств[1] в $\mathbb{F}_q^n$ (ср. с зад. 7.12). В частности, предел дроби (8-24) при $q\to 1$ равен числу слагаемых в правой части (8-23), т. е. биномиальному коэффициенту $\binom{n}{k}$.

Задачи для самостоятельного решения к §8

Задача 8.1. Допишите в таблицу (8-22) все недостающие строки и составьте аналогичную таблицу для грассманиана $\mathrm{Gr}(2,4)$.

Задача 8.2. Система линейных уравнений имеет бесконечно много решений. Верно ли, что каждое из неизвестных может принимать бесконечно много значений?

Задача 8.3. Укажите для каждой из матриц

$$\begin{pmatrix}-2&-1&-7&5&-4\\-1&4&1&-2&1\\-1&-2&-5&4&-3\\1&-1&2&-1&1\end{pmatrix}\quad\begin{pmatrix}2&-1&0&-1&0\\-2&-2&1&2&0\\-7&-1&2&2&-2\\4&0&-1&-1&1\end{pmatrix}\quad\begin{pmatrix}1&3&-6&2&-5\\7&-2&3&-2&0\\-1&0&-2&1&-2\\-4&0&-1&1&0\end{pmatrix}$$

размерность и какой-нибудь базис а) в линейной оболочке столбцов
б) в аннуляторе линейной оболочки строк
в) в факторе $\mathbb{Q}^5$ по линейной оболочке строк
г) в факторе $\mathbb{Q}^4$ по аннулятору линейной оболочки столбцов
д) в двойственном пространстве к фактору $\mathbb{Q}^5$ по линейной оболочке строк.

Задача 8.4. Найдите размерность и базис в сумме и в пересечении следующих пар подпространств в $\mathbb{Q}^4$:
а) линейная оболочка векторов $(1,1,1,1)$, $(1,-1,1,-1)$, $(1,3,1,3)$, и линейная оболочка векторов $(1,2,0,2)$, $(1,2,1,2)$, $(3,1,3,1)$
б) линейная оболочка векторов $(1,1,0,0)$, $(0,1,1,0)$, $(0,0,1,1)$, и подпространство, заданное уравнениями

$$x_1+x_3=2\,x_2+x_3+x_4=x_1+2\,x_2+x_3+2\,x_4=0$$

в) подпространство, заданное уравнениями $x_1+x_2=x_2+x_3=x_3+x_4=0$, и подпространство, заданное уравнениями $x_1+2\,x_2+2\,x_4=x_1+2\,x_2+x_3+2\,x_4=3\,x_1+x_2+3\,x_3+x_4=0$.

[1] в числителе и знаменателе средней дроби стоят количества упорядоченных линейно независимых наборов из k векторов, соответственно, в n-мерном и k-мерном пространствах над $\mathbb{F}_q$

Задача 8.5. Выясните, является ли прямой сумма следующих пар подпространств в $\mathbb{Q}^4$, и во всех случаях, когда является, найдите проекции стандартных базисных векторов $\mathbb{Q}^4$ на первое из них вдоль второго.

а) линейная оболочка векторов $(-11,8,-1,2)$, $(-6,5,2,3)$, $(-3,2,-1,0)$ и линейная оболочка векторов $(-8,4,12,-4)$, $(-6,-5,-9,1)$, $(-2,-3,-6,1)$

б) линейная оболочка векторов $(30,5,-9,1)$, $(2,8,4,-3)$, $(-6,-4,0,1)$ и подпространство, заданное системой уравнений

$$\begin{cases} 2\,x_1 + 3\,x_2 - 4\,x_3 + x_4 = 0 \\ -x_1 - 2\,x_2 + 3\,x_3 - x_4 = 0 \\ \qquad -x_2 + 2\,x_3 - x_4 = 0 \end{cases}$$

в) подпространства, заданные системами уравнений

$$\begin{cases} -3\,x_1 - 10\,x_2 + 20\,x_3 - 6\,x_4 = 0 \\ -15\,x_1 + 4\,x_2 + 19\,x_3 - 3\,x_4 = 0 \\ \qquad 6\,x_1 - 10\,x_3 + 2\,x_4 = 0 \end{cases} \quad \text{и} \quad \begin{cases} 6\,x_1 - 7\,x_2 - 3\,x_3 - 2\,x_4 = 0 \\ -7\,x_1 - x_2 + 6\,x_3 - x_4 = 0 \\ 5\,x_1 - 4\,x_2 - 3\,x_3 - x_4 = 0 \end{cases}$$

Задача 8.6. Те же вопросы про подпространство, заданное в $\mathbb{Q}^n$ одним уравнением $x_1 + x_2 + \dots + x_n = 0$, и подпространство, заданное системой уравнений

$$x_1 = x_2 = \dots = x_n\,.$$

Задача 8.7. Покажите, что в n-мерном пространстве у любого набора из $\geqslant n+2$ векторов есть нетривиальная линейная зависимость с нулевой суммой коэффициентов.

Задача 8.8. На клетчатой бумаге нарисован по линиям сетки прямоугольник, и во все клетки, граничащие с внешней стороны с контуром этого прямоугольника, написаны произвольные числа. Докажите, что во все клетки прямоугольника можно поставить числа так, чтобы каждое из них равнялось среднему арифметическому четырех соседей[1].

Задача 8.9. На ребрах тетраэдра написаны числа $b_1, b_2, \dots, b_6$. При каких условиях на эти числа можно написать ещё 4 числа на грани так, чтобы число на каждом из рёбер оказалось равно сумме чисел, написанных на двух примыкающих к этому ребру гранях? Опишите все решения этой задачи для всех $b_1, b_2, \dots, b_6$, для которых задача имеет решения.

Задача 8.10. На вершинах куба написаны числа $b_1, b_2, \dots, b_8$. При каких условиях на эти числа можно написать ещё 6 чисел на грани так, чтобы число в каждой из вершин оказалось равно сумме чисел, написанных на трёх сходящихся в этой вершине гранях? Опишите все решения этой задачи для всех $b_1, b_2, \dots, b_8$, для которых задача имеет решения.

[1]из клеток, имеющих с рассматриваемой общую сторону

Задача 8.11. В рамках конструкции из n° 8.1.2 обозначим через

$$\delta_a^{(k)} : f \mapsto f^{(k)}(a)$$

линейную форму на пространстве многочленов $\Bbbk[x]$, сопоставляющую каждому многочлену значение его k-той производной в точке $a \in \Bbbk$. Каким формальным рядам отвечают эти формы при изоморфизме $\Bbbk[[t]] \xrightarrow{\sim} \Bbbk[x]^*$ из n° 8.1.2? Является ли множество этих форм (со всевозможными $a \in \Bbbk$ и целыми неотрицательными k) линейно независимым?

Задача 8.12. Покажите, что $\operatorname{rk} A = 1$ тогда и только тогда, когда $a_{ij} = x_i y_j$ для некоторых ненулевых наборов чисел $x_1, x_2, \dots, x_m$ и $y_1, y_2, \dots, y_n$.

Задача 8.13. Пусть $a_{ij} = x_i + y_j$ для некоторых $x_1, x_2, \dots, x_m$ и $y_1, y_2, \dots, y_n$ покажите, что $\operatorname{rk}(a_{ij}) \leqslant 2$.

Задача 8.14. Для $A_1, A_2 \in \mathrm{Mat}_{m\times n}(\Bbbk)$ обозначим через $V_1, V_2 \in \Bbbk^n$ и $W_1, W_2 \in \Bbbk^m$ линейные оболочки их строк и столбцов соответственно. Докажите эквивалентность друг другу следующих трёх условий:
а) $\operatorname{rk}(A_1 + A_2) = \operatorname{rk}(A_1) + \operatorname{rk}(A_2)$ б) $V_1 \cap V_2 = 0$ в) $W_1 \cap W_2 = 0$

Задача 8.15. Докажите, что любую матрицу ранга r можно представить в виде суммы r матриц ранга 1, но нельзя представить в виде суммы меньшего числа таких матриц.

Задача 8.16. Пусть оператор $F : V \longrightarrow W$ переводит подпространство $U \subset V$ в подпространство $T \subset W$. Покажите, что оператор $\widetilde{F} : V/U \longrightarrow W/T$, переводящий класс $v \pmod U$ в класс $F(v) \pmod T$ корректно определён и линеен.

Задача 8.17. Для любых трёх вложенных друг в друга векторных пространств

$$U \subset V \subset W$$

постройте вложение V/U в качестве подпространства в W/U и установите изоморфизм $(W/U)/(V/U) \xrightarrow{\sim} W/V$.

Задача 8.18. Докажите, что для любого линейного оператора F на конечномерном векторном пространстве V при любом $n \in \mathbb{N}$ имеют место равенства
а) $\dim\ker(F^k) = \dim\ker(F) + \sum\limits_{i=1}^{n} \dim(\operatorname{im} F^n \cap \ker F)$
б) $\dim\operatorname{im}(F) = \dim\operatorname{im}(F^{n+1}) + \sum\limits_{i=1}^{n} \dim(\operatorname{im} F^n \cap \ker F)$

Задача 8.19 (коммутативный треугольник). Диаграмма из отображений множеств называется *коммутативной*, если все различные цепочки стрелок, ведущие из одного множества в другое, имеют равные композиции. В идущем далее наборе импликаций, относящихся к коммутативному треугольнику векторных пространств и линейных отображений

$$\begin{tikzcd} U \arrow[rr, "\gamma"] \arrow[dr, "\alpha"'] & & W \\ & V \arrow[ur, "\beta"'] & \end{tikzcd}$$

верные докажите, а неверные опровергните конкретными контрпримерами.
а) α, β эпи $\Rightarrow \gamma$ эпи б) α, β моно $\Rightarrow \gamma$ моно в) γ эпи $\Rightarrow \alpha$ эпи
г) γ эпи $\Rightarrow \beta$ эпи д) γ моно $\Rightarrow \alpha$ моно е) γ моно $\Rightarrow \beta$ моно
ж) если α эпи, то (γ эпи $\iff \beta$ эпи) з) если α эпи, то (γ моно $\iff \beta$ моно)
и) если β эпи, то (γ эпи $\iff \alpha$ эпи) к) если β эпи, то (γ моно $\iff \alpha$ моно)
л) если γ изоморфизм, то α моно, а β эпи.

Задача 8.20 (точные тройки и коядра). Диаграмма линейных отображений

$$U \overset{G}{\hookrightarrow} V \overset{F}{\twoheadrightarrow} W \tag{8-25}$$

в которой F сюрьективен, G инъективен, и $\operatorname{im} G = \ker F$, называется *точной тройкой*. Покажите, что двойственная диаграмма

$$U^* \overset{G^*}{\twoheadleftarrow} V^* \overset{F^*}{\hookleftarrow} W^* \tag{8-26}$$

также является точной тройкой (по этой причине фактор по образу линейного отображения $V_1 \xrightarrow{\varphi} V_2$ называется *коядром* этого отображения и обозначается $\operatorname{coker}\varphi = V_2/\operatorname{im}\varphi = (\ker\varphi^*)^*$).

Задача 8.21. Не прибегая к фиксации каких-либо базисов, постройте изоморфизмы для любых векторных пространств U, V, W изоморфизмы
а) $\operatorname{Hom}(U\oplus W, V) \simeq \operatorname{Hom}(U,V)\oplus\operatorname{Hom}(W,V)$ б) $\operatorname{Hom}(V, U\oplus W) \simeq \operatorname{Hom}(V,U)\oplus\operatorname{Hom}(V,W)$

Задача 8.22. Цепочка линейных отображений называется *точной*, если для любых двух последовательных отображений $\varphi\circ\psi$ этой цепочки $\ker\varphi = \operatorname{im}\psi$ (т. е. ядро каждого из отображений совпадает с образом предыдущего). Покажите, что в диаграмме линейных отображений с точными строками

$$\begin{tikzcd} 0 \arrow[r] & V' \arrow[r] \arrow[d, "\varphi'"] & V \arrow[r] \arrow[d, "\varphi"] & V'' \arrow[r] \arrow[d, "\varphi''"] & 0 \\ 0 \arrow[r] & W' \arrow[r] & W \arrow[r] & W'' \arrow[r] & 0 \end{tikzcd} \tag{8-27}$$

а) из того, что φ' и φ'' изоморфизмы, следует, что φ изоморфизм. Приведите пример, опровергающий обратное утверждение, но покажите, что из биективности φ всё-таки вытекает инъективность φ' и сюрьективность φ''.

Задача 8.23 (лемма о пяти гомоморфизмах). Покажите, что в диаграмме линейных отображений

$$\begin{tikzcd} V_1' \arrow[r] \arrow[d, "\varphi_1'"'] & V_2' \arrow[r] \arrow[d, "\varphi_2'"'] & V \arrow[r] \arrow[d, "\varphi"] & V_2'' \arrow[r] \arrow[d, "\varphi_2''"] & V_1'' \arrow[d, "\varphi_1''"] \\ W_1' \arrow[r] & W_2' \arrow[r] & W \arrow[r] & W_2'' \arrow[r] & W_1'' \end{tikzcd}$$

с точными строками биективность четырёх боковых стрелок φ_1', φ_1'', φ_2', φ_2'' влечёт биективность центральной стрелки φ, и приведите примеры, показывающие, что одна только инъективность (соотв. одна только сюрьективность) четырёх боковых стрелок не гарантирует инъективности (соотв. сюрьективности) центральной.

Задача 8.24. Покажите, что в диаграмме

$$\begin{tikzcd} 0 \arrow[r] & V' \arrow[r] & V \arrow[r] \arrow[d, "\varphi"] & V'' \arrow[r] \arrow[d, "\varphi''"] & 0 \\ 0 \arrow[r] & W' \arrow[r] & W \arrow[r] & W'' \arrow[r] & 0 \end{tikzcd}$$

с точными строками и коммутативным квадратом имеется единственное линейное отображение $V' \xrightarrow{\varphi'} W'$, дополняющее её коммутативным квадратом слева. Докажите аналогичное утверждение про диаграмму

$$\begin{tikzcd} 0 \arrow[r] & V' \arrow[r] \arrow[d, "\varphi'"'] & V \arrow[r] \arrow[d, "\varphi"'] & V'' \arrow[r] & 0 \\ 0 \arrow[r] & W' \arrow[r] & W \arrow[r] & W'' \arrow[r] & 0 \end{tikzcd}$$

Задача 8.25 (лемма о змее). Напомним (см. n° 8.5), что *коядром* линейного отображения $\varphi : U \longrightarrow W$ называется фактор по его образу: $\operatorname{coker}\varphi = W/\operatorname{im}\varphi$. Постройте для диаграммы (8-27) с точными строками постройте длинную точную последовательность

$$\begin{tikzcd} 0 \arrow[r] & \ker\varphi' \arrow[r] & \ker\varphi \arrow[r] & \ker\varphi'' \arrow[dll] & \\ & \operatorname{coker}\varphi' \arrow[r] & \operatorname{coker}\varphi \arrow[r] & \operatorname{coker}\varphi'' \arrow[r] & 0\,. \end{tikzcd}$$

§9. Матрицы

9.1. Алгебры над полем. Векторное пространство A над полем $\Bbbk$ называется *алгеброй* над $\Bbbk$ (или $\Bbbk$-*алгеброй*), если на нём имеется операция умножения

$$A \times A \longrightarrow A\,,$$

такая что при каждом $a \in \Bbbk$ операторы левого и правого умножения на a

$$A \xrightarrow{v \mapsto av} A \quad \text{и} \quad A \xrightarrow{v \mapsto va} A \tag{9-1}$$

линейны. Алгебра A называется *ассоциативной*, если

$$(ab)c = a(bc) \quad \forall\, a, b, c \in A\,.$$

Алгебра называется *коммутативной*, если

$$ab = ba \quad \forall\, a, b \in A\,.$$

Алгебра, в которой имеется нейтральный элемент по отношению к умножению, т. е. такой $e \in A$, что $ea = ae = a$ для всех $a \in A$, называется *алгеброй с единицей* (а e называется *единицей*).

Упражнение 9.1. Покажите, что $0 \cdot a = 0$ для всех a в любой алгебре A и что единичный элемент единственен (если существует).

Линейность отображений (9-1) означает привычное правило раскрытия скобок:

$$(\lambda_1 a_1 + \mu_1 b_1)(\lambda_2 a_2 + \mu_2 b_2) = \lambda_1\lambda_2 a_1 a_2 + \lambda_1\mu_2 a_1 b_2 + \mu_1\lambda_2 b_1 a_2 + \mu_1\mu_2 b_1 b_2\,,$$

а также перестановочность умножения векторов на константы с умножением в алгебре:

$$(\lambda a)b = \lambda(ab) = a(\lambda b) \quad \forall\, \lambda \in \Bbbk \quad \text{и} \quad \forall\, a, b \in A\,.$$

Примерами *коммутативных* ассоциативных алгебр с единицами являются алгебра многочленов $\Bbbk[x_1, x_2, \dots, x_n]$ и прочие коммутативные $\Bbbk$-алгебры в смысле опр. 6.3. Модельным примером некоммутативной ассоциативной алгебры является алгебра $\mathrm{End}(V)$ линейных эндоморфизмов произвольного векторного пространства V.

9.1.1. Пример: композиция линейных операторов. Композиция

$$FG : U \longrightarrow W$$

линейных отображений $G : U \longrightarrow V$ и $F : V \longrightarrow W$ тоже является линейным отображением, поскольку

$$FG(\lambda u + \mu w) = F(\lambda G(u) + \mu G(w)) = \lambda FG(u) + \mu FG(w)\,,$$

и линейна по каждому из сомножителей при фиксированном втором:

$$(\lambda_1 F_1 + \lambda_2 F_2)G = \lambda_1 F_1 G + \lambda_2 F_2 G \quad \text{и} \quad F(\mu_1 G_1 + \mu_2 G_2) = \mu_1 F G_1 + \mu_2 F G_2 \,.$$

Если ограничиться линейными эндоморфизмами $\mathrm{End}(V) = \mathrm{Hom}(V, V)$ одного пространства V, то композиция будет определена для любых двух операторов $F, G \in \mathrm{End}(V)$, а тождественный оператор Id_V будет нейтральным элементом по отношению к композиции. Таким образом, $\mathrm{End}(V)$ является алгеброй с единицей.

Упражнение 9.2. Составьте таблицу умножения базисных операторов[1] $E_{ij} \in \mathrm{End}(\Bbbk^n)$ и покажите, что при $\dim V \geqslant 2$ композиция в $\mathrm{End}(\Bbbk^n)$ не коммутативна.

Поскольку композиция любых отображений между множествами ассоциативна (ибо $F(GH) = (FG)H : u \longmapsto F(G(H(u)))$ всякий раз, когда $F(G(H(u)))$ определено), алгебра линейных эндоморфизмов $\mathrm{End}(V)$ ассоциативна.

9.1.2. Обратимые элементы. Элемент a алгебры A с единицей $e \in A$ называется *обратимым*, если существует $a^{-1} \in A$, такой что $aa^{-1} = a^{-1}a = e$. В ассоциативной алгебре A это требование можно ослабить до существования отдельно левого и правого обратных к a элементов $a', a'' \in A$, таких что $a'a = aa'' = e$, поскольку в ассоциативной алгебре они автоматически совпадут друг с другом

$$a' = a'e = a'(aa'') = (a'a)a'' = ea'' = a''$$

(это же вычисление показывает, что обратный к a элемент единственен).

Согласно предл. 1.4 обратимыми элементами алгебры $\mathrm{End}(V)$ являются изоморфизмы $V \xrightarrow{\sim} V$. Они образуют группу преобразований пространства V (см. n° 1.6). Эта группа называется *полной линейной группой* пространства V и обозначается $\mathrm{GL}(V) \subset \mathrm{End}(V)$.

9.2. Умножение матриц.

9.2. Умножение матриц. Обозначим через

$$u_1, u_2, \dots, u_n \in \Bbbk^n \,, \;\; v_1, v_2, \dots, v_s \in \Bbbk^s \,, \;\; w_1, w_2, \dots, w_m \in \Bbbk^m \tag{9-2}$$

стандартные базисы этих координатных пространств и рассмотрим пару линейных операторов $\Bbbk^n \xrightarrow{B} \Bbbk^s$ и $\Bbbk^s \xrightarrow{A} \Bbbk^m$, матрицы которых в базисах (9-2) мы обозначим теми же буквами A и B. Матрица P их композиции

$$P = AB : U \longrightarrow W$$

называется *произведением* матриц A и B (сомножители стоят в том же порядке, что и операторы в композиции). Тем самым, для любой пары матриц

$$(a_{ik}) \in \mathrm{Mat}_{m\times s}(\Bbbk) \quad \text{и} \quad (b_{kj}) \in \mathrm{Mat}_{s\times n}(\Bbbk)$$

[1] напомним (см. предл. 7.1), что линейный оператор $E_{ij} : \Bbbk^n \longrightarrow \Bbbk^n$ переводит e_j в e_i, а все остальные стандартные базисные векторы — в нуль

(важно, что ширина первой матрицы совпадает с высотой второй) определена матрица-произведение $(p_{ij}) = (a_{ik}) \cdot (b_{kj}) \in \mathrm{Mat}_{m\times n}(\Bbbk)$, которая имеет столько же строк, сколько первый сомножитель, и столько же столбцов, сколько второй. Элемент p_{ij} в пересечении i-той строки и j-того столбца произведения равен коэффициенту при w_i в разложении

$$AB(u_j) = A\Big(\sum_k v_k b_{\nu j}\Big) = \sum_k A(v_k) b_{kj} = \sum_i \sum_k w_i a_{ik} b_{kj}\,, \quad \text{т. е.}$$
$$p_{ij} = \sum_k a_{ik} b_{kj} = a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots + a_{is}b_{sj}$$

Это правило для вычисления произведения двух матриц можно переформулировать несколькими эквивалентными способами, каждый из которых по-своему полезен при практических вычислениях.

Во-первых, произведение матриц полностью определяется правилом умножения строки ширины s на столбец высоты s:

$$(a_1, a_2, \dots, a_s) \cdot \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_s \end{pmatrix} = a_1 b_1 + a_2 b_2 + \cdots + a_s b_s\,,$$

и результат умножения матрицы A из m строк на матрицу B из n столбцов той же высоты, что ширина строк в A, — это таблица всех попарных произведений строк A на столбцы B:

$$p_{ij} = (a_{i1},\, a_{i2},\, \dots\,,\, a_{is}) \cdot \begin{pmatrix} b_{1j} \\ b_{2j} \\ \vdots \\ b_{sj} \end{pmatrix}$$

(в позиции (i,j) этой таблицы стоит произведение i-той строки A на j-тый столбец B).

Второе описание таково: в j-том столбце произведения AB стоит линейная комбинация s столбцов матрицы A (рассматриваемых как векторы координатного пространства $\Bbbk^m$), взятых с коэффициентами, стоящими в j-том столбце матрицы B. Если, к примеру, в матрице

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \end{pmatrix} \tag{9-3}$$

хочется написать вместо второго столбца сумму первого и третьего, а первый и третий столбец заменить на их суммы со вторым, умноженным, соответственно, на λ и на μ, после чего добавить к полученной матрице ещё один, четвёртый столбец, равный сумме столбцов матрицы A, умноженных на их номера, то это достигается умножением A справа на матрицу

$$\begin{pmatrix} 1 & 1 & 0 & 1 \\ \lambda & 0 & \mu & 2 \\ 0 & 1 & 1 & 3 \end{pmatrix}$$

Упражнение 9.3. Проверьте это прямым вычислением по первому способу.

Третье описание произведения двойственно второму и получается заменой слова «столбец» на слово «строка» во втором описании транспонированного произведения $(AB)^t = B^t A^t$

Упражнение 9.4. Убедитесь, что операция транспонирования матриц $A \mapsto A^t$ (см. n° 8.3.2) взаимодействует с умножением матриц по правилу $(AB)^t = B^t A^t$.

А именно, в i-той строке матрицы AB стоит линейная комбинация s строк матрицы B (рассматриваемых как векторы координатного пространства $\Bbbk^n$), взятых с коэффициентами, стоящими в i-той строке матрицы A. Например, если в той же матрице (9-3) хочется поставить вторую строку на место первой, а вместо второй написать её сумму с первой строкой, умноженной на λ, то это достигается умножением слева на матрицу

$$\begin{pmatrix} 0 & 1 \\ \lambda & 1 \end{pmatrix}$$

Упражнение 9.5. Проверьте это прямым вычислением по первому способу.

9.2.1. Алгебра матриц. Поскольку композиция операторов ассоциативна и линейна по каждому сомножителю, произведение матриц также ассоциативно и линейно по каждому сомножителю, т. е.

$$(FG)H = H(FG) \quad \forall\, F \in \mathrm{Mat}_{m\times k}\,,\ G \in \mathrm{Mat}_{k\times \ell}\,,\ H \in \mathrm{Mat}_{\ell\times n}$$
$$(\lambda_1 F_1 + \mu_1 G_1)(\lambda_2 F_2 + \mu_2 G_2) = \lambda_1\lambda_2 F_1 F_2 + \lambda_1\mu_2 F_1 G_2 + \mu_1\lambda_2 G_1 F_2 + \mu_1\mu_2 G_1 G_2$$

Таким образом, пространство $\mathrm{Mat}_n(\Bbbk) \stackrel{\text{def}}{=} \mathrm{Mat}_{n\times n}(\Bbbk) \simeq \mathrm{End}(\Bbbk^n)$ квадратных матриц размера $n \times n$ является ассоциативной $\Bbbk$-алгеброй с единицей

$$E = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & 1 \end{pmatrix}$$

(по диагонали стоят единицы, в остальных местах — нули).

При $n \geqslant 2$ алгебра $\mathrm{Mat}_n(\Bbbk)$ некоммутативна. Например,

$$\begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix} \cdot \begin{pmatrix} 3 & 0 \\ 4 & 5 \end{pmatrix} = \begin{pmatrix} 7 & 10 \\ 12 & 15 \end{pmatrix}$$
$$\begin{pmatrix} 3 & 0 \\ 4 & 5 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix} = \begin{pmatrix} 3 & 6 \\ 4 & 23 \end{pmatrix}$$

9.2.2. Аннулирующие многочлены. Любой элемент ξ любой ассоциативной $\Bbbk$-алгебры A с единицей определяет гомоморфизм вычисления

$$\mathrm{ev}_\xi : \Bbbk[t] \xrightarrow{x\mapsto\xi} A \tag{9-4}$$

который переводит многочлен $f(x) = a_0x^m + a_1x^{m-1} + \dots + a_{m-1}x + a_m$ в результат подстановки в него $x = \xi$

$$f(x) \longmapsto a(\xi) = a_0\xi^m + a_1\xi^{m-1} + \dots + a_{m-1}\xi + a_m$$

(свободный член a_m в правой части по определению понимается как $a_m\xi^0 = a_m \cdot e \in A$, где e — единица алгебры A).

Если гомоморфизм 9-4 инъективен, то элемент ξ называется *трансцендентным* над $\Bbbk$. Отметим, что в этом случае алгебра A обязательно бесконечномерна как векторное пространство над $\Bbbk$, поскольку все степени элемента ξ линейно независимы.

Если гомоморфизм 9-4 имеет ненулевое ядро, то элемент ξ называется *алгебраическим* над $\Bbbk$. В этом случае ядро $\ker \mathrm{ev}_\xi = (\mu_\xi)$ является главным идеалом в $\Bbbk[x]$ (ибо $\Bbbk[x]$ — это кольцо главных идеалов). Приведённый многочлен, порождающий этот идеал, называется *минимальным многочленом* элемента ξ и обозначается $\mu_\xi(x)$. Иначе минимальный многочлен можно охарактеризовать как многочлен наименьшей степени с единичным старшим коэффициентом, такой что $\mu_\xi(\xi) = 0$. Отметим, что все остальные многочлены, аннулирующие ξ, делятся на минимальный.

Сказанное применимо, в частности, к алгебрам $\mathrm{End}(V)$ и $\mathrm{Mat}_n(\Bbbk)$. Обе эти алгебры конечномерны как векторные пространства над $\Bbbk$ (если $\dim V < \infty$), и стало быть, любой оператор и любая матрица алгебраичны над $\Bbbk$. Если $\dim V = n$, то $\dim \mathrm{End}(V) = \dim \mathrm{Mat}_n(\Bbbk) = n^2$. Поэтому любой оператор и любая матрица аннулируются в этом случае многочленом степени не более n^2 (поскольку набор векторов ξ^0, ξ_1, … , ξ^{n^2} линейно зависим). В n° 11.3.1 мы увидим, что эта оценка сильно завышена, и всякий оператор на n-мерном пространстве, равно как и любая квадратная матрица размера $n\times n$, аннулируется некоторым многочленом степени n.

Например, произвольная 2×2-матрица $F = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ имеет

$$F^2 = \begin{pmatrix} a^2 + bc & ab + bd \\ ca + dc & cb + d^2 \end{pmatrix} = \begin{pmatrix} a^2 + bc & b(a + d) \\ c(a + d) & cb + d^2 \end{pmatrix}$$

откуда

$$F^2 - (a + d) \cdot F = \begin{pmatrix} a^2 + bc & b(a + d) \\ c(a + d) & cb + d^2 \end{pmatrix} - \begin{pmatrix} a(a + d) & b(a + d) \\ c(a + d) & d(a + d) \end{pmatrix} =$$

$$= \begin{pmatrix} (bc - ad) & 0 \\ 0 & (bc - ad) \end{pmatrix} = (bc - ad) \cdot E$$

Тем самым, F удовлетворяет квадратному уравнению

$$F^2 - (a+b)\,F + (ad-bc)\,E = 0\,. \tag{9-5}$$

9.2.3. Обратимые матрицы. Обратимые элементы алгебры $\mathrm{Mat}_n(\Bbbk)$ называются *обратимыми матрицами*. Это в точности матрицы линейных изоморфизмов координатного пространства $\Bbbk^n$, записанные в стандартном базисе. Группа обратимых матриц обозначается $\mathrm{GL}_n(\Bbbk) \subset \mathrm{Mat}_n(\Bbbk)$.

Для матриц размера 2×2, формула (9-5), будучи переписана как

$$(ad-bc)\,E = (a+b)\,F - F^2 = F\big((a+b)\,E - F\big)\,,$$

показывает, что при $(ad-bc)=0$ матрица F необратима, поскольку иначе, умножая обе части слева на F^{-1}, мы получаем

$$0 = (a+b)\,E - F = \begin{pmatrix} a+d & 0 \\ 0 & a+d \end{pmatrix} - \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

откуда $F=0$. А при $(ad-bc)\neq 0$ та же формула говорит, что матрица F обратима, и $F^{-1} = (ad-bc)^{-1}\big((a+b)\,E - F\big)$, т. е.

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = (ad-bc)^{-1}\begin{pmatrix} a & -b \\ -c & d \end{pmatrix} \tag{9-6}$$

Таким образом, при обращении матрицы размера 2×2 числа на её *главной* диагонали меняются местами, а числа на *побочной* диагонали меняют знак, после чего все четыре элемента матрицы делятся на $ad-bc$. Число $ad-bc$ называется *определителем* 2×2-матрицы F и обозначается $\det F$.

9.2.4. Обращение матриц методом Гаусса. Выяснить, обратима ли данная матрица $A \in \mathrm{Mat}_n(\Bbbk)$, и если да, то явно вычислить A^{-1}, можно умножая матрицу A слева на *заведомо обратимые* матрицы с таким расчётом, чтобы в результате линейных преобразований строк, которые матрица A при этом будет испытывать, в конце концов получилась либо единичная матрица, либо матрица с нулевой строкой или нулевым столбцом.

Если после k последовательных умножений слева на обратимые матрицы $S_1, S_2, \dots, S_k$ получится заведомо необратимая матрица $N = S_k S_{k-1} \cdots S_2 S_1 A$, то матрица A тоже не обратима, поскольку существование A^{-1} повлекло бы за собой существование $N^{-1} = A^{-1} S_1^{-1} S_2^{-1} \,\dots\, S_k^{-1}$.

Если же после k преобразований $S_1, S_2, \dots, S_k$ получится единичная матрица $S_k S_{k-1} \cdots S_2 S_1 A = E$, то умножая это равенство слева на $S_1^{-1} S_2^{-1} \,\dots\, S_k^{-1}$, мы приходим к соотношению $A = S_1^{-1} S_2^{-1} \,\dots\, S_k^{-1}$, из которого вытекает, что A обратима, и $A^{-1} = S_k S_{k-1} \cdots S_2 S_1 E$ получается применением к единичной матрице E ровно той же цепочки преобразований, которая позволила получить из матрицы A матрицу E.

Таким образом, если с самого начала преобразовывать $n \times 2n$-матрицу

$$\boxed{A|E}$$

(полученную простым приписыванием матрицы E справа к матрице A), то, получив в результате матрицу вида $\boxed{E|B}$, мы заключаем, что $A^{-1} = B$, а придя к матрице $\boxed{N|C}$, в которой N заведомо необратима, заключаем, что матрица A тоже необратима.

Поскольку все обратимые матрицы 2×2 нам известны, проще всего на каждом шагу изменять только какие-нибудь две строки матрицы A, а все остальные строки оставлять без изменения. Умножение пары строк ϱ_1 и ϱ_2 слева на обратимую матрицу $S = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ приведёт к замене этих строк на их линейные комбинации

$$\begin{pmatrix} \varrho_1 \\ \varrho_2 \end{pmatrix} \longmapsto \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \varrho_1 \\ \varrho_2 \end{pmatrix} = \begin{pmatrix} a\varrho_1 + b\varrho_2 \\ c\varrho_1 + d\varrho_2 \end{pmatrix}.$$

Подчеркнём, что $ad - bc$ должно быть отлично от нуля, т. е. коэффициенты используемых двух линейных комбинаций должны быть не пропорциональны.

Согласно второму описанию произведения матриц, чтобы осуществить написанное преобразование с i-той и j-той строкой матрицы $\boxed{A|E}$ мы должны умножить её слева на матрицу S', той же высоты, что и A, содержащую 2×2-подматрицу S в пересечениях i-той и j-той строк с i-тым и j-тым столбцами и имеющую $s'_{kk} = 1$ при $k \neq i, j$ и нули в остальных местах.

Классический метод Гаусса, описанный в n° 8.5, полностью укладывается в эту схему: три типа элементарных преобразований строк матрицы A из n° 8.5 реализуются умножением этих двух строк слева на обратимые 2×2 матрицы S соответствующих трёх типов:

1) $S = \begin{pmatrix} 1 & 0 \\ \lambda & 1 \end{pmatrix}$ с $S^{-1} = \begin{pmatrix} 1 & 0 \\ -\lambda & 1 \end{pmatrix}$ или $S = \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}$ с $S^{-1} = \begin{pmatrix} 1 & -\lambda \\ 0 & 1 \end{pmatrix}$;

2) $S = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ с $S^{-1} = S$;

3) $S = \begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}$ с $S^{-1} = \begin{pmatrix} \lambda^{-1} & 0 \\ 0 & \mu^{-1} \end{pmatrix}$, где $\lambda, \mu \in \Bbbk$ отличны от нуля.

Предложение 9.1
Приведение матрицы $\boxed{A|E}$ к строгому ступенчатому виду методом Гаусса позволяет за конечное число шагов либо найти A^{-1}, либо убедиться, что A необратима.

Доказательство. Итоговая строгая ступенчатая матрица будет содержать в левой половине либо единичную матрицу E, либо матрицу с нулевой нижней строкой. Матрица с нулевой нижней строкой необратима, поскольку образ отвечающего ей оператора не содержит последнего базисного вектора. □

Выясним, к примеру, обратима ли матрица

$$A = \begin{pmatrix} 6 & 3 & -2 & 1 \\ 1 & 4 & 1 & 1 \\ 1 & 1 & 3 & -1 \\ -1 & 0 & -2 & 1 \end{pmatrix}$$

Для этого припишем к ней справа единичную матрицу и применим метод Гаусса

$$\left(\begin{array}{rrrr|rrrr} 6 & 3 & -2 & 1 & 1 & 0 & 0 & 0 \\ 1 & 4 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 3 & -1 & 0 & 0 & 1 & 0 \\ -1 & 0 & -2 & 1 & 0 & 0 & 0 & 1 \end{array}\right)$$

меняем знак нижней строки, потом меняем её местами с верхней

$$\left(\begin{array}{rrrr|rrrr} 1 & 0 & 2 & -1 & 0 & 0 & 0 & -1 \\ 1 & 4 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 3 & -1 & 0 & 0 & 1 & 0 \\ 6 & 3 & -2 & 1 & 1 & 0 & 0 & 0 \end{array}\right)$$

зануляем первый столбец под первой строкой, отнимая из всех строк надлежащие кратности первой строки

$$\left(\begin{array}{rrrr|rrrr} 1 & 0 & 2 & -1 & 0 & 0 & 0 & -1 \\ 0 & 4 & -1 & 2 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 3 & -14 & 7 & 1 & 0 & 0 & 6 \end{array}\right)$$

меняем вторую и третью строки местами и зануляем нижние два элемента второго столбца

$$\left(\begin{array}{rrrr|rrrr} 1 & 0 & 2 & -1 & 0 & 0 & 0 & -1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & -5 & 2 & 0 & 1 & -4 & -3 \\ 0 & 0 & -17 & 7 & 1 & 0 & -3 & 3 \end{array}\right) \tag{9-7}$$

Теперь, чтобы избежать вычислений с дробями, отклонимся от классического метода Гаусса и умножим нижние две строки на матрицу[1]

$$\begin{pmatrix} -5 & 2 \\ -17 & 7 \end{pmatrix}^{-1} = \begin{pmatrix} 7 & -2 \\ 17 & -5 \end{pmatrix}$$

[1] что соответствует умножению всей матрицы слева на $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 7 & -2 \\ 0 & 0 & 17 & -5 \end{pmatrix}$

Получим

$$\left(\begin{array}{cccc|cccc} 1 & 0 & 2 & -1 & 0 & 0 & 0 & -1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 2 & -7 & 22 & 27 \\ 0 & 0 & 0 & 1 & 5 & -17 & 53 & 66 \end{array}\right)$$

Остаётся вычесть из 2-й строки 3-ю, а из 1-й — 4-ю и удвоенную 3-ю

$$\left(\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 1 & -3 & 9 & 11 \\ 0 & 1 & 0 & 0 & -2 & 7 & -21 & -26 \\ 0 & 0 & 1 & 0 & 2 & -7 & 22 & 27 \\ 0 & 0 & 0 & 1 & 5 & -17 & 53 & 66 \end{array}\right)$$

Итак, A обратима и

$$A^{-1} = \begin{pmatrix} 1 & -3 & 9 & 11 \\ -2 & 7 & -21 & -26 \\ 2 & -7 & 22 & 27 \\ 5 & -17 & 53 & 66 \end{pmatrix}$$

9.2.5. Пример: решение системы линейных уравнений. Система из n (неоднородных) линейных уравнений с n неизвестными

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = b_2 \\ a_{31}x_1 + a_{32}x_2 + \cdots + a_{3n}x_n = b_3 \\ \qquad\cdots\cdots\cdots\cdots\cdots \\ a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nn}x_n = b_n \end{cases}$$

в матричных обозначениях сворачивается до одного линейного уравнения

$$Ax = b$$

где $A = (a_{ij})$ есть матрицы коэффициентов, а x и b суть матрицы-столбцы размеров $n \times 1$, представляющие собою столбец переменных и столбец правых частей. Если матрица A обратима, то решение задаётся формулой

$$x = A^{-1}b$$

причём вместо поиска $A^{-1} = S_k S_{k-1} \cdots S_2 S_1$ методом Гаусса, можно искать решение конкретной системы: поскольку $A^{-1}b = S_k S_{k-1} \cdots S_2 S_1 b$ получается применением к столбцу b той же цепочки преобразований, что приводит от A к E, преобразовав по Гауссу $n \times (n+1)$-матрицу $\boxed{A \mid b}$ к виду $\boxed{E \mid s}$, мы получаем в правом столбце решение s. Однако, если требуется искать решения многих уравнений с одной и той же матрицей A и меняющимися правыми частями, то может оказаться выгоднее всё-таки вычислить A^{-1}, а потом находить решения умножая правые части на A^{-1}.

9.3. Матрицы перехода. Пусть некий вектор v линейно выражается через какие-то векторы w_i

$$v = \sum_{i=1}^{m} x_i w_i = w_1 x_1 + w_2 x_2 + \cdots + w_m x_m \,. \tag{9-8}$$

Организуем коэффициенты $x_i \in \Bbbk$ в матрицу-столбец размера $m \times 1$

$$x = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_m \end{pmatrix} \tag{9-9}$$

а векторы w_i — в матрицу-строку $w = (w_1, w_2, \ldots, w_m)$ размера $1 \times n$ с элементами $w_i \in V$. Тогда формула (9-8) свернётся в матричное равенство

$$v = wx \,,$$

в котором v рассматривается как матрица размера 1×1 с элементом из V. Такая матричная запись позволяет упростить многие вычисления, связанные с линейным выражением одних векторов через другие.

Пусть, например, заданы два набора векторов

$$u = (u_1, u_2, \ldots, u_n) \,, \quad w = (w_1, w_2, \ldots, w_m)$$

и пусть каждый из векторов u_j линейно выражен через векторы w_i

$$u_j = \sum_{\nu=1}^{m} c_{\nu j} w_\nu = w_1 \cdot c_{1j} + w_2 \cdot c_{2j} + \cdots + w_m \cdot c_{mj} \,.$$

Эти n равенств сокращённо записывается одной матричной формулой

$$u = w \cdot C_{wu} \,,$$

в которой $u = (u_1, u_2, \ldots, u_n)$, $w = (w_1, w_2, \ldots, w_m)$, а матрица

$$C_{wu} = (c_{ij}) = \begin{pmatrix} c_{11} & c_{12} & \ldots & c_{1n} \\ c_{21} & c_{22} & \ldots & c_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ c_{m1} & c_{m2} & \ldots & c_{mn} \end{pmatrix} \tag{9-10}$$

получается подстановкой в матрицу u вместо каждого из векторов u_j столбца коэффициентов его линейного выражения через векторы w_i.

Матрица (9-10) называется *матрицей перехода* от векторов u к векторам w. Отметим, что столбец (9-9) коэффициентов линейного выражения вектора

v через векторы u_j является частным случаем матрицы перехода: $x = C_{uv}$. Название «матрица перехода» вызвано тем, что C_{uw} позволяет переходить от линейных выражений векторов $v \in V$ через векторы u_j к их линейным выражениям через векторы w_i : $v = uC_{uv} \Rightarrow v = wC_{wu}C_{uv}$, т. е.

$$C_{wu}C_{uv} = C_{wv}\,. \tag{9-11}$$

Иными словами, произведение матрицы перехода от векторов u к векторам w и матрицы перехода от векторов v к векторам u является матрицей перехода от векторов v к векторам w.

Замечание 9.1. Если набор векторов $w = (w_1, w_2, \dots, w_m)$ линейно зависим, то каждый вектор v из их линейной оболочки допускает много *различных* линейных выражений[1] через векторы w_j. Поэтому обозначение C_{wv} не корректно в том смысле, что элементы матрицы C_{wv} определяются по векторам w и v не однозначно. Тем не менее, равенство (9-11) содержательно и означает, что имея какие-нибудь линейные выражения C_{wu} и C_{uv} векторов u через v и векторов v через w, мы можем предъявить явное линейное выражение C_{wv} векторов u через w *перемножив матрицы* C_{wu} и C_{uv}.

Если набор векторов $e = (e_1, e_2, \dots, e_n)$ является базисом, то матрица перехода C_{ew}, выражающая произвольный набор векторов $w = (w_1, w_2, \dots, w_m)$ через базис e, однозначно определяется по e и w, и два набора векторов u и w совпадают тогда и только тогда, когда совпадают матрицы перехода $C_{eu} = C_{ew}$ от них к базису e.

Лемма 9.1
Пусть набор векторов $e = (v_1, v_2, \dots, v_n)$ образует базис пространства V. Для того, чтобы набор векторов $u = vC_{vu}$ тоже составлял базис, необходимо и достаточно, чтобы матрица C_{vu} была обратима, и в этом случае $C_{vu}^{-1} = C_{uv}$.

Доказательство. Если u базис, то векторы e линейно выражается через u и по (9-11) выполнены равенства $C_{ee} = C_{eu}C_{ue}$ и $C_{uu} = C_{ue}C_{eu}$. Так как каждый набор векторов (в том числе, и базис) имеет единственное выражение через базис, $C_{ee} = C_{uu} = E$, откуда $C_{ue}C_{eu} = C_{ue}C_{eu} = E$. Наоборот, если u не базис, то это линейно зависимая система векторов, и $u\lambda = 0$ для некоторого *ненулевого* столбца коэффициентов λ. Тогда $eC_{eu}\lambda = 0$, откуда $C_{eu}\lambda = 0$. Такое равенство невозможно с обратимым C_{eu} и ненулевым λ, поскольку умножение обеих частей слева на C_{eu}^{-1} даёт $\lambda = 0$. □

9.3.1. Пример: замена координат при смене базиса. Пусть некий набор векторов $w = (w_1, w_2, \dots, w_m)$ выражаются через базис $e = (e_1, e_2, \dots, e_n)$ как

[1] как мы видели в n° 8.4.2 эти выражения представляют собою смежный класс подпространства линейных зависимостей $U \subset \Bbbk^m$ между векторами w_j

$w = eC_{ew}$. Если $v = eC_{ev}$ — другой базис, то в выражении $w = vC_{vw}$ векторов w через базис v матрица

$$C_{vw} = C_{ve}C_{ew} = C_{ev}^{-1}C_{vw}\,.$$

В частности столбец координат произвольного вектора w в базисе v получаются из столбца его координат в базисе e умножением слева на матрицу C_{ev}^{-1}, обратную к матрице координат векторов базиса v в базисе e.

9.3.2. Пример: замена матрицы оператора при смене базиса. Для произвольных линейного оператора $F : U \longrightarrow W$ и строки векторов

$$v = (v_1, v_2, \dots, v_r)$$

будем обозначать через $F(v)$ строку значений оператора F на этих векторах

$$F(v) \stackrel{\text{def}}{=} \big(F(v_1),\, F(v_2),\, \dots\,,\, F(v_r)\big)\,.$$

В силу линейности оператора F для любой числовой матрицы $M \in \mathrm{Mat}_{r\times s}(\Bbbk)$ выполняется равенство $F(vM) = F(v)M$.

Упражнение 9.6. Убедитесь в этом.

В таких обозначениях матрица F_{wu} оператора F, записанная в базисах u и w пространств U и W, однозначно определяется равенством[1] $F(u) = wF_{wu}$. При переходе к другим базисам $\widetilde{u} = uC_{u\widetilde{u}}$ и $\widetilde{w} = wC_{w\widetilde{w}}$ она меняется по правилу

$$F_{\widetilde{w}\widetilde{u}} = C_{w\widetilde{w}}^{-1}F_{wu}C_{u\widetilde{u}}\,. \tag{9-12}$$

ибо $F(\widetilde{u}) = F(uC_{u\widetilde{u}}) = F(u)\,C_{u\widetilde{u}} = w\,F_{wu}C_{u\widetilde{u}} = \widetilde{w}\,C_{\widetilde{w}w}F_{wu}C_{u\widetilde{u}} = \widetilde{w}\,C_{\widetilde{w}w}^{-1}F_{wu}C_{u\widetilde{u}}\,.$

В частности, если линейный эндоморфизм $F : V \longrightarrow V$ задаётся матрицей $F_e = F_{ee}$, j-тый столбец которой есть столбец координат $F(e_j)$ в *том же самом* базисе e, то при замене базиса e на базис $u = eC_{eu}$ матрица оператора F в новом базисе будет равна

$$F_u = C_{eu}^{-1}F_eC_{eu}\,. \tag{9-13}$$

9.4. Некоммутативные кольца. Абелева группа R с операцией умножения

$$R \times R \longrightarrow R$$

называется *кольцом*, если умножение ассоциативно, т. е.

$$f(gh) = (fg)h \quad \forall\, f,g,h \in R\,,$$

и двусторонне дистрибутивно, т. е. для любых $f,g,h \in R$

$$f(g+h) = fg + fh \quad \text{и} \quad (f+g)h = fh + gh\,.$$

[1] напомним (см. формулу (7-15) на стр. 113), что j-тый столбец матрицы F_{wu} есть столбец координат вектора $F(u_j)$ по базису w

Если в кольце R существует элемент e, такой что $ef = fe = f$ для всех $f \in R$, этот элемент называется *единицей* и кольцо называется *кольцом с единицей*.

Упражнение 9.7. Покажите, что $0 \cdot f = 0$ для всех f в любом кольце R и что единичный элемент единственен (если существует).

Всякая (некоммутативная) алгебра является одновременно (некоммутативным) кольцом, так что рассмотренные выше алгебра эндоморфизмов векторного пространства и алгебра матриц с элементами из поля доставляют примеры некоммутативных колец. Последний из них можно обобщить.

9.4.1. Матрицы над некоммутативным кольцом. Квадратные матрицы размера $n \times n$ с элементами из произвольного кольца R образуют кольцо $\mathrm{Mat}_n(R)$, сложение и умножение в котором задаются теми же правилами, что и сложение и умножение матриц с элементами из поля: сумма $S = F + G$ и произведение $P = FG$ матриц $F = (f_{ij})$ и $G = (g_{ij})$ имеют в качестве матричных элементов

$$s_{ij} = f_{ij} + g_{ij} \quad \text{и} \quad p_{ij} = \sum_{\nu} f_{i\nu} g_{\nu j}$$

Упражнение 9.8. Проверьте выполнение свойств ассоциативности и дистрибутивности для умножения матриц с элементами из произвольного кольца.

Замечание 9.2. Вычисления с матрицами, элементы которых лежат в некоммутативном кольце отличаются от вычислений с матрицами, элементы которых лежат в поле, двумя существенными особенностями: сомножители в произведениях нельзя переставлять друг с другом (последствие некоммутативности) и не на все ненулевые элементы можно делить (последствие того, что не все элементы кольца обратимы).

Например, формула (9-5) перестаёт быть верной над некоммутативным кольцом, поскольку при её выводе мы переставили сомножители, когда выделили на побочной диагонали матрицы F^2 общий множитель $(a + d)$ — над некоммутативным кольцом этот множитель, вообще говоря, не выносится.

Аналогично, критерий обратимости матрицы размера 2×2 и формула (9-6) для обратной матрицы над некоммутативным кольцом, вообще говоря, неверны, а над коммутативным кольцом, не являющимся полем, нуждаются в уточнении: 2×2-матрица над коммутативным кольцом обратима тогда и только тогда, когда её определитель $\det F$ обратим, и если это так, то имеет место формула (9-6) для обратной матрицы.

Упражнение 9.9. Докажите последнее утверждение.

9.4.2. Примеры обратимых матриц 2×2. Матрица вида

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$$

с элементами из произвольного (некоммутативного) кольца R обратима тогда и только тогда, когда обратимы её диагональные элементы. В самом деле, из равенства
$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \begin{pmatrix} x & y \\ z & w \end{pmatrix} = \begin{pmatrix} ax+bz & ay+bw \\ dz & dw \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$
вытекает, что $dw = 1$ и $dz = 0$, откуда d обратим, а $w = d^{-1}$ и $z = 0$. Поэтому $ax = 1$, откуда a обратим, а $x = a^{-1}$. Тогда в правом верхнем углу получаем соотношение $ay + bd^{-1} = 0$, из которого $y = -a^{-1}bd^{-1}$. Таким образом,
$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}^{-1} = \begin{pmatrix} a^{-1} & -a^{-1}bd^{-1} \\ 0 & d^{-1} \end{pmatrix}$$
Аналогичные рассуждения показывают, что обратимость матрицы вида
$$\begin{pmatrix} a & 0 \\ c & d \end{pmatrix}$$
равносильна обратимости диагональных элементов a, d, и в этом случае
$$\begin{pmatrix} a & 0 \\ c & d \end{pmatrix}^{-1} = \begin{pmatrix} a^{-1} & 0 \\ -d^{-1}ca^{-1} & d^{-1} \end{pmatrix}$$

Упражнение 9.10. Покажите, что матрицы $\begin{pmatrix} a & b \\ c & 0 \end{pmatrix}$ и $\begin{pmatrix} 0 & b \\ c & d \end{pmatrix}$ обратимы тогда и только тогда, когда обратимы оба элемента c и b, и в этом случае
$$\begin{pmatrix} a & b \\ c & 0 \end{pmatrix}^{-1} = \begin{pmatrix} 0 & c^{-1} \\ b^{-1} & -b^{-1}ac^{-1} \end{pmatrix} \quad \text{и} \quad \begin{pmatrix} 0 & b \\ c & d \end{pmatrix}^{-1} = \begin{pmatrix} -c^{-1}db^{-1} & c^{-1} \\ b^{-1} & 0 \end{pmatrix}$$

Из проделанных вычислений вытекает, что гауссовы элементарные преобразования строк:

1) прибавление к одной из строк другой, умноженной *слева* на любой элемент кольца

2) перемена двух строк местами

3) умножение строки *слева* на *обратимый* элемент кольца

задаются умножениями на обратимые матрицы и, стало быть, могут применяться для обращения матриц методом Гаусса над произвольным некоммутативным кольцом с единицей.

9.4.3. Пример: обратимость унитреугольных матриц. Диагонали

$$\begin{pmatrix} * & & \\ & * & \\ & & * \end{pmatrix} \quad \text{и} \quad \begin{pmatrix} & & * \\ & * & \\ * & & \end{pmatrix}$$

квадратной матрицы называются, соответственно, *главной* и *побочной*. Квадратная матрица называется *верхней* (соотв. *нижней*) *треугольной*, если у неё обращаются в нуль все элементы, стоящие под (соотв. над) *главной* диагональю.

Упражнение 9.11. Проверьте, что над любым (в том числе некоммутативным) кольцом R верхние и нижние треугольные матрицы составляют подкольца в $\mathrm{Mat}_n(R)$.

Если в кольце R есть единица, то треугольные матрицы с единицами на главной диагонали называются *унитреугольными*.

Лемма 9.2

Любая верхняя унитреугольная матрица $A = (a_{ij})$ над произвольным (в том числе, некоммутативным) кольцом с единицей обратима, причём $B = A^{-1}$ тоже верхняя унитреугольная с наддиагональными элементами

$$b_{ij} = -a_{ij} + \sum_{s=2}^{j-i} (-1)^s \sum_{i<\nu_1<\ldots\nu_{s-1}<j} a_{i\nu_1} a_{\nu_1\nu_2} \cdots a_{\nu_{s-1}j} \tag{9-14}$$

Доказательство. Прямое вычисление методом Гаусса. Для матрицы 4×4

$$A = \begin{pmatrix} 1 & a_{12} & a_{13} & a_{14} \\ 0 & 1 & a_{23} & a_{24} \\ 0 & 0 & 1 & a_{34} \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

оно выглядит так: приписываем справа единичную матрицу

$$\left(\begin{array}{cccc|cccc} 1 & a_{12} & a_{13} & a_{14} & 1 & 0 & 0 & 0 \\ 0 & 1 & a_{23} & a_{24} & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & a_{34} & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{array}\right)$$

зануляем 1-й столбец над главной диагональю используя 2-ю строку

$$\left(\begin{array}{cccc|cccc} 1 & 0 & a_{13} - a_{12}a_{23} & a_{14} - a_{12}a_{24} & 1 & -a_{12} & 0 & 0 \\ 0 & 1 & a_{23} & a_{24} & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & a_{34} & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{array}\right)$$

зануляем 2-й столбец над главной диагональю используя 3-ю строку

$$\left(\begin{array}{cccr|cccc} 1 & 0 & 0 & a_{14}-a_{12}a_{24}-a_{13}a_{34}+a_{12}a_{23}a_{34} & 1 & -a_{12} & -a_{13}+a_{12}a_{23} & 0 \\ 0 & 1 & 0 & a_{24}-a_{23}a_{34} & 0 & 1 & -a_{23} & 0 \\ 0 & 0 & 1 & a_{34} & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{array}\right)$$

наконец, зануляем последний столбец, используя 4-ю строку, получая справа

$$A^{-1} = \begin{pmatrix} 1 & -a_{12} & -a_{13}+a_{12}a_{23} & -a_{14}+a_{12}a_{24}+a_{13}a_{34}-a_{12}a_{23}a_{34} \\ 0 & 1 & -a_{23} & -a_{24}+a_{23}a_{34} \\ 0 & 0 & 1 & -a_{23} \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

В общем случае удобно нарисовать n различных точек $1, 2, \dots, n$ и воспринимать матричный элемент a_{ij} как стрелку, ведущую из j в i, а левое умножение на a_{ij} — как проход из j в i по этой стрелке. Тогда формула (9-14) гласит, что b_{ij} равен сумме всех маршрутов, ведущих из j в i, в которую все маршруты, состоящие из s стрелок, входит со знаком $(-1)^s$. По индукции, умножая $n \times (2n)$-матрицу $\boxed{A|E}$ слева на матрицу

$$S = \begin{pmatrix} 1 & b_{12} & b_{13} & \dots & b_{1\,(n-1)} & 0 \\ 0 & 1 & b_{23} & \dots & b_{2\,(n-1)} & 0 \\ & & \ddots & \ddots & \vdots & \vdots \\ 0 & \dots & 0 & 1 & b_{(n-2)\,(n-1)} & 0 \\ 0 & \dots & \dots & 0 & 1 & 0 \\ 0 & \dots & \dots & \dots & 0 & 1 \end{pmatrix}$$

в левом верхнем углу которой стоит матрица размера $(n-1)\times(n-1)$, обратная к верхней левой угловой подматрице в A, образованной первыми $(n-1)$ строками и столбцами, мы получим в последнем n-том столбце левой половины матрицы

$$S \cdot \boxed{A|E}$$

в позиции (i, n) сумму $a_{1n} + b_{12}a_{2n} + b_{13}a_{3n} + \cdots + b_{1\,(n-1)}a_{(n-1)\,n}$ всех маршрутов, ведущих из n в i, в которую каждый маршрут длины s входит со знаком $(-1)^{s-1}$. Обнуляя этот столбец методом Гаусса, получаем в n-м столбце правой половины матрицы требуемые значения b_{in}. □

Задачи для самостоятельного решения к §9

Задача 9.1. Найдите все матрицы, коммутирующие а) с матрицей $\begin{pmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{pmatrix}$ б) со всеми $n \times n$-матрицами.

Задача 9.2. Пусть матрица A диагональна, и все её диагональные элементы различны. Покажите, что любая матрица, коммутирующая с A, имеет вид $f(A)$, где $f(x) \in \Bbbk[x]$ — некоторый многочлен (ср. с зад. 9.8 ниже).

Задача 9.3. На побочной диагонали $n \times n$-матрицы A стоят числа $\cos(2\pi/a_k) + i\,\sin(2\pi/a_k)$ с некими $a_1, a_2, \dots, a_n \in \mathbb{N}$, в остальных местах — нули. Найдите наименьшее m, такое что $A^m = E$.

Задача 9.4. Найдите в $\mathrm{Mat}_2(\Bbbk)$ все решения уравнений
а) $X^2 = 0$ б) $X^3 = 0$ в) $X^2 = X$ г) $X^2 = E$ д) $X^2 = -E$.

Задача 9.5. Покажите, что любая квадратная матрица A удовлетворяет полиномиальному уравнению вида $A^m + a_1 A^{m-1} + \dots + a_{m-1}A + a_m E = 0$, где $a_i \in \Bbbk$.

Задача 9.6. Покажите, что всякая матрица $A \in \mathrm{Mat}_2(\Bbbk)$ удовлетворяет квадратному уравнению.

Задача 9.7. Покажите, что всякая матрица ранга 1 пропорциональная своему квадрату.

Задача 9.8 (минимальный многочлен матрицы). Для для каждого многочлена $f = a_0 x^n + a_1 x^{n-1} + \dots + a_{n-1}x + a_n \in \Bbbk[x]$ положим $f(A) = a_0 A^n + a_1 A^{n-1} + \dots + a_{n-1}A + a_n E$, и обозначим через $\Bbbk[A] \subset \mathrm{Mat}_n(\Bbbk)$ образ гомоморфизма вычисления

$$\mathrm{ev}_A : \Bbbk[x] \xrightarrow{f \mapsto f(A)} \mathrm{Mat}_n(\Bbbk)$$

Приведённая образующая главного идеала $\ker \mathrm{ev}_A \subset \Bbbk[x]$ называется *минимальным многочленом* матрицы A и обозначается $\mu_A(x)$. а) Укажите хоть одну матрицу $A \in \mathrm{Mat}_2(\mathbb{Z})$ с $\mu_A(x) = x^2 - 2$ и покажите, что $\mathbb{Q}[A]$ является полем.
б) Подберите $A \in \mathrm{Mat}_2(\mathbb{R})$ с $\mathbb{R}[A] \simeq \mathbb{C}$ и явно опишите все матрицы, из которых состоит это поле.
в) Найдите минимальный многочлен матрицы

$$E = \begin{pmatrix} 0 & 0 & \dots & 0 & -a_n \\ 1 & 0 & \dots & 0 & -a_{n-1} \\ 0 & 1 & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & -a_2 \\ 0 & \dots & 0 & 1 & -a_1 \end{pmatrix}$$

г) Покажите, что $\dim \Bbbk[A] \leqslant n$.

Задача 9.9. Докажите следующие неравенства на ранги матриц A, B и C размеров $k \times \ell$, $\ell \times m$ и $m \times n$ соответственно: а) $\mathrm{rk}\,(AB) \leqslant \min(\mathrm{rk}\,A, \mathrm{rk}\,B)$
б) $\mathrm{rk}\,(AB) + \mathrm{rk}\,(BC) \leqslant \mathrm{rk}\,(ABC) + \mathrm{rk}\,(B)$ в) $\mathrm{rk}\,(A) + \mathrm{rk}\,(B) \leqslant \mathrm{rk}\,(AB) + \ell$

Задача 9.10. Имеются семь одинаковых банок, каждая из которых на $\frac{9}{10}$ заполнена краской одного из семи цветов радуги (в каждой банке – свой цвет и все цвета разные). Можно ли переливая краску из банки в банку (и равномерно размешивая содержимое) получить хотя бы в одной из банок колер, в котором все семь красок смешаны в равной пропорции?

Задача 9.11 (коммутаторы). Разность $[A,B] = AB - BA$ называется *коммутатором* квадратных матриц $A, B \in \mathrm{Mat}_n(k)$. Докажите, что для любых A, B, C имеют место следующие два *правила Лейбница*: а) $[A, BC] = [A,B]C + B[A,C]$ б) $[A,[B,C]] = [[A,B],C] + [B,[A,C]]$.

Задача 9.12. Выразите $(A+B)^n$ через A^iB^j, если а) $[A,B]=0$; б*) $[A,B]=B$; в*) $[A,B]=A$.

Задача 9.13 (след). Сумма $\mathrm{tr}\,A = \sum a_{ii}$ стоящих на главной диагонали элементов квадратной матрицы A называется *следом* этой матрицы. Покажите, что
а) след коммутатора $\mathrm{tr}\,[A,B] = 0\ \forall\, A, B \in \mathrm{Mat}_n(\Bbbk)$
б) $\mathrm{tr}\,(C^{-1}AC) = \mathrm{tr}\,(A)$ для любых $A \in \mathrm{Mat}_n(\Bbbk)$ и $C \in \mathrm{GL}_n(\Bbbk)$ (в частности, след матрицы $F_e = F_{ee}$ линейного эндоморфизма $F : V \longrightarrow V$ не зависит от выбора базиса e, в котором записывается эта матрица)
в) если $\mathrm{tr}\,(AX) = 0$ для любой квадратной матрицы X с нулевым следом, то $A = \lambda E$ для некоторого $\lambda \in \Bbbk$.

Задача 9.14 (нильпотентные матрицы). Ненулевая матрица $A \in \mathrm{Mat}_n(\Bbbk)$ называется *нильпотентной*, если $A^n = 0$ для некоторого $n \in \mathbb{N}$. Покажите, что
а) если A нильпотентна, то обе матрицы $E \pm A$ обратимы
б) сумма нильпотентных матриц A и B не обязательно нильпотентна
в) $A+B$ нильпотентна для нильпотентных A и B с $[A,B]=0$
г*) $A+B$ нильпотентна для нильпотентных A и B с $[A,[A,B]] = [B,[B,A]] = 0$.

Задача 9.15. Пусть A нильпотентна. Покажите, что матрицы вида $f(A)$, где $f \in x \cdot \Bbbk[[x]]$ пробегает ряды без свободного члена, образуют абелеву группу с операцией $f(A) * g(A) \overset{\text{def}}{=} f(A) + g(A) - f(A)g(A)$.

Задача 9.16 (унипотентные матрицы). Матрица $A \in \mathrm{Mat}_n(\Bbbk)$ над называется *унипотентной*, если $A = E + N$, где N нильпотентна. Покажите, что а) над полем положительной характеристики унипотентность матрицы A равносильна тому, что $A \neq E$, но $A^n = E$ для некоторого $n \in \mathbb{N}$ б) над полем характеристики нуль унипотентность матрицы A равносильна тому, что $A = e^N = \sum\limits_{k \geqslant 0} N^k/k!$, где N нильпотентна[1].

Задача 9.17. Докажите, что подстановка фиксированной матрицы $A \in \mathrm{Mat}_n(\mathbb{C})$ в степенные ряды задаёт гомоморфизм из подкольца $\mathbb{C}[[z]]$, состоящего из абсолютно сходящихся рядов, в кольцо $\mathbb{C}[A]$, причём для любого абсолютно сходящегося ряда F существует многочлен $f_{F,A}(z) \in \mathbb{C}[z]$ степени $\leqslant (n-1)$, такой что $f_{F,A}(A) = F(A)$.

[1] тем не менее, мы полагаем, что $N^0 \overset{\text{def}}{=} E$

Задача 9.18. Пусть $W = V \oplus V$ и $\dim V = n$. Покажите, что

а) $\mathrm{End}(W) \simeq \mathrm{Mat}_{2\times 2}(\mathrm{End}(V))$.

б) если $A, B, C, D \in \mathrm{Mat}_n(\Bbbk)$, A обратима, и ранг $(2n)\times(2n)$-матрицы $\begin{pmatrix} A & B \\ C & D \end{pmatrix}$ равен рангу матрицы A, то $D = CA^{-1}B$

в) если все четыре матрицы $A, B, C, D \in \mathrm{Mat}_n(\Bbbk)$ обратимы, то матрицы

$$A - BD^{-1}C\,, \quad C - DB^{-1}A\,, \quad B - AC^{-1}D\,, \quad D - CA^{-1}B$$

тоже обратимы и

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix}^{-1} = \begin{pmatrix} (A - BD^{-1}C)^{-1} & (C - DB^{-1}A)^{-1} \\ (B - AC^{-1}D)^{-1} & (D - CA^{-1}B)^{-1} \end{pmatrix}$$

Задача 9.19 (локально конечные чумы). Напомним (см. зад. 1.18), что множество $\mathfrak{P}$ называется *частично упорядоченным* (сокращённо чумом) если на нём задано бинарное отношение $x \leqslant y$, которое рефлексивно[1], транзитивно[2] и *кососимметрично*: из $x \leqslant y$ и $y \leqslant x$ следует, что $x = y$. чум $\mathfrak{P}$ называется *локально конечным*, если $\forall\ x, y \in \mathfrak{P}\times\mathfrak{P}$ множество $[x, y] \stackrel{\text{def}}{=} \{\, z \mid x \leqslant z \leqslant y \,\}$ конечно. Покажите, что следующие множества являются локально конечными чумами:

а) $\mathbb{N}$ с отношением $n|m$

б) конечные подмножества произвольного множества X с отношением $X \subseteq Y$

Задача 9.20 (обращение Мёбиуса). Для локально конечного чума $\mathfrak{P}$ обозначим через $\mathscr{A}(\mathfrak{P})$ множество всех функций $\varrho(x, y) : \mathfrak{P}\times\mathfrak{P} \longrightarrow \mathbb{R}$, обращающихся в нуль на всех парах (x, y), не находящихся в отношении $x \leqslant y$, и зададим на нём *сложение* и *умножение* формулами

$$\varrho_1 + \varrho_2 \,:\, (x, y) \longmapsto \varrho_1(x, y) + \varrho_2(x, y)$$
$$\varrho_1 * \varrho_2 \,:\, (x, y) \longmapsto \sum_{x \leqslant z \leqslant y} \varrho_1(x, z)\varrho_2(z, y)$$

Покажите, что а) $\mathscr{A}(\mathfrak{P})$ является (некоммутативным) кольцом с единицей

б) функция $\varrho \in \mathscr{A}(\mathfrak{P})$ тогда и только тогда обладает двусторонней обратной, когда $\varrho(x, x) \neq 0 \quad \forall\, x \in \mathfrak{P}$

в) функция $\mu(x, y)$, двусторонне обратная к функции

$$\zeta(x, y) \stackrel{\text{def}}{=} \begin{cases} 1 \text{ при } x \leqslant y \\ 0 \text{ в остальных случаях} \end{cases}$$

может вычислена по любой из следующих двух формул[3]

$$\mu(x, y) = -\sum_{x \leqslant z < y} \mu(x, z) = -\sum_{x < z \leqslant y} \mu(z, y)$$

---

[1] т. е. $x \leqslant x\ \forall x$

[2] т. е. из $x \leqslant y$ и $y \leqslant z$ следует, что $x \leqslant z$

[3] запись $x < y$ означает, что $x \leqslant y$ и $x \neq y$

(μ называется *функцией Мебиуса* ЧУМа $\mathfrak{P}$).
г) Явно опишите функцию Мебиуса для ЧУМа $\mathbb{N}$ с отношением $x|y$.
д) Пусть для функции $g : \mathfrak{P} \xrightarrow{g} \mathbb{R}$ известны значения всех сумм

$$\sigma(x) = \sum_{y<x} g(y)\,.$$

Покажите, что g восстанавливается из σ по формуле

$$g(x) = \sum_{y<x} \sigma(y)\mu(y,x)\,.$$

е) Явно опишите функцию Мёбиуса для ЧУМа всех подмножеств данного n-элементного множества X с отношением $X \subset Y$ и убедитесь, что предыдущая формула обращения есть не что иное как «формула включения-исключения» (другие примеры функций и обращения Мёбиуса встречались нам в зад. 3.20, зад. 4.22 (в), зад. 4.28 и зад. 4.31).

§10. Определители

10.1. Объём. Интуитивным геометрическим критерием линейной зависимости набора векторов $v_1, v_2, \ldots, v_n$ в n-мерном векторном пространстве V является обращение в нуль *объёма* параллелепипеда, для которого эти векторы составляют множество рёбер, исходящих из одной вершины (см. рис. 10◇1).

Не ставя себе задачу определить объём сколь-нибудь общей фигуры, отметим, что объём параллелепипеда, как бы он ни определялся, должен обладать по крайней мере следующими двумя геометрическими свойствами: во-первых, он не должен меняться при «параллельном перекосе» параллелепипеда в любой плоскости вдоль любой из сторон, если при этом сохраняется высота, как на рис. 10◇2 (ибо «отрезаемый» при этом кусок параллельно переносится и «приставляется» с другой стороны); во-вторых при растяжении одной из сторон параллелепипеда в λ раз объём должен умножаться на λ (например, при удвоении любой стороны объём удваивается). Покажем, что эти свойства определяют объём параллелепипеда однозначно с точностью до постоянного множителя.

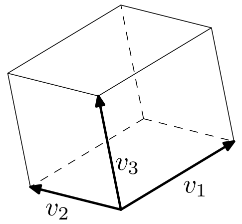


Рис. 10◇1.

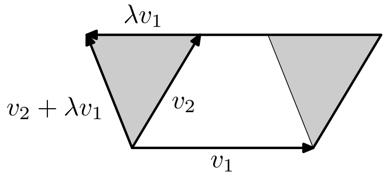


Рис. 10◇2.

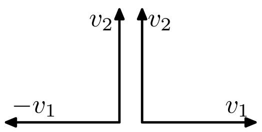


Рис. 10◇3.

Определение 10.1

Функция $\omega : V_1 \times V_2 \times \cdots \times V_n \longrightarrow \Bbbk$, сопоставляющая каждому упорядоченному набору векторов $(v_1, v_2, \ldots, v_n)$ n-мерного векторного пространства V число $\omega(v_1, v_2, \ldots, v_n) \in \Bbbk$, называется *формой объёма* (или просто *объёмом*) на пространстве V, если она удовлетворяет следующим двум свойствам:

1) при добавлений к одному из аргументов произвольной кратности любого другого аргумента объём не меняется:

$$\omega(\ldots, v_i + \lambda v_j, \ldots, v_j, \ldots,) = \omega(\ldots, v_i, \ldots, v_j, \ldots,)$$

2) при умножении одного из аргументов на число объём умножается на это число: $\omega(v_1, \ldots, v_{i-1}, \lambda \cdot v_i, v_{i+1}, \ldots, v_n) = \lambda \cdot \omega(v_1, \ldots, v_{i-1}, v_i, v_{i+1}, \ldots, v_n)$.

10.1.1. Комментарий к определению. Главным отличием определённой выше формы объёма от понятия объёма, принятого в школьном курсе геометрии, является следующее свойство, заложенное нами в (2): при замене любого из векторов на противоположный объём умножается на -1. Над полем вещественных чисел $\mathbb{R}$ это означает, что форма объёма, удовлетворяющая n° 10.1 учитывает не только абсолютную величину объёма, но и *ориентацию* набора векторов (см. рис. 10◇3): при замене упорядоченной пары векторов (v_1, v_2) парой $(-v_1, v_2)$ кратчайший угол поворота от первого вектора ко второму меняет свой знак на противоположный, как и наша форма объёма. Над произвольным полем говорить про знаки чисел нет смысла, и следствием условий (1) и (2) будет *кососимметричность* объёма: он умножается на -1 при перемене между собою местами любых двух векторов (см. лем. 10.1 ниже).

Из свойства (2) также вытекает, что объём зануляется, если один из векторов нулевой: $\omega(\,\dots, 0, \dots) = \omega(\,\dots, 0\cdot 0, \dots) = 0\cdot\omega(\,\dots, 0, \dots) = 0$. Поэтому объём линейно зависимой системы векторов равен нулю: скажем, если

$$v_1 = \lambda_2 v_2 + \cdots + \lambda_n v_n\,,$$

то $\omega(v_1, v_2, \dots, v_n) = \omega(v_1 - \lambda_2 v_2 - \cdots - \lambda_n v_n,\, v_2, \dots, v_n) = \omega(0, v_2, \dots, v_n) = 0$. В частности, объём обращается в нуль если какие-то два аргумента совпадают.

Определение 10.2
Функция $\eta : V_1 \times V_2 \times \cdots \times V_m \longrightarrow \Bbbk$, сопоставляющая каждому упорядоченному набору из m векторов[1] число $\eta(v_1, v_2, \dots, v_n) \in \Bbbk$, называется *полилинейной кососимметричной формой* от m векторов (или, короче, *кососимметричной m-формой* на V), если η линейна по каждому своему аргументу (при фиксированных остальных) и меняет знак при перестановке любых двух своих аргументов местами.

Лемма 10.1
Объём является полилинейной кососимметричной формой от $n = \dim V$ аргументов.

Доказательство. Для доказательства линейности

$$\omega(\,\dots, \lambda v + \mu w, \dots) = \lambda\,\omega(\,\dots, v, \dots) + \mu\,\omega(\,\dots, w, \dots) \tag{10-1}$$

заметим, что если оба набора аргументов в правой части линейно зависимы, то набор аргументов в левой части тоже линейно зависим, и стало быть, обе части равенства нулевые. Поэтому мы можем считать, что аргументы первого слагаемого правой части образуют базис пространства V. Выразив w через этот базис, мы представим его в виде $w = \varrho v + u$, где u является линейной комбинацией остальных $(n-1)$ аргументов. По первому свойству объёма левая часть (10-1) равна

$$\omega(\,\dots, \lambda v + \mu w, \dots) = \omega(\,\dots, (\lambda + \mu\varrho)v + \mu u, \dots) = \omega(\,\dots, (\lambda + \mu\varrho)v, \dots)\,,$$

а второе слагаемое правой части (10-1) равно

$$\mu\omega(\,\dots, w, \dots) = \mu\omega(\,\dots, \varrho v + u, \dots) = \mu\omega(\,\dots, \varrho v, \dots)\,.$$

[1] подчеркнём, что в этом определении m может отличаться от $\dim V = n$

Тем самым, по второму свойству объёма, правая часть

$$\lambda\omega\,(\,\dots\,,\,v,\,\dots)+\mu\omega\,(\,\dots\,,\,\varrho v,\,\dots)=(\lambda+\varrho\mu)\,\omega\,(\,\dots\,,\,v,\,\dots)$$

совпадает с левой. Для доказательства соотношения кососимметричности:

$$\omega(\dots,v,\,\dots,w,\,\dots)=-\omega(\dots,w,\,\dots,v,\,\dots) \tag{10-2}$$

применим к левой части три элементарных преобразования первого типа: сначала прибавим w к v, потом отнимем $v+w$ из w, потом прибавим $-v$ к $v+w$:

$$\begin{aligned}\omega(\dots,v,\,\dots,w,\,\dots)&=\omega(\dots,v+w,\,\dots,w,\,\dots)=\\&=\omega(\dots,v+w,\,\dots,-v,\,\dots)=\omega(\dots,w,\,\dots,-v,\,\dots)\,.\end{aligned}$$

По второму свойству объёма это совпадает с правой частью (10-2). □

10.2. Отступление: знак перестановки. Назовём перестановку между собою каких-нибудь двух элементов из некоего упорядоченного набора *транспозицией* этих двух элементов. Легко видеть, что любая перестановка является композицией транспозиций.

Упражнение 10.1. Убедитесь в этом.

Перестановки, представимые в виде композиции чётного числа транспозиций, называются *чётными*, а перестановки, раскладывающиеся в композицию нечётного числа транспозиций — *нечётными*.

Отметим, что каждая перестановка имеет *много различных* разложений в композицию транспозиций. Например, перестановку $(3,2,1)$ чисел $(1,2,3)$ можно получить как $\sigma_{12}\sigma_{23}\sigma_{12}$ и как $\sigma_{23}\sigma_{12}\sigma_{23}$, где мы обозначаем через σ_{ij} транспозицию i-того и j-того (считая слева) символов набора. Таким образом, вовсе не очевидно, что множества чётных и нечётных перестановок не пересекаются.

Покажем, что никакая перестановка не может быть чётной и нечётной одновременно. Для этого мы укажем способ определения чётности перестановки, не использующий её разложения в композицию транспозиций. Будем интерпретировать перестановки как элементы *симметрической группы* S_n всех биективных отображений из n-элементного множества $\{1,\,2,\,\dots\,,\,n\}$ в себя, как в n° 1.6.1 (см. стр. 18). Напомним, что при такой интерпретации биективному отображению $g:\{1,\,2,\,\dots\,,\,n\}\longrightarrow\{1,\,2,\,\dots\,,\,n\}$ отвечает перестановка $(g_1,g_2,\dots,g_n)$, на i-том месте которой стоит значение $g_i=g(i)$ отображения g.

Назовём упорядоченную пару чисел (i,j), в которой $1\leqslant i<j\leqslant n$, *инверсной парой* перестановки $g\in S_n$, если $g(i)>g(j)$. Таким образом, каждая перестановка g разбивает $\binom{n}{2}$-элементное множество всех пар

$$\{i<j\}\subset\{1,\,2,\,\dots\,,\,n\}$$

на два непересекающихся подмножества — инверсные пары и неинверсные пары. Это разбиение зависит только от g и «ничего не знет» про разложения g в произведения транспозиций.

Покажем, что чётность числа инверсных пар каждой перестановки совпадает с чётностью количества транспозиций, на которые её можно разложить. Для начала проверим, что для любой перестановки g и транспозиции σ_{ij} i-того и j-того (считая слева) элементов набора чётность числа инверсных пар у перестановок g и $\sigma_{ij}\circ g$ различна. Перестановки g и $\sigma_{ij}\circ g$ отличаются друг от друга перестановкой элементов $g_i = g(i)$ и $g_j = g(j)$, стоящих на i-том и j-том местах в словах

$$\begin{aligned} g &= (g_1, \dots, g_{i-1}, \boldsymbol{g_i}, g_{i+1}, \dots, g_{i-1}, \boldsymbol{g_j}, g_{j+1}, \dots, g_n) \\ \sigma_{i,j}\circ g &= (g_1, \dots, g_{i-1}, \boldsymbol{g_j}, g_{i+1}, \dots, g_{i-1}, \boldsymbol{g_i}, g_{j+1}, \dots, g_n) . \end{aligned} \tag{10-3}$$

Упражнение 10.2. Проверьте, что у двух перестановок (10-3) инверсность пары (i, j), а также $2(j-i-1)$ пар вида (i, m) и (m, j) с произвольным m из промежутка $i < m < j$ противоположна[1], а инверсность всех остальных пар одинакова.

Из упражнения вытекает, то взятие композиции с транспозицией меняет чётность числа инверсных пар. Таким образом, если перестановка g разложена в композицию транспозиций, то чётность числа инверсных пар в ней отличается от чётности числа инверсных пар в тождественной перестановке в точности на чётность количества транспозиций, в которую разложилась g, и, тем самым, не зависит от способа разложения g в композицию транспозиций.

Теорема 10.1 (знак перестановки)
Существует единственный гомоморфизм из группы перестановок в мультипликативную группу знаков $\mathrm{sgn} : S_n \longrightarrow \{\pm 1\}$, такой что $\mathrm{sgn}(\mathrm{Id}) = 1$ и $\mathrm{sgn}(\sigma_{ij}) = -1$ для любой транспозиции $\sigma_{ij} \in S_n$.

Доказательство. Так как любая перестановка является произведением транспозиций, знак всех чётных перестановок должен быть равен $+1$, а знак всех нечётных -1. Поскольку множества чётных и нечётных перестановок не пересекаются, это правило корректно определяет отображение из S_n в группу знаков. Гомоморфность этого отображения, т. е. соотношение

$$\mathrm{sgn}(g_1 g_2) = \mathrm{sgn}(g_1)\,\mathrm{sgn}(g_2) ,$$

вытекает из того, что композиция перестановок одинаковой чётности чётна, а противоположной чётности — нечётна. □

10.2.1. Пример: правило ниточек. Интерпретация чётности перестановки как чётности числа инверсных пар даёт конкретный способ отыскания чётности, в некоторых случаях оказывающийся полезным. Напишем друг под другом исходные числа $1, 2, \dots, n$ и их перестановку $g = (g_1, g_2, \dots, g_n)$, после чего соединим одинаковые числа нитями так, чтобы ни одна из нитей не вылезала

[1] т. е. если были инверсными в g, то являются неинверсными в $g\circ\langle i, j\rangle$ и наоборот, если были неинверсными в g, то стали инверсными в $g\circ\langle i, j\rangle$

за пределы четырёхугольника $1\,n\,g_n\,g_1$ (см. рис. 10◇4) и чтобы все точки пересечения нитей были простыми двойными[1]. Тогда чётность числа инверсных пар будет равна чётности числа точек пересечения нитей.

Упражнение 10.3. Докажите это и найдите при помощи правила ниточек чётность *тасующей перестановки* $(i_1, i_2, \dots, i_k, j_1, j_2, \dots, j_m)$, в которой наборы номеров $\{i_\nu\}, \{j_\mu\} \subset \{1, 2, \dots, n\}$ не пересекаются, и каждый из них строго возрастают слева направо.

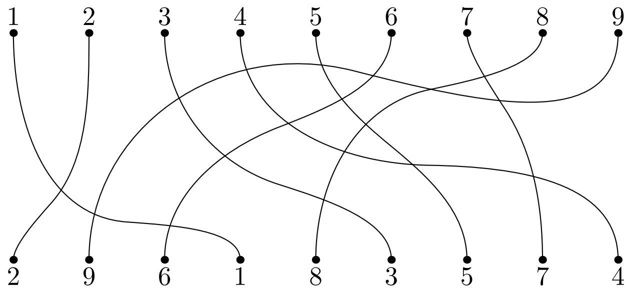


Рис. 10◇4. $\mathrm{sgn}(2, 9, 6, 1, 8, 3, 5, 7, 4) = +1$ (всего 18 пересечений)

Теорема 10.2

На каждом ненулевом векторном пространстве V существует единственная с точностью до пропорциональности ненулевая форма объёма ω. Если векторы $e_1, e_2, \dots, e_n$ образуют базис V, то объём произвольного набора векторов

$$(v_1, v_2, \dots, v_n) = (e_1, e_2, \dots, e_n)\, C\,, \quad \text{где } C = (c_{ij}) \in \mathrm{Mat}_n(\Bbbk)\,,$$

выражается через объём базиса по формуле

$$\omega(v_1, v_2, \dots, v_n) = \omega(e_1, e_2, \dots, e_n) \cdot \det C\,, \quad \text{где} \tag{10-4}$$

$$\det C = \sum_{g \in S_n} \mathrm{sgn}(g) \cdot c_{g_1 1} c_{g_2 2} \cdots c_{g_n n} \tag{10-5}$$

(число $\det C \in \Bbbk$ называется *определителем* матрицы C).

Доказательство. Формулы (10-4), (10-6) являются частным случаем более общего факта, справедливого для кососимметрических форм от любого числа переменных.

Лемма 10.2

Пусть набор векторов $w = (w_1, w_2, \dots, w_m)$ линейно выражается через набор векторов $v = (v_1, v_2, \dots, v_m)$ как $v = wC$, где $C = (c_{ij}) \in \mathrm{Mat}_m(\Bbbk)$. Тогда значения любой кососимметричной m-формы ω на векторах v и w связаны соотношением $\omega(w_1, w_2, \dots, w_m) = \omega(v_1, v_2, \dots, v_m) \cdot \det C$.

[1] это означает, что в каждой точке пересечения встречается ровно две нити, причём пересечение происходит трансверсально: , а не по касательной:

Доказательство. Подставим в $\omega(w_1, w_2, \dots, w_m)$ вместо каждого аргумента его разложение $w_j = g_{1j}v_1 + g_{2j}v_2 + \cdots + g_{mj}v_m$ и воспользуемся линейностью объёма по каждому из аргументов:

$$\omega(w_1, w_2, \dots, w_m) = \omega\Big(\sum_{\nu_1} c_{\nu_1 1} v_{\nu_1}\,,\ \sum_{\nu_2} c_{\nu_2 2} v_{\nu_2}\,,\ \dots\,,\ \sum_{\nu_m} c_{\nu_m m} v_{\nu_m}\Big) = \\ = \sum_{\nu_1 \nu_2 \dots \nu_m} c_{\nu_1 1} \cdot c_{\nu_2 2} \cdot \ \cdots \ \cdot c_{\nu_m m} \cdot \omega\left(v_{\nu_1},\, v_{\nu_2},\, \dots,\, v_{\nu_m}\right).$$

Так как при совпадении двух аргументов объём обращается в нуль, ненулевой вклад в последнюю сумму дают только наборы $(\nu_1, \nu_2, \dots, \nu_m)$, являющиеся *перестановками* чисел $(1,\, 2,\, \dots\,,\, m)$. Поскольку для каждого $g \in S_m$

$$\omega(v_{g_1}, v_{g_2}, \dots, v_{g_m}) = \operatorname{sgn}(g)\, \omega(v_1, v_2, \dots, v_m)\,,$$

мы получаем в правой части $\sum\limits_{g \in S_n} \operatorname{sgn}(g) \cdot c_{g_1 1} c_{g_2 2} \cdots c_{g_n n} \cdot \omega(v_1, v_2, \dots, v_m)$. □

Из (10-4) вытекает, что любые две формы объёма ω_1 , ω_2 пропорциональны. В самом деле, зафиксируем в V какой-нибудь базис e. Тогда для любого набора векторов $v = eC$

$$\omega_1(v_1, v_2, \dots, v_n) = \omega_1(e_1, e_2, \dots, e_n)\ \det C = \\ = \frac{\omega_1(e_1, e_2, \dots, e_n)}{\omega_2(e_1, e_2, \dots, e_n)} \cdot \omega_2(e_1, e_2, \dots, e_n)\ \det C = \\ = \frac{\omega_1(e_1, e_2, \dots, e_n)}{\omega_2(e_1, e_2, \dots, e_n)} \cdot \omega_2(v_1, v_2, \dots, v_n)\,.$$

Остаётся только показать, что на любом ненулевом пространстве V существует ненулевая форма объёма. Для этого фиксируем базис $e_1, e_2, \dots, e_n \in V$, положим $\omega(e_1, e_2, \dots, e_n) = 1$ и продолжим форму ω на произвольные наборы векторов по формулам (10-4), (10-6):

$$\omega(v_1, v_2, \dots, v_n) = \det C \quad \text{для } (v_1, v_2, \dots, v_n) = (e_1, e_2, \dots, e_n) \cdot C\,.$$

Поскольку $\det C$ линеен по каждому столбцу матрицы C , построенная форма ω линейна по каждому аргументу. В частности, она удовлетворяет свойству (2) из определения объёма, а по отношению к преобразованиям из свойства (1) ведёт себя так:

$$\omega\left(\dots\,,\, v_i + \lambda v_j,\, \dots\,,\, v_j,\, \dots\,,\right) = \\ = \omega\left(\dots\,,\, v_i,\, \dots\,,\, v_j,\, \dots\,,\right) + \lambda\, \omega\left(\dots\,,\, v_j,\, \dots\,,\, v_j,\, \dots\,,\right).$$

Второе слагаемое зануляется по идущей следом лем. 10.3. Тем самым, первое свойство объёма тоже выполнено, и теор. 10.2 полностью доказана. □

Лемма 10.3
Если в матрице C есть пара совпадающих столбцов, то $\det C = 0$.

Доказательство. Пусть $c_{\nu k} = c_{\nu\ell}$ при всех ν. Обозначим через $\sigma \in S_n$ транспозицию i-того и j-того элемента. Поскольку отображение $S_n \xrightarrow{g\mapsto g\sigma} S_n$ правого умножения на σ является обратной самой себе биекцией, и $g\sigma \neq g$ ни при каком g, все слагаемые суммы (10-6) разбиваются на непересекающиеся пары вида $\mathrm{sgn}(g)\cdot c_{g_1 1}c_{g_2 2}\cdots c_{g_n n}+\mathrm{sgn}(h)\cdot c_{h_1 1}c_{h_2 2}\cdots c_{h_n n}$, где $h = g\sigma$. Знаки слагаемых $\mathrm{sgn}(h) = -\mathrm{sgn}(g)$ в каждой такой паре различны, а произведения матричных элементов одинаковы, так как

$$h_j = g\sigma(j) = \begin{cases} g_j & \text{при } j \neq k,\, \ell \\ g_\ell & \text{при } j = k \\ g_k & \text{при } j = \ell \end{cases}$$

откуда $c_{h_j j} = c_{g_j j}$ при $j \neq k, \ell$ и $c_{h_k k}c_{g_\ell \ell} = c_{g_\ell k}c_{g_k \ell} = c_{g_\ell \ell}c_{g_k k}$ (ибо $c_{\nu k} = c_{\nu\ell}$ при всех ν). Тем самым, слагаемые каждой пары сокращают друг друга. □

10.3. Свойства определителей. Сумма

$$\det C = \sum_{g\in S_n} \mathrm{sgn}(g)\cdot c_{g_1 1}c_{g_2 2}\cdots c_{g_n n} \tag{10-6}$$

устроена следующим образом. В $n\times n$-матрице C всеми возможными способами выбирается n элементов так, чтобы в каждой строке и в каждом столбце оказалось выбрано ровно по одному элементу. Множество клеток, в которых стоят выбранные элементы, можно воспринимать как график биективного отображения $j \mapsto g(j)$ из номеров строк в номера столбцов. Это отображение является перестановкой. Выбранные элементы перемножаются, и все полученные таким образом $m!$ произведений складываются со знаками, равными знакам соответствующих перестановок g.

Например, определители второго и третьего порядка имеют вид

$$\det\begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix} = c_{11}c_{22} - c_{12}c_{21}$$

$$\det\begin{pmatrix} c_{11} & c_{12} & c_{13} \\ c_{21} & c_{22} & c_{23} \\ c_{31} & c_{32} & c_{33} \end{pmatrix} = c_{11}c_{22}c_{33} + c_{13}c_{21}c_{32} + c_{12}c_{23}c_{31} - \\ - c_{11}c_{23}c_{32} - c_{13}c_{22}c_{31} - c_{12}c_{21}c_{33}$$

(во втором равенстве сначала выписаны тождественная и две циклических перестановки, потом — три транспозиции).

Отметим, что если в данном выше описании заменить друг на друга слова «строка» и «столбец», а перестановку g на обратную перестановку g^{-1}, то мы получим определитель транспонированной матрицы. Поскольку $\operatorname{sgn}(g) = \operatorname{sgn}(g^{-1}$ (если $g = \sigma_1\sigma_2\,\ldots\,\sigma_k$, то $g^{-1} = \sigma_k\sigma_{k-1}\ldots\sigma_1$ состоит из тех же транспозиций), мы получаем такое

Предложение 10.1
Определитель не меняется при транспонировании матрицы: $\det C = \det C^t$. □

Предложение 10.2
Определитель $\det C$ полилинеен и кососимметричен и как функция от столбцов матрицы, и как функция от строк матрицы. При гауссовых элементарных преобразованиях строк (соотв. столбцов) первого типа определитель не меняется, при преобразованиях второго типа — меняет знак, при преобразованиях третьего типа — умножается на ту же константу, что и преобразуемая строка (соотв. столбец). Если ранг матрицы C меньше, чем её размер, то $\det C = 0$.

Доказательство. Зададим на координатном пространстве $\Bbbk^n$ объём ω так, чтобы объём стандартного базисного параллелепипеда $\omega(e_1, e_2, \ldots, e_n) = 1$. По теор. 10.2 определитель $\det C$ тогда равен объёму параллелепипеда, натянутого на столбцы матрицы C. Поскольку для объёма все перечисленные в предложении свойства имеют место, они выполняются и для определителя. Утверждения про строки получается транспонированием матрицы C. □

Предложение 10.3
$\det(AB) = \det(A)\det(B) \qquad \forall\, A, B \in \operatorname{Mat}_n(\Bbbk)$.

Доказательство. Если столбцы $v_1, v_2, \ldots, v_n \in \Bbbk^n$ матрицы A линейно зависимы, то столбцы матрицы AB, лежащие в линейной оболочке столбцов матрицы A, тоже линейно зависимы, и обе части равенства нулевые. Если же векторы v_i линейно независимы, то зададим на пространстве $\Bbbk^n$ две формы объёма: ω_e, такую что объём стандартного базисного параллелепипеда $\omega_e(e_1, e_2, \ldots, e_n) = 1$, и ω_v, такую что $\omega_v(v_1, v_2, \ldots, v_n) = 1$. По теор. 10.2 эти две формы пропорциональны друг другу с коэффициентом пропорциональности $\det A$:

$$\omega_e = \omega_e(v_1, v_2, \ldots, v_n) \cdot \omega_v = \det(A) \cdot \omega_v\,.$$

Набор векторов $w = vB = eAB$, координаты которого в базисе v задаются столбцами матрицы B, имеет в базисе e координаты, задаваемые столбцами матрицы AB. По теор. 10.2

$$\omega_e(w_1, w_2, \ldots, w_n) = \det(AB) \quad \text{и} \quad \omega_v(w_1, w_2, \ldots, w_n) = \det(B)\,.$$

Из предыдущего равенства мы заключаем, что $\det(AB) = \det(A)\det(B)$. □

Следствие 10.1
$\det(AB) = \det(BA) \qquad \forall\, A, B \in \operatorname{Mat}_n(K)$.

Следствие 10.2
Матрица $A \in \mathrm{Mat}_n(\Bbbk)$ обратима тогда и только тогда, когда когда $\det A \neq 0$.

Доказательство. означает Если A обратима, то $\det(A)\det(A^{-1}) = \det(E) = 1$, откуда $\det(A) \neq 0$. Если матрица необратима, то по лем. 9.1 её столбцы линейно зависимы, и тогда $\det A = 0$ по предл. 10.2. □

10.3.1. Невырожденные матрицы. Как мы видели, следующие условия на квадратную матрицу A размера $n \times n$ и на оператор $A : \Bbbk^n \longrightarrow \Bbbk^n$, имеющий матрицу A в стандартном базисе пространства $\Bbbk^n$, равносильны друг другу:

$\circ$ $\det A \neq 0$ $\circ$ $\operatorname{rk} A = n$ $\circ$ A обратима

$\circ$ $\forall\, b \in \Bbbk^n$ система уравнений $Ax = b$ имеет единственное решение

$\circ$ оператор $A : \Bbbk^n \longrightarrow \Bbbk^n$ биективен $\circ$ $\ker A = 0$ $\circ$ $\operatorname{im} A = \Bbbk^n$.

Матрицы (и операторы), обладающие этими свойствами называются *невырожденными*.

10.3.2. Специальная линейная группа. Выберем в пространстве V базис $e = (e_1, e_2, \dots, e_n)$ и сопоставим каждому линейному оператору $F : V \longrightarrow V$ его матрицу F_e, так что $F(e) = e\,F_e$ (в обозначениях из n° 9.3.2). Поскольку при выборе другого базиса $\varepsilon = e\,C_{e\varepsilon}$ матрица оператора заменяется на $F_\varepsilon = C_{e\varepsilon}^{-1} F_e C_{e\varepsilon}$, её определитель $\det F_\varepsilon = \det C_{e\varepsilon}^{-1} \cdot \det F_e \cdot \det C_{e\varepsilon} = \det F_e$ не зависит от выбора базиса. Поэтому у каждого линейного оператора F есть корректно определённый определитель $\det F \in \Bbbk$. Геометрически $\det F$ можно описать как коэффициент, на который умножаются объёмы всех невырожденных параллелепипедов в результате применения к ним оператора F:

$$\det(F) = \frac{\omega\,(Fv_1,\ Fv_2,\ \dots\ ,\ Fv_n)}{\omega(v_1, v_2, \dots, v_n)}\,, \tag{10-7}$$

где ω — любая ненулевая форма объёма на V, а $v_1, v_2, \dots, v_n$ — любая линейно независимая система векторов.

Упражнение 10.4. Покажите, что правая часть (10-7) не зависит ни от выбора ненулевой формы объёма, ни от выбора линейно независимой системы векторов $v_1, v_2, \dots, v_n$.

Операторы определителя один образуют в полной линейной группе $\mathrm{GL}(V)$ подгруппу, которая обозначается $\mathrm{SL}(V)$ и называется *специальной линейной группой* пространства V. Геометрически, специальная линейная группа состоит из всех операторов, сохраняющих объём. Специальная линейная группа координатного пространства $\Bbbk^n$ состоит из матриц определителя 1 и обозначается $\mathrm{SL}_n(\Bbbk) \subset \mathrm{GL}_n(\Bbbk)$.

10.3.3. Пример: правило Крамера. Обозначим через $a_1, a_2, \dots, a_n \in \Bbbk^n$ столбцы квадратной матрицы $A \in \mathrm{Mat}_n(\Bbbk)$ и договоримся, что $\det(v_1, v_2, \dots, v_n)$ означает определитель квадратной матрицы со столбцами $v_1, v_2, \dots, v_n \in \Bbbk^n$. В этих обозначениях столбец $x \in \Bbbk^n$ решений системы линейных уравнений $Ax = b$, доставляет линейное разложение $b = x_1a_1 + x_2a_2 + \dots + x_na_n$. Используя описанное в предл. 10.2 поведение определителя при элементарных преобразованиях 1-го и 3-го типа, получаем равенство

$$\det(a_1,\dots,a_{i-1},b,a_{i+1},\dots,a_n) = \\ = x_i\cdot\det(a_1,\dots,a_{i-1},a_i,a_{i+1},\dots,a_n) = x_i\det(A)\,.$$

Таким образом, для каждого $i = 1,\,2,\,\dots\,,\,n$ произведение определителя $\det A$ матрицы системы $Ax=b$ на i-тую координату любого решения равно определителю матрицы, которая получается из матрицы системы заменой i-того столбца на столбец правых частей. Этот факт известен как *правило Крамера*.

В частности, при $\det A\neq 0$ (единственное) решение системы $Ax=b$ даётся формулами $x_i = \det(a_1,\dots,a_{i-1},b,a_{i+1},\dots,a_n)/\det(A)$. Например, система

$$\begin{cases} ax+by=\xi\\ cx+dy=\eta\end{cases}$$

имеет решения $x=(\xi d-\eta b)/(ad-bc)$ и $y=(a\eta-c\xi)/(ad-bc)$. Отметим, что полагая $\begin{pmatrix}\xi'\\ \eta'\end{pmatrix}=\begin{pmatrix}1\\0\end{pmatrix}$ и $\begin{pmatrix}\xi''\\ \eta''\end{pmatrix}=\begin{pmatrix}0\\1\end{pmatrix}$, мы получим решения $\begin{pmatrix}x'\\ y'\end{pmatrix}=(ad-bc)^{-1}\begin{pmatrix}d\\-c\end{pmatrix}$ и $\begin{pmatrix}x''\\ y''\end{pmatrix}=(ad-bc)^{-1}\begin{pmatrix}-b\\a\end{pmatrix}$, представляющие собою столбцы обратной к A матрицы A^{-1}, ибо $\begin{pmatrix}a&b\\c&d\end{pmatrix}\begin{pmatrix}x'&x''\\y'&y''\end{pmatrix}=\begin{pmatrix}1&0\\0&1\end{pmatrix}$. Таким образом,

$$A^{-1}=(ad-bc)^{-1}\begin{pmatrix}d&-b\\-c&a\end{pmatrix}\,,$$

что согласуется с полученной в предыдущем параграфе формулой (9-6).

Упражнение 10.5. Выведите из правила Крамера, что стоящий в i-той строке и j-том столбце элемент b_{ij} матрицы $B=A^{-1}$, обратной к невырожденной матрице $A\in\mathrm{Mat}_n(\Bbbk)$, находятся по формуле: $b_{ij}=(-1)^{i+j}A_{\widehat{j}\widehat{i}}/\det(A)$, где через $A_{\widehat{j}\widehat{i}}$ обозначен определитель матрицы размера $(n-1)\times(n-1)$, остающейся после выкидывания из матрицы A j-той и строки и i-того столбца.

10.4. Грассмановы многочлены. Полезным инструментом при вычислениях с определителями является *грассманова алгебра* (или *алгебра грассмановых многочленов*) $\Bbbk\langle\xi_1,\xi_2,\dots,\xi_n\rangle$, которая определяется точно также, как алгебра обычных многочленов $\Bbbk[x_1,x_2,\dots,x_n]$, но только *грассмановы переменные* $\xi_1,\xi_2,\dots,\xi_n$, в отличие от обычных, не коммутируют, а *антикоммутируют* друг с другом, т. е. подчиняются соотношениям[1]

$$\xi_i\wedge\xi_j=-\xi_j\wedge\xi_i \quad\text{и}\quad \xi_i\wedge\xi_i=0\quad\forall\, i,j\,, \tag{10-8}$$

[1]если $\mathrm{char}(\Bbbk)\neq 2$ второе соотношение следует из первого, написанного для $i=j$; напротив, в характеристике 2 первое соотношение превращается в обычное коммутирование, тогда как второе накладывает содержательное дополнительное ограничение, отличающее грассмановы многочлены от обычных

где символ «$\wedge$» здесь и далее используется для обозначения умножения в грассмановой алгебре (чтобы не путать его с обычным, коммутативным умножением в алгебре многочленов).

Отметим, что из коммутационных соотношений (10-8) следует, что любая переменная входит в грассманов моном не более, чем в первой степени, и для каждого набора переменных I имеется, с точностью до знака, ровно один моном, куда входят эти и только эти переменные. Иначе говоря, базис грассмановой алгебры $\Bbbk\langle\xi_1, \xi_2, \dots, \xi_n\rangle$ как векторного пространства над $\Bbbk$, по определению, составляют мономы $\xi_I = \xi_{i_1} \wedge \xi_{i_2} \wedge \dots \wedge \xi_{i_m}$, $\quad i_1 < i_2 < \dots < i_m$. Все остальные произведения переменных выражаются через них согласно соотношениям (10-8): $\xi_{j_1} \wedge \xi_{j_2} \wedge \dots \wedge \xi_{j_m} = \operatorname{sgn}(g) \cdot \xi_{j_{g(1)}} \wedge \xi_{j_{g(2)}} \wedge \dots \wedge \xi_{j_{g(m)}}$, где $g \in S_m$ — перестановка, выстраивающая индексы $j_1, j_2, \dots, j_m$ в порядке возрастания.

Таким образом, однородные грассмановы многочлены степени m образуют векторное пространство размерности $\binom{n}{m}$, а вся грассманова алгебра имеет размерность $\dim \Bbbk\langle\xi_1, \xi_2, \dots, \xi_n\rangle = 2^n$. Мономов степени выше n в Грассмановой алгебре нет, а грассмановы многочлены самой старшей степени n образуют одномерное пространство с базисом $\xi_1 \wedge \xi_2 \wedge \dots \wedge \xi_n$.

Легко видеть, что грассмановы мономы коммутируют по правилу

$$(\xi_{i_1} \wedge \xi_{i_2} \wedge \dots \wedge \xi_{i_m}) \wedge (\xi_{j_1} \wedge \xi_{j_2} \wedge \dots \wedge \xi_{j_k}) = \\ = (-1)^{km} (\xi_{j_1} \wedge \xi_{j_2} \wedge \dots \wedge \xi_{j_k}) \wedge (\xi_{i_1} \wedge \xi_{i_2} \wedge \dots \wedge \xi_{i_m})$$

(для перенесения каждой из k переменных ξ_j через m переменных ξ_i требуется m транспозиций). Поэтому любые два *однородных* грассмановых многочлена f и g коммутируют по правилу

$$f \wedge g = (-1)^{\deg f \deg g} g \wedge f\,. \tag{10-9}$$

В частности, однородные многочлены чётной степени коммутируют с любым грассмановым многочленом.

Упражнение 10.6. Опишите *центр* грассмановой алгебры (т. е. грассмановы многочлены, перестановочные со всеми элементами грассмановой алгебры).

10.4.1. Пример: линейная замена переменных. Пусть грассмановы переменные $\xi = (\xi_1, \xi_2, \dots, \xi_n)$ линейно выражены через другие грассмановы переменные $\eta = (\eta_1, \eta_2, \dots, \eta_n)$ как $\xi = \eta \cdot A$. Тогда каждый грассманов моном ξ_J линейно выражается через грассмановы мономы η_I той же степени:

$$\xi_J = \xi_{j_1} \wedge \xi_{j_2} \wedge \dots \wedge \xi_{j_m} = \\ = \Big(\sum_{i_1} \eta_{i_1} a_{i_1 j_1}\Big) \wedge \Big(\sum_{i_2} \eta_{i_2} a_{i_2 j_2}\Big) \wedge \dots \wedge \Big(\sum_{i_n} \eta_{i_m} a_{i_m j_m}\Big) = \\ = \sum_{1 \leqslant i_1 < i_2 < \dots < i_n \leqslant n} \eta_{i_1} \wedge \eta_{i_2} \wedge \dots \wedge \eta_{i_n} \cdot \sum_{g \in S_m} \operatorname{sgn}(g)\, a_{i_{g(1)} j_1} a_{i_{g(2)} j_2} \cdots a_{i_{g(n)} j_n} = \\ = \sum_I \eta_I \cdot a_{IJ}\,,$$

где $I = (j_1, j_2, \ldots, j_m)$ пробегает все наборы из m возрастающих номеров

$$1 \leqslant i_1 < i_2 < \cdots < i_m \leqslant n\,,$$

а a_{IJ} обозначает определитель $m \times m$-подматрицы в A, сосредоточенной в пересечениях строк с номерами I и столбцов с номерами J. Такой определитель называется IJ-тым *минором* m-того порядка.

Таким образом, IJ-тый элемент матрицы перехода от базиса $\{\xi_J\}$ к базису $\{\eta_I\}$ в пространстве однородных грассмановых многочленов степени m равен IJ-тому минору m-того порядка в матрице перехода от переменных ξ к переменным η.

Если как-либо упорядочить все наборы из m возрастающих индексов, то миноры m-того порядка в матрице A можно организовать в квадратную матрицу (a_{IJ}) размера $\binom{n}{m} \times \binom{n}{m}$. Эта матрица обозначается $\Lambda^m A$ и называется m-той *внешней степенью* матрицы A.

Для грассмановых многочленов старшей степени матрица (a_{IJ}) состоит из одного элемента и формула $\xi_J = \sum\limits_I \eta_I \cdot a_{IJ}$ превращается в равенство

$$\xi_1 \wedge \xi_2 \wedge \cdots \wedge \xi_n = \det(A) \cdot \eta_1 \wedge \eta_2 \wedge \cdots \wedge \eta_n \tag{10-10}$$

Отметим, что отсюда получается ещё одно доказательство мультипликативности определителя: сделав вторую замену $\eta = \zeta\, B$, получим

$$\eta_1 \wedge \eta_2 \wedge \cdots \wedge \eta_n = \det(B) \cdot \zeta_1 \wedge \zeta_2 \wedge \cdots \wedge \zeta_n\,,$$

откуда $\xi_1 \wedge \xi_2 \wedge \cdots \wedge \xi_n = \det(A)\det(B) \cdot \zeta_1 \wedge \zeta_2 \wedge \cdots \wedge \zeta_n$, но, с другой стороны, $\xi = \zeta\, BA$, откуда $\xi_1 \wedge \xi_2 \wedge \cdots \wedge \xi_n = \det(BA) \cdot \zeta_1 \wedge \zeta_2 \wedge \cdots \wedge \zeta_n$. Следовательно,

$$\det(BA) = \det(A)\det(B)\,. \tag{10-11}$$

Упражнение 10.7 (приведение грассмановой квадратичной формы). Покажите, что любой однородный грассманов многочлен второй степени

$$f(\xi) = \sum a_{ij}\, \xi_i \wedge \xi_j$$

над любым полем линейной обратимой заменой координат приводится к виду

$$\eta_1 \wedge \eta_2 + \eta_3 \wedge \eta_4 + \cdots + \eta_{2r-1} \wedge \eta_{2r} \tag{10-12}$$

(грассманова квадратичная форма (10-12) называется *симплектической*, а координаты $\eta_1, \eta_2, \ldots, \eta_n$, в которых форма приобретает такой вид, называются *координатами Дарбу*).

10.4.2. Соотношения Сильвестра. Для каждого набора возрастающих индексов $J = (j_1, j_2, \dots, j_m)$ положим $\deg J = m$, $|J| = \sum\limits_{\nu} j_\nu$, и обозначим через

$$\overline{J} = (\overline{j}_1, \overline{j}_2, \dots, \overline{j}_{n-m}) = \{1, 2, \dots, n\} \smallsetminus J$$

дополнительный набор возрастающих индексов длины $\deg \overline{J} = n - m$.

В этих обозначениях базисные грассмановы мономы ξ_J и $\xi_{\overline{I}}$ дополнительных степеней $\deg J = m$ и $\deg \overline{I} = n - m$ перемножаются по правилу

$$\xi_J \wedge \xi_{\overline{I}} = \begin{cases} (-1)^{|J| + \frac{m(m+1)}{2}} \xi_1 \wedge \xi_2 \wedge \dots \wedge \xi_n & \text{при } I = J \\ 0 & \text{при } I \neq J \end{cases} \tag{10-13}$$

где $(-1)^{|J| + \frac{m(m+1)}{2}} = \operatorname{sgn}(j_1, j_2, \dots, j_m, \overline{j}_1, \overline{j}_2, \dots, \overline{j}_{n-m})$ — это знак *тасующей перестановки*, вычисленный читателем в упр. 10.3.

Заменим в равенстве (10-13) переменные ξ на переменные η, через которые ξ линейно выражаются по формуле $\xi = \eta \cdot A$. В левой части получим

$$\Big(\sum_K \eta_K a_{KJ}\Big) \wedge \Big(\sum_L \eta_L a_{L\overline{I}}\Big) = (-1)^{\frac{m(m+1)}{2}} \eta_1 \wedge \eta_2 \wedge \dots \wedge \eta_n \sum_K (-1)^{|K|} a_{KJ} a_{\overline{KI}},$$

где K пробегает все индексы длины $\deg K = m$. А в правой части получим нуль при $I \neq J$ и $(-1)^{\frac{m(m+1)}{2}} (-1)^{|J|} \det A \cdot \eta_1 \wedge \eta_2 \wedge \dots \wedge \eta_n$ при $I = J$.

Следовательно, для любых двух наборов J, I из m строк любой квадратной матрицы A выполняются *соотношения Сильвестра*

$$\sum_K (-1)^{|K| + |I|} a_{KJ} a_{\overline{KI}} = \begin{cases} \det A & \text{при } I = J \\ 0 & \text{при } I \neq J \end{cases} \tag{10-14}$$

где суммирование идёт по всем наборам K из $m = \deg K$ строк матрицы A.

При $I = J$ соотношение (10-14) даёт формулу для вычисления определителя[1]

$$\det A = \sum_K (-1)^{|K| + |J|} a_{KJ} a_{\overline{KJ}} \tag{10-15}$$

через всевозможные миноры a_{KJ} порядка m, сосредоточенные в m фиксированных столбцах матрицы A с номерами J, и *дополнительные* к ним миноры $a_{\overline{JK}}$ порядка $n - m$, равные определителям матриц, получающихся из A вычёркиванием всех строк и столбцов, содержащих минор a_{KJ}. Произведение $(-1)^{|K|+|J|} a_{\overline{KJ}}$ называется *алгебраическим дополнением* к минору a_{KJ}.

Соотношение, которое получается в (10-14) при $I \neq J$

$$\sum_K (-1)^{|K| + |I|} a_{JK} a_{\overline{IK}} = 0 \tag{10-16}$$

[1] с геометрической точки зрения эта формула вычисляет объём n-мерного параллелепипеда через объёмы его m-мерных и $(n-m)$-мерных граней

иногда называют *теоремой об умножении на чужие алгебраические дополнения*, поскольку левая часть равенства (10-16) отличается от формулы (10-15) для вычисления определителя через сосредоточенные в заданном наборе столбцов J миноры a_{JK} тем, что эти миноры умножаются не на свои, а на «чужие» алгебраические дополнения (а именно, на дополнения к минорам a_{IK}, сосредоточенным в тех же строках K, но в другом наборе столбцов $I \neq J$).

Упражнение 10.8. Установите двойственную версию соотношений Сильвестра

$$\sum_K (-1)^{|I|+|K|} a_{JK} a_{\overline{IK}} = \begin{cases} \det A & \text{при } I = J \\ 0 & \text{при } I \neq J \end{cases} \tag{10-17}$$

Если как-либо занумеровать $\binom{n}{m}$ наборов J длины $\deg J = m$, после чего занумеровать $\binom{n}{m}$ наборов $\overline{J}$ длины $n-m$ так, чтобы набор $\overline{J}$ имел тот же номер, что и J, то соотношения Сильвестра запишутся одним равенством

$$\Lambda^m A \cdot \Lambda^{n-m} A^\vee = \det A \cdot E\,,$$

на матрицы размера $\binom{n}{m} \times \binom{n}{m}$, где через $\Lambda^{n-m}A^\vee$ обозначена матрица, (JI)-тый элемент которой равен $(-1)^{|J|+|I|} a_{\overline{IJ}}$.

10.4.3. Присоединённая матрица. При $m = 1$ соотношение (10-15) называется *формулой для разложения определителя по столбцу*. В этом случае $I = (i)$ и $K = (k)$ суть одноэлементные наборы, а минор $a_{KI} = a_{ki}$ это просто матричный элемент. Алгебраическое дополнение к нему обычно обозначается через

$$A_{ki} \stackrel{\text{def}}{=} (-1)^{i+k} a_{\overline{ki}}$$

и представляет собою умноженный на $(-1)^{k+j}$ минор порядка $(n-1)$, равный определителю матрицы, которая получается из A вычёркиванием k-й строки и i-го столбца. Формулы (10-15) и (10-15) приобретают вид

$$\begin{gathered} \det(A) = \sum_k^{k+j} a_{kj} A_{kj} \\ \sum_k^{k+i} a_{kj} A_{ki} = 0 \end{gathered} \tag{10-18}$$

Например, раскладывая определитель 3×3 по первому столбцу, получаем

$$\det \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} = \\ = a_{11}\left(a_{22}a_{33} - a_{23}a_{32}\right) - a_{21}\left(a_{12}a_{33} - a_{13}a_{32}\right) + a_{31}\left(a_{12}a_{23} - a_{13}a_{22}\right)$$

что согласуется с вычислением со стр. 175.

Упражнение 10.9. Напишите двойственные к (10-18) для разложения определителя по строке.

Матрица, транспонированная к матрице алгебраических дополнений к элементам матрицы A

$$\widehat{A} = (\widehat{a}_{ij}) \quad \text{с} \quad \widehat{a}_{ij} \stackrel{\text{def}}{=} A_{ji} = (-1)^{i+j} a_{\overline{j}\overline{i}} \tag{10-19}$$

называется *присоединённой матрицей* матрицы A. При помощи присоединённой матрицы все соотношения (10-18) можно свернуть в одну матричную формулу

$$A\widehat{A} = \widehat{A}A = \det(A) \cdot E = \begin{pmatrix} \det(A) & & & 0 \\ & \det(A) & & \\ & & \ddots & \\ 0 & & & \det(A) \end{pmatrix}$$

откуда получается явная формула для обратной матрицы к невырожденной матрице A

$$A^{-1} = \frac{1}{\det A}\,\widehat{A}$$

Замечание 10.1. Отметим, что определитель

$$\det A = \sum_{g \in S_n} \operatorname{sgn}(g) \cdot a_{1g_1} a_{g_2 2} \cdots a_{ng_n}$$

определён для квадратных матриц с коэффициентами в произвольном коммутативном кольце K.

Упражнение 10.10. Покажите, что в такой общности определитель тоже является полилинейной кососимметричной формой от строк и от столбцов матрицы, обращается в нуль, если строки или столбцы линейно зависимы, и удовлетворяет равенствам $\det A^t = \det A$, $\det(AB) = \det A \cdot \det B$.

Алгебру грассмановых многочленов $K\langle \xi_1, \xi_2, \dots, \xi_n \rangle$ также можно рассматривать с коэффициентами в произвольном коммутативном кольце K с единицей, и все формулы из этого раздела останутся при этом в силе (их вывод нигде не использовал деления). В частности, мы получаем такой полезный критерий обратимости матрицы.

Следствие 10.3 (критерий обратимости матрицы)
Квадратная матрица $A \in \operatorname{Mat}_n(K)$ с элементами из произвольного коммутативного кольца K обратима тогда и только тогда, когда $\det(A)$ обратим в K, и в этом случае $A^{-1} = \frac{1}{\det(A)}\widehat{A}$.

Доказательство. Если A обратима, то $AA^{-1} = E$, откуда $\det(A)\det(A^{-1}) = 1$. Наоборот, если $\det A$ обратим, то $\frac{1}{\det A}\,\widehat{A} \cdot A = E$ в силу соотношений Сильвестра. □

Задачи для самостоятельного решения к §10

Во всех задачах к этому параграфу $\Bbbk$ означает произвольное поле, а K — произвольное коммутативное кольцо с единицей.

Задача 10.1. Покажите, что определитель верхней (или нижней) треугольной матрицы равен произведению диагональных элементов.

Задача 10.2. Вычислите $\operatorname{sgn}(n,\,(n-1),\,\dots\,,\,2,\,1)$ и выразите определитель матрицы с нулями правее и ниже побочной диагонали через элементы побочной диагонали. Изменится ли ответ, если нули стоят левее и выше побочной диагонали (а правая нижняя часть матрицы неизвестна)?

Задача 10.3. Пусть $A\in\operatorname{Mat}_n(\Bbbk)$, $C\in\operatorname{Mat}_m(\Bbbk)$, $B\in\operatorname{Mat}_{n\times m}(\Bbbk)$. Докажите в $\operatorname{Mat}_{m+n}(\Bbbk)$ равенство $\det\begin{pmatrix}A & B\\ 0 & C\end{pmatrix}=\det(A)\det(C)$, где $0\in\operatorname{Mat}_{m\times n}(\Bbbk)$ — нулевая матрица.

Задача 10.4. Две строки матрицы 3×3-матрицы заполнены целыми числами так, что НОД чисел в каждой из этих строке равен единице. Всегда ли третью строку этой матрицы можно заполнить целыми числами так, чтобы определитель матрицы оказался равным единице?

Задача 10.5. Выпишите все вырожденные 2×2-матрицы с коэффициентами из поля $\mathbb{F}_2$. Сколько всего имеется 2×2-матриц с заданным определителем над полем $\mathbb{F}_p$?

Задача 10.6. Числа $1,\,2,\,3,\,\dots\,,\,n^2$ всевозможными способами организуются в квадратные матрицы размера $n\times n$. Найдите сумму определителей всех этих матриц.

Задача 10.7. Вычислите определитель матрицы с нулями на главной диагонали и единицами во всех остальных местах.

Задача 10.8. Покажите, что определитель 3-диагональной матрицы с единицами по главной диагонали и непосредственно над нею и минус единицами непосредственно под главной диагональю является числом Фиббоначчи.

Задача 10.9. Для правила $f:\mathbb{N}\times\mathbb{N}\longrightarrow K$, перерабатывающего пару натуральных чисел (i,j) в элемент $f(i,j)\in K$, будем обозначать через $\big(f(i,j)\big)\in\operatorname{Mat}_n(K)$ квадратную матрицу, у которой элемент в пересечении i-той строки с j-тым столбцом равен $f(i,j)$. Вычислите определители следующих матриц:

а) $\det\left(\alpha_i\beta_j\right)$ б) $\det\big(\cos(\alpha_i-\beta_j)\big)$ в) $\det\left(\alpha_i^{j-1}\right)$ г*) $\det\left(\alpha^{j-i-1\,(\mathrm{mod}\,n)}\right)$

(где $\alpha_1,\alpha_2,\dots,\alpha_n$ и $\beta_1,\beta_2,\dots,\beta_n$ произвольные наборы вещественных чисел)

Задача 10.10. Покажите, что для линейной независимости набора функций

$$f_1,f_2,\dots,f_n:M\longrightarrow\Bbbk$$

на произвольном множестве M необходимо и достаточно существования n точек $x_1,x_2,\dots,x_n\in M$ с $\det\left(f_i(t_j)\right)\neq0$.

Задача 10.11 (теорема об окаймляющих минорах). Пусть матрица A содержит невырожденную квадратную подматрицу размера $m \times m$, такую что все содержащие её подматрицы размера $(m+1) \times (m+1)$ вырождены. Докажите, что $\operatorname{rk} A = m$.

Задача 10.12 (кососимметричные матрицы). Квадратная матрица A называется *кососимметричной*, если $A^t = -A$. Покажите, что
а) любая кососимметрическая матрица нечетного размера вырождена
б) определители кососимметрических матриц размеров 2×2 и 4×4 являются полными квадратами в кольцах многочленов от матричных элементов

Задача 10.13. Вершины связного графа Γ занумерованы числами от 1 до n. Матрица $A_\Gamma = (a_{ij})$ имеет диагональные элементы a_{ii}, равные числу ребер, сходящихся в i-той вершине, а остальные элементы a_{ij} равны единице, если вершины i и j соединены ребром, и нулю — если не соединены. Докажите, что $\det A = 0$, а все алгебраические дополнения A_{ii} к элементам главной диагонали отличны от нуля и равны между собой. Если общий случай вызывает затруднения, решите задачу в предположении, что граф Γ дерево. Покажите, что Γ дерево, если и только если $A_{ii} = 1$.

Задача 10.14. Выясните, при каких a, b, c матрицы обратимы и вычислите:

а) $\begin{pmatrix} 1 & 1 \\ 1 & a+1 \end{pmatrix}^{-1}$ б) $\begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix}^{-1}$ в) $\begin{pmatrix} 1 & 0 & c \\ 0 & b & 0 \\ a & 0 & 1 \end{pmatrix}^{-1}$ г) $\begin{pmatrix} 1 & a & 0 \\ 0 & b & 0 \\ 0 & c & 1 \end{pmatrix}^{-1}$

Задача 10.15. Пусть $A(x) = a_0x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n$, $B(x) = b_0x^m + b_1x^{m-1} + \dots + b_{m-1}x + b_m$ имеют $a_0b_0 \neq 0$. Обозначим через $P_d \subset \Bbbk[x]$ ($\Bbbk$ – любое поле) подпространство многочленов степени $\leqslant d$, и рассмотрим отображение $P_{n-1} \oplus P_{m-1} \xrightarrow{(f,g)\mapsto Ag+Bf} P_{m+n-1}$. Проверьте, что оно линейно над $\Bbbk$ и напишите его матрицу в стандартных базисах из одночленов $\{x^\nu\}$ и докажите, что её невырожденность равносильна взаимной простоте A и B.

Задача 10.16 (детерминант Сильвестра). Для $\nu = 0, 1, 2, \dots$ обозначим через d_ν определитель матрицы, которая получается выкидыванием по ν строк и ν столбцов сверху, снизу, слева и справа из матрицы (мы считаем, что $m \leqslant n$ и пустые места заполнены нулями)

$$\underbrace{\begin{pmatrix}
a_0 & \dots & \dots & a_{n-1} & a_n & & & \\
 & a_0 & \dots & \dots & a_{n-1} & a_n & & \\
 & & \ddots & & & \ddots & \ddots & \\
 & & & a_0 & \dots & \dots & a_{n-1} & a_n \\
 & & & & b_0 & \dots & b_{m-1} & b_m \\
 & & & \iddots & & \iddots & \iddots & \\
 & & \iddots & & \iddots & \iddots & & \\
 & b_0 & \dots & b_{m-1} & b_m & & & \\
b_0 & \dots & b_{m-1} & b_m & & & &
\end{pmatrix}}_{m+n}
\begin{array}{l}
\left.\begin{array}{l} \\ \\ \\ \\ \end{array}\right\} m \\
\left.\begin{array}{l} \\ \\ \\ \\ \\ \end{array}\right\} n
\end{array}
\tag{10-20}$$

Покажите, что $\deg$ нод(A, B) пары многочленов A и B из зад. 10.15 с индексом первого ненулевого члена последовательности d_0, d_1, d_2, ...?

Задача 10.17 (результант). В $\mathbb{Z}[t, a_0, b_0, \alpha_1, \alpha_2, \ldots, \alpha_n, \beta_1, \beta_2, \ldots, \beta_m]$ положим

$$A(t) \stackrel{\text{def}}{=} a_0 t^n + a_1 t^{n-1} + \cdots + a_{n-1} t + a_n \stackrel{\text{def}}{=} a_0 \prod_{i=1}^{n} (t - \alpha_i)$$

$$B(t) \stackrel{\text{def}}{=} b_0 t^m + b_1 t^{m-1} + \cdots + b_{m-1} t + b_m \stackrel{\text{def}}{=} b_0 \prod_{j=1}^{m} (t - \beta_j)$$

а) Проверьте равенства $a_0^m \prod\limits_i B(a_i) = a_0^m b_0^n \prod\limits_{i,j} (\alpha_i - \beta_j) = (-1)^{mn} b_0^n \prod\limits_j A(\beta_j)$ (этот полином называется *результантом* многочленов A и B и обозначается $R_{A,B}$)

б) докажите, что $R_{A,B}$ равен определителю (10-20)

в) докажите, что $\forall\, A, B \in \mathbb{Z}[x]\ \exists\, f, g \in \mathbb{Z}[x] \ :\ R_{A,B} = fA + gB$ в $\mathbb{Z}[x]$.

Задача 10.18. Докажите для обратных друг другу матриц A и B соотношение

$$a_{IJ} = (-1)^{|I|+|J|} b_{\overline{JI}}$$

Задача 10.19. Вычислите все частные производные определителя по матричным элементам

$$\frac{\partial^k \det(A)}{\partial a_{i_1 j_1} \partial a_{i_2 j_2} \ldots \partial a_{i_k j_k}}$$

Задача 10.20. Для $A, B \in \mathrm{Mat}_n(K)$ докажите следующее разложение Тейлора в $K[x, y]$ (x и y — скалярные переменные):

$$\det(xA + yB) = \sum_{k=0}^{n} x^k y^{n-k} \cdot \mathrm{tr}\left(\Lambda^k A\right) \cdot \mathrm{tr}\left(\Lambda^{n-k} A\right).$$

Задача 10.21. Покажите, что однородный грассманов квадратичный многочлен ω от четырёх переменных тогда и только тогда является произведением двух линейных форм, когда $\omega \wedge \omega = 0$.

Задача 10.22* (соотношение Плюккера). Для матрицы $A \in \mathrm{Mat}_{2\times 4}(K)$ (2 строки и 4 столбца) обозначим через A_{ij} 2×2-минор, расположенный в i-том и j-том столбцах. Покажите, что 6 чисел $A_{ij} \in K$ тогда и только тогда образуют набор 2×2-миноров 2×4-матрицы, когда $A_{12}A_{34} - A_{13}A_{24} + A_{14}A_{23} = 0$. Выясните, существуют ли 2×4 матрицы с 2×2 наборами миноров

а) $\{2,\ 3,\ 4,\ 5,\ 6,\ 7\}$ б) $\{3,\ 4,\ 5,\ 6,\ 7,\ 8\}$

(миноры написаны просто в порядке возрастания их значений). Если матрица с указанными минорами существует, приведите пример такой матрицы.

Задача 10.23 (характеристический многочлен). Многочлен

$$\chi_A(t) = \det(tE - A) = \sigma_0 t^n + \sigma_1 t^{n-1} + \cdots + \sigma_{n-1} t + \sigma_n \in K[t]$$

называется *характеристическим многочленом* матрицы $A \in \mathrm{Mat}_n(K)$.

Докажите, что а) если $B = CAC^{-1}$, то $\chi_B = \chi_A$
б) $(-1)^k \sigma_k$ равен сумме всех миноров k-го порядка, главная диагональ которых содержится в главной диагонали A (такие миноры называются *главными*).
в) $\frac{d}{dt}\big|_{t=0} \det(E + tA) = \mathrm{tr}\, A$ г*) $\chi_A(A) = 0$ д) $\dim \Bbbk[A] \leqslant n \ \forall\, A \in \mathrm{Mat}_n(\Bbbk)$.

§11. Модули.

11.1. Определение модулей. Абелева группа M называется *левым модулем* над кольцом[1] K (или *левым K-модулем*), если задана операция *левого умножения* элементов группы M на элементы кольца: $K \times M \longrightarrow M$ со свойствами:

$$\lambda(\mu a) = (\lambda\mu)a \quad \forall\, a\in M\ ,\ \forall\, \lambda,\mu \in K \tag{11-1}$$
$$(\lambda+\mu)a = \lambda a + \mu a \quad \forall\, a\in M\ ,\ \forall\, \lambda,\mu \in K \tag{11-2}$$
$$\lambda(a+b) = \lambda a + \lambda b \quad \forall\, \lambda\in K\ ,\ \forall\, a,b \in K \tag{11-3}$$

Симметричным образом, M называется *правым K-модулем*, если задана операция *правого умножения* элементов группы M на элементы кольца: $M \times K \longrightarrow M$ со свойствами:

$$(a\mu)\lambda = a(\mu\lambda) \quad \forall\, a\in M\ ,\ \forall\, \lambda,\mu \in K \tag{11-1$'$}$$
$$a(\lambda+\mu) = a\lambda + a\mu \quad \forall\, a\in M\ ,\ \forall\, \lambda,\mu \in K \tag{11-2$'$}$$
$$(a+b)\lambda = a\lambda + b\lambda \quad \forall\, \lambda\in K\ ,\ \forall\, a,b \in K\,. \tag{11-3$'$}$$

Второе и третье свойства в этих двух определениях одинаковы, и утверждают, что операция умножения векторов на числа дистрибутивна. Левое умножение отличается от правого только первым свойством, которое утверждает, что результат умножения вектора a сначала на μ, а потом на λ, совпадает в левом модуле с результатом умножения a на $\lambda\mu$, а в правом — с результатом умножения a на $\mu\lambda$. Таким образом, структура левого модуля над кольцом K — это то же самое, что структура правого модуля над *противоположным кольцом* K°, которое состоит из тех же элементов, что K, но отличается порядком следования сомножителей в произведениях:

$$a \underset{K^\circ}{\cdot} b \overset{\text{def}}{=} b \underset{K}{\cdot} a\,.$$

Над коммутативным кольцом между левой и правой модульной структурой разницы нет.

Если кольцо K содержит единицу, то к свойствам (11-1) – (11-3$'$) обычно добавляют свойства

$$1\cdot a = 1 \quad \text{и} \quad a\cdot 1 = a \qquad \forall\, a\in M\ .$$

Модули, удовлетворяющие этим условиям называются *унитальными*.

В случае, когда кольцо K является полем, K-модули — это в точности векторные пространства над полем K. Хотя модуль над произвольным коммутативным кольцом может далеко отстоять по своим свойствам от векторного пространства, интуиция геометрических векторов часто оказывается полезной

[1] подчеркнём, что кольцо не предполагается коммутативным

и при работе с модулями, так что мы часто будем называть элементы модулей «векторами», а элементы кольца — «числами».

Далее в этом курсе, если специально не оговаривается противное, мы будем иметь дело только унитальными модулями над коммутативными кольцами с единицей и не будем делать разницы между левым и правым умножением элементов модуля на элементы кольца, записывая произведение вектора $v \in V$ на число $\lambda \in K$ и как $\lambda \cdot v$, и как $v \cdot \lambda$ — как мы уже поступали и ранее.

11.1.1. Подмодули, фактор модули и гомоморфизмы. Абелева подгруппа $N \subset M$ в K-модуле M называется K-подмодулем, если она выдерживают умножение на элементы кольца, т. е.

$$\lambda a \in N \quad \forall\, a \in N \;, \;\; \forall\, \lambda \in K \;.$$

Подмодуль называется *собственным*, если он отличен от нуля и от всего модуля.

Фактор модуль M/N по подмодулю $N \subset M$ определяется как множество смежных классов

$$[m]_N = m \,(\mathrm{mod}\, N) = m + N = \{m' \in M \mid m' - m \in N\}$$

которые являются классами эквивалентности по отношению $m \underset{N}{\sim} m'$, означающему, что $m' - m \in N$. Сложение классов и их умножение на элементы кольца определяются обычными формулами

$$[m_1] + [m_2] = [m_1 + m_2]$$
$$\lambda[m] = [\lambda m]$$

Упражнение 11.1. Проверьте, что эти операции корректно определены и удовлетворяют определению модуля.

Гомоморфизм (или K-или K-*линейным отображение*) между K-модулями M и M' это гомоморфизм абелевых групп $M \longrightarrow M'$, перестановочный с умножением на элементы кольца:

$$\varphi(\lambda v) = \lambda \varphi(v) \quad \forall\, \lambda \in K \;, \; \forall\, v, w \in M \,.$$

Таким образом, гомоморфизм модулей обладает всеми свойствами гомоморфизма абелевых групп. Например, $\varphi(0) = 0$, $\varphi(v - w) = \varphi(v) - \varphi(w)$ и т. п.. Инъективность K-линейного отображения φ равносильна тому, что φ имеет нулевое *ядро* $\ker(\varphi) = \{\, a \in M_1 \mid \varphi(a) = 0 \,\}$.

Упражнение 11.2. Убедитесь, что ядро и образ произвольного гомоморфизма K-модулей $\varphi : M_1 \longrightarrow M_2$ являются K-подмодулями в M_1 и M_2 соответственно, и постройте канонический изоморфизм $M_1/\ker(\varphi) \xrightarrow{\sim} \mathrm{im}\,(\varphi)$.

11.2. Образующие и соотношения. Говорят, что множество векторов $\mathscr{E} = \{e_i\} \subset M$ *порождает* модуль M, если всякий элемент $a \in M$ является *конечной* линейной комбинацией элементов e_i с коэффициентами из K:

$$a = \lambda_1 e_{i_1} + \lambda_2 e_{i_2} + \cdots + \lambda_n e_{i_n} . \tag{11-4}$$

Векторы $e_i \in \mathscr{E}$ называются в этом случае *образующими* модуля M. Модуль, допускающий конечное множество образующих, называется *конечно порожденным*.

Множество образующих $\mathscr{E}$ называется *базисом*, если представление (11-4) единственно для любого вектора $a \in M$. Поскольку наличие двух различных разложений $\sum \lambda_i e_i = \sum \mu_i e_i$ равносильно равенству $\sum (\lambda_i - \mu_i) e_i = 0$, в котором присутствуют ненулевые коэффициенты, множество $\mathscr{E}$ образующих модуля M является базисом тогда и только тогда, когда оно *линейно независимо*, т. е. когда любое равенство вида

$$\lambda_1 e_{i_1} + \lambda_2 e_{i_2} + \cdots + \lambda_n e_{i_n} = 0 \tag{11-5}$$

влечёт, что все $\lambda_j = 0$. Линейные зависимости (11-5) с ненулевыми коэффициентами называются *соотношениями* между образующими. Таким образом, базис — это система образующих, не связанных никакими соотношениями.

Модуль, обладающий базисом, называется *свободным*. Согласно теореме о существовании базиса в векторном пространстве, всякий модуль над полем является свободным. Над кольцом K, имеющим необратимые элементы, это неверно: существуют модули, у которых любой набор образующих линейно зависим, и модули, в которых вообще нет непустых линейно независимых наборов векторов. Причина заключается в том, что наличие линейной зависимости

$$\lambda_1 e_{i_1} + \lambda_2 e_{i_2} + \cdots + \lambda_n e_{i_n} = 0$$

с необратимыми коэффициентами λ_j, вообще говоря, не позволяет выразить какой-нибудь из векторов через остальные.

11.2.1. Пример: идеалы. Любое кольцо K является модулем над самим собой. Его подмодули $I \subset K$ — это в точности идеалы кольца K. Если идеал не является главным, то любое множество его образующих содержит хотя бы два элемента и, тем самым, линейно зависимо, поскольку любые два элемента $a, b \in K$ линейно зависимы над K:

$$a \cdot b - b \cdot a = 0 .$$

Тем самым, для подмодулей кольца, не являющегося кольцом главных идеалов, теорема о базисе заведомо не выполняется. Например, в кольце многочленов $K = \Bbbk[x, y]$ (где $\Bbbk$ — поле) имеется подмодуль M, состоящий из многочленов без свободного члена. Согласно упр. 6.7 идеал $M \subset \Bbbk[x, y]$ не является главным, т. е. не может быть задан одной образующей. Но его можно задать двумя образующими $e_1 = x$ и $e_2 = y$, между которыми имеется линейная зависимость $y e_1 - x e_2 = 0$.

11.2.2. Пример: абелевы группы. Всякая абелева группа A имеет каноническую структуру модуля над кольцом целых чисел $\mathbb{Z}$, заданную правилом

$$n \cdot a \overset{\text{def}}{=} \operatorname{sgn}(n)(\underbrace{a + a + \cdots + a}_{n}), \tag{11-6}$$

где $\operatorname{sgn}(n)$ означает знак целого числа n.

Упражнение 11.3. Проверьте выполнение аксиом $\mathbb{Z}$-модуля.

В частности, аддитивная группа вычетов $\mathbb{Z}/(k)$ может рассматриваться как $\mathbb{Z}$-модуль с операцией

$$n \cdot [m]_k \overset{\text{def}}{=} [nm]_k ,$$

где мы обозначаем через $[m]_k = m \pmod k$ класс числа m по модулю k. Модуль $\mathbb{Z}/(k)$ порождается одним элементом $[1]_k$, который удовлетворяет соотношению $k \cdot [1]_k = 0$, и значит, не является базисом. Таким образом, теорема о базисе не выполняется в $\mathbb{Z}$-модуле $\mathbb{Z}/(k)$.

Из соотношения $k \cdot [1]_k = 0$ вытекает отсутствие ненулевых гомоморфизмов $\mathbb{Z}/(k) \longrightarrow \mathbb{Z}$. В самом деле, для такого гомоморфизма φ в кольце $\mathbb{Z}$ выполняется равенство

$$k \cdot \varphi([1]_k) = \varphi(k \cdot [1]_k) = \varphi(0) = 0 ,$$

откуда $\varphi([1]_k) = 0$, поскольку в $\mathbb{Z}$ нет делителей нуля. Но тогда $\forall\ m\ \varphi([m]_k) = \varphi(m \cdot [1]_k) = m \cdot \varphi([1]_k) = 0$.

Упражнение 11.4. Покажите, что класс $[n]_k$ порождает $\mathbb{Z}$-модуль $\mathbb{Z}/(k)$ тогда и только тогда, когда n взаимно просто с k.

11.2.3. Пример: делители нуля и кручение. Пусть в кольце K нет делителей нуля. Элемент m из K-модуля M называется *элементом кручения*, если $\lambda m = 0$ для некоторого ненулевого $\lambda \in K$. Ненулевое число $\lambda \in K$ называется *делителем нуля* в модуле M, если $\lambda m = 0$ для некоторого ненулевого $m \in M$.

Элементы кручения образуют подмодуль в M: если $\lambda_1 m_1 = 0$ и $\lambda_2 m_2 = 0$, то $\lambda_1\lambda_2(m_1 \pm m_2) = 0$ (причём $\lambda_1\lambda_2 \neq 0$, т. к. в K нет делителей нуля) и $\lambda_1(\mu m_1) = \lambda_2(\mu m_2) = 0 \quad \forall\, \mu \in K$. Этот подмодуль называется *подмодулем кручения* и обозначается

$$\operatorname{Tors}(M) = \{m \in M \mid \exists\ \lambda \neq 0 : \lambda m = 0\} .$$

Если $\operatorname{Tors}(M) = 0$, то говорят, что M — модуль без кручения (или что M свободен от кручения).

Например, любой подмодуль кольца K, рассматриваемого как модуль над собой, а также любой свободный K-модуль свободны от кручения. Напротив, в $\mathbb{Z}$-модуле вычетов $\mathbb{Z}/(k)$ все элементы являются элементами кручения.

Упражнение 11.5. Покажите, что любой гомоморфизм $M \xrightarrow{\varphi} N$ в свободный от кручения модуль N переводит $\operatorname{Tors}(M)$ в нуль.

11.2.4. Задание гомоморфизмов. Пусть модуль M порождается элементами e_i. Тогда любой гомоморфизм модулей $\varphi : M \longrightarrow N$ однозначно восстанавливается по образам $\varphi(e_i)$ этих образующих элементов: представим каждый вектор $a \in M$ как $a = \sum \lambda_i e_i$ и получим, что

$$\varphi(a) = \varphi\big(\sum \lambda_i e_i\big) = \sum \lambda_i \varphi(e_i)\,.$$

Однако, если мы захотим *определить* гомоморфизм $\varphi : M \longrightarrow N$ указав в модуле N некоторые элементы $b_i = \varphi(e_i)$ и затем продолжив φ по линейности на все остальные элементы модуля M формулой $\varphi(\sum \lambda_i e_i) = \sum \lambda_i b_i$, то такое определение может оказаться некорректным из-за того, что у каждого вектора имеется несколько разных выражений через образующие. Поэтому элементы $b_i = \varphi(e_i)$, вообще говоря, нельзя выбирать произвольно.

Лемма 11.1

Для того, чтобы правило $e_i \longmapsto b_i \in N$ корректно продолжалось по линейности до гомоморфизма модулей $M \longrightarrow N$, необходимо и достаточно, чтобы каждое соотношение между векторами e_i в модуле M выполнялось бы и между векторами b_i в модуле N:

$$\lambda_1 e_1 + \lambda_2 e_2 + \cdots + \lambda_n e_n = 0 \quad \Rightarrow \quad \lambda_1 b_1 + \lambda_2 b_2 + \cdots + \lambda_n b_n = 0\ .$$

Доказательство. Необходимость этого условия очевидна из определения гомоморфизма:

$$\sum \lambda_i e_i = 0 \quad \Rightarrow \quad \sum \lambda_i b_i = \sum \lambda_i \varphi(e_i) = \varphi\big(\sum \lambda_i e_i\big) = \varphi(0) = 0\,.$$

Наоборот, если все соотношения между e_i выполняются и между b_i, то продолжение по линейности корректно, поскольку для любых двух выражений произвольного вектора $a \in M$ через образующие

$$a = x_1 e_1 + x_2 e_2 + \cdots + x_n e_n = y_1 e_1 + y_2 e_2 + \cdots + y_n e_n \tag{11-7}$$

выполняется соотношение $\sum (x_i - y_i) e_i = 0$, а значит — и соотношение $\sum (x_i - y_i) b_i = 0$, из которого следует, что $x_1 b_1 + x_2 b_2 + \cdots + x_n b_n = y_1 b_1 + y_2 b_2 + \cdots + y_n b_n$ в модуле N, т.е. что $\varphi(a)$ не зависит от того, каким из разложений (11-7) пользоваться для вычисления $\varphi(a)$. □

11.2.5. Универсальное свойство базиса. Если множество векторов $\mathscr{E} = \{e_i\} \subset M$ является базисом модуля M, т.е. никаких соотношений между векторами e_i нет вообще, то любое отображение $\varphi : \mathscr{E} \longrightarrow N$ множества $\mathscr{E}$ в произвольный K-модуль N имеет единственное продолжение до гомоморфизма K-модулей $\varphi : M \longrightarrow N$. Верно и обратное:

Лемма 11.2

Множество векторов $\mathscr{E} = \{e_i\} \subset M$ тогда и только тогда является базисом K-модуля M, когда любое отображение $\varphi : \mathscr{E} \longrightarrow N$ множества $\mathscr{E}$ в произвольный K-модуль N единственным способом продолжается до гомоморфизма K-модулей $\varphi : M \longrightarrow N$.

Доказательство. Необходимость этого условия мы уже установили выше. Для доказательства достаточности образуем множество $\mathscr{E}' \simeq \mathscr{E}$, состоящее из формальных символов e_i', взаимно однозначно соответствующих векторам $e_i \in \mathscr{E}$, и рассмотрим свободный K-модуль N с базисом $\mathscr{E}'$. По определению, N состоит из всевозможных конечных формальных линейных комбинаций символов e_i' с коэффициентами из K, все эти комбинации считаются различными и складываются и умножаются на числа по очевидным естественным правилам.

По условию леммы, отображение множеств $\mathscr{E} \longrightarrow N$, переводящее e_i в e_i' однозначно продолжается до гомоморфизма модулей $\varphi : M \longrightarrow N$. Так как по построению элементы e_i' образуют базис свободного модуля N, отображение множеств $\mathscr{E}' \longrightarrow M$, переводящее e_i' в e_i, также однозначно продолжается до гомоморфизма модулей $\psi : N \longrightarrow M$. Поскольку гомоморфизм $\psi\varphi : M \longrightarrow M$ и тождественный гомоморфизм $\mathrm{Id}_M : M \longrightarrow M$ оба продолжают тавтологическое вложение $\mathscr{E} \subset M$ до K-модульного гомоморфизма $M \longrightarrow M$, они — в силу единственности продолжения — совпадают: $\psi\varphi = \mathrm{Id}_M$. По той же самой причине $\varphi\psi = \mathrm{Id}_N$. Тем самым, гомоморфизмы φ и ψ обратны друг другу, и модули M и N изоморфны. Поскольку векторы e_i' составляют базис модуля N, их образы e_i при изоморфизме ψ составляют базис в M. □

11.3. Матрицы гомоморфизмов. Если K-модуль M порождается элементами $w = (w_1, w_2, \dots, w_m)$, а K-модуль N — элементами $v = (v_1, v_2, \dots, v_n)$, то всякому гомоморфизму K-модулей $F : M \longrightarrow N$ можно сопоставить матрицу F_{vw}, в j-том столбце которой стоят коэффициенты какого-нибудь линейного выражения вектора $F(w_j)$ через образующие v. Иначе говоря, матрица F_{vw} удовлетворяет соотношению

$$F(w) = vF_{vw} \tag{11-8}$$

(где $F(w) = \big(F(w_1),\, F(w_2),\, \dots\,,\, F(w_r)\big)$, как в n° 9.3.2).

Обозначение F_{vw} не корректно в том смысле, что матрица F_{vw} определяется равенством (11-8) неоднозначно, и одному и тому же гомоморфизму F можно, вообще говоря, сопоставить много *разных* матриц в одних и тех же системах порождающих, но оно удобно и мы будем им пользоваться. Если $F : M \longrightarrow M$ является эндоморфизмом K-модуля M, порождённого векторами $w = (w_1, w_2, \dots, w_m)$, то вместо F_{ww} мы пишем F_w и называем F_w матрицей F в системе образующих w.

Лемма 11.3

Если квадратная матрица $F_w \in \mathrm{Mat}_n(K)$ является матрицей эндоморфизма

$F : M \longrightarrow M$ в какой-то системе образующих, то $\operatorname{im} F$ содержит образ гомоморфизма $\det(F_w) \cdot \mathrm{Id}_M : u \mapsto u \cdot \det F_w$ умножения на $\det(F_w)$.

Доказательство. Гомоморфизм $\det(F_w) \cdot \mathrm{Id}_M$ имеет в системе образующих w матрицу $\det(F_w) \cdot E = F_w \widehat{F} w$. Поэтому образы образующих, т. е. столбцы матрицы $w \det(F_w) \cdot E = w\, F_w \widehat{F} w$ являются линейными комбинациями столбцов матрицы $w\, F_w = F(w)$, т. е. образов образующих при гомоморфизме F, что и утверждается. □

11.3.1. Пример: тождество Гамильтона – Кэли. Пусть $A \in \mathrm{Mat}_n(K)$ — произвольная квадратная матрица над коммутативным кольцом K. Наделим свободный K-модуль K^n структурой модуля над кольцом многочленов $K[t]$, полагая по определению, что результатом умножения столбца $v \in K^n$ на многочлен $f(t) = f_0 + f_1 t + \dots + f_m t^m$ является столбец

$$f(t)v \overset{\text{def}}{=} f_0 v + f_1 A v + f_2 A^2 v + \dots + f_m A^m v$$

получающийся умножением столбца v слева на матрицу $f(A)$ — результат подстановки матрицы A в многочлен $f(t)$ (ср. с зад. 9.8).

Упражнение 11.6. Проверьте выполнения аксиом $K[t]$-модуля для K^n.

Стандартный базис $e_1, e_2, \dots, e_n$ модуля K^n над K тем более порождает K^n над $K[t]$. Гомоморфизм $t\mathrm{Id} : u \longmapsto tu$ умножения на t имеет в этой системе порождающих две различных матрицы: tE и A. Поэтому нулевой гомоморфизм, отображающий все векторы k^n в нуль, можно задать в образующих $e_1, e_2, \dots, e_n$ матрицей $tE - A$. Согласно лем. 11.3 умножение на $\det(tE - A)$ отображает любой вектор K^n в нуль.

Но умножение на $\det(tE - A)$ является K-линейным эндоморфизмом, матрица которого в стандартном базисе получается подстановкой матрицы A вместо t в многочлен $\chi_A(t) = \det(tE - A)$. Поскольку K^n свободен над K, матрица $\chi_A(A)$ нулевая. Нами доказана фундаментальная

Теорема 11.1 (тождество Гамильтона – Кэли)
Над любым коммутативным кольцом K при подстановке квадратной матрицы A вместо переменной t в многочлен $\chi_A(t) = \det(tE - A) \in K[t]$ получается нулевая матрица. □

Многочлен $\chi_A(t) = \det(tE - A)$ называется *характеристическим многочленом* матрицы A. Согласно зад. 10.23 коэффициент многочлена $\chi_A(t)$ при t^k равен умноженной на $(-1)^{n-k}$ сумме главных диагональных миноров порядка $n - k$ матрицы A. В частности, свободный член $\chi_A(t)$ равен $(-1)^n \det A$, а коэффициент при t^{n-1} равен минус сумме диагональных элементов матрицы A. Сумма диагональных элементов называется *следом* и обозначается $\operatorname{tr} A$.

Из теор. 11.1 следует, к примеру, что всякая 2×2 матрица A удовлетворяет квадратному уравнению $t^2 + \operatorname{tr}(A) \cdot t + \det(A) = 0$ (что согласуется с формулой

(9-5) на стр. 154), а всякая 3×3 матрица

$$A=\begin{pmatrix} a_{11} & a_{12} & a_{13}\\ a_{21} & a_{22} & a_{23}\\ a_{31} & a_{32} & a_{33}\end{pmatrix}$$

удовлетворяет кубическому уравнению $t^3-\operatorname{tr}(A)\cdot t^2+\sigma_2(A)\cdot t-\det(A)=0$, где

$$\sigma_2(A)=(a_{11}a_{22}-a_{12}a_{21})+(a_{11}a_{33}-a_{13}a_{31})+(a_{22}a_{33}-a_{23}a_{32})\ .$$

11.4. Разложимость. Прямые суммы и прямые произведения модулей определяются дословно также, как для векторных пространств (см. n° 7.3.3).

Упражнение 11.7. Покажите, что прямая сумма свободных модулей с базисами $\mathscr{E}_1$ и $\mathscr{E}_2$ является свободным модулем с базисом $\mathscr{E}_1\sqcup\mathscr{E}_2$ ($\mathscr{E}_1$ и $\mathscr{E}_2$ обозначают множества базисных векторов).

Если набор подмодулей $N_1,N_2,\dots,N_s\subset M$ таков, что гомоморфизм сложения

$$N_1\oplus N_2\oplus\ \cdots\ \oplus N_s\xrightarrow{(a_1,a_2,\dots,a_s)\mapsto a_1+a_2+\dots+a_s} M$$

является изоморфизмом, то говорят, что модуль M является *прямой суммой подмодулей* N_i. Это условие означает, что каждый вектор $a\in M$ имеет единственное разложение вида $a=\sum b_i$ с $b_i\in N_i$. Например, свободный K-модуль с n линейно независимыми образующими изоморфен прямой сумме $K^n=K\oplus K\oplus\ \cdots\ \oplus K$ (всего n слагаемых).

Лемма 11.4
Для того чтобы модуль M распадался в прямую сумму двух своих подмодулей L и N необходимо и достаточно, чтобы L и N порождали M и $L\cap N=0$.

Доказательство. Сюрьективность гомоморфизма сложения

$$\sigma: L\oplus N\xrightarrow{(a,b)\mapsto a+b} M$$

равносильна тому, что L и N порождают M, а инъективность (т. е. отсутствие ядра) равносильна условию $L\cap N=0$, поскольку $(a,b)\in\ker\sigma\Rightarrow a=-b\in L\cap N$, и наоборот, $a\in L\cap N\Rightarrow(a,-a)\in\ker\sigma$. □

Упражнение 11.8. Пусть модуль M является прямой суммой $M=L\oplus N$ двух своих подмодулей $L,N\subset M$. Покажите, что $M/N\simeq L$ и $M/L\simeq N$.

11.4.1. Неразложимые модули и дополнительные подмодули. Модули, не представимые в виде прямой суммы двух своих собственных подмодулей называются *неразложимыми*.

Например, $\mathbb{Z}$-модуль $\mathbb{Z}$ неразложим, поскольку всякий собственный подмодуль $I\subset\mathbb{Z}$ — это главный идеал $I=(d)$, и из наличия разложения $\mathbb{Z}=(d)\oplus N$

вытекало бы, что в $\mathbb{Z}$ есть подмодуль N, изоморфный по упр. 11.8 модулю $\mathbb{Z}/(d)$. Но это невозможно, т. к. в $\mathbb{Z}$ нет кручения.

Этот пример показывает, что над кольцом K, содержащим необратимые элементы, у подмодуля $N \subset M$ может не оказаться *дополнительного подмодуля* $L \subset M$, такого что $M = L \oplus N$, как это происходит для векторных пространств над полем.

Упражнение 11.9. Пусть $M = \mathbb{Z}^2 = \mathbb{Z} \oplus \mathbb{Z}$ и $N \subset M$ — подмодуль, порождённый векторами $(2, 1)$ и $(1, 2)$. Покажите, что $N \simeq \mathbb{Z}^2$, $M/N \simeq \mathbb{Z}/(3)$, и не существует подмодуля $L \subset M$, такого что $M = L \oplus N$.

11.5. Ранг свободного модуля. В этом разделе мы докажем, что число элементов в базисе конечно порождённого свободного модуля M не зависит от выбора базиса. Это число называется *рангом* свободного модуля M и обозначается $\operatorname{rk} M$.

Наличие в модуле M базиса $(e_1, e_2, \dots, e_m)$ равносильно тому, что гомоморфизм K-модулей

$$K^m = \underbrace{K \oplus K \oplus \cdots \oplus K}_{m} \longrightarrow M,$$

переводящий вектор $(\lambda_1, \lambda_2, \dots, \lambda_m) \in K^m$ в вектор $\lambda_1 e_1 + \lambda_2 e_2 + \cdots + \lambda_m e_m \in M$, является изоморфизмом. Мы покажем, что существование изоморфизма $M \simeq K^n$ возможно при единственном n. Для этого нам понадобится две алгебраические конструкции, каждая из которых важна сама по себе.

11.5.1. Факторизация модуля по идеалу кольца. Для любого идеала $I \subset K$ и произвольного K-модуля M обозначим через $IM \subset M$ подмодуль, образованный всевозможными линейными комбинациями элементов модуля M с коэффициентами из идеала I:

$$IM = \{x_1 a_1 + x_2 a_2 + \cdots + x_n a_n \mid x_i \in I,\ a_i \in M\}.$$

Упражнение 11.10. Проверьте, что IM действительно является K-подмодулем в M.

Фактор модуль M/IM обладает канонической структурой модуля над фактор кольцом K/I, которая корректно задаётся правилом

$$[\lambda]_I \cdot [a]_{[IM]} = [\lambda a]_{[IM]}$$

где мы, как обычно, обозначаем квадратными скобками класс эквивалентности соответствующего элемента:

$$[\lambda]_I = \lambda \pmod{I}, \quad [a]_{[IM]} = a \pmod{[IM]}.$$

В самом деле, если $\lambda' = \lambda + x$ и $a' = a + v$, где $x \in I$, $v \in IM$, то $\lambda' a' = \lambda a + (xa + \lambda v + xv)$, где взятая в скобки сумма лежит в IM.

Если применить эту конструкцию к прямой сумме модулей $M = M_1 \oplus M_2 \oplus \cdots \oplus M_m$, то, поскольку все операции в прямой сумме выполняются покомпонентно, мы получим на выходе прямую сумму

$$M/IM = (M_1/IM_1) \oplus (M_2/IM_2) \oplus \cdots \oplus (M_m/IM_m).$$

В частности, результатом факторизации свободного K-модуля $M = K^n$ по идеалу $I \subset K$ является свободный K/I-модуль $M/IM = (K/I)^n$ того же ранга.

Для доказательства независимости ранга от выбора базиса достаточно найти в кольце K такой идеал I, чтобы фактор кольцо $\Bbbk = K/I$ было полем: наличие изоморфизма $M \simeq K^n$ означает, что $M/IM \simeq (K/I)^n \simeq \Bbbk^n$ является n-мерным векторным пространством над $\Bbbk$, и число $n = \dim_{\Bbbk}(M/IM)$ однозначно определяется модулем M.

11.5.2. Максимальные идеалы. Напомним, что отличный от всего кольца идеал $I \subset K$ называется *максимальным*, если для любого элемента $\lambda \in K \smallsetminus I$ идеал (λ, I), порождённый I и этим элементом, совпадает со всем кольцом.

Покажем, что фактор кольцо K/I является полем тогда и только тогда, когда идеал $I \subset K$ максимален. В самом деле, для любого элемента $\lambda \in K \smallsetminus I$ равенство $(\lambda, I) = K$ равносильно тому, что идеал (λ, I) содержит единицу, что в свою очередь, равносильно разрешимости уравнения $\lambda x + y = 1$ относительно $x \in K$ и $y \in I$. С другой стороны, разрешимость этого уравнения означает в точности, что класс $[\lambda]_I$ обратим в фактор кольце K/I.

Таким образом, для доказательства независимости ранга свободного модуля от выбора базиса нам достаточно показать, что в любом кольце имеется хоть один максимальный идеал.

Стандартное теоретико-множественное рассуждение с использованием *леммы Цорна*[1] позволяет доказать даже более сильное утверждение: любой отличный от всего кольца идеал $J \subset K$ содержится в некотором максимальном идеале. Действительно, множество отличных от всего кольца идеалов, содержащих данный идеал J, удовлетворяет условиям леммы Цорна: оно непусто, частично упорядочено по включению, и любое семейство вложенных друг в друга идеалов содержится в идеале, полученном объединением всех идеалов семейства. Тем самым, среди отличных от кольца идеалов, содержащих J, найдётся идеал I, такой что для любого элемента $a \in K \smallsetminus I$, идеал $(a, I) \supsetneq I$ совпадёт со всем кольцом, что и требовалось.

11.5.3. Модули бесконечного ранга. Предыдущее рассуждение остаётся в силе и для свободных модулей с бесконечным базисом. В этом случае оно показывает, что мощность множества базисных векторов не зависит от выбора

[1] напомним, что лемма Цорна утверждает, что если частично упорядоченное множестве X таково, что для любого линейно упорядоченного подмножества $Y \subset X$ существует $x \in X$ со свойством $\forall y \in Y \;\; y \leqslant x$, то в множестве X существует элемент μ, максимальный в том смысле, что $\forall x \in X \;\; \mu \leqslant x \Rightarrow x = \mu$ (см. зад. 1.19 и доказательство теор. 7.1)

базиса и равна мощности базиса векторного пространства M/IM над полем $\Bbbk = K/I$, где $I \subset K$ — какой-нибудь максимальный идеал кольца K.

Задачи для самостоятельного решения к §11

Задача 11.1. Покажите, что если фактор модуль $L = M/N$ свободен, то $M \simeq N \oplus L$.

Задача 11.2. Покажите, что если порядки[1] конечных подгрупп $A_1, A_2, \dots, A_n$ в абелевой группе A взаимно просты, то их сумма в A является прямой.

Задача 11.3. Найдите все разложения абелевой группы $\mathbb{Z}/(5) \oplus \mathbb{Z}/(5)$ в прямую сумму двух циклических подгрупп.

Задача 11.4. Пусть M — свободный $\mathbb{Z}$-модуль с базисом $e_1, e_2, \dots, e_n$ и

$$w = x_1e_1 + x_2e_2 + \dots + x_ne_n \in M$$

отличен от нуля. Докажите, что подмодуль $\langle w \rangle \subset M$, порождённый w, выделяется прямым слагаемым[2] тогда и только тогда, когда $\text{нод}(x_1, x_2, \dots, x_n) = 1$.

Задача 11.5. Является ли $\mathbb{Z}$-подмодуль $M \subset \mathbb{Z}[x]$, состоящий из всех многочленов с чётным свободным членом: а) конечно порожденным? б) свободным? в) Существует ли $N \subset \mathbb{Z}[x]$, такой что $M \oplus N = \mathbb{Z}[x]$?

Задача 11.6 (полупростые $\mathbb{Z}$-модули). $\mathbb{Z}$-модуль M называется *полупростым*, если для любого собственного ненулевого подмодуля $N \subset M$ можно указать подмодуль $L \subset M$, такой что $M = L \oplus M$. Какие из перечисленных ниже $\mathbb{Z}$-модулей полупросты (далее $m, n \geqslant 2$ произвольные целые):
а) $\mathbb{Z}$ б) $\mathbb{Z}^n$ в) $\mathbb{Z}/(p)$ г) $\big(\mathbb{Z}/(p)\big)^n$ д) $\mathbb{Z}/(p^m)$ е) $\big(\mathbb{Z}/(p^m)\big)^n$

Задача 11.7. Докажите, что $\operatorname{Hom}(M_1 \oplus M_2, N_1 \oplus N_2) = \bigoplus\limits_{\mu,\nu=1}^{2} \operatorname{Hom}(M_\mu, N_\nu)$.

Задача 11.8. Опишите модуль всех $\mathbb{Z}$-линейных гомоморфизмов $\operatorname{Hom}(\mathbb{Z}/(m), \mathbb{Z}/(n))$ в случае, когда а) $m = p^\mu$, $n = p^\nu$ (p простое, $\mu, \nu \in \mathbb{N}$ любые) б) $\text{нод}(m, n) = 1$ в) m, n любые

Задача 11.9 (целозначные многочлены). Многочлен $f \in \mathbb{Q}[x]$ называется *целозначным*, если $f(m) \in \mathbb{Z}\ \forall m \in \mathbb{Z}$. Например, многочлен $x(x+1)/2$ является целозначным. Докажите, что целозначные многочлены образуют свободный $\mathbb{Z}$-подмодуль $M \subset \mathbb{Q}[x]$ с базисом $\gamma_k(x) = (x+1)...(x+k)/k!$ (где $k \geqslant 0$ и мы полагаем $\gamma_0 = 1$). Для этого покажите, что
а) многочлены γ_k составляют базис векторного пространства $\mathbb{Q}[x]$ над $\mathbb{Q}$
б) разностный оператор $\nabla : f(x) \mapsto f(x) - f(x-1)$ переводит γ_k в γ_{k-1}

[1] напомним, что *порядком* конечной группы называется количество элементов в ней
[2] т.е. $\exists$ подмодуль $L \subset M$, такой что $M = \langle w \rangle \oplus L$

в) коэффициент при γ_k в разложении произвольного многочлена $f \in \mathbb{Q}[x]$ по γ-базису над полем $\mathbb{Q}$ равен $\nabla^k f(0)$.
г) Докажите, что $n+1$ многочленов n-той степени

$$c_k^{(n)}(x) = (x+k+1)...(x+k+n)/n! \quad (\text{где } 0 \leqslant k \leqslant n)$$

составляют базис подмодуля $M_{\leqslant d} \subset M$ целозначных многочленов степени $\leqslant n$.
д) Покажите, что фактор[1] $M_d/\mathbb{Z}[x]_{\leqslant d}$ конечен и выясните, сколько в нём элементов.
е*) Покажите, что кольцо $\mathbb{Z}$-линейных эндоморфизмов $M \longrightarrow M$, перестановочных со всеми операторами сдвига: $f(x) \longmapsto f(x+n)$, изоморфно $\mathbb{Z}[[\nabla]]$, где $\nabla : f(x) \mapsto f(x) - f(x-1)$ (в частности, это кольцо коммутативно).

Задача 11.10 (двойственные решётки). Пусть $\mathbb{Z}$-подмодуль $N \subset \mathbb{Z}^n$ таков, что фактор модуль $\mathbb{Z}^n/N$ конечен, и пусть $L = \mathrm{Hom}(\mathbb{Z}^n, \mathbb{Z})$ и

$$N' = \{\varphi \in \mathrm{Hom}(\mathbb{Z}^n, \mathbb{Q}) \mid \varphi(N) \subset \mathbb{Z}\}.$$

Как связаны между собой $\mathbb{Z}^n/N$ и N'/L ? Одинаково ли у них число элементов?

Задача 11.11 (циклические абелевы группы). $\mathbb{Z}$-модуль (или, что то же самое, абелева группа) A, порождённый одним элементом, называется *циклическим*. Покажите что а) любой циклический $\mathbb{Z}$-модуль изоморфен $\mathbb{Z}$ или $\mathbb{Z}/(n)$
б) модуль $\mathbb{Z}/(n) \oplus \mathbb{Z}/(m)$ циклический, если и только если нод$(m, n) = 1$.

Задача 11.12. Докажите, что мультипликативная абелева группа ненулевых комплексных чисел $\mathbb{C}^*$ является прямой суммой мультипликативной подгруппы положительных вещественных чисел $\mathbb{R}^*_{>0} \subset \mathbb{C}^*$ и мультипликативной подгруппы $S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$

Задача 11.13. Докажите, что при $n \geqslant 3$ мультипликативная группа обратимых вычетов в $(\mathbb{Z}/(2^n)$ изоморфна прямой сумме мультипликативной группы знаков $\{\pm 1\}$ и циклической аддитивной группы $\mathbb{Z}/\left(2^{n-2}\right)$.

Задача 11.14 (лемма Накаямы). Пусть в коммутативном кольце K к с единицей имеется ровно один максимальный идеал $\mathfrak{m} \subset K$ (такие кольца называются *локальными*). Для конечно порождённого K-модуля M докажите, что
а) фактор модуль $V = M/\mathfrak{m}M$ является конечномерным векторным пространством над полем $\mathbb{k} = K/\mathfrak{m}$
б) если $V = 0$ (т.е. $M = gM$), то $M = 0$ (подсказка: фиксируйте некоторую систему образующих модуля M и воспользуйтесь тем, что тождественное отображение Id_M имеет две различных матрицы — единичную и с элементами из $\mathfrak{m}$, и вычислите определитель их разности[2])
в) если классы элементов $w_1, w_2, \dots, w_m \in M$ составляют базис V над $\mathbb{k}$, то сами эти элементы порождают M над K

[1]целозначные многочлены степени $\leqslant d$ по модулю многочленов с целыми коэффициентами
[2]ср. с доказательством тождества Гамильтона–Кели из n° 11.3.1

Задача 11.15 (целые элементы). Пусть $A \subset B$ коммутативные кольца с единицей. Покажите, что следующие свойства элемента $b \in B$ эквивалентны друг другу (элемент $b \in B$ с такими свойствами, называется *целым* над A):

а) $b^m = a_1 b^{m-1} + \cdots + a_{m-1} b + a_0$ для неких $m \in \mathbb{N}$, $a_1, a_2, \ldots, a_m \in A$;

б) A-модуль, порождённый всеми неотрицательными степенями $\{b^i\}_{i \geqslant 0}$, конечно порождён над A;

в) существует B-*точный*[1] конечно порожденный A-модуль $M \subset B$, такой что[2] $bM \subset M$.

Задача 11.16 (целое замыкание). В условиях зад. 11.15 множество всех $b \in B$, целых над A, называется *целым замыканием* A в B. Если оно совпадает с A, то A называется *целозамкнутым* в B. Если оно совпадает с B, то расширение $A \subset B$ называется *целым* (а B называется *целой A-алгеброй*). Покажите, что

а) целое замыкание A в B является подкольцом в B

б) элемент $c \in C \supset B \supset A$, целый над целым замыканием A в B, цел и над A

в) если поле $B \supset A$ цело над A, то A тоже поле

г) если целостное $B \supset A$ цело над A, и A поле, то B тоже поле.

Задача 11.17 (нормальные кольца). Целостное коммутативное кольцо, целозамкнутое в своём поле частных, называется *нормальным*. Покажите, что всякое факториальное кольцо нормально (если общий случай вызывает затруднения, сначала докажите это для колец $\mathbb{Z}$ и $\mathbb{Q}[x_1, x_2, \ldots, x_n]$).

Задача 11.18 (лемма Гаусса – Кронекера – Дедекинда).

а) Пусть $A \subset B$ — произвольное расширение коммутативных колец. Докажите, что все коэффициенты произведения fg двух приведённых многочленов $f, g \in B[x]$ целы над A, если и только если каждый коэффициент и у f и у g цел[3] над A.

б) Пусть A — нормальное кольцо с полем частных $\mathbb{F}$. Докажите, что произведение fg двух приведённых многочленов $f, g \in \mathbb{F}[x]$ лежит в $A[x]$ тогда и только тогда, когда и f, и g лежат в $A[x]$.

Задача 11.19. Рассмотрим произвольную алгебру B над полем частных $\mathbb{F}$ произвольного целостного кольца A.

а) Пусть $b \in B$ алгебраичен над $\mathbb{F}$ и имеет минимальный многочлен $\mu_b \in \mathbb{F}[x]$. Докажите, что если b цел над A, то все коэффициенты μ_b целы над A.

б) Пусть кольцо A нормально. Докажите, что для целости $b \in B$ над A необходимо и достаточно, чтобы b был алгебраичен над $\mathbb{F}$ и его минимальный полином μ_b над $\mathbb{F}$ лежал в $A[x]$.

---

[1] абелева подгруппа $M \subset B$ называется B-*точной*, если $bM = 0 \Rightarrow b = 0$

[2] подсказка: при выводе в) из а) можно воспользоваться тем, что $\det(F) \cdot M \subset F(M)$ $\forall$ $M \xrightarrow{F} M$

[3] подсказка: рассмотрите всё в построенном в зад. 4.19 расширении $C \supset B \supset A$, где оба сомножителя раскладываются в произведение приведённых линейных двучленов

§12. Конечно порождённые модули над кольцами главных идеалов

12.1. Теорема об инвариантных множителях. Всюду в этом параграфе мы обозначаем через K произвольное кольцо главных идеалов. Все K-модули по умолчанию предполагаются конечно порождёнными. Договоримся понимать под свободным модулем ранга нуль нулевой модуль.

Лемма 12.1
Всякий подмодуль $N \subset K^m$ свободен и имеет $\operatorname{rk}(N) \leqslant m$.

Доказательство. Индукция по m. Если $m = 1$, то подмодуль $N \subset K$ — это главный идеал $(d) \subset K$. Если $d = 0$, то $N = 0$ свободен ранга нуль. Если $d \neq 0$, то (d) свободен с базисом d, поскольку $xd = yd \Rightarrow (x - y)d = 0 \Rightarrow x = y$, т. к. в K нет делителей нуля.

Пусть теперь $m > 1$. Будем записывать векторы $v \in K^m$ строчками их координат в стандартном базисе $e_1, e_2, \ldots, e_m$ координатного свободного модуля K^m. Тогда первые координаты $x_1(v)$ всевозможных векторов $v \in N$ образуют идеал в K. Если он нулевой, то N содержится в свободном модуле ранга $m - 1$ с базисом $e_2, \ldots, e_m$, и по индукции свободен ранга $\leqslant (m - 1)$. Если идеал первых координат векторов из N не нулевой, то это — главный идеал $(d) \subset K$ с образующей $d \neq 0$. Обозначим через $v_1 \in N$ какой-нибудь вектор с первой координатой d. Тогда $N = K \cdot v_1 \oplus N'$, где $N' \subset N$ — подмодуль, состоящий из векторов с нулевой первой координатой. Действительно, $(K \cdot v_1) \cap N' = 0$, и любой вектор $v \in N$ представляется в виде $\lambda v_1 + w$, где $\lambda = x_1(v)/x_1(v_1)$ (деление возможно, поскольку первые координаты всех векторов $v \in N$ делятся на $d = x_1(v_1)$), а $w = v - \lambda v_1 \in N'$. Модуль Kv_1, порождённый вектором v_1, свободен ранга 1, поскольку в объемлющем свободном модуле K^m нет кручения. Модуль N' содержится в свободном модуле ранга $m - 1$ с базисом $e_2, \ldots, e_m$, и по индукции свободен ранга $\leqslant (m - 1)$. Поэтому $N = K \cdot v_1 \oplus N'$ свободен ранга $\leqslant m$. □

12.1.1. Инвариантные множители. Основным результатом о свободных модулях конечного ранга является

Теорема 12.1 (об инвариантных множителях)
Для любого подмодуля N свободного модуля M конечного ранга над кольцом главных идеалов K в модуле M существует базис $(e_1, e_2, \ldots, e_m)$, такой что некоторые кратности $\lambda_1 e_1, \lambda_2 e_2, \ldots, \lambda_n e_n$ первых $n \leqslant m$ базисных векторов составляют базис в N и каждый из множителей λ_i делится на все предыдущие множители λ_j с $j < i$. Набор множителей $\lambda_1, \lambda_2, \ldots, \lambda_n$ с точностью до умножения на обратимые элементы кольца не зависит от выбора такого базиса.

Множители $\lambda_1, \lambda_2, \ldots, \lambda_n$, о которых идёт речь в теореме, называются *инвариантными множителями* подмодуля $N \subset M$, а базисы $e_1, e_2, \ldots, e_m \in M$

и $\lambda_1 e_1, \lambda_2 e_2, \dots, \lambda_n e_n \in N$ — *взаимными базисами* модуля M и подмодуля $N \subset N$. Остаток этого раздела будет посвящён доказательству теор. 12.1.

12.1.2. Матричная переформулировка теоремы. Рассмотрим какие-нибудь базисы $w = (w_1, w_2, \dots, w_m) \subset M$, $v = (v_1, v_2, \dots, v_n) \subset N$ и обозначим через C_{wv} матрицу, в j-том столбце которой стоят координаты вектора v_j в базисе w, так что $v = wC_{wv}$. Наборы векторов $w' = wF_{ww'}$ и $v' = vG_{vv'}$ тогда и только тогда являются базисами в M и N, когда матрицы $F_{ww'}$ и $G_{vv'}$ обратимы над кольцом K, и при переходе от базисов w и v к базисам $w' = wF_{ww'}$ и $v' = vG_{vv'}$, матрица C_{wv} преобразуется в матрицу $C_{w'v'} = F_{ww'}^{-1} C_{wv} G_{vv'}$.

Обозначим через $\mathrm{GL}_k(K) \subset \mathrm{Mat}_k(K)$ группу обратимых матриц. Утверждение теоремы об инвариантных множителях (теор. 12.1) равносильно существованию таких матриц $F \in \mathrm{GL}_m(K)$ и $G \in \mathrm{GL}_n(K)$, что матрица

$$D = F^{-1} C_{wv} G = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \\ & 0 & \end{pmatrix} \tag{12-1}$$

имеет $d_{ij} = 0$ при $i \neq j$, а каждый её «диагональный» элемент $d_{ii} = \lambda_i$ делится на все предыдущие $d_{jj} = \lambda_j$ с $j < i$. Действительно, наличие таких матриц означает, что базис $e = wF$ модуля M и базис

$$vG = wC_{vw}G = eF^{-1}C_{vw}G = eD = (\lambda_1 e_1, \lambda_2 e_2, \dots, \lambda_n e_n)$$

подмодуля N являются искомыми взаимными базисами.

12.1.3. Независимость инвариантных множителей от выбора базиса означает независимость диагональных элементов λ_k матрицы (12-1) от выбора матриц F и G, удовлетворяющих соотношению (12-1). Дадим инвариантную характеризацию этих элементов. Поскольку $\lambda_i \,\vdots\, \lambda_j$ при $i > j$, произведение первых k диагональных элементов $\lambda_1 \lambda_2 \cdots \lambda_k$ равно наибольшему общему делителю всех $k \times k$-миноров матрицы D (для каждого $k = 1, \dots, n$). Обозначить наибольший общий делитель всех $k \times k$-миноров данной прямоугольной матрицы A через $\Delta_k(A)$. Тогда k-тый множитель λ_k равен

$$\lambda_k = \Delta_k(D)/\Delta_{k-1}(D) = \Delta_k(C_{wv})/\Delta_{k-1}(C_{wv}),$$

поскольку из следующей далее леммы вытекает, что $\Delta_k(C_{wv})$ с точностью до обратимого множителя не зависит от выбора базисов $w \subset M$ и $v \subset N$.

Лемма 12.2

Для любой матрицы $A \in \mathrm{Mat}_{m\times n}(K)$ и любых $F \in \mathrm{GL}_m(K)$ и $G = \mathrm{GL}_n(K)$ с точностью до умножения на обратимые множители выполнены равенства

$$\Delta_k(AG) = \Delta_k(A) = \Delta_k(FA).$$

Доказательство. Мы докажем первое равенство $\Delta_k(AG) = \Delta_k(A)$ (второе получается из него транспонированием). Рассмотрим три набора грассмановых переменных $\xi = (\xi_1, \xi_2, \ldots, \xi_m)$, $\eta = (\eta_1, \eta_2, \ldots, \eta_n)$, $\zeta = (\zeta_1, \zeta_2, \ldots, \zeta_n)$, связанных линейными преобразованиями: $\eta = \xi \cdot A$ и $\zeta = \eta \cdot G = \xi \cdot (AG)$. Базисные грассмановы мономы степени k от этих наборов переменных связаны линейными преобразованиями, матрицы которых $\Lambda^k A$, $\Lambda^k G$ и $\Lambda^k(AG)$ суть матрицы $k \times k$-миноров матриц A, G и AG. Поскольку преобразование с матрицей $\Lambda^k(AG)$, выражающее мономы от ζ через мономы от ξ, является композицией преобразований с матрицами $\Lambda^k G$ и $\Lambda^k A$, выражающих мономы от ζ через мономы от η, а мономы от η — через мономы от ξ, выполняется равенство $\Lambda^k(AG) = \Lambda^k A \cdot \Lambda^k G$. Тем самым, $k \times k$-миноры матрицы AG являются линейными комбинациями $k \times k$-миноров матрицы A, и стало быть, $\Delta_k(AG)$ делится на $\Delta_k(A)$. Поскольку $A = (AG) \cdot G^{-1}$ и $\Lambda^k(A) = \Lambda^k(AG) \cdot \Lambda^k(G^{-1})$, то и наоборот, $\Delta_k(A)$ делится на $\Delta_k(AG)$. Таким образом, $\Delta_k(A)$ и $\Delta_k(AG)$ отличаются обратимым множителем. □

12.1.4. Обобщённые элементарные преобразования. Чтобы доказать теорему об инвариантных множителях, нам остаётся построить для произвольной прямоугольной матрицы C такие обратимые матрицы F и G, чтобы матрица $F^{-1}CG$ была диагональной, причём каждый из её диагональных элементов делил бы все последующие (стоящие правее и ниже). В духе метода Гаусса будем делать последовательные *обобщённые элементарные преобразования базисов* (ср. с n° 9.2.4). Каждое такое преобразование будет заменять пару базисных векторов a, b в модуле M или в модуле N на их линейные комбинации $a' = \alpha a + \beta b$ и $b' = \gamma a + \delta b$, так что

$$(a', b') = (a, b) \cdot \begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix} , \quad \text{где} \quad \alpha\delta - \beta\gamma = 1 , \tag{12-2}$$

оставляя все остальные базисные векторы обоих модулей неизменными. Применение такого преобразования к базисным векторам $(a, b) = (v_i, v_j)$ подмодуля N состоит в умножении i-того и j-того столбцов c_{*i} и c_{*j} матрицы C_{wv} справа на 2×2 матрицу

$$\begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix} ,$$

что заменяет их линейными комбинациями $\alpha c_{*i} + \beta c_{*j}$, $\gamma c_{*i} + \delta c_{*j}$ и не меняет остальных столбцов. Аналогичное преобразование базисных векторов $(a, b) = (w_i, w_j)$ объемлющего модуля M умножает i-тую и j-тую строки c_{i*} и c_{j*} матрицы C_{wv} слева на 2×2 матрицу

$$\begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix}^{-1} = \begin{pmatrix} \delta & -\gamma \\ -\beta & \alpha \end{pmatrix} ,$$

т. е. заменят их линейными комбинациями $\delta c_{i*} - \beta c_{j*}$, $-\gamma c_{i*} + \alpha c_{j*}$, и не меняет остальных строк.

Лемма 12.3

Преобразование (12-2) позволяет заменить любую пару стоящих в одной строке или в одном столбце элементов (α, β), таких что $\alpha \nmid \beta$ и $\beta \nmid \alpha$, парой $(d, 0)$, где $d = \text{нод}(\alpha, \beta)$.

Доказательство. Пусть $\alpha = ad$, $\beta = bd$ и, тем самым, $\alpha b = \beta a$. Представим $d = \text{нод}(\alpha, \beta)$ в виде $d = \alpha x + \beta y$. Тогда $1 = ax + by$. Таким образом,

$$\det \begin{pmatrix} x & -b \\ y & a \end{pmatrix} = 1$$

и если α и β стоят в одной строчке, то подойдёт такое умножение справа

$$(\alpha, \beta) \begin{pmatrix} x & -b \\ y & a \end{pmatrix} = (d, 0)$$

а если в одном столбце — умножение слева, задаваемое транспонированным равенством. □

Теорема об инвариантных множителях вытекает теперь из следующей леммы:

Лемма 12.4

Любая прямоугольная матрица C над кольцом главных идеалов обобщёнными элементарными преобразованиями строк и столбцов приводится к «диагональному» виду (12-1).

Доказательство. Заменяя по лем. 12.3 пары (a, b) не пропорциональных друг другу матричных элементов, стоящих в одной строке или в одном столбце парами $(\text{нод}(a, b), 0)$, а также применяя к строкам и столбцам гауссовы элементарные преобразования первого и второго типов, мы можем добиться того, чтобы левый верхний угловой матричный элемент c_{11} стал равен наибольшему общему делителю всех матричных элементов. Чтобы убедиться в этом, покажем, что пока в матрице есть не делящиеся на c_{11} элементы, мы можем преобразовать её так, чтобы идеал (c_{11}) строго увеличился.

Пусть не делящийся на c_{11} элемент a стоит в первой строке или первом столбце. Если $a|c_{11}$, то мы просто поменяем a и c_{11} местами, переставив строки или столбцы. Если $a \nmid c_{11}$, то мы заменим пару (c_{11}, a) на $(\text{нод}(c_{11}, a), 0)$ преобразованием из лем. 12.3. Если все элементы первой строки и первого столбца делятся на c_{11}, а a стоит строго ниже и строго левее c_{11}, то мы сначала занулим все кроме c_{11} элементы первой строки и первого столбца, добавив ко всем столбцам подходящие кратные первого столбца, а ко всем строкам — подходящие кратные первой строки. К элементу a при этом будут добавляться числа, кратные c_{11}, и он останется не делящимся на c_{11}. Прибавляя ту строку, где он стоит, к первой строке, получаем в первой строчке копию этого элемента, после чего строго увеличиваем идеал (c_{11}) так, как мы уже описывали.

Поскольку в кольце K не существует бесконечных возрастающих цепочек строго вложенных друг в друга идеалов, мы рано или поздно получим матрицу, все элементы которой делятся на c_{11}. Если занулить у такой матрицы все кроме c_{11} элементы первой строки и первого столбца, то все элементы подматрицы, стоящей в остальных строках и столбцах, будут делиться на c_{11}. По индукции, эту подматрицу можно диагонализовать элементарными преобразованиями строк и столбцов, не затрагивающих первую строку и первый столбец исходной матрицы. Это доказывает лемму и теор. 12.1. □

Упражнение 12.1. Припишем к матрице $C \in \mathrm{Mat}_{m\times n}(K)$ справа и снизу единичные матрицы размеров $m \times m$ И $n \times n$ соответственно, так что получится Г-образная таблица вида $\begin{array}{|c|c|}\hline C & E \\ \hline E & \\ \cline{1-1}\end{array}$, и приведём матрицу C к диагональному виду D, делая элементарные преобразования строк и столбцов сразу во всей Г-образной таблице. Покажите, что в получившейся в результате таблице $\begin{array}{|c|c|}\hline D & F \\ \hline G & \\ \cline{1-1}\end{array}$ матрицы F и G таковы, что $FCG = D$.

12.2. Пример: подрешётки в $\mathbb{Z}^m$. Рассмотрим в целочисленной решётке $\mathbb{Z}^m$ произвольную абелеву подгруппу $L \subset \mathbb{Z}^m$. По теореме об инвариантных множителях в $\mathbb{Z}^m$ существует такой базис $u_1, u_2, \dots, u_m$, что некоторые кратности m_1u_1, m_2u_2, … , $m_\ell u_\ell$ первых ℓ базисных векторов составляют базис в L как модуля над $\mathbb{Z}$. Отсюда вытекает, что L тоже является решёткой (свободным $\mathbb{Z}$-модулем), и что фактор модуль

$$\mathbb{Z}^m/L \simeq \frac{\mathbb{Z}}{(m_1)} \oplus \cdots \oplus \frac{\mathbb{Z}}{(m_\ell)} \oplus \mathbb{Z}^{m-\ell}\,. \tag{12-3}$$

Выясним, к примеру, как устроена подрешётка $L \subset \mathbb{Z}^3$, порождённая столбцами матрицы

$$C = \begin{pmatrix} 126 & 51 & 72 & 33 \\ 30 & 15 & 18 & 9 \\ 60 & 30 & 36 & 18 \end{pmatrix} \tag{12-4}$$

Для этого перейдём к взаимным базисам. Заметим, что нод всех элементов матрицы (12-4) равен 3, и мы можем получить -3 в позиции $(1,4)$, прибавляя к 1-й строке учетверённую 2-ю:

$$\begin{pmatrix} 6 & -9 & 0 & -3 \\ 30 & 15 & 18 & 9 \\ 60 & 30 & 36 & 18 \end{pmatrix}.$$

Умножаем 1-ю строку на -1 и меняем местами первый и последний столбцы

$$\begin{pmatrix} 3 & 9 & 0 & -6 \\ 9 & 15 & 18 & 30 \\ 18 & 30 & 36 & 60 \end{pmatrix}.$$

Теперь мы можем занулить левый столбец и верхнюю строку вне левого углового элемента, отнимая из 2-й и 3-й строк подходящие кратности 1-й строки, а затем из 2-го и 4-го столбцов подходящие кратности 1-го столбца

$$\begin{pmatrix} 3 & 0 & 0 & 0 \\ 0 & -12 & 18 & 48 \\ 0 & -24 & 36 & 96 \end{pmatrix}$$

Зануляем 3-ю строку, отнимая из неё удвоенную 2-ю, и видим, что нод элементов второй строки можно получить, прибавляя ко 2-му столбцу 3-й

$$\begin{pmatrix} 3 & 0 & 0 & 0 \\ 0 & 6 & 18 & 48 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Остаётся переставить третий столбец на место второго и занулить 3-й и 4-й столбцы, добавляя к ним подходящие кратности второго

$$\begin{pmatrix} 3 & 0 & 0 & 0 \\ 0 & 6 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Таким образом, $L \simeq \mathbb{Z}^2$, а $\mathbb{Z}^3/L \simeq \mathbb{Z}/(3) \oplus \mathbb{Z}/(6) \oplus \mathbb{Z}$.

Согласно n° 9.2, проделанные нами элементарные преобразования строк заключались в последовательном умножении слева на

$$\begin{pmatrix} -1 & 4 & 0 \\ 3 & -11 & 0 \\ 0 & -2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -4 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ -3 & 1 & 0 \\ -6 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -2 & 1 \end{pmatrix},$$

а преобразования столбцов — в последовательном умножении справа на

$$\begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & -3 & 0 & 2 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & -3 & -8 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} =$$

$$= \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & -3 & -8 \\ 0 & 1 & -2 & -8 \\ 1 & -3 & 9 & 26 \end{pmatrix}.$$

Упражнение 12.2. Проверьте эти формулы проделав предыдущие преобразования строк и столбцов с Г-образной матрицей $\begin{array}{|c|c|} \hline C & E \\ \hline E & \\ \cline{1-1} \end{array}$ (как в упр. 12.1).

Таким образом базис в решётке L составляют векторы

$$3\,u_1 = c_4 \quad \text{и} \quad 6\,u_2 = c_2 + c_3 - 3\,c_4\,,$$

где c_2, c_3, c_4 суть последние три столбца исходной матрицы C, а u_1, u_2 — первые два вектора взаимного с L базиса объемлющей решётки $\mathbb{Z}^3$, образованного столбцами матрицы

$$U = \begin{pmatrix} -1 & 4 & 0 \\ 3 & -11 & 0 \\ 0 & -2 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 11 & 4 & 0 \\ 3 & 1 & 0 \\ 6 & 2 & 1 \end{pmatrix}$$

Упражнение 12.3. Убедитесь, что следующие условия на подрешётку $L \subset \mathbb{Z}^m \subset \mathbb{Q}^m$, порождённую столбцами матрицы $C \in \mathrm{Mat}_{m\times n}(\mathbb{Z})$, эквивалентны друг другу: а) $\mathrm{rk}\, L = m$ б) абелева группа $\mathbb{Z}^m/L$ конечна

в) $\mathbb{Q}$-линейная оболочка L в $\mathbb{Q}^m$ равна всему пространству $\mathbb{Q}^m$

г) ранг матрицы C (рассматриваемой как матрица над полем $\mathbb{Q}$) равен m

12.2.1. Соизмеримые подрешётки. Подрешётки $L \subset \mathbb{Z}^m$, удовлетворяющие условию предыдущего упражнения называются *соизмеримыми* с $\mathbb{Z}^m$.

Отметим, что для доказательства соизмеримости с $\mathbb{Z}^m$ подрешётки L, заданной как линейная оболочка столбцов некоторой целочисленной матрицы C, достаточно указать в этой матрице ненулевой минор порядка m, а для отыскания ранга L можно привести C или C^t (смотря по тому, в какой из матриц меньше строк) над полем $\mathbb{Q}$ методом Гаусса к ступенчатому виду.

Предложение 12.1
Столбцы матрицы $C \in \mathrm{Mat}_n(\mathbb{Z})$ тогда и только тогда порождают соизмеримую подрешётку $L \subset \mathbb{Z}^n$, когда $\det C \neq 0$. В этом случае $|\mathbb{Z}^n/L| = |\det C|$ (иначе говоря, число элементов в факторе по соизмеримой подрешётке равно объёму параллелепипеда, натянутого на любой её базис).

Доказательство. Рассмотрим в $\mathbb{Z}^m$ базис $u_1, u_2, \dots, u_m$, некоторые кратности m_1u_1, m_2u_2, … , $m_\ell u_\ell$ первых ℓ базисных векторов которого составляют базис в L. Как мы видели при доказательстве теоремы об инвариантных множителях, переходу к таким базисам отвечает матричное равенство $F^{-1}CG = D$, где

$$D = \begin{pmatrix} m_1 & & & \\ & \ddots & 0 & \\ & & m_\ell & \\ & 0 & 0 & \\ & & & \ddots \end{pmatrix}$$

а $F, G \in \mathrm{GL}_n(\mathbb{Z})$ обратимы в $\mathrm{Mat}_n(\mathbb{Z})$. Согласно сл. 10.3, обратимость матриц F и G над кольцом $\mathbb{Z}$ равносильна равенствам $\det F = \pm 1$ и $\det G = \pm 1$. Поэтому $|\det C| = \det D$ нулевой, если $\ell < n$, и равен $m_1 m_2 \dots m_n$, если $\ell = n$. Во втором случае $\mathbb{Z}^n/L = \bigoplus\limits_i \mathbb{Z}/(m_i)$, откуда $|\det C| = |\mathbb{Z}^n/L|$. $\square$

12.3. Теорема об элементарных делителях. Вместо упорядоченного набора инвариантных множителей $\lambda_1, \lambda_2, \dots, \lambda_n$ иногда бывает удобнее иметь дело с неупорядоченным дизъюнктным объединением всех степеней p^n простых $p \in K$, входящих в разложения чисел $\lambda_1, \lambda_2, \dots, \lambda_n$ на простые множители. Точнее, рассмотрим для каждого $i = 1, \dots, n$ разложение

$$\lambda_i = p_{i1}^{m_{i1}} p_{i2}^{m_{i2}} \cdots p_{ik_i}^{m_{ik_i}}$$

в котором все числа p_{ij} просты и $p_{ij} \neq p_{ik}$ при $j \neq k$. Неупорядоченное дизъюнктное[1] объединение всех степеней $p_{ij}^{m_{ij}}$, входящих в эти разложения, называется набором *элементарных делителей* подмодуля $N \subset M$.

Набор инвариантных множителей $\lambda_1, \lambda_2, \dots, \lambda_n$ однозначно восстанавливается по набору элементарных делителей. Для этого надо упорядочить все степени каждого простого элемента p, входящие в набор элементарных делителей, так чтобы их показатели не убывали, и отправить максимальную из степеней каждого p в разложение последнего множителя λ_n, степень, предшествующую максимальной — в разложение λ_{n-1} и т. д. Например, набор элементарных делителей

$$\begin{array}{lllll} 3^2 & 3^2 & 3 & 3 & 3 \\ 2^3 & 2^3 & 2^2 & 2 & \\ 5 & 5 & & & \\ 7 & & & & \end{array}$$

даёт такой набор инвариантных множителей:

$$\begin{aligned} \lambda_5 &= 3^2 \cdot 2^3 \cdot 5 \cdot 7 \\ \lambda_4 &= 3^2 \cdot 2^3 \cdot 5 \\ \lambda_3 &= 3 \cdot 2^2 \\ \lambda_2 &= 3 \cdot 2 \\ \lambda_1 &= 3 \end{aligned}$$

Иными словами, если разместить элементарные делители по строкам диаграммы Юнга, записав в первую строку в порядке убывания степени того простого числа, степеней которого наличествует более всего, во вторую строку — степени следующего по количеству представленных в наборе степеней простого числа и т. д., то произведения элементарных делителей, оказавшихся в одном столбце, составят прочитанную справа налево последовательность инвариантных множителей.

Таким образом, имеется биекция между упорядоченными наборами элементов[2] $\lambda_1, \lambda_2, \dots, \lambda_n \in K$, в которых $\lambda_i | \lambda_j$ при $i < j$, и неупорядоченными наборами из (возможно повторяющихся) степеней $p_\nu^{m_\nu}$ простых элементов[3].

[1] *дизъюнктность* означает, что степень p^m, входящая в разложение ровно k инвариантных множителей λ_i, присутствует в итоговом неупорядоченном наборе в точности k раз

[2] рассматриваемых с точностью до умножения на обратимые элементы

[3] также рассматриваемых с точностью до умножения на обратимые элементы

12.3.1. Строение конечно порождённого модуля. Остаток этого раздела будет посвящён доказательству следующей фундаментальной теоремы.

Теорема 12.2 (теорема об элементарных делителях)
Всякий конечно порождённый модуль M над кольцом главных идеалов K изоморфен модулю вида

$$M = K^{n_0} \oplus \frac{K}{(p_1^{n_1})} \oplus \cdots \oplus \frac{K}{(p_\alpha^{n_\alpha})} \tag{12-5}$$

где $p_\nu \in K$ — простые элементы (не обязательно различные). Два таких модуля

$$K^{n_0} \oplus \frac{K}{(p_1^{n_1})} \oplus \cdots \oplus \frac{K}{(p_\alpha^{n_\alpha})} \quad \text{и} \quad K^{m_0} \oplus \frac{K}{(q_1^{m_1})} \oplus \cdots \oplus \frac{K}{(q_\beta^{m_\beta})}$$

изоморфны тогда и только тогда, когда $n_0 = m_0$, $\alpha = \beta$ и слагаемые можно переставить так, чтобы $n_\nu = m_\nu$, а p_ν были ассоциированы с q_ν. $\square$

Набор степеней $p_i^{n_i}$, по которым происходит факторизация в правых слагаемых разложения (12-5) (среди этих степеней могут встречаться повторяющиеся), называется *набором элементарных делителей* модуля M. По этой причине теор. 12.2 иногда называют *теоремой об элементарных делителях*

12.3.2. Существование разложения (12-5). Пусть M порождается элементами $v_1, v_2, \dots, v_N$. Тогда гомоморфизм $\varphi : K^N \twoheadrightarrow M$, переводящий стандартные базисные векторы координатного модуля K^N в образующие v_i, сюрьективен и $M \simeq K^N/\ker(\varphi)$, где $\ker\varphi \subset K^N$ есть модуль линейных зависимостей между образующими v_i (ср. с n° 8.4.2). По теореме об инвариантных множителях, в K^N существует базис $u_1, u_2, \dots, u_N$, такой, что некоторые кратности

$$\lambda_1 u_1,\ \lambda_2 u_2,\ \dots\ ,\lambda_{N-n_0} u_{N-n_0}$$

первых $(N - n_0)$ базисных векторов составляют базис в $\ker\varphi$. Тогда

$$M = K^N/\ker(\varphi) = \frac{K}{(\lambda_1)} \oplus \cdots \oplus \frac{K}{(\lambda_{N-n_0})} \oplus K^{n_0}\,.$$

Разложим каждый инвариантный множитель λ_i в произведение степеней различных простых элементов $\lambda_i = p_{i_1}^{m_{i_1}} p_{i_2}^{m_{i_2}} \cdots p_{i_{s_i}}^{m_{i_{s_i}}}$. Тогда по китайской теореме об остатках (см. упр. 6.13)

$$\frac{K}{(\lambda_i)} = \frac{K}{\left(p_{i_1}^{m_{i_1}}\right)} \oplus \frac{K}{\left(p_{i_2}^{m_{i_2}}\right)} \oplus \cdots \frac{K}{\left(p_{i_{s_i}}^{m_{i_{s_i}}}\right)}\,,$$

что и приводит к разложению вида (12-5). Чтобы доказать его единственность, мы дадим независящее от выбора такового разложения инвариантное описание его ингредиентов во внутренних терминах модуля M.

12.3.3. Отщепление кручения. Сумма

$$\frac{K}{(p_1^{n_1})} \oplus \cdots \oplus \frac{K}{(p_\alpha^{n_\alpha})}$$

в разложении (12-5) представляет собою подмодуль кручения

$$\operatorname{Tors}(M) = \{w \in M \mid \exists \lambda \neq 0 : \lambda w = 0\}\,.$$

И из факта существования разложении (12-5) мы получаем

Следствие 12.1

Всякий конечно порождённый модуль над кольцом главных идеалов является прямой суммой свободного модуля и подмодуля кручения (в частности, любой модуль без кручения свободен). □

Таким образом n_0 в (12-5) есть ранг свободного модуля $M/\operatorname{Tors}(M)$ и, тем самым, не зависит от выбора разложения (12-5).

12.3.4. Отщепление p-кручения. Дадим инвариантную характеризацию прямой сумме всех тех слагаемых из разложения

$$\operatorname{Tors}(M) = \frac{K}{(p_1^{n_1})} \oplus \cdots \oplus \frac{K}{(p_\alpha^{n_\alpha})}\,, \tag{12-6}$$

в которых факторизация происходит по степеням простых элементов, ассоциированных с заданным простым $p \in K$. Назовём p-кручением в M подмодуль

$$\operatorname{Tors}_p(M) = \{w \in M \mid \exists k > 0 : p^k w = 0\}\,,$$

состоящий из всех векторов, аннулируемых умножениями на различные степени заданного простого $p \in K$. В силу того, что p^k взаимно прост с q^m, если простое q не ассоциированно с p, класс p^k обратим в $K/(q^m)$, и значит, гомоморфизм умножения на p^k

$$K/(q^m) \xrightarrow{x \mapsto p^k x} K/(q^m)$$

является изоморфизмом. Следовательно, прямая сумма всех слагаемых вида $K/(p^m)$ в (12-6) — это в точности подмодуль p-кручения $\operatorname{Tors}_p(M) \subset \operatorname{Tors}(M)$, который тоже не зависит от выбора разложения (12-6), а из наличия разложения (12-6) вытекает

Следствие 12.2

Всякий конечно порождённый модуль кручения над кольцом главных идеалов является прямой суммой подмодулей p-кручения (по всем простым $p \in K$, для которых p-кручение ненулевое). □

Упражнение 12.4. Обозначим через $\varphi_n : K/(p^m) \xrightarrow{x \mapsto p^n x} K/(p^m)$ гомоморфизм умножения на p^n. Покажите, что $\varphi_n = 0$ при $n \geqslant m$, а при

$$\operatorname{im}\varphi_n \simeq K/\left(p^{m-n}\right) \quad \text{и} \quad \ker\varphi_n \simeq K/\left(p^n\right) \simeq \frac{K/\left(p^m\right)}{\operatorname{im}\varphi_n}$$

12.3.5. Инвариантность показателей p-кручения. Для завершения доказательства теор. 12.2 нам осталось проверить, что два модуля p-кручения

$$T = \frac{K}{(p^{n_1})} \oplus \dots \oplus \frac{K}{(p^{n_k})} \quad \text{и} \quad W = \frac{K}{(p^{m_1})} \oplus \dots \oplus \frac{K}{(p^{m_\ell})}$$

изоморфны тогда и только тогда, когда $k = \ell$ и (после надлежащей перестановки слагаемых) $n_i = m_i$ для каждого i.

Воспользуемся индукцией по $n_1 + \dots + n_k$, базовое утверждение которой заключается в том, что модуль $K/(p)$ изоморфен модулю вида

$$\frac{K}{(p^{m_1})} \oplus \dots \oplus \frac{K}{(p^{m_\ell})}$$

только при $\ell = 1$ и $m_1 = 1$. Поскольку $K/(p)$ аннулируется умножением на p, по упр. 12.4 во втором модуле не может быть прямых слагаемых отличных от $K/(p)$. Но тогда оба модуля суть векторные пространства над полем $K/(p)$, и их изоморфность означает совпадение размерностей, так что слагаемое в W тоже одно.

Пусть, по индукции, любой модуль T с $n_1+\dots+n_k < n$ изоморфен модулю W только если $k = \ell$ и все $n_i = m_i$ после надлежащей перенумерации. Если модуль T с $n_1 + \dots + n_k = n$ изоморфен модулю W, то ядра и образы гомоморфизмов умножения на p в обоих модулях тоже изоморфны. Согласно упр. 12.4, ядро гомоморфизма умножения на p представляет собой сумму всех слагаемых вида $K/(p)$. Как и выше, это векторное пространство над полем $K/(p)$, и два таких пространства изоморфны только если их размерности одинаковы. Поэтому количество слагаемых вида $K/(p)$ в T и W одинаково. Образы гомоморфизмов умножения на p в T и в W по упр. 12.4 изоморфны

$$pT \simeq \bigoplus_{\nu: n_\nu > 1} K/(p^{n_\nu - 1}) \quad \text{и} \quad pW \simeq \bigoplus_{\mu: m_\mu > 1} K/(p^{m_\mu - 1}) .$$

По индуктивному предположению, число слагаемых в обоих суммах одинаково и после надлежащей перенумерации каждое $n_\nu > 1$ совпадёт с соответствующим $m_\mu > 1$, что и требовалось. Теорема об элементарных делителях полностью доказана.

12.4. Пример: конечно порождённые абелевы группы. Если $K = \mathbb{Z}$, теорема об элементарных делителях превращается в теорему о классификации конечно порождённых абелевых групп.

Теорема 12.3

Всякая конечно порождённая абелева группа изоморфна прямой сумме аддитивных групп

$$\mathbb{Z}^r \oplus \frac{\mathbb{Z}}{(p_1^{n_1})} \oplus \dots \oplus \frac{\mathbb{Z}}{(p_\alpha^{n_\alpha})} \tag{12-7}$$

где $p_\nu \in \mathbb{N}$ — простые числа (не обязательно различные). Две аддитивных группы

$$\mathbb{Z}^r \oplus \frac{\mathbb{Z}}{(p_1^{n_1})} \oplus \dots \oplus \frac{\mathbb{Z}}{(p_\alpha^{n_\alpha})} \quad \text{и} \quad \mathbb{Z}^s \oplus \frac{\mathbb{Z}}{(q_1^{m_1})} \oplus \dots \oplus \frac{\mathbb{Z}}{(q_\beta^{m_\beta})}$$

изоморфны тогда и только тогда, когда $r = s$, $\alpha = \beta$ и (после надлежащей перестановки) $n_\nu = m_\nu$ и $p_\nu = q_\nu$ при всех ν. □

Единственное представление данной конечно порождённой абелевой группы A в виде прямой суммы аддитивных групп (12-7) называется *каноническим*.

12.4.1. Группы, заданные «образующими и соотношениями». На практике довольно часто приходится иметь дело с такого рода описаниями: абелева группа A, порождённая элементами $a_1, a_2, \dots, a_n$, удовлетворяющими соотношениям

$$\begin{cases} \mu_{11}a_1 + \mu_{12}a_2 + \dots + \mu_{1n}a_n = 0 \\ \mu_{21}a_1 + \mu_{22}a_2 + \dots + \mu_{2n}a_n = 0 \\ \mu_{31}a_1 + \mu_{32}a_2 + \dots + \mu_{3n}a_n = 0 \\ \dots\dots\dots\dots\dots \\ \mu_{\mu 1}a_1 + \mu_{\mu 2}a_2 + \dots + \mu_{mn}a_n = 0\,, \end{cases} \tag{12-8}$$

где $\mu_{ij} \in \mathbb{Z}$. По определению, такая группа A представляет собою фактор $\mathbb{Z}^n/M$, где подрешётка $M \subset \mathbb{Z}^n$ порождается строками $\mu_1, \mu_2, \dots, \mu_m$ матрицы (μ_{ij}).

В каноническом разложении (12-7) группы A ранг r свободного слагаемого равен $n - \mathrm{rk}\,(\mu_{ij})$, а степени $p_i^{n_i}$ суть элементарные делители подрешётки $M \subset \mathbb{Z}^n$, о которых шла речь в самом начале n° 12.3.

Про конкретный элемент $w = x_1a_1 + x_2a_2 + \dots + x_na_n$ часто бывает нужно знать, отличен он от нуля в A или нет, и если нет, то каков его порядок[1] $\mathrm{ord}\,(w)$. Выяснить это можно, работая не в внутри модуля $\mathbb{Z}^n$ над кольцом $\mathbb{Z}$, а в содержащем его векторном пространстве $\mathbb{Q}^n \supset \mathbb{Z}^n$ над полем $\mathbb{Q}$.

Если вектор $w \in \mathbb{Q}^n$ не лежит в $\mathbb{Q}$-линейной оболочке строк матрицы (μ_{ij}), то никакое его целое кратное mw не лежит в M, т. е. $w \neq 0$ в A и $\mathrm{ord}\, w = \infty$.

Если же $w = \lambda_1\mu_1 + \lambda_2\mu_2 + \dots + \lambda_m\mu_m$, где $\lambda_i = p_i/q_i \in \mathbb{Q}$ несократимые дроби, то $\mathrm{ord}\,(w) = \text{нок}(q_1, q_2, \dots, q_m)$. В частности, если все $q_i = 1$ (т. е. все $\lambda_i \in \mathbb{Z}$), то $w = 0$ в фактор группе $A = \mathbb{Z}^n/M$.

Задачи для самостоятельного решения к §12

Задача 12.1. Изоморфны ли абелевы группы $\mathbb{Z}/(6) \oplus \mathbb{Z}/(36)$ и $\mathbb{Z}/(12) \oplus \mathbb{Z}/(18)$?

[1] напомним (см. n° 4.4.3), что *порядком* элемента w в аддитивной абелевой группе называется наименьшее $n \in \mathbb{N}$, такое что $nw = 0$ (если такого нет, полагают $\mathrm{ord}\,(w) = \infty$

Задача 12.2. Напишите каноническое разложение (12-7) для (аддитивных) абелевых групп $\mathbb{Z}/(6)$, $\mathbb{Z}/(12)$, $\mathbb{Z}/(24)$ и $\mathbb{Z}/(60)$.

Задача 12.3. Напишите каноническое разложение (12-7) для всех абелевых групп порядка 4, 6, 8, 12, 16, 24, 36, 48.

Задача 12.4. Напишите каноническое разложение (12-7) для (аддитивных) абелевых групп[1]: а) $\mathrm{Hom}\big(\mathbb{Z}/(6), \mathbb{Z}/(12)\big)$ б) $\mathrm{Hom}\big(\mathbb{Z}/(12), \mathbb{Z}/(6)\big)$ в) $\mathrm{Hom}\big(\mathbb{Z}/(12), \mathbb{Z}/(18)\big)$ г) $\mathrm{Hom}\big(\mathbb{Z}/(4), \mathbb{Z}/(8)\big)$ д) $\mathrm{Hom}\big(\mathbb{Z}/(2) \oplus \mathbb{Z}/(2), \mathbb{Z}/(8)\big)$

Задача 12.5. Есть ли в абелевой группе $\mathbb{Z}/(2) \oplus \mathbb{Z}/(16)$ подгруппа, изоморфная а) $\mathbb{Z}/(2) \oplus \mathbb{Z}/(8)$ б) $\mathbb{Z}/(4) \oplus \mathbb{Z}/(4)$ в) $\mathbb{Z}/(2) \oplus \mathbb{Z}/(2) \oplus \mathbb{Z}/(2)$

Задача 12.6. Сколько подгрупп порядков 2 и 6 в нециклической абелевой группе порядка 12?

Задача 12.7. Напишите каноническое разложение (12-7) для фактора решётки $\mathbb{Z}^3$ по подрешётке, порождённой векторами: а) $(7,2,3)$, $(21,8,9)$, $(5,-4,3)$ б) $(4,5,3)$, $(5,6,5)$, $(8,7,9)$ в) $(2,-4,6)$, $(6,-6,10)$, $(2,5,8)$, $(6,0,5)$ г) $(-81,-6,-33)$, $(60,6,24)$, $(-3,6,-3)$, $(18,6,6)$ д) $(-62,-8,-26)$, $(40,10,16)$, $(22,-8,10)$, $(20,2,8)$

Задача 12.8. Найдите в абелевой группе, порождённой элементами a_1, a_2, a_3 порядок элемента а) $a_1 + 2a_3$, если $a_1 + a_2 + 4a_3 = 2a_1 - a_2 + 2a_3 = 0$ б) $32a_1 + 31a_3$, если $2a_1 + a_2 - 50a_3 = 4a_1 + 5a_2 + 60a_3 = 0$

Задача 12.9. Пусть $a = [1]_9 \in \mathbb{Z}/(9)$, и $b = [1]_{27} \in \mathbb{Z}/(27)$. Напишите каноническое разложение (12-7) для фактор группы $\mathbb{Z}/(9) \oplus \mathbb{Z}/(27)$ по подгруппе, порождённой элементом $3a + 9b$.

Задача 12.10. Пусть порядок конечно порождённой абелевой группы A делится на m. Покажите, что в A есть подгруппа порядка m.

Задача 12.11. Пусть для любого $m \in \mathbb{N}$ число элементов порядка m в двух конечных абелевых группах A и B одинаково. Покажите, что $A \simeq B$.

Задача 12.12. Пусть для конечно порождённых модулей A, B, C над кольцом главных идеалов имеет место изоморфизм $A \oplus C \simeq B \oplus C$. Покажите, что $A \simeq B$.

Задача 12.13. Докажите, что любой подмодуль и любой фактор модуль конечно порождённого модуля над кольцом главных идеалов[2] тоже конечно порождены.

Задача 12.14. Докажите следующий вариант *теоремы о ранге* $m \times n$-матрицы над кольцом главных идеалов: столбцы и строки любой матрицы $M \in \mathrm{Mat}_{m \times n}(K)$

[1] через $\mathrm{Hom}(A, B)$ в этой задаче обозначается $\mathbb{Z}$-модуль гомоморфизмов из $\mathbb{Z}$-модуля A в $\mathbb{Z}$-модуль B

[2] в действительности это утверждение верно над любым *нётеровым* кольцом (см. n° 6.4)

порождают в K^m и K^n свободные подмодули одинакового ранга, равного числу ненулевых диагональных элементов, возникающих в результате приведения матрицы к диагональному виду обобщёнными элементарными преобразованиями строк и столбцов.

Задача 12.15. Пусть v_1, v_2, $v_3 \in \mathbb{Z}^3 \subset \mathbb{R}^3$ — три линейно независимых над $\mathbb{R}$ целых вектора, $L \subset \mathbb{Z}^3$ — порождённый ими $\mathbb{Z}$-подмодуль, Π — натянутый на эти векторы параллелепипед. Покажите, что объём Π (равный числу элементов в фактор модуле $\mathbb{Z}^3/L$) равен $в + г/2 + р/4 + 1$, где $в$, $г$ и $р$ суть количества целых точек, находящихся строго внутри самого Π, строго внутри его граней и строго внутри его рёбер соответственно? Обобщите этот результат на произвольную размерность.

Задача 12.16. Пусть $\Bbbk$ — поле. Покажите, что всякий линейный оператор

$$\Bbbk[t]/(f) \xrightarrow{G} \Bbbk[t]/(f)\,,$$

перестановочный с умножением на t, является оператором умножения на многочлен $g(t) = G([1])$, где $[1] = 1 \pmod{f}$.

Задача 12.17. Пусть $\Bbbk$ — поле. Найдите размерность векторного пространства гомоморфизмов $\operatorname{Hom}\bigl(\Bbbk[x]/(f), \Bbbk[x]/(g)\bigr)$ $\Bbbk[x]$-модуля $\Bbbk[x]/(f)$ в $\Bbbk[x]$-модуль $\Bbbk[x]/(g)$ в случаях, когда а) $f = p^\mu$, $g = p^\nu$, где $p \in \Bbbk[x]$ неприводим, а $\mu, \nu \in \mathbb{N}$ любые б) нод$(f, g) = 1$

§13. Пространство с оператором

13.1. Классификация операторов. Этот параграф посвящён описанию линейных операторов $F : V \longrightarrow V$, действующих в конечномерных векторных пространствах над заданным полем $\Bbbk$. Будем называть линейные операторы

$$U_1 \xrightarrow{F_1} U_1 \quad \text{и} \quad U_2 \xrightarrow{F_2} U_2$$

изоморфными (или *подобными*), если существует линейный изоморфизм

$$\varphi : U_1 \xrightarrow{\sim} U_2 \,,$$

отождествляющий действие оператора F_1 на U_1 с действием оператора F_2 на U_2 в том смысле, что диаграмма

$$\begin{tikzcd} U_1 \arrow[r, "\varphi", "\sim"'] & U_2 \\ U_1 \arrow[u, "F_1"] \arrow[r, "\sim", "\varphi"'] & U_2 \arrow[u, "F_2"'] \end{tikzcd}$$

коммутативна, т. е. $\varphi F_1 = F_2 \varphi$ или, что то же самое, $F_2 = \varphi F_1 \varphi^{-1}$.

В частности, два оператора F и G на одном и том же пространстве V изоморфны, если существует $C \in \mathrm{GL}(V)$, такой что $G = CAC^{-1}$. В этой ситуации говорят, что G получается из F *сопряжением* посредством C.

Представить себе действие линейного оператора $V \xrightarrow{F} V$ на большом пространстве V проще всего ограничивая F на меньшие подпространства $U \subset V$.

Подпространство U называется F-*инвариантным*, если $F(U) \subset U$.

Оператор $V \xrightarrow{F} V$ называется *разложимым*, если пространство V можно разложить в прямую сумму двух ненулевых F-инвариантных подпространств, и *неразложимым* — в противном случае.

Упражнение 13.1. Покажите, что оператор умножения на t в фактор кольце $\Bbbk[t]/\,(t^n)$ неразложим (таким образом, над любым полем $\Bbbk$ имеются неразложимые операторы на пространстве любой размерности).

Очевидно, что всякое пространство с оператором является прямой суммой неразложимых F-инвариантных подпространств. Поэтому полное описание линейных операторов над заданным полем $\Bbbk$ включает в себя решение следующих двух задач:

1) описать с точностью до изоморфизма все неразложимые операторы;

2) выяснить, насколько однозначно разложение произвольного оператора в прямую сумму неразложимых.

Обе эти задачи решает идущая ниже теор. 13.1.

Упражнение 13.2. Покажите, что двойственные операторы

$$V \xrightarrow{F} V \quad \text{и} \quad V^* \xleftarrow{F^*} V^*$$

либо оба разложимы, либо оба неразложимы.

Теорема 13.1

Любой линейный оператор в конечномерном векторном пространстве над произвольным полем $\Bbbk$ подобен оператору умножения на t в прямой сумме фактор колец

$$\frac{\Bbbk[t]}{(p_i^{m_1}(t))} \oplus \cdots \oplus \frac{\Bbbk[t]}{(p_k^{m_k}(t))}, \tag{13-1}$$

где все многочлены $p_\nu(t) \in \Bbbk[t]$ приведены и неприводимы. Каждое прямое слагаемое в этой сумме неразложимо. Операторы умножения на t, действующие в суммах

$$\frac{\Bbbk[t]}{(p_i^{m_1}(t))} \oplus \cdots \oplus \frac{\Bbbk[t]}{(p_k^{m_k}(t))} \quad \text{и} \quad \frac{\Bbbk[t]}{(q_i^{n_1}(t))} \oplus \cdots \oplus \frac{\Bbbk[t]}{(q_\ell^{n_\ell}(t))}$$

изоморфны тогда и только тогда, когда $k = \ell$, и прямые слагаемые можно переставить так, чтобы $p_\nu = q_\nu$ и $m_\nu = n_\nu$ при всех ν.

Доказательство. Задание линейного оператора $F : V \longrightarrow V$ эквивалентно заданию на V структуры модуля над кольцом многочленов $\Bbbk[t]$. В самом деле, структура $\Bbbk[t]$-модуля отличается от структуры $\Bbbk$-модуля наличием ровно одной дополнительной операции — умножения векторов $v \in V$ на $t \in \Bbbk[t]$. Если определить её правилом $t \cdot v = F(v)$, то умножение векторов v на многочлены $f \in \Bbbk[t]$ будет задаваться формулой $g(t)\cdot v = [g(F)](v)$ и свойства (11-1)–(11-3) из определения модуля будут выполнены (ср. с n° 11.3.1). Обозначим $\Bbbk[t]$-модуль, полученный таким способом из оператора $V \xrightarrow{F} V$, через V_F.

Так как пространство V конечномерно, модуль V_F конечно порождён: любой базис $e_1, e_2, \dots, e_n$ векторного пространства V над полем $\Bbbk$ тем более порождает V_F над $\Bbbk[t]$. По теор. 12.2 модуль V_F изоморфен прямой сумме свободного модуля $\Bbbk[t]^{\oplus r}$ и модулей вида $\Bbbk[t]/(p^m)$, где многочлены $p_\nu[t] \in \Bbbk[t]$ неприводимы и приведены[1]. Поскольку свободное слагаемое $\Bbbk[t]^{\oplus r}$ бесконечномерно как векторное пространство над $\Bbbk$, в разложении конечномерного пространства V_F его быть не может. Таким образом,

$$V_F \simeq \frac{\Bbbk[t]}{(p_i^{m_1}(t))} \oplus \cdots \oplus \frac{\Bbbk[t]}{(p_k^{m_k}(t))}$$

[1] простые $p_i \in K$ в теор. 12.2 определялись K-модулем однозначно с точностью до умножения на обратимые элементы кольца K; при $K = \Bbbk[t]$ эта неоднозначность устраняется требованием, чтобы старшие коэффициенты неприводимых многочленов p_i были равны единице

и оператор $F : V \longrightarrow V$ переходит при этом изоморфизме в оператор умножения на t.

Гомоморфизм $\Bbbk[t]$-модулей $V_F \xrightarrow{\varphi} W_G$, построенных по пространствам V и W с операторами $F : V \longrightarrow V$ и $G : W \longrightarrow W$ — это линейное отображение

$$\varphi : V \longrightarrow W ,$$

перестановочное с умножением векторов на t, т. е. такое что $\varphi F_1 = F_2\varphi$. Поэтому операторы F и G изоморфны тогда и только тогда, когда изоморфны $\Bbbk[t]$-модули V_F и W_G. Согласно теор. 12.2 изоморфность модулей (13-1) означает, что их прямые слагаемые можно привести во взаимно однозначное соответствие друг с другом так, чтобы соответственные приведённые неприводимые многочлены были равны и имели равные показатели. Из этой однозначности вытекает, в частности, все прямые слагаемые $\Bbbk[t]/(p^m)$ в (13-1) далее не разложимы. □

13.1.1. Элементарные делители. Дизъюнктное объединение[1] всех многочленов $p_\nu^{m_\nu}$, стоящих в правой части разложения (13-1), называется *набором элементарных делителей* оператора $V \xrightarrow{F} V$ и обозначается через $\mathrm{El}(F)$.

Следствие 13.1

Линейные операторы F и G подобны тогда и только тогда, когда у них одинаковые наборы элементарных делителей: $\mathrm{El}(F) = \mathrm{El}(G)$.

Следствие 13.2

Многочлен $f \in \Bbbk[t]$ тогда и только тогда аннулирует оператор $V \xrightarrow{F} V$, когда он делится на все элементарные делители оператора F.

13.1.2. Минимальный многочлен. Для каждого неприводимого приведённого многочлена $p \in \Bbbk[t]$ положим

$$m_p(F) = \max\left(m \in \mathbb{N} \cup \{0\} \mid p^m \in \mathrm{El}(F)\right)$$

(таким образом, $m_p(F) = 0$ для всех p кроме конечного числа). Из теор. 13.1 вытекает, что приведённый многочлен $\mu_F(t)$ наименьшей возможной степени, аннулирующий оператор F, равен

$$\mu_F(t) = \prod_p p^{m_p(F)}$$

(произведение по всем приведённым неприводимым $p \in \Bbbk[t]$). Многочлен $\mu_F(t)$ называется *минимальным многочленом* оператора F (ср. с зад. 7.31).

---

[1] подчеркнём, что каждый элементарный делитель p^m входит в него ровно столько раз, сколько прямых слагаемых вида $\Bbbk[t]/(p^m)$ входит в разложение V

13.1.3. Пример: диагонализуемые операторы. Простейшие неразложимые операторы — одномерные. Линейный оператор $V \xrightarrow{F} V$ называется *диагонализуемым*, если пространство V является прямой суммой одномерных инвариантных подпространств. Название вызвано тем, что если выбрать в V базис, состоящий из базисных векторов u_i одномерных F-инвариантных подпространств, то действие F на эти базисные векторы будет происходить по правилу $u_i \mapsto \lambda_i u_i$, т. е. матрица оператора F в базисе u будет диагональной.

Лемма 13.1
Оператор $V \xrightarrow{F} V$ диагонализуем над полем $\Bbbk$ тогда и только тогда, когда $f(F) = 0$ для некоторого $f \in \Bbbk[t]$, полностью раскладывающегося над $\Bbbk$ в произведение попарно различных линейных множителей.

Доказательство. По теор. 13.1 диагонализуемый оператор $V \xrightarrow{F} V$ изоморфен оператору умножения на t в прямой сумме одномерных колец вычетов

$$\frac{\Bbbk[t]}{(t-\lambda_1)} \oplus \cdots \oplus \frac{\Bbbk[t]}{(t-\lambda_n)} \tag{13-2}$$

где в наборе чисел $\lambda_1, \lambda_2, \ldots, \lambda_n \in \Bbbk$ могут быть повторяющиеся. Пусть

$$\lambda_1, \lambda_2, \ldots, \lambda_s$$

составляют полный список всех *различных* чисел из этого набора. Тогда оператор умножения на $f(t) = (t-\lambda_1)(t-\lambda_2) \cdots (t-\lambda_s)$ аннулирует всё пространство (13-2). Тем самым, $f(F) = 0$.

Наоборот, если $g(F) = 0$ для некоторого многочлена $g \in \Bbbk[t]$, то умножение на $g(t)$ должно аннулировать прямую сумму фактор колец (13-1), которой изоморфен оператор $V \xrightarrow{F} V$, а значит, g должен делиться на все элементарные делители оператора F. Если g является произведением попарно различных линейных форм, то в силу однозначности разложения многочленов на простые множители, все элементарные делители F должны содержаться среди этих линейных форм. Следовательно, разложение (13-1) имеет вид (13-2) и F диагонализуем. □

Следствие 13.3
Если оператор $V \xrightarrow{F} V$ диагонализуем, то его ограничение на любое инвариантное подпространство тоже диагонализуемо (на этом подпространстве).

13.1.4. Пример: нильпотентные операторы. Напомним (см. зад. 7.19), что линейный оператор $F : V \longrightarrow V$ называется *нильпотентным*, если $F^m = 0$ для некоторого $m \in \mathbb{N}$. Поскольку нильпотентный оператор аннулируется многочленом t^m, все его элементарные делители являются степенями t. Поэтому, согласно теор. 13.1, нильпотентный оператор изоморфен оператору умножения на t в прямой сумме фактор колец вида

$$\frac{\Bbbk[t]}{(t^{\nu_1})} \oplus \cdots \oplus \frac{\Bbbk[t]}{(t^{\nu_k})} \tag{13-3}$$

и два таких оператора изоморфны друг другу тогда и только тогда, когда выстроенные в порядке (нестрогого) убывания наборы показателей

$$\nu_1 \geqslant \nu_2 \geqslant \cdots \geqslant \nu_k$$

у них одинаковы. Таким образом, нильпотентные операторы над произвольным полем $\Bbbk$ взаимно однозначно соответствуют диаграммам Юнга ν.

Действие оператора умножения на t на базис $\Bbbk[t]/\,(t^m)$, состоящий из классов

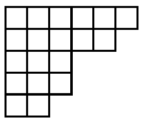
$$e_0 = t^{m-1} \,(\mathrm{mod}\, t^m),\ e_1 = t^{m-2} \,(\mathrm{mod}\, t^m),\ \dots\ ,\ e_{m-1} = 1 \,(\mathrm{mod}\, t^m)$$

происходит по правилу $0 \leftarrow e_0 \leftarrow e_1 \leftarrow e_2 \leftarrow\ \cdots\ \leftarrow e_{m-2} \leftarrow e_{m-1}$ и задаётся матрицей

$$J_m(0) \overset{\text{def}}{=} \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ 0 & & \ddots & \ddots & 1 \\ 0 & 0 & \cdots & 0 & 0 \end{pmatrix}$$

которая называется *нильпотентной жордановой клеткой* размера m.

Таким образом, для нильпотентного оператора $V \xrightarrow{F} V$, отвечающего диаграмме Юнга ν, в пространстве V имеется базис, векторы которого размещаются в клетки этой диаграммы так, что оператор переводит каждый базисный вектор в левый соседний, а векторы самого левого столбца — в нуль:



$$\leftrightsquigarrow \qquad \begin{array}{l} 0 \leftarrow \bullet \leftarrow \bullet \leftarrow \bullet \leftarrow \bullet \leftarrow \bullet \leftarrow \bullet \\ 0 \leftarrow \bullet \leftarrow \bullet \leftarrow \bullet \leftarrow \bullet \leftarrow \bullet \\ 0 \leftarrow \bullet \leftarrow \bullet \leftarrow \bullet \\ 0 \leftarrow \bullet \leftarrow \bullet \leftarrow \bullet \\ 0 \leftarrow \bullet \leftarrow \bullet \end{array} \tag{13-4}$$

Базис такого вида называется *циклическим* (или *жордановым*) базисом, соответствующая ему диаграмма Юнга ν называется *цикловым типом* нильпотентного оператора F, а наборы базисных векторов, стоящие по строкам диаграммы, называются *жордановыми цепочками*.

Описать цикловой тип нильпотентного оператора и увидеть его независимость от выбора циклического базиса можно и не прибегая к классификационной теор. 13.1. Сумма длин первых m столбцов диаграммы ν равна $\dim\ker F^m$, откуда длина m-того столбца диаграммы ν однозначно находится как

$$\nu^t_m = \dim\ker F^m - \dim\ker F^{m-1}\,.$$

13.1.5. Пример: жорданова клетка. Умножение на $t = \lambda+(t-\lambda)$ в фактор кольце $V = \Bbbk[t]/\big((t-\lambda)^m\big)$ представляет собой сумму скалярного оператора

$$\lambda\,\mathrm{Id}_V : f \longmapsto \lambda\, f$$

и нильпотентного оператора $\eta : f \longmapsto (t-\lambda)\cdot f$, для которого многочлены

$$(t-\lambda)^{m-1}\,,\ (t-\lambda)^{m-2}\,,\ \dots\ ,\ (t-\lambda)\,,\ 1$$

образуют жорданову цепочку длины $m = \dim V$. В базисе из этих многочленов оператор умножения на t задаётся двудиагональной матрицей

$$J_m(\lambda) \stackrel{\text{def}}{=} \begin{pmatrix} \lambda & 1 & & & \\ & \lambda & 1 & & \\ & & \ddots & \ddots & \\ & & & \lambda & 1 \\ & & & & \lambda \end{pmatrix} \tag{13-5}$$

(нули в остальных местах). Эта матрица называется называется *жордановой клеткой* размера m с собственным значением λ.

13.1.6. Жорданова нормальная форма. Если поле $\Bbbk$ алгебраически замкнуто, то неприводимые многочлены в $\Bbbk[t]$ исчерпываются линейными двучленами $(t-\lambda)$. По теор. 13.1 всякий оператор $V \xrightarrow{F} V$ в этом случае подобен оператору умножения на t в прямой сумме фактор колец

$$\frac{\Bbbk[t]}{((t-\lambda_1)^{m_1})} \oplus \dots \oplus \frac{\Bbbk[t]}{((t-\lambda_s)^{m_s})} \tag{13-6}$$

и два оператора такого вида подобны, если и только если прямые слагаемые в их разложениях можно привести во взаимно однозначное соответствие друг с другом так, чтобы соответственные λ_i и m_i были равны. Действие оператора умножения на t в пространстве (13-6) было описано нами выше. Мы получаем

Следствие 13.4 (жорданова нормальная форма)
Над алгебраически замкнутым полем $\Bbbk$ для любого оператора $V \xrightarrow{F} V$ в V существует базис, в котором матрица оператора F имеет блочный вид

$$\begin{pmatrix} J_{m_1}(\lambda_1) & & & \\ & J_{m_2}(\lambda_2) & & \\ & & \ddots & \\ & & & J_{m_k}(\lambda_k) \end{pmatrix} \tag{13-7}$$

по главной диагонали которого стоят жордановы клетки

$$J_{m_1}(\lambda_1),\ J_{m_2}(\lambda_2)\ \dots\ ,\ J_{m_k}(\lambda_k)$$

вида (13-5) (числа λ_i и m_i могут повторяться), а в остальных местах стоят нули. С точностью до перестановки блоков матрица (13-7) не зависит от выбора такого базиса. Два оператора подобны тогда и только тогда, когда их матрицы (13-7) отличаются друг от друга перестановкой блоков. □

Определение 13.1
Матрица (13-7) называется *жордановой нормальной формой* оператора F. Всякий базис пространства V, в котором матрица оператора F имеет жорданову нормальную форму, называется *жордановым базисом* оператора F.

13.2. Аннулирующие многочлены. Судить о неразложимых компонентах оператора $V \xrightarrow{F} V$ во внутренних терминах действия F на V можно по тому, какие многочлены аннулируют оператор F.

По крайней мере один такой многочлен написать нетрудно. А именно, выберем в V какой-нибудь базис $v = (v_1, v_2, \dots, v_n)$, и пусть F_v — матрица оператора F в этом базисе. В силу тождества Гамильтона – Кэли (см. n° 11.3.1), характеристический многочлен этой матрицы аннулирует оператор F.

Упражнение 13.3. Покажите, что многочлен $\det(tE - F_v) \in \Bbbk[t]$ не зависит от выбора базиса.

Характеристический многочлен матрицы оператора F в произвольном базисе пространства V называется *характеристическим многочленом* оператора F и обозначается $\chi_F(t) = \det(t \cdot \mathrm{Id}_V - F) \in \Bbbk[t]$. Тождество Гамильтона – Кели означает равенство $\chi_F(F) = 0$.

Лемма 13.2
Пусть оператор $F : V \longrightarrow V$ (над произвольным полем $\Bbbk$) аннулируется многочленом $q \in \Bbbk[t]$, который является произведением r попарно взаимно простых многочленов: $q(t) = q_1(t) \cdot q_2(t) \cdot \dots \cdot q_r(t)$, $\text{нод}(q_i, q_j) = 1 \ \forall\, i, j$. Положим $Q_j = q/q_j = \prod\limits_{\nu \neq j} q_\nu$. Тогда справедливы следующие три утверждения:

1) $\forall\, j \quad \mathrm{im}\,(Q_j(F)) \subset \ker\,(q_j(F))$

2) $\forall\, i \neq j \quad \ker\,(q_i(F)) \cap \ker\,(q_j(F)) = 0$

3) подпространства $\mathrm{im}\,(Q_j(F))$ линейно порождают V.

Доказательство. Первое следует из того, что $q(F) = q_j(F) \circ Q_j(F) = 0$. Второе — из того, что в силу взаимной простоты многочленов $q_i(t)$ и $q_j(t)$ существуют многочлены $h_i(t)$ и $h_j(t)$, такие что $1 = h_i(t)q_i(t) + h_j(t)q_j(t)$. Подставляя в это равенство $t = F$ и применяя оператор $E = h_i(F) \circ q_i(F) + h_j(t) \circ q_j(F)$ к любому вектору $v \in \ker\,(q_i(F)) \cap \ker\,(q_j(F))$, заключаем, что

$$v = Ev = h_i(F) \circ q_i(F)v + h_j(t) \circ q_j(F)v = 0\,.$$

Третье утверждение аналогичным образом выводится из взаимной простоты многочленов $Q_1, Q_2, \ldots, Q_r$. Существуют $H_1, H_2, \ldots, H_r \in \Bbbk[t] : 1 = \sum Q_j H_j$. Подставляя в это равенство $t = F$ и применяя обе части к любому $v \in V$, видим, что $v = Ev = \sum Q_j(F) H_j(F) v \in \sum \operatorname{im}\,(Q_j(F))$. □

Следствие 13.5

В условиях лем. 13.2 пространство V является прямой всех тех инвариантных подпространств $\ker\,(q_j(F)) = \operatorname{im} Q_j(F)$, которые отличны от нуля. □

13.2.1. Пример: собственные подпространства. Ненулевое подпространство вида

$$V_\lambda = \ker(\lambda \operatorname{Id}_V - F) = \{v \in V \mid F(v) = \lambda v\}$$

называется *собственным подпространством* оператора F с *собственным значением* $\lambda \in \Bbbk$. Ограничение оператора F на собственное подпространство V_λ представляет собою скалярный оператор умножения на λ.

Все $\lambda \in \Bbbk$, для которых $V_\lambda \neq 0$, называются *собственными числами* (или *собственными значениями*) оператора λ. Совокупность собственных чисел оператора F обозначается $\operatorname{Spec} F$ и называется *спектром* оператора F. Поскольку условие $\ker(\lambda \operatorname{Id}_V - F) \neq 0$ равносильно условию $\det(\lambda \operatorname{Id}_V - F) = 0$ (см. n° 10.3.1), спектр оператора F можно иначе описать как множество корней его характеристического многочлена $\chi_F(t) = \det(\lambda \operatorname{Id}_V - F)$. В частности, оператор $V \xrightarrow{F} V$ имеет не более $\dim V$ собственных чисел.

Последний факт независимо вытекает из сл. 13.5: ограничение оператора F на сумму всех его собственных подпространств аннулируется многочленом

$$\prod_{\lambda \in \operatorname{Spec} F} (t - \lambda)$$

(λ без повторений пробегает все различные собственные числа), и стало быть, сумма всех собственных подпространств является *прямой суммой*. Отметим, что заодно мы получаем независимое от теор. 13.1 доказательство критерия диагонализуемости оператора F из лем. 13.1: если оператор аннулируется многочленом вида $\prod\limits_{\lambda}(t-\lambda)$, то по сл. 13.5 пространство V раскладывается в прямую сумму собственных подпространств $V_\lambda = \ker(F - \lambda E)$.

Ненулевые векторы $v \in V_\lambda$ называются *собственными векторами* оператора F с собственным значением λ. Из предыдущего вытекает, что всякий набор собственных векторов с попарно разными собственными значениями линейно независим. Диагонализуемость оператора означает наличие у него базиса из собственных векторов. Если все собственные числа оператора F известны (или, что то же самое, известны все корни его характеристического многочлена), то отыскание собственных векторов и собственных подпространств сводится к решению систем линейных однородных уравнений $(\lambda \operatorname{Id}_V - F)\, v = 0$, имеющих ненулевые решения (что равносильно условию $\lambda \in \operatorname{Spec} F$).

Следствие 13.6
Над алгебраически замкнутым полем $\Bbbk$ любой оператор обладает хотя бы одним собственным вектором.

Следствие 13.7
Над полем вещественных чисел $\mathbb{R}$ любой оператор обладает одномерным или двумерным инвариантным подпространством.

Доказательство. Пусть $\chi_F = q_1 q_2 \ldots q_m$, где все q_i неприводимы (и не обязательно различны). Если среди них есть линейные, то у F есть вещественное собственное число и, стало быть, ненулевое собственное подпространство с таким собственным значением. Если все q_i квадратичные, применим нулевой оператор $\prod q_\nu(F) = 0$ к какому-нибудь ненулевому вектору $v \in V$ и найдём такое i, что $w = q_{i+1}(F)q_{i+2}(F) \cdots q_m(F)v \neq 0$, а $q_i(F)w = 0$. Последнее равенство означает, что $F(Fw)$ лежит в линейной оболочке w и Fw, которая, тем самым, является двумерным инвариантным подпространством. □

Упражнение 13.4. Покажите, что $\operatorname{Spec} F$ содержится в множестве корней любого многочлена, аннулирующего F.

13.2.2. Пример: инволюции. Оператор F называется *инволюцией*, если $F^2 = \mathrm{Id}$. Инволюция $F = \mathrm{Id}_V$ называется *тривиальной*. Поскольку любая инволюция, по определению, аннулируется многочленом $F^2 - 1 = (F+1)(F-1) = 0$, она диагонализуема, и пространство V распадается в прямую сумму собственных подпространств $V = V_+ \oplus V_-$ с собственными значениями ± 1:

$$V_\pm = \ker(\mathrm{Id} \mp F) = \operatorname{im}(\mathrm{Id} \pm F) = \{v \in V \mid Fv = \pm v\},$$

и любой вектор однозначно представим в виде $v = v_+ + v_-$, где

$$v_+ = (v + Fv)/2 \in V_+ \quad \text{и} \quad v_- = (v - Fv)/2 \in V_-.$$

13.2.3. Пример: проекторы. Оператор F называется *идемпотентом*, если $F^2 = F$. Равенство $F(F-1) = 0$ означает, что

$$\operatorname{im} F = \ker(F - 1) = \{v \mid F(v) = v\} \quad \text{и} \quad V = \ker F \oplus \operatorname{im} F.$$

Таким образом, всякий идемпотент F является проекцией $V = \ker(F) \oplus \operatorname{im}(F)$ на $\operatorname{im} F$ вдоль $\ker F$. Отметим, что оператор $\mathrm{Id} - F$ тоже является идемпотентом, проектирующим V на $\ker F$ вдоль $\operatorname{im} F$. Наоборот, любому прямому разложению $V = U \oplus W$ отвечают два идемпотентных оператора: проектор $\pi_U : V \twoheadrightarrow U$ вдоль W и проектор $\pi_W : V \twoheadrightarrow U$ вдоль W, которые связаны соотношениями $\pi_U + \pi_W = 1$ и $\pi_U \pi_W = \pi_W \pi_U = 0$.

13.2.4. Пример: корневое разложение. Если поле $\Bbbk$ алгебраически замкнуто, то характеристический многочлен любого оператора F является произведением степеней попарно разных линейных форм

$$\chi_F(t) = \prod_{\lambda \in \operatorname{Spec} F} (t - \lambda)^{m_\lambda}\,, \qquad .$$

где m_λ равно кратности корня λ характеристического многочлена

$$\chi_F(t) = \det(t\,\mathrm{Id} - F)\,.$$

Каждое подпространство $K_\lambda = \ker\,(\lambda\,\mathrm{Id} - F)^{m_\lambda}$ отлично от нуля, поскольку оно содержит ненулевое собственное подпространство $V_\lambda = \ker\,(\lambda\,\mathrm{Id} - F)$. Подпространство K_λ называется *корневым подпространством* оператора F, отвечающим корню λ_ν . Согласно сл. 13.5 пространство V является прямой суммой корневых подпространств:

$$V = \bigoplus_{\lambda \in \operatorname{Spec} F} K_\lambda\,.$$

Это разложение называется *корневым разложением* оператора F.

Предложение 13.1
В описании оператора F, данном в теореме (теор. 13.1), корневое подпространство $K_\lambda \subset V$ переходит в прямую сумму фактор колец $\Bbbk[t]/\left((t-\lambda)^m\right)$, отвечающих всем элементарным делителям $(t-\lambda)^m \in \mathrm{El}(F)$ с данным $\lambda \in \operatorname{Spec} F$, и может быть охарактеризовано как

$$K_\lambda = \bigcup_{n \in \mathbb{N}} \ker(\lambda\,\mathrm{Id} - F)^n\,.$$

Доказательство. Поскольку при $\lambda \neq \mu$ многочлен $(t-\lambda)$ обратим по модулю любого многочлена $(t-\mu)^m$, умножение на $(t-\lambda)$ в каждом фактор кольце $\Bbbk[t]/\left((t-\mu)^m\right)$ с $\mu \neq \lambda$ из разложения (13-1) является обратимым оператором и, как следствие, не имеет ядра. Поэтому корневое подпространство K_λ трансверсально прямой сумме всех $\Bbbk[t]/\left((t-\mu)^m\right)$ с $\mu \neq \lambda$. Напротив, все слагаемые вида $\Bbbk[t]/\left((t-\lambda)^m\right)$ аннулируются достаточно большой[1] степенью оператора $\lambda\,\mathrm{Id} - F$. □

Упражнение 13.5. Выведите из существования корневого разложения не опирающееся на (теор. 13.1) доказательство существования и единственности жордановой нормальной формы, и покажите, что $K_\nu = \bigcup_{m \geqslant 1} \ker(F - \lambda_\nu E)^m$ является прямой суммой всех жордановых клеток оператора F с собственным значением λ_ν (в частности, суммарный размер всех жордановых клеток с собственным значением λ равен кратности λ как корня характеристического многочлена).

[1] а именно, равной $m_{t-\lambda}(F)$ — максимальной из степеней элементарных делителей F вида $(t-\lambda)^m$ (ср. с n° 13.1.2); поскольку $\chi_F(t)$ (как и любой другой аннулирующий многочлен) делится на все элементарные делители, кратность, которую имеет корень λ в $\chi_F(t)$ заведомо не меньше $m_{t-\lambda}(F)$

13.3. Перестановочные операторы. Если линейный оператор $V \xrightarrow{F} V$ на векторном пространстве V (над произвольным полем $\Bbbk$) перестановочен с оператором $V \xrightarrow{G} V$, т. е. $FG = GF$, то ядро и образ любого многочлена $f(F)$ от оператора F переводятся оператором G в себя:

$$G\Big(\ker\big(f(F)\big)\Big) \subset \ker\big(f(F)\big) \quad \text{и} \quad G\Big(\operatorname{im}\big(f(F)\big)\Big) \subset \operatorname{im}\big(f(F)\big)\,.$$

В самом деле, $f(F)\,v = 0 \Rightarrow f(F)G\,v = Gf(F)\,v = 0$ и, аналогично,

$$v = f(F)\,w \;\Rightarrow\; Gv = Gf(F)\,w = f(F)G\,w\,.$$

В частности, собственные подпространства $V_\lambda = \ker(F - \lambda E)$ и корневые подпространства $K_\lambda = \bigcup\limits_n \ker(\lambda\,\mathrm{Id} - F)^n$ оператора F инвариантны относительно любого оператора G, перестановочного с F. Следующее следствие этого наблюдения используется особенно часто:

Лемма 13.3
Над алгебраически замкнутым полем любое множество коммутирующих операторов обладает общим собственным вектором. Над произвольным полем любое множество диагонализуемых коммутирующих операторов может быть диагонализовано одновременно в одном общем базисе.

Доказательство. Индукция по размерности пространства. Если она равна единице или если все операторы скалярны, то доказывать нечего (годится любой ненулевой вектор и, соответственно, любой базис). Если среди операторов есть нескалярный, то его собственные подпространства имеют меньшую размерность и инвариантны для всех операторов, причём если операторы были диагонализуемы во всём пространстве, то их ограничения на инвариантные подпространства будут диагонализуемы на этих подпространствах (см. сл. 13.3). Применяя к ним предположение индукции, получаем требуемое. □

Теорема 13.2 (разложение Жордана)
Для каждого оператора F над алгебраически замкнутым полем $\Bbbk$ существует единственная пара операторов F_s и F_n, таких что F_n нильпотентен, F_s диагонализуем, $F = F_s + F_n$ и $F_sF_n = F_nF_s$. Кроме того, операторы F_s и F_n являются многочленами с нулевым свободным членом от оператора F.

Доказательство. Представим F как оператор умножения на t в прямой сумме фактор колец

$$\frac{\Bbbk[t]}{((t-\lambda_1)^{m_1})} \oplus \cdots \oplus \frac{\Bbbk[t]}{((t-\lambda_s)^{m_s})}\,. \tag{13-8}$$

Пусть $\lambda_1, \lambda_2, \ldots, \lambda_r$ составляют полный список всех *различных* чисел $\lambda_i \in \Bbbk$, встречающихся в (13-8). Для каждого $i = 1,\ 2,\ \ldots\ ,\ r$ зафиксируем какое-нибудь

$a_i \in \mathbb{N}$, строго большее всех степеней, в которых $(t-\lambda_i)$ встречается в (13-8). По китайской теореме об остатках существуют многочлены $f_1, f_2, \dots, f_r \in \Bbbk[t]$, такие что

$$f_\nu \equiv \begin{cases} 1 \,(\mathrm{mod}\ (t-\lambda_\nu)^{a_\nu}) \\ 0 \,(\mathrm{mod}\ (t-\lambda_\mu)^{a_\mu}) \text{ при } \mu \neq \nu\,. \end{cases}$$

Если $\lambda_\nu \neq 0$, многочлен t обратим по модулю $(t-\lambda_\nu)^{a_\nu}$, и найдётся многочлен $g_\nu(t)$, такой что $t \cdot g_\nu(t) \equiv \lambda_\nu \,(\mathrm{mod}\ (t-\lambda_\nu)^{a_\nu})$. Для $\lambda_\nu = 0$, положим $g_\nu = 0$. В этих обозначениях, многочлен $p_s(t) = t\sum\limits_{\nu=1}^{r} g_\nu f_\nu$ не имеет свободного члена и удовлетворяет сравнениям

$$p_s(t) \equiv \lambda_\nu \,(\mathrm{mod}\ (t-\lambda_\nu)^{a_\nu})$$

одновременно для всех ν. Поэтому умножение на $p_s(t)$ действует на каждом факторе $\Bbbk[t]/\left((t-\lambda_\nu)^m\right)$ из разложения (13-8) как умножение на λ_ν. Тем самым, оператор $F_s = p_s(F)$ диагонализуем. Оператор $F_n = F - F_s$ действует на каждом факторе $\Bbbk[t]/\left((t-\lambda_\nu)^m\right)$ умножением на многочлен $t-\lambda_\nu$ и, тем самым, нильпотентен. Будучи многочленами от F, операторы F_s и F_n перестановочны между собою и с F. Итак, мы доказали существование требуемых операторов F_s и F_n, а также последнее утверждение. Остаётся доказать их единственность.

Пусть разложение $F = F'_s + F'_n$ удовлетворяет условиям теоремы. Поскольку F'_s и F'_n перестановочны между собой, они перестановочны и с $F = F'_s + F'_n$, а также с построенными выше F_s и F_n, являющимися многочленами от F. Но тогда каждое собственное подпространство V_λ оператора F_s переводится оператором F'_s в себя, и F'_s диагонализуем на V_λ. Если бы F'_s имел на V_λ собственный вектор v с собственным значением $\mu \neq \lambda$, то вектор v был собственным для оператора $F_n - F'_n = F_s - F'_s$ с ненулевым собственным значением $\lambda - \mu$, что невозможно, поскольку оператор $F_n - F'_n$ нильпотентен.

Упражнение 13.6. Докажите это.

Таким образом, F'_s действует на каждом V_λ умножением на λ, откуда $F'_s = F_s$, и $F'_n = F - F'_s = F - F_s = F_n$. □

Определение 13.2

Операторы F_s и F_n из теор. 13.2 называются, соответственно, *полупростой*[1] (или *диагонализуемой*) и *нильпотентной составляющими* оператора F.

Упражнение 13.7. Покажите, что если оператор $V \xrightarrow{F} V$ переводит некоторое подпространство $U \subset V$ в некоторое подпространство $W \subset V$, то его жордановы компоненты F_s, и F_n тоже переводят U в W.

[1]индекс «s» в обозначении F_s происходит именно от *semisimple*; термин «полупростой» пришёл из теории представлений, где объекты, не имеющие нетривиальных подобъектов (в нашем случае это операторы, не имеющие нетривиальных инвариантных подпространств, т. е. — над замкнутым полем — скалярные операторы на одномерных пространствах) принято называть *простыми*, а прямые простых объектов (в нашем случае это диагонализуемые операторы) принято называть *полупростыми*

13.4. Функции от оператора. Пусть поле $\Bbbk = \mathbb{C}$. Мы хотим продолжить гомоморфизм вычисления значения многочленов на операторе $V \xrightarrow{F} V$

$$\mathrm{ev}_F : \mathbb{C}[z] \xrightarrow{f \mapsto f(F)} \mathrm{End}(V) \tag{13-9}$$

до гомоморфизма $\mathrm{ev}_F : \mathscr{C} \longrightarrow \mathrm{End}(V)$, определённого на большей алгебре $\mathscr{C} \supset \mathbb{C}[x]$ функций $f : \mathbb{C} \longrightarrow \mathbb{C}$. Аналитический подход к решению этой задачи состоит в том, чтобы представить функцию $f \in \mathscr{C}$ как предел последовательности многочленов[1] f_n, и определить $f(F)$ как предел операторов $f_n(F) \in \mathrm{End}(V)$. Для этого надо определить в пространствах $\mathscr{C}$ и $\mathrm{End}V$ сходимость, и проверить, что $f(F)$ зависит только от f, а не от выбора сходящейся к f последовательности многочленов[2].

Алгебраический взгляд на задачу заключается в том, что какие бы определения сходимости не использовались, гомоморфизм $\mathrm{ev}_F : \mathscr{C} \longrightarrow \mathrm{End}(V)$, который получится в результате, однозначно определяется своими алгебраическими свойствами, а оператор $f(F) \in \mathrm{End}V$ эффективно вычисляется при помощи конечного числа сложений и умножений через матричные элементы F в произвольном базисе пространства V и значения функции f и её производных в точках $\lambda \in \mathrm{Spec}\, F$.

Говоря неформально, причина заключается в том, что любая последовательность многочленов $f_n(F)$, используемая при аналитическом построении $f(F)$ лежит в конечномерном пространстве $\mathbb{C}[F]$, линейно порождённом степенями F^m с $0 \leqslant m < \dim V$, и поэтому предел такой последовательности тоже является *многочленом* от F степени, меньшей[3] $\dim V$. Этот «предельный» многочлен называется *интерполяционным многочленом* для вычисления $f(F)$. Мы будем обозначать его через $P_{f,F}(F)$.

Подчеркнём, что интерполяционный многочлен определяется по функции f и оператору F не однозначно, а лишь по модулю минимального многочлена μ_F оператора F, и что значения $f(F) = P_{f,F}(F)$ и $f(G) = P_{f,G}(G)$ одной и той же функции f на разных операторах F и G получаются подстановкой F и G в вообще говоря *разные* интерполяционные многочлены

$$P_{f,F}(t) \not\equiv P_{f,G}(t) \pmod{\mu_F(t)}\,.$$

Отметим также, что если операторы $V \xrightarrow{F} V$ и $W \xrightarrow{G} W$ подобны, т. е. $G = CFC^{-1}$ для некоторого изоморфизма $C : V \xrightarrow{\sim} W$, то и функции от

[1] например, если $f = \sum a_k z^k$ это абсолютно сходящийся всюду в $\mathbb{C}$ степенной ряд, то в качестве f_n можно взять сумму первых n членов этого ряда

[2] читателю рекомендуется попробовать самостоятельно реализовать эту программу, используя в качестве сходимости в $\mathbb{C}[x]$ равномерную сходимость на каждом круге, а в качестве сходимости в $\mathrm{End}V$ поэлементную сходимость матриц операторов, записываемых в каком-нибудь фиксированном базисе пространства V

[3] если сходимость в $\mathrm{End}V$ такова, что $\lim\limits_{n\to\infty}(\lambda F_n + \mu G_n) = \lambda \lim\limits_{n\to\infty} F_n + \mu \lim\limits_{n\to\infty} G_n$ (когда оба предела в правой части существуют), то предел последовательности операторов, удовлетворяющих некоторому линейному уравнению, тоже удовлетворяет этому уравнению

них подобны: $f(G) = Cf(F)C^{-1}$, поскольку соотношение $f_n(G) = Cf_n(F)C^{-1}$ выполнено для всех многочленов, приближающих функцию f, а стало быть, останется выполненным и в пределе[1].

Теперь дадим формальные определения. Пусть оператор $F \in \mathrm{End}V$ имеет спектр $\mathrm{Spec}\, F = \{\lambda_1, \lambda_2, \ldots, \lambda_r\} \subset \mathbb{C}$ и минимальный многочлен

$$\mu_F = \prod_{\lambda \in \mathrm{Spec}\, F} (t-\lambda)^{m_\lambda}$$

(напомним, что m_λ равно максимальной степени $m_{t-\lambda}(F)$, встречающейся среди элементарных делителей $(t-\lambda)^m \in \mathrm{El}(F)$, см. n° 13.1.2). Будем называть алгебру $\mathscr{C} \supset \mathbb{C}[x]$ функций $f : \mathbb{C} \longrightarrow \mathbb{C}$ *приспособленной* к гомоморфизму

$$\mathrm{ev}_F : \mathbb{C}[z] \longrightarrow \mathbb{C}[F] = \mathbb{C}[t]/\left(\mu_F\right) \tag{13-10}$$

вычисления на операторе F, если каждая функция $f \in \mathscr{C}$ допускает для каждого $\lambda \in \mathrm{Spec}\, F$ представление в виде

$$f(z) = f(\lambda) + \frac{f'(\lambda)}{1!}(z-\lambda) + \cdots + \frac{f^{(m_\lambda - 1)}(\lambda)}{(m_\lambda - 1)!}(z-\lambda)^{m_\lambda - 1} + g_\lambda(z)\cdot(z-\lambda)^{m_\lambda} \tag{13-11}$$

с $g_\lambda \in \mathscr{C}$. Если алгебра $\mathscr{C}$ приспособлена к гомоморфизму вычисления на операторе F, то она приспособлена и к гомоморфизму вычисления на всех подобных F операторах CFC^{-1}. Будем называть *естественным продолжением* гомоморфизма вычисления (13-10) на алгебру $\mathscr{C}$ набор гомоморфизмов алгебр

$$\mathrm{ev}_G : \mathscr{C} \longrightarrow \mathbb{C}[G]$$

заданных для всех $G = CFC^{-1}$ и удовлетворяющих соотношениям

$$\mathrm{ev}_{CFC^{-1}}(f) = C \cdot \mathrm{ev}_F(f) \cdot C^{-1}\,.$$

Замечание 13.1. Алгебра степенных рядов $f(z) = \sum a_k z^k$, абсолютно сходящихся в любой точке $z_0 \in \mathbb{C}$, приспособлена к гомоморфизму вычисления на любом операторе: для получения выражения (13-11) надо просто переразложить ряд f по степеням $(z-\lambda)$ в окрестности точки $z_0 = \lambda$. Более общим образом, приспособленной к вычислению на данном операторе F является алгебра всех функций $\mathbb{C} \longrightarrow \mathbb{C}$, раскладывающихся в некоторой окрестности каждой точки $\lambda \in \mathrm{Spec}\, F$ в ряд Тейлора, абсолютно сходящийся во всех точках этой окрестности. Например, функция $\mathrm{th}\, z$ приспособлена к вычислению на любом операторе, спектр которого не содержит чисел вида $2\pi i k$, $k \in \mathbb{Z}$.

[1] для этого достаточно, чтобы сходимость в пространствах $\mathrm{End}V$ и $\mathrm{End}W$ была такой, чтобы все *линейные* отображения $\mathrm{End}V \longrightarrow \mathrm{End}W$ были непрерывны

Теорема 13.3
Для любого оператора F на конечномерном комплексном векторном пространстве V существует единственное естественное продолжение гомоморфизма вычисления (13-10) на любую алгебру $\mathscr{C}$, приспособленную к этому гомоморфизму вычисления. При этом для каждой функции $f \in \mathscr{C}$ в качестве интерполяционного многочлена $P_{f,F}$, такого что $P_{f,F}(F) = f(F)$, можно взять (единственный) многочлен $P_{f,F}(t) \in \mathbb{C}[t]$ степени, меньшей $\dim V$, такой что

$$P_{f,F}^{(k)}(\lambda) = f^{(k)}(\lambda) \quad \forall\, k = 0,\, 1,\, \dots\,,\, m_\lambda - 1\,.$$

в каждой точке $\lambda \in \operatorname{Spec} F$

Доказательство. Достаточно изучить продолжения на алгебру $\mathscr{C}$ гомоморфизма вычисления ev_F на каком-нибудь одном операторе F в классе подобных операторов — продолжения на все остальные элементы класса однозначно из него получаются. Возьмём в качестве такового F оператор умножения на t в прямой сумме фактор колец

$$\frac{\mathbb{C}[t]}{((t-\lambda_1)^{s_1})} \oplus \dots \oplus \frac{\mathbb{C}[t]}{((t-\lambda_r)^{s_r})} \tag{13-12}$$

из теор. 13.1 (слагаемые этой суммы биективно соответствуют элементарным делителям оператора F и могут повторяться).

Пусть искомое продолжение ev_F на алгебру $\mathscr{C}$ существует. Поскольку его образ содержится в алгебре многочленов от оператора F, оператор $\mathrm{ev}_F(f)$ для $f \in \mathscr{C}$ является оператором умножения на некоторый многочлен от t, который мы обозначим через $\widetilde{f}(t)$. Так как ev_F является гомоморфизмом алгебр, из наличия представления (13-11) вытекает, что умножение на $\widetilde{f}(t)$ действует на (13-12) точно так же, как умножение на многочлен

$$f(\lambda) + f'(\lambda)(t-\lambda) + \dots + f^{(m_\lambda - 1)}(t-\lambda)^{m_\lambda - 1}/(m_\lambda - 1)! + (t-\lambda)^{m_\lambda}\widetilde{g}_\lambda(t)\,.$$

Тем самым, на каждом прямом слагаемом вида $\mathbb{C}[t]/\big((t-\lambda)^k\big)$ в сумме (13-12) $\widetilde{f}(t)$ действует умножением на класс

$$\big[f(\lambda) + f'(\lambda)(t-\lambda) + \dots + f^{(m_\lambda - 1)}(t-\lambda)^{m_\lambda - 1}/(m_\lambda - 1)!\big] \pmod{(t-\lambda)^{m_\lambda}}$$

Но по китайской теореме об остатках существует единственный класс

$$\widetilde{f}(t) \pmod{\mu_F(t)}$$

сравнимый с $f(\lambda) + f'(\lambda)(t-\lambda) + \dots + f^{(m)}(\lambda)(t-\lambda)^m/m! \pmod{(t-\lambda)^{m_\lambda}}$ одновременно для всех $\lambda \in \operatorname{Spec} F$. Таким образом, продолжение ev_F на алгебру $\mathscr{C}$ единственно. Покажем, что оно существует. Обозначим через

$$s_\lambda^m f = \sum_{k=0}^{m-1} f^{(k)}(\lambda)\,(t-\lambda)^k \pmod{(t-\lambda)^m}$$

$(m-1)$-*струю* функции f в точке $\lambda \in \mathbb{C}$, рассматриваемую как элемент фактор кольца $\mathbb{C}[t]/\left((t-\lambda)^m\right)$, и рассмотрим отображение

$$s : \mathscr{C} \longrightarrow \prod_{\lambda \in \operatorname{Spec} F} \frac{\mathbb{C}[t]}{\left((t-\lambda)^{m_\lambda}\right)}, \tag{13-13}$$

сопоставляющее каждой функции $f \in \mathscr{C}$ набор её струй

$$\left(s_{\lambda_1}^{m_{\lambda_1}-1} f, \, \dots \, , \, s_{\lambda_r}^{m_{\lambda_r}-1} f\right)$$

в точках спектра оператора F.

Упражнение 13.8. Проверьте, что отображение (13-13) является гомоморфизмом алгебр.

Таким образом, сопоставляя функции $f \in \mathscr{C}$ оператор, действующий на каждом прямом слагаемом вида $\mathbb{C}[t]/\left((t-\lambda)^k\right)$ в сумме (13-12) умножением на класс струи $s_\lambda^{m_\lambda - 1} f$, мы получаем требуемый гомоморфизм из алгебры $\mathscr{C}$ в алгебру многочленов от оператора F.

Поскольку указанный в формулировке теоремы интерполяционный многочлен $P_{f,F}$ имеет тот же образ при отображении (13-13), что и функция f, умножение на него действует на (13-12) точно также, как $\widetilde{f}$. □

13.4.1. Пример: рекуррентные уравнения и вычисление степеней. Задачу отыскания n-того члена числовой последовательности $a_n \in \mathbb{C}$, удовлетворяющей рекуррентному уравнению m-того порядка

$$a_n = \alpha_1 a_{n-1} + \alpha_2 a_{n-2} + \, \cdots \, + \alpha_m a_{n-m} \, ,$$

если заданы её начальные m членов $(a_0, a_1, \dots, a_{m-1})$, можно решать следующим образом. Рассмотрим $m \times m$ -матрицу

$$S = \begin{pmatrix} 0 & 0 & \cdots & 0 & \alpha_m \\ 1 & 0 & \ddots & 0 & \alpha_{m-1} \\ 0 & 1 & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & \alpha_2 \\ 0 & \cdots & 0 & 1 & \alpha_1 \end{pmatrix}$$

Умножение фрагмента последовательности a_n, состоящего из m подряд идущих членов, справа на матрицу S, приводит к сдвигу этого фрагмента на единицу вправо:

$$(a_{k+1}, \, a_{k+2}, \, \dots \, , \, a_{k+m}) \cdot S = (a_{k+2}, \, a_{k+3}, \, \dots \, , \, a_{k+m+1})$$

Поэтому n-тый член последовательности a_n равен первой координате вектора

$$(a_0, a_1, \, \dots, \, a_{m-1}) \cdot S^n = (a_n, \, a_{n+1}, \, \dots \, , \, a_{n+m-1}) \, .$$

Таким образом, задача отыскания последовательности a_n полностью сводится к задаче отыскания n-той степени оператора правого умножения на матрицу S, причём решив эту задачу мы без дополнительных вычислений сможем находить последовательности a_n с *любыми* начальными условиями $(a_0, a_1, \dots, a_{m-1})$.

Найти явную формулу для S^n нетрудно по теор. 13.3. Проиллюстрируем это на примере матрицы

$$S = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

умножение на которую задаёт сдвиг в последовательности Фиббоначчи φ_n, определяемой рекуррентным уравнением второго порядка $a_n = a_{n-1} + a_{n-2}$. Характеристический многочлен

$$\chi_S(t) = \det \begin{pmatrix} t & -1 \\ -1 & t-1 \end{pmatrix} = t^2 - t - 1 = (t - \lambda_+)(t - \lambda_-) \;, \quad .$$

где $\lambda_\pm = (1 \pm \sqrt{5})/2$. Значения функции $f(x) = x^n$ на точках спектра S суть $f(\lambda_\pm) = \lambda_\pm^n$. Интерполяционный многочлен $P_{f,S}(t) = at + b$ линеен[1] и находится из уравнений

$$\begin{cases} a\,\lambda_+ + b = \lambda_+^n \\ a\,\lambda_- + b = \lambda_-^n \,. \end{cases}$$

Решая их, получаем

$$a = \frac{\lambda_+^n - \lambda_-^n}{\lambda_+ - \lambda_-} \;, \quad b = \lambda_+^n - a\,\lambda_+ = \frac{\lambda_+^{n-1} - \lambda_-^{n-1}}{\lambda_+ - \lambda_-} \;,$$
$$S^n = aS + bE = \begin{pmatrix} b & a \\ a & a+b \end{pmatrix}$$

Беря классическое начало $\varphi_0 = 0$, $\varphi_1 = 1$, получаем $(\varphi_n, \varphi_{n+1}) = (0,1) \cdot S^n$, откуда

$$\varphi_n = a = \frac{\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n}{\sqrt{5}}$$

(сравните это вычисление с проделанным ранее в n° 5.3.1 на стр. 75).

Предложение 13.2

Спектр оператора $f(F)$ состоит из чисел $f(\lambda)$ с $\lambda \in \operatorname{Spec} F$. Если $f'(\lambda) \neq 0$, то элементарные делители $(t - \lambda)^m \in \operatorname{El}(F)$ биективно соответствуют элементарным делителям $\big(t - f(\lambda)\big)^m \in \operatorname{El}\big(f(F)\big)$ оператора $f(F)$. Если $f'(\lambda) = 0$, то элементарные делители вида $(t - \lambda)^m \in \operatorname{El}(F)$, имеющие $m > 1$, распадаются в объединения элементарных делителей $\big(t - f(\lambda)\big)^\ell \in \operatorname{El}\big(f(F)\big)$, имеющих $\ell < m$.

[1] так как $\dim V = 2$

Доказательство. Из доказательства теор. 13.3 вытекает, что диагональная и нильпотентная составляющие ограничения оператора $\widetilde{f}$ на каждое неразложимое подпространство вида $\mathbb{C}[t]/\left((t-\lambda)^k\right)$ в сумме (13-12) суть $S = f(\lambda)\cdot\mathrm{Id}$ и $N = f'(\lambda)\cdot\eta + \frac{1}{2}f''(\lambda)\cdot\eta^2 + \cdots$, где через η обозначен нильпотентный оператор умножения на $(t-\lambda)$, цикловой тип которого состоит из единственной жордановой цепочки длины k. Если $f'(\lambda)\neq 0$, то $N^{k-1} = f'(\lambda)^{m-1}\cdot\eta^{k-1}\neq 0$. Поэтому цикловой тип N тоже состоит из одной цепочки длины k. При $f'(l)=0$ и $m>1$ равенство $N^m = 0$ наступит при $m<k$, так что цикловой тип N будет состоять из нескольких жордановых цепочек. □

Задачи для самостоятельного решения к §13

Задача 13.1. Найдите все инвариантные подпространства оператора с диагональной матрицей.

Задача 13.2. Есть ли в $\mathrm{Mat}_n(\mathbb{C})$ подпространство размерности $(n+1)$, состоящее из попарно коммутирующих диагонализуемых матриц?

Задача 13.3. Оператор $\mathbb{R}^n \longrightarrow \mathbb{R}^n$ имеет в стандартном базисе матрицу с числами $\lambda_1,\lambda_2,\dots,\lambda_n$ на побочной диагонали и нулями в остальных местах. Когда такой оператор диагонализуем (над $\mathbb{R}$)?

Задача 13.4. Покажите, что разложения пространства V в прямые суммы подпространств взаимно однозначно соответствуют разложениям $\mathrm{Id}_V = \pi_1+\pi_2+\cdots\pi_s$ в которых $\pi^2=\pi$ и $\pi_i\pi_j=\pi_j\pi_i = 0\ \forall\, i\neq j$.

Задача 13.5. Покажите, что для коммутирующих операторов $FG=GF$ жордановы компоненты их суммы равны суммам жордановых компонент: $(F+G)_s = F_s+G_s$ и $(F+G)_n = F_n+G_n$.

Задача 13.6. Найдите все подпространства в $\mathbb{Q}^3$, одновременно инвариантные для пары операторов с матрицами $A = \begin{pmatrix} 5 & -1 & -1\\ -1 & 5 & -1\\ -1 & -1 & 5\end{pmatrix}$ и $B = \begin{pmatrix} -6 & 2 & 3\\ 2 & -3 & 6\\ 3 & 6 & 2\end{pmatrix}$.

Задача 13.7. Расклассифицируйте с точностью до подобия[1] $F\mapsto CFC^{-1}$ все матрицы в $\mathrm{Mat}_2(\mathbb{F}_p)$, $\mathrm{GL}_2(\mathbb{F}_p)$ и $\mathrm{SL}_2(\mathbb{F}_p)$ для $p=2,3,5$.

Задача 13.8. Найдите минимальный многочлен над $\mathbb{R}$ оператора $F:\mathbb{R}^4\longrightarrow\mathbb{R}^4$, матрица которого в стандартном базисе имеет вид

$$\begin{pmatrix} 5 & 5 & 1 & -10\\ 2 & 5 & -2 & -9\\ 0 & -1 & 1 & 0\\ 3 & 4 & 0 & -8\end{pmatrix}$$

[1] т.е. приведите список попарно неподобных матриц, такой что каждая матрица из рассматриваемой группы подобна одной из матриц этого списка

разложите его на неприводимые (над $\mathbb{R}$) множители, и напишите матрицы проекторов на инвариантные подпространства оператора F, отвечающие этому разложению.

Задача 13.9. Найдите (над полем $\mathbb{C}$) минимальный многочлен, собственные и корневые подпространства и жорданову нормальную форму оператора $\mathbb{C}^4 \longrightarrow \mathbb{C}^4$, матрица которого в стандартном базисе та же, что и в предыдущей задаче.

Задача 13.10. Найдите жордановы нормальные формы матриц (над полем $\mathbb{C}$)

а) $\begin{pmatrix} 2 & 1 & -2 & 7 \\ 0 & 4 & -4 & 5 \\ 2 & 3 & -6 & 7 \\ 1 & 1 & -3 & 2 \end{pmatrix}$ б) $\begin{pmatrix} 3 & 1 & -3 & 9 \\ 2 & 4 & -6 & 9 \\ 3 & 3 & -7 & 9 \\ 1 & 1 & -3 & 2 \end{pmatrix}$ в) $\begin{pmatrix} -2 & -8 & 1 & -6 \\ 6 & 11 & -6 & 0 \\ 8 & 10 & -9 & -6 \\ -7 & -11 & 7 & 2 \end{pmatrix}$

г) $\begin{pmatrix} n & n-1 & n-2 & \cdots & 1 \\ 0 & n & n-1 & \cdots & 2 \\ 0 & 0 & n & \cdots & 3 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & n \end{pmatrix}$ д) $\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ 0 & & \ddots & \ddots & 1 \\ 1 & 0 & \cdots & 0 & 0 \end{pmatrix}$

Задача 13.11. Докажите, что степень минимального многочлена нескалярной квадратной матрицы ранга 1 равна 2.

Задача 13.12. Докажите, что если степень минимального многочлена линейного оператора $F : V \longrightarrow V$ равна $\dim V$, то всякий оператор, перестановочный с F, является многочленом от F.

Задача 13.13. Пусть минимальный многочлен линейного оператора $F : V \longrightarrow V$ является произведением двух взаимно простых многочленов $g_1 g_2$. Покажите, что V является прямой суммой двух F-инвариантных подпространств, на которые F ограничивается в операторы с минимальными многочленами g_1 и g_2.

Задача 13.14. Пусть минимальный многочлен линейного оператора $F : V \longrightarrow V$ неприводим и имеет степень d. Покажите, что $\dim V = d$ и для любого ненулевого $v \in V$ векторы v, Fv, ..., $F^{d-1}v$ составляют базис в V.

Задача 13.15. Докажите, что оператор F на n-мерном векторном пространстве нильпотентен тогда и только тогда, когда $\operatorname{tr} F = \operatorname{tr} F^2 = \cdots = \operatorname{tr} F^n = 0$.

Задача 13.16. Рассмотрим пространство $\mathrm{Mat}_{n\times n}$ всех $n \times n$-матриц и свяжем с данной матрицей $A = (a_{\mu,\nu}) \in \mathrm{Mat}_{n\times n}$ три оператора $\mathrm{Mat}_{n\times n} \longrightarrow \mathrm{Mat}_{n\times n}$:

$$L_A : X \mapsto A \cdot X\,, \quad R_A : X \mapsto X \cdot A\,, \quad \mathrm{Ad}_A : X \mapsto \mathrm{Ad}_A(X) = A \cdot X \cdot A^{-1}$$

Вычислите их следы и определители при а) $n = 2$ б) $n = 3$ в) любом n.

Задача 13.17. Обозначим через W пространство однородных многочленов второй степени от двух переменных (x_0, x_1) с базисом $(x_0^2\,, 2x_0x_1\,, x_1^2)$. Свяжем с данной матрицей $A \in \mathrm{Mat}_2(\Bbbk)$ оператор $S^2A : W \longrightarrow W$, переводящий $f(x_0, x_1)$ в $f\left((x_0, x_1) \cdot A\right)$. Найдите его матрицу и вычислите её след и определитель.

Задача 13.18. Обозначим через $\Bbbk[x_1, x_2, \dots, x_n]_{\leqslant n}$ пространство многочленов степени $\leqslant n$. Найдите собственные векторы, собственные числа, собственные и корневые подпространства и минимальные многочлены следующих операторов: а) $\frac{d}{dx}$ в линейной оболочке функций $\sin(x)$, $\cos(x)$, ... , $\sin(nx)$, $\cos(nx)$

б) $\frac{d}{dz}$ на $(n+1)$-мерном пространстве функций $\mathbb{C} \longrightarrow \mathbb{C}$ вида[1]

$$f(z) = e^{\lambda z}(a_0 + a_1 z + \dots + a_n z^n)$$

в) $x\frac{d}{dx}$ на $\Bbbk[x]_{\leqslant n}$ и $\sum x_i \frac{\partial}{\partial x_i}$ на $\Bbbk[x_1, x_2, \dots, x_n]_{\leqslant n}$ при $\mathrm{char}(\Bbbk) = 0$

г) $f(x) \mapsto f(x-1, y+1)$ в линейной оболочке мономов $x^n y^m$ с $0 \leqslant m, n \leqslant 2$

д) $f(x) \mapsto \displaystyle\int_0^1 (x^2 y + xy^2) f(y)\, dy$ на пространстве $\mathbb{R}[x]_{\leqslant 3}$

е) $f(x) \mapsto f(ax+b)$ (a, b — фиксированные числа) на пространстве $\Bbbk[x]_{\leqslant n}$

ж) $\mathrm{Mat}_{m\times n}(\Bbbk) \xrightarrow{X \mapsto AX} \mathrm{Mat}_{m\times n}(\Bbbk)$, где $A \in \mathrm{Mat}_m(\Bbbk)$ фиксированная квадратная матрица с известным минимальным многочленом $\mu_A(x) \in \Bbbk[x]$.

Выясните, диагонализуемы ли эти операторы (над тем полем, где они заданы).

Задача 13.19. Докажите, что над алгебраически замкнутым полем максимальное количество линейно независимых собственных векторов с одним и тем же собственным значением λ у данного линейного оператора равно числу его жордановых клеток с диагональным элементом λ.

Задача 13.20. Докажите, что любая матрица сопряжена своей транспонированной.

Задача 13.21. На векторном пространстве над алгебраически замкнутым полем действует оператор F. Покажите, что оператор G, перестановочный с любым оператором, перестановочным с F, является многочленом от F.

Задача 13.22. Пусть операторы A и B удовлетворяют соотношению $AB - BA = B$. Покажите, что B нильпотентен.

Задача 13.23* (лемма Барта). Покажите, что над алгебраически замкнутым полем любые два оператора A и B, для которых $\mathrm{rk}\,(AB - BA) = 1$, имеют общий собственный вектор.

Задача 13.24. Диагонализуем ли оператор, удовлетворяющий уравнению $A^3 - 6A^2 + 11A - 6E = 0$?

Задача 13.25. Найдите жорданову нормальную форму квадрата жордановой клетки $J_m(\lambda)^2$ а) при $\lambda \neq 0$ б) при $\lambda = 0$.

Задача 13.26. Решите в $\mathrm{Mat}_2(\mathbb{C})$ уравнения $X^2 = \begin{pmatrix} 3 & 1 \\ -1 & 5 \end{pmatrix}$ и $X^2 = \begin{pmatrix} 6 & 2 \\ 3 & 7 \end{pmatrix}$

[1] в курсе дифференциальных уравнений такие функции часто называют *квазимногочленами* веса λ и степени $\leqslant n$

Задача 13.27. Найдите $\begin{pmatrix} 1 & 1 \\ -1 & 3 \end{pmatrix}^{50}$ и $\begin{pmatrix} 7 & -4 \\ 4 & -8 \end{pmatrix}^{50}$

Задача 13.28. Вычислите а) A^n б) $\sin A$ в) $\cos A$ г) e^A для матриц

$$A = \begin{pmatrix} 1 & 2 \\ 3 & 0 \end{pmatrix} \quad \text{и} \quad A = \begin{pmatrix} 1 & 2 \\ 3 & 2 \end{pmatrix}$$

Задача 13.29. Найдите $f(J_m(\lambda))$, где $f : \mathbb{R} \longrightarrow \mathbb{R}$ — аналитическая в окрестности точки $\lambda \in \mathbb{R}$ функция, а $J_m(\lambda)$ — жорданова клетка размера $m \times m$ с собственным числом λ.

Задача 13.30. Существует ли целочисленная матрица Z с $Z^2 = \begin{pmatrix} 4 & -5 & 7 \\ 1 & -4 & 9 \\ -4 & 0 & 5 \end{pmatrix}$?

Раздел IV
Геометрические структуры

§14. Евклидовы пространства

14.1. Евклидова структура. Пусть V — произвольное векторное пространство над полем вещественных чисел $\mathbb{R}$. Функция

$$(\,*\,,\,*\,) : V \times V \longrightarrow \mathbb{R}\,,$$

сопоставляющая паре векторов $u, w \in V$ вещественное число $(u, w) \in \mathbb{R}$ называется *евклидовым скалярным произведением* (или *евклидовой структурой*) на пространстве V, если она *билинейна*, *симметрична* и *положительна*. Первое свойство означает линейность по каждому из аргументов при фиксированном втором, т. е. стандартное правило раскрытия скобок

$$(\lambda_1 u_1 + \lambda_2 u_2\,,\, \mu_1 w_1 + \mu_2 w_2) = \sum_{i,j} \lambda_i \mu_j (u_i, w_j)\,.$$

Второе свойство означает равенство $(u, w) = (w, u)$ для всех $u, w \in V$. Положительность, по определению, означает положительность скалярных квадратов всех ненулевых векторов: $(v, v) > 0 \quad \forall\, v \neq 0\,.$

Вещественное векторное пространство V, снабжённое евклидовой структурой, называется *евклидовым.*

Модельными примерами евклидовых пространств являются евклидова плоскость и трёхмерное евклидово пространство, изучаемые в школьных курсах планиметрии и стереометрии. Все геометрические понятия, имеющиеся в этих «школьных» пространствах, без изменений переносятся в любое евклидово пространство.

14.1.1. Пример: координатное пространство $\mathbb{R}^n$ имеет *стандартную евклидову структуру* в которой скалярное произведение векторов

$$u = (x_1, x_2, \dots, x_n) \quad \text{и} \quad w = (y_1, y_2, \dots, y_n)$$

задаётся формулой

$$(u, w) = x_1 y_1 + x_2 y_2 + \,\cdots\, + x_n y_n \tag{14-1}$$

которая очевидным образом билинейна, симметрична и положительна.

14.1.2. Пример: пространство непрерывных функций на отрезке $[a,b]$ имеет скалярное произведение

$$(f,g) = \int\limits_a^b f(x)g(x)\,dx\,. \tag{14-2}$$

Упражнение 14.1. Проверьте, что это произведение билинейно и положительно.

Если понимать функции на отрезке как элементы прямого произведения континуального семейства одномерных пространств, биективно соответствующих точкам отрезка, то формула (14-2) является прямым обобщением формулы (14-1). Эта конструкция допускает разнообразные вариации. Во-первых, вместо непрерывных функций можно рассматривать другие классы функций, для которых выполняется свойство

$$f \not\equiv 0 \;\Rightarrow\; \int\limits_a^b f^2(x)\,dx \neq 0\,,$$

или ограничивать произведение (14-2) на подпространства — например, на многочлены степени не выше n. Во-вторых можно варьировать само понятие интеграла (интеграл Лебега, интеграл Римана и т. п.) или интегрировать с весом (см. зад. 14.19). В-третьих, можно заменить отрезок любой другой областью, рассматривать несобственный интеграл и т. п.

14.1.3. Ортогонализация Грама – Шмидта. Векторы $u,w \in V$ называются *ортогональными*, если $(u,w)=0$. Набор попарно ортогональных векторов называется *ортогональным* набором. Ортогональный набор называется *ортонормальным*, если скалярные квадраты всех его векторов равны 1.

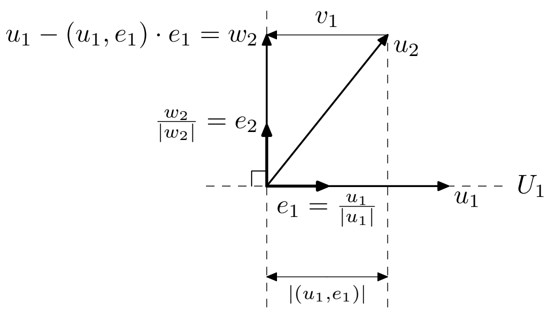


Рис. 14◇1. Второй шаг ортогонализации.

Покажем, что для любого базиса u евклидова пространства V существует ортонормальный базис $e=uC_{ue}$ с верхнетреугольной матрицей перехода C_{ue}.

Алгоритм построения такого базиса называется *процессом Грама – Шмидта*. Он заключается в последовательной замене векторов $u_1,u_2,\dots,u_n$ векторами $w_k=u_k-v_{k-1}$, где вектор v_{k-1} выбирается в линейной оболочке U_{k-1} предыдущих векторов $u_1,u_2,\dots,u_{k-1}$ так, чтобы w_k оказался ортогонален ко всем векторам подпространства U_{k-1} (см. рис. 14◇1).

А именно, положим на первом шагу $w_1=u_1$ и $e_1=w_1/|w_1|$, где через $|v|$ здесь и далее обозначается *длина* $|v|=\sqrt{(v,v)}$ вектора v. Тогда $(e_1,e_1)=1$

и e_1 порождает то же одномерное пространство, что и u_1. Пусть на $(k-1)$-том шагу нами уже построены векторы $e_1, e_2, \dots, e_{k-1}$ составляющие ортонормальный базис в линейной оболочке U_{k-1} векторов $u_1, u_2, \dots, u_{k-1}$. Положим $w_k = u_k - (u_k, e_1)\cdot e_1 - (u_k, e_2)\cdot e_2 - \cdots - (u_k, e_{k-1})\cdot e_{k-1}$. Тогда в силу ортонормальности векторов $e_1, e_2, \dots, e_{k-1}$ имеем для каждого i равенство $(w_k, e_i) = (u_k, e_i) - (u_k, e_i)(e_i, e_i) = 0$. Полагая $e_k = w_k/|w_k|$ оказываемся в исходном положении для $(k+1)$-го шага.

14.2. Матрицы Грама. С любым набором векторов $u = (u_1, u_2, \dots, u_m)$ евклидова пространства V можно связать их «таблицу умножения» — квадратную матрицу попарных скалярных произведений

$$G_u = \big((u_i, u_j)\big)\ .$$

Она называется *матрицей Грама* набора векторов u. Например, матрица Грама ортогонального набора диагональна, а ортонормального набора — единичная.

Если набор векторов $w = (w_1, w_2, \dots, w_m)$ линейно выражаются через набор векторов $w = (w_1, w_2, \dots, w_m)$ как $w = uC_{uw}$, то матрица Грама G_w пересчитывается через матрицу Грама G_u по формуле

$$G_w = C_{uw}^t G_w C_{uw}\ , \tag{14-3}$$

где матрица C_{uw}^t транспонирована к C_{wv}. В самом деле,

$$(v_i, v_j) = \Big(\sum_\alpha c_{\alpha i} w_\alpha\,,\ \sum_\beta c_{\beta j} w_\beta\Big) = \sum_{\alpha,\beta} c_{\alpha i}\cdot(w_\alpha, w_\beta)\cdot c_{\beta j} = \\ = \sum_\alpha c_{i\alpha}^t \cdot \sum_\beta (w_\alpha, w_\beta)\cdot c_{\beta j}\ .$$

Эта выкладка допускает сокращённую матричную запись в духе n° 9.3, если договориться понимать под произведением векторов $v, u \in V$ их скалярное произведение $vu \overset{\text{def}}{=} (v, u)$. При таком соглашении матрица Грама

$$G_w = w^t w$$

является произведением столбца векторов w^t на строку векторов w и, подставив $w = vC_{vW}$, получаем

$$G_w = w^t w = (vC_{vw})^t\, v\, C_{vw} = C_{vw}^t v^t v\, C_{vw} = C_{vw}^t G_v C_{vw}\ .$$

14.2.1. Определители Грама. Определитель $\det G_v$ матрицы Грама G_v набора векторов v называется *определителем Грама* этих векторов.

Лемма 14.1
Определитель Грама любого набора векторов $v_1, v_2, \dots, v_m$ неотрицателен, и его обращение в нуль равносильно линейной зависимости этих векторов.

Доказательство. Выберем в линейной оболочке векторов $v_1, v_2, \ldots, v_m$ ортонормальный базис $e_1, e_2, \ldots, e_n$. Тогда $v = eC_{ev}$ и

$$G_v = C_{ev}^t G_e C_{ev} = C_{ev}^t E C_{ev} = C_{ev}^t C_{ev}$$

Если $n < m$, то $\operatorname{rk} G_v \leqslant \operatorname{rk} C_{ev} \leqslant m < n$ и $\det G_v = 0$. Если $n = m$, то векторы v тоже образуют базис, и $\det C_{ev} \neq 0$, а $\det G_v = \det C_{ev}^t \cdot \det C_{ev} = \det^2 C_{ev} > 0$. □

14.2.2. Пример: неравенство Коши – Буняковского – Шварца. Для набора из двух векторов $v, w \in V$ неравенство

$$\det \begin{pmatrix} (v,v) & (v,w) \\ (w,v) & (w,w) \end{pmatrix} \geqslant 0$$

из леммы (лем. 14.1) означает, что

$$(v,v) \cdot (w,w) \geqslant (v,w)^2 , \tag{14-4}$$

и равенство равносильно тому, что v и w пропорциональны.

Неравенство (лем. 14.1), написанное в координатном евклидовом пространстве $\mathbb{R}^n$ из n° 14.1.1 выглядит как

$$(x_1^2 + x_2^2 + \ \cdots \ + x_n^2)(y_1^2 + y_1^2 + \ \cdots \ + y_n^2) \geqslant (x_1 y_1 + x_1 y_1 + \ \cdots \ + x_n y_n)^2$$

и называется *неравенством Коши – Буняковского*. Оно справедливо для любых двух наборов вещественных чисел $x_1, x_2, \ldots, x_n$ и $y_1, y_2, \ldots, y_n$ и обращается в равенство тогда и только тогда, когда эти наборы пропорциональны.

Неравенство (лем. 14.1), написанное в пространстве непрерывных функций на отрезке $[a, b]$ из n° 14.1.2 выглядит как

$$\Big(\int\limits_a^b f^2(x)\,dx\Big) \cdot \Big(\int\limits_a^b g^2(x)\,dx\Big) \geqslant \Big(\int\limits_a^b f(x)g(x)\,dx\Big)^2 .$$

и называется *неравенство Шварца*. Оно имеет место для любых двух непрерывных функций f и g и обращается в равенство тогда и только тогда, когда функции f отличаются скалярным множителем.

14.3. Евклидова геометрия. Длина вектора и угол между двумя векторами определяются в евклидовом пространстве формулами:

$$|v| \stackrel{\text{def}}{=} \sqrt{(v,v)} \tag{14-5}$$

$$\cos(\widehat{vw}) \stackrel{\text{def}}{=} \frac{(v,w)}{|v| \cdot |w|} \tag{14-6}$$

Из неравенства (14-4) вытекает, что правая часть формулы (14-6) действительно лежит в множестве значений косинуса $[-1, 1]$, а длина (14-5) удовлетворяет неравенству треугольника:

$$\forall\, u, w \quad |u| + |w| \geqslant |u + w| \,. \tag{14-7}$$

В самом деле: $|u+w|^2 = |u|^2 + |w|^2 + 2(u,w) \leqslant |u|^2 + |w|^2 + 2|u| \cdot |w|$.

Упражнение 14.2. Покажите, что равенство в (14-7) равносильно тому, что векторы u и w *сонаправлены* (пропорциональны с неотрицательным коэффициентом пропорциональности).

Отметим, что скалярное произведение однозначно восстанавливается, если известны длины всех векторов, по формулам

$$(v, w) = (|v + w|^2 - |v - w|^2)/4 = (|v + w|^2 - |v|^2 - |w|^2)/2 \,. \tag{14-8}$$

В самом деле, $|v \pm w|^2 = (v \pm w, v \pm w) = (v, v) \pm 2(v, w) + (w, w)$.

14.3.1. Евклидов объём и ориентация. Согласно теор. 10.2 на любом векторном пространстве имеется единственная с точностью до пропорциональности форма объёма. Зафиксируем такую форму на евклидовом пространстве.

Лемма 14.2
Объём любых двух ортонормальных базисов евклидова пространства одинаков с точностью до знака.

Доказательство. Пусть $u = (u_1, u_2, \dots, u_n)$ и $w = (w_1, w_2, \dots, w_n)$ два ортонормальных базиса, связанных переходом $w = u\, C_{uw}$. Поскольку

$$E = G_w = C_{uw}^t G_u C_{uw} = C_{uw}^t E C_{uw} = C_{uw}^t C_{uw} \,,$$

беря определители, получаем $\det^2 C_{uw} = 1$, откуда $\det C_{uw} = \pm 1$. □

Определение 14.1 (евклидов объём и ориентация)
Ортонормальные базисы, имеющие одинаковый объём, называются *одинаково ориентированными*, а базисы, противоположного по знаку объёма, называются *противоположно ориентированными*. Фиксация на евклидовом пространстве V одной из двух форм объёма, для которых все ортонормальные базисы имеют объёмы ± 1, называется *выбором ориентации* на V. Абсолютная величина значения любой из этих двух форм на наборе векторов $(v_1, v_2, \dots, v_n)$ называется *евклидовым объёмом* параллелепипеда, натянутого на эти векторы, и обозначается $\operatorname{Vol}(v_1, v_2, \dots, v_n)$. Ориентация координатного пространства $\mathbb{R}^n$, принимающая значение $+1$ на стандартном базисе, называется *стандартной*.

Лемма 14.3
$\operatorname{Vol}^2(v_1, v_2, \dots, v_n) = \det G_v$.

Доказательство. Зафиксируем ортонормальный базис $e = (e_1, e_2, \dots, e_n)$, и пусть $v = e\, C_{ev}$. Тогда $\operatorname{Vol}^2(v_1, v_2, \dots, v_n) = \det^2 C_{ev} = \det (C_{ev}^t C_{ev}) = \det G_v$. □

14.4. Двойственность. Евклидова структура на вещественном векторном пространстве V задаёт каноническое линейное отображение

$$g : V \xrightarrow{u \mapsto (\,*\,,u\,)} V^* \,, \tag{14-9}$$

переводящее вектор u в линейную форму $g_u : w \mapsto (w, u)$. Это отображение инъективно: для любого $v \neq 0$ функционал $g_v \in V^*$ имеет ненулевое значение

$$g_v(v) = (v, v) > 0$$

и, следовательно, ненулевой. Для конечномерного пространства V отсюда следует, что отображение (14-9) является изоморфизмом, и любую линейную форму на пространстве V можно воспринимать как скалярное произведение с некоторым однозначно определённым вектором.

Упражнение 14.3. Убедитесь, что матрица G_{e^*e} отображения g в произвольном базисе e пространства V и двойственном ему базисе e^* пространства V^* совпадает с матрицей Грама G_e.

14.4.1. Двойственный базис. В частности, для любого базиса

$$e = (e_1, e_2, \dots, e_n)$$

пространства V координатные функционалы $e_1^*, e_2^*, \dots, e_n^* \in V^*$, составляющие двойственный базис в V^*, также представляются скалярными произведениями с некоторыми векторами $e_1^\vee, e_2^\vee, \dots, e_n^\vee \in V$, которые однозначно определяются из соотношений

$$(e_i^\vee, e_j) = \begin{cases} 0, & \text{при } i \neq j\,, \\ 1, & \text{при } i = j\,. \end{cases} \tag{14-10}$$

Базис $e_1^\vee, e_2^\vee, \dots, e_n^\vee$ пространства V называется *евклидово двойственным* к базису $e_1, e_2, \dots, e_n$. Например, евклидово двойственным к ортонормальному базису будет он сам, а евклидово двойственным к ортогональному базису $\{e_i\}$ будет базис из векторов $\{e_i/(e_i, e_i)\}$.

По упр. 14.3, координаты векторов двойственного базиса $e_i^\vee$ в исходном базисе e_i суть столбцы матрицы $G^{-1}_{e_1,e_2,\dots,e_n}$, обратной к матрице Грама $G_{e_1,e_2,\dots,e_n}$ исходного базиса:

$$e^\vee = e\, G_e^{-1}\,. \tag{14-11}$$

Упражнение 14.4. Проверьте это, и покажите, что $e_i^{\vee\vee} = e_i$.

Коэффициенты разложения произвольного вектора $v \in V$ по любому базису $e_1, e_2, \dots, e_n$ суть скалярные произведения с векторами двойственного базиса:

$$v = \sum_i e_i \cdot (v, e_i^\vee) \tag{14-12}$$

(чтобы убедиться в этом, достаточно скалярно умножить обе части на $e_i^\vee$ для каждого i).

14.4.2. Ортогональные дополнения. Для произвольного подпространства $U \subset V$ подпространство

$$U^{\perp} = g^{-1}(\mathrm{Ann}\,(U)) = \{w \in V \mid (u,w) = 0 \;\; \forall\, u \in U\;\}$$

называется *ортогоналом* к U. Из теор. 8.2 вытекает, что на конечномерном векторном пространстве V соответствие $U \rightleftarrows U^{\perp}$ представляет собою оборачивающую включения биекцию между подпространствами дополнительных размерностей, причём

$$U^{\perp\perp} = U\;, \quad (U \cap W)^{\perp} = U^{\perp} + W^{\perp}\;, \quad (U + W)^{\perp} = U^{\perp} \cap W^{\perp}\,.$$

Лемма 14.4 (об ортогональном проектировании)
Пусть $U \subset V$ конечномерное подпространство любого евклидова пространства V (возможно бесконечномерного). Тогда $V = U \oplus U^{\perp}$, и образ $\pi_U(v)$ произвольного вектора $v \in V$ при проекции $\pi_U : V \twoheadrightarrow U$ вдоль $U^{\perp}$ однозначно определяется любым из следующих эквивалентных друг другу свойств:

1) $\pi_U(v) = \sum_{\nu}(v, u^{\vee}) \cdot u_{\nu}$, где $u_1, u_2, \ldots, u_k$ и $u_1^{\vee}, u_2^{\vee}, \ldots, u_k^{\vee}$ любые евклидово двойственные базисы подпространства U

2) $(v,u) = (\pi_U(v), u) \;\; \forall\, u \in U$

3) $v - \pi_U(v) \in U^{\perp}$

4) $|v - \pi_U(v)| < |v - u| \;\; \forall\, u \in U\;,\; u \neq \pi_U(v)$

Доказательство. Пересечение $U \cap U^{\perp} = 0$, поскольку вектор $u \in U \cap U^{\perp}$ имеет $(u,u) = 0$. Чтобы показать, что $U + U^{\perp} = V$, зафиксируем в U произвольный базис $u_1, u_2, \ldots, u_k$ и определим вектор $\pi_U(v) \in U$ формулой (1). Тогда он автоматически обладает свойством (2), поскольку для любого базисного вектора $u_j^{\vee}$ пространства U равенство (2) выполняется:

$$\big(\pi_U(v), u_j^{\vee}\big) = \Big(\sum_{\nu}\,(v, u^{\vee}) \cdot u_{\nu}\,,\; u_j^{\vee}\Big) = (v, u^{\vee})\;,$$

а стало быть, оно выполняется и для всех векторов пространства U. Наоборот, вектор $\pi_U(v)$, обладающий свойством (2), согласно формуле (14-12) выражается через базис u по формуле (1). С другой стороны, свойство (2) эквивалентно свойству (3):

$$(v,u) = (\pi_U(v), u) \;\; \forall\, u \in U \quad \Longleftrightarrow \quad (v - \pi_U(v), u) \;\; \forall\, u \in U$$

Тем самым, любой вектор v представим как $v = \pi_U(v) + (v - \pi_U(v))$, где первое слагаемое лежит в U, а второе в $U^{\perp}$. Таким образом, $V = U \oplus U^{\perp}$, свойства (1), (2), (3) равносильны друг другу и проекция V на U вдоль $U^{\perp}$ переводит v в $\pi_U(v)$.

Остаётся показать, что вектор $w = \pi_U(v)$ это единственный ближайший к v вектор подпространства U. Поскольку $v - w \in U^\perp$, для любого $u \in U$ имеем

$$|v-(w+u)|^2 = \big((v-w)-u\,,\,(v-w)-u\big) = \\ = (v-w, v-w) + (u,u) = |v-w|^2 + |u|^2\,.$$

Таким образом, расстояние между v и $w{+}u$ при $u \neq 0$ строго меньше расстояния между v и w. $\square$

14.4.3. Пример: угол между вектором и подпространством. Неравенство $|v - \pi_U(v)| < |v - u|\ \forall\, u{\in}U$ можно переформулировать в терминах углов. А именно, если вектор $v \notin U^\perp$, то вектор $w = \pi_U(v)$ это единственный с точностью до умножения на положительную константу вектор подпространства U, на котором достигается минимум углов

$$\min_{u\in U} \widehat{vu} = \widehat{vw}\,,\quad \text{где } w = \pi_U(v).$$

В самом деле, наименьшему значению угла $\widehat{vu}$ отвечает наибольшее значение

$$\cos(\widehat{vu}) = \frac{(v,u)}{|v|\cdot|u|}\,,$$

По лем. 14.4 $(v,u) = (w,u)$. В силу неравенства Коши – Буняковского – Шварца (14-4) максимум отношения $(w,u)/|u| = (w, u/|u|)$ достигается, когда вектор единичной длины $u/|u|$ сонаправлен с w.

Угол между вектором $v \notin U^\perp$ и вектором $\pi_U(v) \in U$ называется *углом между вектором v и подпространством U*. Если $v \in U^\perp$, то $(v,u) = 0\ \forall\, u{\in}U$ и v перпендикулярен любому $u \in U$.

14.5. Ортогональные операторы. Линейный оператор $F : V \longrightarrow V$ на евклидовом пространстве V называется *ортогональным* или *изометрией*, если он сохраняет длины всех векторов:

$$\forall\, v{\in}V\ |Fv| = |v|\,.$$

Из равенства (14-8) следует, что вместе с длинами всех векторов ортогональный оператор сохраняет и скалярные произведения:

$$\forall\ v, w \quad (Fv, Fw) = (v, w)\,.$$

Из сохранения скалярных произведений, в свою очередь, следует, что ортогональный оператор сохраняет не только длины векторов, но и углы между ними, и переводит ортонормальные базисы в ортонормальные базисы.

Наоборот, если оператор F переводит какой-нибудь ортонормальный базис в ортонормальный же базис, то он сохраняет скалярные произведения базисных, а значит, и любых векторов и, стало быть, является ортогональным.

14.5.1. Ортогональные матрицы и ортогональная группа. Если оператор F имеет в некотором ортонормальном базисе $e = (e_1, e_2, \ldots, e_n)$ матрицу F_e, т. е. $F(e) = e\,F_e$, то ортонормальность набора $F(e)$ равносильна равенству

$$E = G_{F(e)} = F_e^t G_e F_e = F_e^t E F_e = F_e^t F_e$$

Матрица $C \in \mathrm{Mat}_n(\mathbb{R})$ называется *ортогональной*, если $C^t C = E$ или, что то же самое, если $C^{-1} = C^t$. Таким образом, для ортогональности оператора f необходимо и достаточно, чтобы его матрица в каком-нибудь (а значит, и в любом) ортонормальном базисе была ортогональна.

Отметим, что из ортогональности оператора (соотв. матрицы) вытекает, что определитель этого оператора (соотв. матрицы) равен ± 1. Ортогональные операторы определителя $+1$ называются *собственными*. Они переводят ортонормальный базис в базис той же ориентации. Ортогональные операторы определителя -1 называются *несобственными*. Применение такого оператора меняет ориентацию базиса на противоположную.

Ортогональные операторы на евклидовом пространстве V образуют в полной линейной группе $\mathrm{GL}(V)$ подгруппу, которая называется *ортогональной группой* и обозначается $O(V) \subset \mathrm{GL}(V)$. Пересечение $\mathrm{SO}(V) = O(V) \cap \mathrm{SL}(V)$ называется *специальной* (или *собственной*) ортогональной группой. Соответствующие группы матриц (т. е. ортогональных преобразований координатного евклидова пространства $\mathbb{R}^n$) обозначаются $O_n(\mathbb{R})$ и $\mathrm{SO}_n(\mathbb{R})$.

Теорема 14.1
Конечномерное евклидово пространство V, на котором действует ортогональный оператор F, является прямой суммой ортогональных друг другу одномерных и двумерных инвариантных подпространств оператора F. Собственные значения F на одномерных инвариантных подпространствах равны ± 1. На двумерных неразложимых инвариантных подпространствах оператор F действует поворотом, т. е. задаётся в подходящем ортонормальном базисе матрицей

$$\begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix}, \quad \varphi \in \mathbb{R}$$

Доказательство. Первое утверждение доказывается индукцией по $\dim V$. Если $\dim V = 1$, то $Fv = \lambda v$ и из равенства $(FV, Fv) = (v, v)$ вытекает, что $\lambda = \pm 1$. Это заодно доказывает и утверждение про собственные числа.

Пусть $\dim V > 1$. По сл. 13.7 F обладает одномерным или двумерным инвариантным подпространством. Пусть U — такое подпространство. По лем. 14.4 $V = U \oplus U^\perp$. Покажем, что $U^\perp$ тоже инвариантно.

Поскольку $\ker(F) = 0$, ограничение F на инвариантное подпространство U биективно. В частности, $F^{-1}u \in U \ \ \forall\, u \in U$. Поэтому $\forall\, u \in U$ и $\forall\, w \in U^\perp$ получаем $(Fw, u) = (Fw, FF^{-1}u) = (w, F^{-1}u) = 0$, т. е. $Fw \in U^\perp \ \forall\, w \in U^\perp$.

По индукции, пространство $U^\perp$, а с ним и V, является прямой суммой попарно ортогональных одномерных и двумерных инвариантных подпространств.

Остаётся описать действие F на двумерном инвариантном подпространстве. Выберем в нём ортонормальный базис e_1, e_2 и запишем F матрицей

$$F = \begin{pmatrix} a & b \\ c & d \end{pmatrix} .$$

Условие ортогональности $F^tF = E$ равносильно системе уравнений

$$\begin{cases} a^2 + c^2 = 1 \\ b^2 + d^2 = 1 \\ ab + cd = 0 \end{cases}$$

Решения первых двух уравнений суть

$$\begin{aligned} a &= \cos\varphi \qquad & c &= \sin\varphi \\ b &= \sin\psi \qquad & d &= \cos\psi \end{aligned}$$

Третье уравнение накладывает на углы φ и ψ соотношение $\sin(\psi + \varphi) = 0$, откуда, с точностью до целого числа оборотов, $\psi = \varphi$ или $\psi = \pi - \varphi$. В первом случае оператор задаётся матрицей

$$\begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix}$$

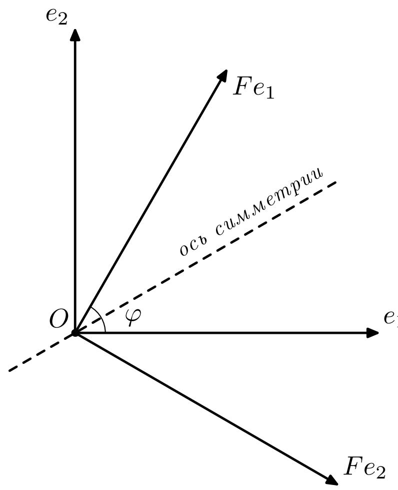


Рис. 14◇2. Композиция поворота с отражением является отражением.

и является поворотом на угол φ. Во втором случае оператор задаётся матрицей

$$\begin{pmatrix} \cos\varphi & \sin\varphi \\ \sin\varphi & -\cos\varphi \end{pmatrix}$$

и является отражением относительно биссектрисы угла между e_1 и $f(e_1)$ (см. рис. 14◇2). В этом случае рассматриваемая плоскость является ортогональной суммой двух одномерных собственных подпространств с собственными значениями ± 1. □

14.5.2. Пример: изометрии трёхмерного пространства. Ортогональный оператор на трёхмерном евклидовом пространстве по теор. 14.1 в подходящем базисе задаётся матрицей вида $\begin{pmatrix} \cos\varphi & -\sin\varphi & 0 \\ \sin\varphi & \cos\varphi & 0 \\ 0 & 0 & \pm 1 \end{pmatrix}$. Все разложения пространства в сумму трёх одномерных собственных подпространств с собственными значениями ± 1 также охватываются этой формулой и отвечают поворотам на углы $\varphi = 0$ и $\varphi = \pi$. Значению $+1$ в правом нижнем углу отвечает поворот на угол φ вокруг оси e_3 (это собственное движение), а значению -1 —

композиция такого поворота с отражением в плоскости, натянутой на e_1, e_2 (это несобственное движение).

Таким образом, всякий изометрический оператор в трёхмерном евклидовом пространстве является поворотом вокруг некоторой оси (если он собственный) или композицией такого поворота с отражением в плоскости, перпендикулярной оси поворота (если он несобственный). Этот результат известен как *теорема Эйлера*.

14.6. Аффинные пространства. Зафиксируем векторное пространство V над произвольным полем $\Bbbk$. Множество A называется *аффинным*[1] *пространством* над V, если с каждому $v \in V$ сопоставлено преобразование *сдвига* (или *параллельный перенос*) $\tau_v : A \longrightarrow A$, так что

$$\tau_0 = \mathrm{Id}_A\,, \quad \tau_u \circ \tau_w = \tau_{u+w} \quad \forall\, v, w \in V \tag{14-13}$$

$$\forall\, p, q \in A\ \exists \text{ единственный } v \in V : \tau_v(p) = q \tag{14-14}$$

Размерностью аффинного пространства A называется размерность векторного пространства V.

Условия (14-13) означают, что параллельные переносы образуют абелеву группу преобразований пространства A, и обратным к сдвигу τ_v на вектор v является сдвиг τ_{-v} на противоположный вектор $-v$.

Иначе параллельный перенос τ_v можно воспринимать как операцию «откладывания» вектора $v \in V$ от точек $p \in A$, и мы часто будем писать $p + v$ вместо $\tau_v(p)$. Единственный в силу свойства (14-14) вектор v, такой что $q = p + v$, обозначается через $\overrightarrow{pq}$. Продуктивно представлять его себе как стрелку с началом в точке $p \in A$ и концом в точке $q \in A$. Свойства (14-13) означают, что

$$\overrightarrow{pp} = 0 \quad \text{и} \quad \overrightarrow{pq} + \overrightarrow{qr} = \overrightarrow{pr} \quad \forall\, p, q, r \in A\,.$$

Упражнение 14.5. Убедитесь, что $\overrightarrow{pq} = -\overrightarrow{qp}$ и что $\overrightarrow{pq} = \overrightarrow{rs} \iff \overrightarrow{ps} = \overrightarrow{qr}$.

14.6.1. Аффинизация и векторизация. Из всякого векторного пространства V можно изготовить аффинное пространство $\mathbb{A}(V)$ над V, точками которого являются векторы $v \in V$, а параллельный перенос $\tau_w : V \longrightarrow V$ переводит v в $v + w$. Пространство $\mathbb{A}(V)$ называется *аффинизацией* векторного пространства V. Точки p пространства $\mathbb{A}(V)$ продуктивно представлять себе как «концы» радиус векторов $\overrightarrow{0p} = p - 0$, выпущенных из начальной точки 0 (нулевого вектора).

Наоборот, если зафиксировать какую-нибудь точку p в произвольном аффинном пространстве A над V, то сопоставление каждой точке $q \in A$ её *радиус-вектора* $\overrightarrow{pq} \in V$ устанавливает, согласно (14-14), биекцию между точками из A и векторами из V. Эта биекция называется *векторизацией* аффинного пространства A с *началом* (или с *центром*) в точке $p \in A$. Набор $p, e_1, e_2, \dots, e_n$, где $e_1, e_2, \dots, e_n$ — какой-нибудь базис в V, называется *аффинной системой координат* (или *репером*) в пространстве V.

[1] это слово является бесхитростной калькой с английского *affine* (ассоциированный)

14.6.2. Барицентрические комбинации. Векторизация аффинного пространства зависит от выбора начальной точки p. Если мы попытаемся при помощи векторизации с началом в p перенести с V на A операции сложения векторов и умножения векторов на числа, полагая

$$\lambda_1 q_1 + \lambda_2 q_2 + \dots + \lambda_m q_m \overset{\text{def}}{=} p + \lambda_1 \overrightarrow{pq}_1 + \lambda_2 \overrightarrow{pq}_2 + \dots + \lambda_m \overrightarrow{pq}_m \,, \tag{14-15}$$

то, взяв векторизации с центрами в p_1 и в p_2, мы получим точки

$$c_1 = p_1 + \lambda_1 \overrightarrow{p_1 q}_1 + \lambda_2 \overrightarrow{p_1 q}_2 + \dots + \lambda_m \overrightarrow{p_1 q}_m$$
$$c_2 = p_2 + \lambda_1 \overrightarrow{p_2 q}_1 + \lambda_2 \overrightarrow{p_2 q}_2 + \dots + \lambda_m \overrightarrow{p_2 q}_m$$

различающиеся на вектор $\overrightarrow{c_1 c}_2 = (1 - \sum\limits_i \lambda_i) \cdot \overrightarrow{p_1 p}_2$.

Таким образом, линейная комбинация точек (14-15) тогда и только тогда не зависит от выбора начальной точки p, когда сумма её коэффициентов равна единице. Такие комбинации называются *барицентрическими*.

Название связано с тем, что точка $c = \sum \lambda_i q_i$ это центр тяжести точек $q_1, q_2, \dots, q_m$ в том смысле, что

$$\overrightarrow{cq}_1 + \overrightarrow{cq}_2 + \dots + \overrightarrow{cq}_m = 0 \,.$$

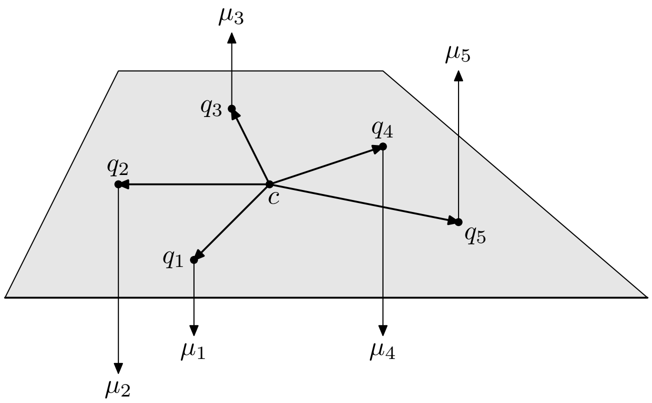


Рис. 14◇3. Моменты сил.

В механике вектор $\overrightarrow{cq_i}$ называется *моментом* относительно точки c силы тяжести, действующей на груз единичного веса, помещённый в точку q_i горизонтально лежащего пространства A. Равенство суммы моментов нулю означает, что шарнирно закреплённое в единственной точке c пространство A будет находиться в равновесии (не будет крутиться) под действием приложенных сил.

Более общим образом, для любого набора точек $q_1, q_2, \dots, q_m$ и любого набора весов $\mu_1, \mu_2, \dots, \mu_m \in \Bbbk$ с ненулевой суммой $\sum \mu_i \neq 0$ существует единственная точка c такая, что

$$\mu_1 \overrightarrow{cp}_1 + \mu_2 \overrightarrow{cp}_2 + \dots + \mu_m \overrightarrow{cp}_m = 0 \,. \tag{14-16}$$

Эта точка называется *центром тяжести* точек p_i с весами μ_i (см. рис. 14◇3) и равна барицентрической комбинации

$$c = \sum_{i=1}^{m} \frac{\mu_i q_i}{\mu_1 + \mu_1 + \dots + \mu_m} \,. \tag{14-17}$$

В самом деле, точка c, определённая равенством (14-17) очевидно удовлетворяет условию равновесия (14-16), и если ещё для какой-нибудь точки c_1 выполнено условие $\mu_1\overrightarrow{c_1p}_1+\mu_2\overrightarrow{c_1p}_2+\cdots+\mu_m\overrightarrow{c_1p}_m=0$, то, почленно вычитая из него (14-16), получим $\left(\sum\mu_i\right)\cdot\overrightarrow{cc}_1=0$.

Упражнение 14.6 (теорема о группировании масс). Пусть точки p_i имеют веса λ_i с ненулевой суммой $\lambda=\sum\lambda_i$ и центром тяжести в точке p, а точки q_j имеют веса μ_j с ненулевой суммой $\mu=\sum\mu_j$ и центром тяжести в точке q. Покажите, что при $\lambda+\mu\neq0$ центр тяжести объединения этих двух наборов точек[1] равен центру тяжести точек p и q, взятых с весами λ и μ.

Отметим, что их этого упражнения следует, что барицентрическая комбинация барицентрических комбинаций является барицентрической комбинацией исходных точек.

14.6.3. Пример: выпуклые фигуры в $\mathbb{R}^n$. Пусть основное поле $\Bbbk=\mathbb{R}$. Барицентрическая комбинация $\sum\lambda_i\cdot p_i$ точек вещественного аффинного пространства называется *выпуклой*, если все $\lambda_i\geqslant0$. Совокупность всех выпуклых барицентрических комбинаций всевозможных конечных наборов точек фигуры Φ называется *выпуклой оболочкой* этой фигуры и обозначается $\operatorname{conv}(\Phi)$. Фигура, совпадающая со своей выпуклой оболочкой, называется *выпуклой*.

Согласно упр. 14.6, отыскание барицентричекой комбинации произвольного конечного набора точек сводится к отысканию барицентричеких комбинаций пар точек. Таким образом, для выпуклости фигуры Φ необходимо и достаточно, чтобы вместе с любыми двумя точками $p,q\in\Phi$ в Φ содержался и соединяющий их *отрезок*

$$[pq]\overset{\text{def}}{=}\operatorname{conv}\{p,q\}=\{\lambda p+\mu q\mid\lambda+\mu=1\,,\ \lambda,\mu>0\}\,.$$

Упражнение 14.7. Убедитесь, что пересечение выпуклых фигур выпукло, и что $\operatorname{conv}(\Phi)$ совпадает с пересечением всех выпуклых множеств, содержащих Φ.

14.6.4. Аффинные отображения. Отображение $F:A_1\longrightarrow A_2$ аффинных пространств над векторными пространствами V_1 и V_2 называется *аффинным*, если существуют точка $p\in A_1$, такая что индуцированное F отображение D_pF из векторизации A_1 с началом p в векторизацию A_2 с началом в $F(p)$

$$V_1\xrightarrow{D_pF}V_2\ :\ D_pF\,(\overrightarrow{pq})=\overrightarrow{F(p)F(q)} \tag{14-18}$$

является линейным. В этом случае линейный оператор (14-18) называется *дифференциалом* аффинного отображения F. На самом деле, если отображение (14-18) линейно для какой-то точки $p\in A_1$, то аналогичное отображение

$$D_r:\overrightarrow{rq}\longmapsto\overrightarrow{F(p_1)F(q_1)}$$

[1] допускается, чтобы наборы точек пересекались — в этом случае «объединение» одинаковых точек означает сложение их весов

построенное по любой точке $r \in A_1$ тоже линейно и совпадает с D_p, так как для любого вектора $v = \overrightarrow{rq} = \overrightarrow{pq} - \overrightarrow{pr} \in V_1$

$$D_r F(v) = \overrightarrow{F(r)F(q)} = \overrightarrow{F(p)F(q)} - \overrightarrow{F(p)F(r)} = \\ = D_p F(\overrightarrow{pq}) - D_p F(\overrightarrow{pr}) = D_p F(\overrightarrow{pq} - \overrightarrow{pr}) = F_p(v)\,.$$

Поэтому мы будем писать просто DF вместо $D_p F$. Аффинное отображение

$$F : A_1 \longrightarrow A_2$$

однозначно восстанавливается по своему дифференциалу

$$DF : V_1 \longrightarrow V_2$$

как только известен образ $F(p)$ какой-нибудь одной точки $p \in A_1$. Тогда

$$F(q) = F(p) + DF(\overrightarrow{pq})\,.$$

В частности, два отображения F и G с одинаковым дифференциалом $DF = DG$ различаются на параллельный перенос: вектор $v_{FG} = \overrightarrow{F(p)G(p)}$ не зависит от выбора точки $p \in A_1$ и

$$G = \tau_{v_{FG}} \circ F\,. \tag{14-19}$$

В случае, когда основное поле $\Bbbk$ это $\mathbb{R}$ или $\mathbb{C}$, использованное выше понятие дифференциала согласуется с тем, что принято в курсе анализа. Напомним, что в анализе *дифференциалом* (произвольного) отображения

$$F : A_1 \longrightarrow A_2$$

в точке $p \in A_1$ называют линейный оператор $D_p F : V_1 \longrightarrow V_2$, такой что

$$F(q) = F(p) + D_p F(\overrightarrow{pq}) + o(|\overrightarrow{pq}|)\,,$$

где через $|\overrightarrow{pq}|$ обозначена длина[1] вектора $\overrightarrow{pq}$. Отображения F, для которых такой оператор существует, называются *дифференцируемыми* в точке p. Таким образом, аффинные отображения над полями $\mathbb{R}$ и $\mathbb{C}$ всюду дифференцируемы и имеют постоянный (не зависящий от точки p) дифференциал.

14.7. Метрики, нормы и топология. В этом разделе мы для удобства читателя напоминаем вкратце некоторые стандартные факты из курса анализа, которые понадобятся нам в дальнейшем.

[1]как определить длину вектора в комплексном векторном пространстве мы обсудим в §20

14.7.1. Метрики и нормы. Напомним, что *метрикой* на множестве X называется функция $\varrho : X \times X \longrightarrow \mathbb{R}$, обладающая $\forall\, x, y, z \in X$ свойствами

$$\begin{aligned}
&\varrho(x,y) = \varrho(y,x) && \text{(симметричность)}\\
&\varrho(x,y) \geqslant 0 && \text{(положительность)}\\
&\varrho(x,y) = 0 \Rightarrow x = y && \text{(невырожденность)}\\
&\varrho(x,z) \leqslant \varrho(x,y) + \varrho(y,z) && \text{(неравенство треугольника)}
\end{aligned}$$

Если X это аффинное пространство над $\mathbb{R}^n$, то естественно ограничиться такими метриками, которые инвариантны относительно параллельных переносов и однородны по отношению к умножению векторов на числа. Первое требование означает, что $\varrho(x,y) = \varrho(\overrightarrow{xy})$ зависит только от *вектора* $\overrightarrow{xy} \in \mathbb{R}^n$, а не от самих точек x и y. Второе, по определению, означает, что $\varrho(\lambda v) = |\lambda| \varrho(v)$ для любого вектора $v \in \mathbb{R}^n$.

Функция $||\ast|| : V \xrightarrow{v \mapsto ||v||} \mathbb{R}$ на вещественном векторном пространстве V называется *нормой*, если $\forall\, \lambda \in \mathbb{R}$ и $\forall\, v, w \in V$ она обладает свойствами

$$\begin{aligned}
&||v|| \geqslant 0 && \text{(положительность)}\\
&||v|| = 0 \Rightarrow v = 0 && \text{(невырожденность)}\\
&||\lambda \cdot v|| = |\lambda| \cdot ||v|| && \text{(однородность)}\\
&||v + w|| \leqslant ||v|| + ||w|| && \text{(неравенство треугольника)}
\end{aligned}$$

Таким образом, всякая однородная инвариантная относительно сдвигов метрика в аффинном пространстве над вещественным векторным пространством V индуцирована некоторой нормой на V: $\varrho(x,y) = ||\overrightarrow{xy}||$.

Упражнение 14.8. Проверьте, что выполнение $\forall\, v, w \in V$ неравенства треугольника равносильно выполнению $\forall\, v, w \in V$ неравенства $||w - v|| \geqslant \big|\, ||w|| - ||v||\, \big|$.

14.7.2. Метрическая топология. В метрическом пространстве X фигура $B_\varepsilon(p) = \{q \in X \mid \varrho(p,q) \leqslant \varepsilon\}$ называется ε-шаром[1] с центром в точке $p \in X$. Подмножества $U \subset X$, которые вместе с каждой своей точкой содержат и некоторый ε-шар с центром в этой точке, называются *открытыми*, и задают на X топологию, называемую *метрической топологией*.

Упражнение 14.9. Убедитесь, что пересечение двух и объединение любого множества открытых множеств тоже открыты.

Дополнения $Z = \mathbb{R}^n \smallsetminus U$ до открытых множеств называются *замкнутыми множествами*. Точка p называется *внутренней точкой* фигуры $\Phi \subset \mathbb{R}^n$, если фигура Φ содержит некоторый ε-куб с центром в этой точке. Множество внутренних точек фигуры Φ обозначается через $\mathring{\Phi}$. Пересечение всех замкнутых множеств, содержащих Φ, называется *замыканием* фигуры Φ и обозначается $\overline{\Phi}$. Точки дополнения $\mathbb{R}^n \smallsetminus \overline{\Phi}$ называются *внешними точками* фигуры Φ, а точки,

[1] под ε мы всегда понимаем положительное вещественное число

не являющиеся ни внешними, ни внутренними, называются *граничными* или *собственными граничными*, смотря по тому, принадлежат ли они фигуре Φ. Множество всех граничных точек Φ мы обозначим через $\partial\Phi$.

Упражнение 14.10. Убедитесь, что $p \in \partial\Phi$ тогда и только тогда, когда любой ε-шар $B_\varepsilon(p)$ содержит как точки из Φ, так и точки, не принадлежащие Φ, и что $p \notin \Phi$ является внешней , если и только если $\Phi \cap B_\varepsilon(p) = \varnothing$ для некоторого $\varepsilon > 0$.

14.7.3. Пример: стандартная топология на $\mathbb{R}^n$ это метрическая топология, индуцированной нормой $||(x_1, x_2, \ldots, x_n)||_{\text{st}} \stackrel{\text{def}}{=} \max_i |x_i|$ (максимум модуля координат). Мы будем называть эту норму *стандартной*. В этой норме ε-шары — это *ε-кубы*

$$B_\varepsilon = \{(x_1, x_2, \ldots, x_n) \mid |x_i - p_i| \leq \varepsilon \;\forall\, i\}$$

и сходимость означает покоординатную сходимость. Подмножество $U \subset \mathbb{R}^n$ открыто в стандартной топологии, если вместе с каждой точкой $p \in U$ в U лежит и некоторый ε-куб с центром в этой точке.

Упражнение 14.11. Докажите, что внутренность и замыкание любого выпуклого множества тоже выпуклы.

14.7.4. Топологическая эквивалентность норм. Говоря формально, определение стандартной топологии в $\mathbb{R}^n$ привязано к конкретной системе координат. В этом разделе мы покажем, что это не так, и покоординатная сходимость в действительности не зависит от выбора координатной системы. Более того, мы покажем, что *все* нормы на $\mathbb{R}^n$ задают одну и ту же топологию.

Лемма 14.5
Любая норма на $\mathbb{R}^n$ непрерывна в стандартной топологии.

Доказательство. Обозначим через $e_i \in \mathbb{R}^n$ стандартные базисные векторы и положим $M = \max\limits_i ||e_i||$. Тогда для любого $v \in \mathbb{R}^n$

$$||v|| = \left\|\sum x_i e_i\right\| \leqslant \sum |x_i| \cdot ||e_i|| \leqslant nM \max_i |x_i| = nM \cdot ||v||_{\text{st}}$$

и для каждого $\varepsilon > 0$ при $||v - w||_{\text{st}} < \delta = \varepsilon/2nM$ выполняется неравенство $\big|\, ||v|| - ||w|| \,\big| \leqslant ||v - w|| < nM \cdot ||v - w||_{\text{st}} < \varepsilon\,.$ □

Лемма 14.6
Для любой нормы $||\ast||$ на $\mathbb{R}^n$ можно подобрать вещественные положительные константы μ и M так, чтобы для всех $v \in \mathbb{R}^n$ выполнялись неравенства

$$\mu \cdot ||v||_{\text{st}} \leqslant ||v|| \leqslant M \cdot ||v||_{\text{st}}\,. \tag{14-20}$$

Доказательство. Граница K стандартного 1-куба с центром в нуле

$$K = \{v \in \mathbb{R}^n \mid ||v||_{\text{st}} = 1\}$$

компактна, и непрерывная функция $||*||$ достигает на ней своих максимального и минимального значений $M = \sup(||v|| \mid v \in K)$ и $\mu = \inf(||v|| \mid v \in K)$, причём $\mu > 0$, т. к. иначе существовала бы сходящаяся в K последовательность $v_i \in K$ с $||v_i|| \to 0$, что в силу непрерывности и невырожденности нормы $|| * ||$ означало бы $\lim v_i = 0 \in K$, что не так. Следовательно, $0 < \mu \leqslant ||w|| \leqslant M < \infty$ для всех $w \in K$. Полагая $w = v/||v||_{\mathrm{st}} \in K$ получаем для любого $v \neq 0$ требуемое неравенство (14-20). □

Следствие 14.1
Любая норма индуцируют на $\mathbb{R}^n$ стандартную топологию (сходимость в которой означает покоординатную сходимость).

14.7.5. Геометрическое описание норм. Для любой нормы $|| * ||$ на векторном пространстве $\mathbb{R}^n$ её единичный шар с центром в нуле

$$B_1(0) = \{v \in V \mid ||v|| \leqslant 1\} \tag{14-21}$$

ограничен, замкнут[1], центрально симметричен относительно нуля, содержит нуль в качестве внутренней точки, и выпукл, поскольку

$$||\lambda v + \mu w|| \leqslant \lambda||v|| + \mu||w|| \leqslant 1$$

$\forall\ v, w$ с $||v||, ||w|| \leqslant 1$ и $\forall\ \lambda, \mu > 0$ с $\lambda + \mu = 1$. Норма $|| * ||$ однозначно восстанавливается по единичному шару (14-21) как

$$||v|| = \inf(\lambda \in \mathbb{R}_{>0} \mid v \in \lambda B_1(0)) \,. \tag{14-22}$$

Предложение 14.1
Формулы (14-21) и (14-22) устанавливают биекцию между центрально симметричными относительно нуля ограниченными замкнутыми выпуклыми фигурами в $\mathbb{R}^n$, имеющими нуль внутренней точкой, и нормами на векторном пространстве $\mathbb{R}^n$.

Доказательство. С учётом сказанного выше, нам остаётся только проверить, что функция $v \mapsto ||v||_\Phi = \inf(\lambda \in \mathbb{R}_{>0} \mid v \in \lambda\Phi)$, построенная по произвольной фигуре Φ, удовлетворяющей условию теоремы, является нормой на $\mathbb{R}^n$. Невырожденность и однородность этой функции достаточно проверить при $n = 1$, где они очевидны. Неравенство треугольника следует из выпуклости: $\forall\ v, w \in V$ точка

$$q = \frac{v + w}{||v||_\Phi + ||w||_\Phi} = \frac{||v||_\Phi}{||v||_\Phi + ||w||_\Phi} \cdot \frac{v}{||v||_\Phi} + \frac{||w||_\Phi}{||v||_\Phi + ||w||_\Phi} \cdot \frac{w}{||w||_\Phi}$$

является выпуклой барицентрической комбинацией лежащих в Φ точек $v/||v||_\Phi$ и $w/||w||_\Phi$. Поэтому $q \in \Phi$, и значит $||v + w||_\Phi \leqslant ||v||_\Phi + ||w||_\Phi$. □

[1] замкнутость вытекает из непрерывности нормы

14.7.6. Евклидовы нормы. Как мы видели в n° 14.3 евклидова длина вектора $|v| = \sqrt{(v,v)}$, определённая при помощи евклидова скалярного произведения на векторном пространстве V, является нормой на V. Такие нормы называются *евклидовыми*. Для любой евклидовой нормы на V выполняется *тождество параллелограмма*[1]:

$$|v+w|^2 + |v-w|^2 = 2\left(|v|^2 + |w|^2\right) . \tag{14-23}$$

Отметим, что стандартная норма на $\mathbb{R}^2$ *не является* евклидовой, так как в ней и стороны, и диагонали квадрата, натянутого на стандартные базисные орты, имеют норму 1.

Предложение 14.2
Норма на векторном пространстве $\mathbb{R}^n$ евклидова тогда и только тогда, когда когда для неё выполняется тождество параллелограмма (14-23).

Доказательство. Необходимость очевидна. Наоборот, для любой нормы мы можем положить $(v,w) = (||v+w|| - ||v-w||)/4$. Это симметричная невырожденная положительная вещественная функция на $V \times V$.

Упражнение 14.12. Покажите, что если $||*||$ удовлетворяет тождеству параллелограмма, то $(v_1+v_2,w) = (v_1,w) + (v_2,w)$ и $(v,w_1+w_2) = (v,w_1) + (v,w_2)$.

Из аддитивности этой функции по каждому аргументу вытекает её билинейность по отношению к линейным комбинациям с целыми, а стало быть, и с рациональными коэффициентами. Билинейность по отношению к любым вещественным линейным комбинациям получается отсюда в силу непрерывности нормы. □

Задачи для самостоятельного решения к §14

Задача 14.1. Найдите ортогональный базис в подпространстве
а) заданном уравнением $x_1 + x_2 + \cdots + x_n = 0$ в $\mathbb{R}^n$
б) порождённом векторами $(1,2,2-1)$, $(1,1,-5,3)$, $(3,2,8,-7)$ в $\mathbb{R}^4$
в) в ортогональном дополнении к предыдущему подпространству.

Задача 14.2. Напишите систему уравнений, задающую ортогональное дополнение к подпространству, заданному в $\mathbb{R}^4$ уравнениями:

$$\begin{cases} 2x_1 + x_2 + 3x_3 - x_4 = 0 \\ \quad 3x_1 + 2x_2 - 2x_4 = 0 \\ 3x_1 + x_2 + 9x_3 - x_4 = 0 \,. \end{cases}$$

[1] сумма квадратов диагоналей равна сумме квадратов четырёх сторон

Задача 14.3 (аффинные гиперплоскости). Аффинная гиперплоскость в евклидовом векторном пространстве V это фигура

$$\Pi_{a,c} = \{x \in V \,|(a,x) = c\}$$

Покажите, что а) если $\Pi_{a,c} \cap \Pi_{b,d} = \varnothing$, то a и b пропорциональны б) если a и b пропорциональны, то гиперплоскости либо не пересекаются, либо совпадают, и напишите формулу, выражающую минимальное минимальное расстояние между точками $\Pi_{a,c}$ и $\Pi_{b,d}$ через $a, b \in V$ и $c, d \in \mathbb{R}$.

Задача 14.4 (аффинные подпространства). Покажите, что пересечение набора аффинных гиперплоскостей Π_{a_ν,c_ν} либо пусто, либо является параллельным переносом ортогонального дополнения $U^\perp$ к линейной оболочке U векторов a_ν (в последнем случае пересечение $\Pi = \bigcap\limits_\nu \Pi_{a_\nu,c_\nu}$ называется *аффинным подпространством* размерности $\dim U^\perp$, а $U^\perp$ называется *направляющим пространством* этого аффинного подпространства).

Задача 14.5. Пусть точки $p_0, p_1, \ldots, p_k \in \mathbb{R}^n$ не лежат в $(k-1)$-мерной аффинной плоскости. Найдите ГМТ равноудаленных от всех p_i.

Задача 14.6 (сферы). Фигура $S^{n-1}_{c,r} = \{x \in \mathbb{R}^n \mid |\overrightarrow{cx}| = r\}$ называется $(n-1)$-мерной сферой радиуса r с центром в точке $c \in \mathbb{R}^n$. Докажите, что через любые $n+1$ не лежащих в гиперплоскости точек в $\mathbb{R}^n$ проходит единственная $(n-1)$-мерная сфера.

Задача 14.7 (куб). Стандартным n-мерным кубом называется множество точек

$$I^n = \{(x_1, x_2, \ldots, x_n) \in \mathbb{R}^n \mid |x_i| \leqslant 1\,,\ i = 1, \ldots, n\}\,.$$

а) Нарисуйте какую-нибудь двумерную проекцию стандартного 4-мерного куба, в которой все его вершины видны как различные точки.
б) Нарисуйте какую-нибудь «развертку» 3-мерной «поверхности» 4-мерного куба с указаниями, как ее склеивать в 4-мерном пространстве.
в) Дайте определение k-мерной грани I^n и подсчитайте у I^n количество граней каждой размерности $0 \leqslant k \leqslant (n-1)$.
г) Внутренней диагональю I^n называется отрезок, соединяющий центрально симметричные вершины. Сколько всего внутренних диагоналей у I^n?
д) Сколько внутренних диагоналей в I^n, ортогонально заданной внутренней диагонали?
е) Найдите длину диагонали I^n и ее предел при $n \to \infty$
ж) В каком отношении делят внутреннюю диагональ ортогональные проекции на неё всех вершин I^n?
з) Сколько у I^n осей и $(n-1)$-мерных плоскостей симметрии?
и) Найдите радиус описанного около I^n шара и его предел при $n \to \infty$
к) Найдите углы между внутренней диагональю I^n и его рёбрами, а также их пределы при $n \to \infty$
л) Найдите в I^n углы между внутренней диагональю и всевозможными m-мерными гранями.

Задача 14.8. Опишите и нарисуйте семейство 3-мерных многогранников, получающихся в сечении стандартного 4-мерного куба в $\mathbb{R}^4$ семейством гиперплоскостей $x_1 + x_2 + x_3 + x_4 = t$, где $-4 \leqslant t \leqslant 4$.

Задача 14.9 (симплекс). Стандартным n-мерным симплексом Δ^n называется выпуклая оболочка концов стандартных базисных векторов пространства $\mathbb{R}^{n+1}$

$$\Delta^n = \{(x_0, x_1, \ldots, x_n) \in \mathbb{R}^{n+1} \mid \sum x_\nu = 1 \,\&\, x_\nu \geqslant 0 \;\forall \nu\}.$$

а) Нарисуйте 1-мерный и 2-мерный симплексы и какие-нибудь двумерные проекции 3-х 4-мерного симплексов, на которых все их вершины видны как различные точки.

б) Нарисуйте «развертку» 3-мерной «поверхности» 4-мерного симплекса с указанием, как её склеивать.

в) Дайте определение k-мерной грани Δ^n и подсчитайте у Δ^n количество граней каждой размерности $0 \leqslant k \leqslant (n-1)$.

г) Докажите, что в Δ^n можно вписать единственный шар, найдите радиус этого шара, и его предел при $n \to \infty$.

д) Докажите, что около Δ^n можно описать единственный шар, найдите радиус этого шара, и его предел при $n \to \infty$.

е) Найдите длину высоты и её предел при $n \to \infty$.

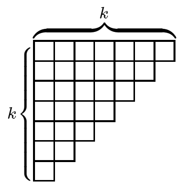
ж) Найдите в Δ^n угол между ребром и не содержащей его гипергранью.

з) Для каждого $1 \leqslant m \leqslant (n-1)$ найдите кратчайшее расстояние между противолежащими m и $(n-m-1)$-мерными гранями.

Задача 14.10. В правильном четырёхмерном симплексе $ABCDE$ обозначим через X середину отрезка, соединяющего центры граней ABC и CDE. Проходящая через точку X прямая YZ пересекает прямую AE в точке Y, а плоскость BCD — в точке Z. Найдите $\overrightarrow{XY} : \overrightarrow{YZ}$.

Задача 14.11 (объём симплекса). 0-мерная ступенчатая пирамида — это точка. 1-мерная ступенчатая пирамида высоты k — это $\Pi_k^1 = \underbrace{\square\square\square\cdots\square\square\square}_{k}$. 2-мерная ступенчатая пирамида высоты k — это

$$\Pi_k^2 = \Pi_1^1 + \Pi_2^1 + \cdots + \Pi_k^1 =$$



Аналогично, n-мерная ступенчатая пирамида высоты k получается из k $(n-1)$-мерных ступенчатых пирамид убывающей высоты, поставленных в стопку вдоль n-той координатной оси: $\Pi_k^n = \Pi_1^{n-1} + \Pi_2^{n-1} + \cdots + \Pi_k^{n-1}$. Сколько кубиков уйдёт на её постройку и как относится объем параллелепипеда к объему симплекса, натянутого на вершину и все соседние с ней вершины?

Задача 14.12. Выразите объем k-мерного симплекса через $(k-1)$-мерный объем его грани и длину опущенной на неё высоты.

Задача 14.13. Какое максимальное число векторов можно выпустить из начала координат евклидова пространства $\mathbb{R}^n$ так, чтобы все углы между ними были тупыми?

Задача 14.14. Опишите и нарисуйте семейство 3-мерных многогранников, получающихся в сечении стандартного 4-мерного симплекса $\Delta^4 \subset \mathbb{R}^5$ семействами плоскостей: а) $x_1 = \text{const}$ б) $x_1 + x_2 = \text{const}$.

Задача 14.15 (кокуб). Выпуклая оболочка концов стандартных базисных векторов и противоположных к ним векторов в $\mathbb{R}^n$ называется стандартным *кокубом* C^n (он подобен выпуклой оболочке центров граней стандартного куба).

а) Задайте кокуб системой линейных неравенств.

б) Нарисуйте какую-нибудь двумерную проекцию стандартного 4-мерного кокуба, в которой все его вершины видны как различные точки.

в) Нарисуйте какую-нибудь «развертку» 3-мерной «поверхности» 4-мерного кокуба с указаниями, как ее склеивать в 4-мерном пространстве.

г) Найдите количество граней каждой размерности.

д) Найдите радиусы вписанного и описанного шаров и их пределы при $n \to \infty$.

Задача 14.16 (октаплекс). Нарисуем в $\mathbb{R}^4$ стандартный куб I^4 и кокуб $\widetilde{C}^4$, который получается из кокуба с вершинами в центрах граней I^4 гомотетией с центром в нуле с таким коэффициентом, чтобы вершины кокуба $\widetilde{C}^4$ попали на описанную вокруг I^4 сферу. Выпуклая оболочка объединения вершин куба I^4 и кокуба $\widetilde{C}^4$ называется *октаплексом* O^4.

а) Покажите, что это правильный многогранник в том смысле, что группа ортогональных преобразований $\mathbb{R}^4$, переводящих O^4 в себя, транзитивно действует[1] на множестве *флагов*: «вершина, примыкающее к ней ребро, примыкающая к нему 2-мерная грань, примыкающая к ней 3-мерная гипергрань».

б) Подсчитайте количество граней каждой размерности.

в) Найдите длины рёбер и радиус вписанного в октаплекс шара.

г) Как выглядят 3-мерные гиперграни и каковы их 3-мерные объёмы?

д) Как выглядят 2-мерные грани и каковы их площади?

е) Найдите 4-мерный объём октаплекса.

Задача 14.17. Докажите, что евклидов объём n-мерного параллелепипеда равен произведению $(n-1)$-мерного евклидова объёма произвольной его $(n-1)$-мерной грани на длину опущенной на эту грань высоты.

Задача 14.18. Докажите, что кратчайшее расстояние от конца вектора v до подпространства с базисом $u_1, u_2, \dots, u_k$ равно отношению определителей Грама $\det G_{v,u_1,u_2,\dots,u_k} / \det G_{u_1,u_2,\dots,u_k}$.

Задача 14.19. Покажите, что скалярные произведения (f,g) на $\mathbb{R}[x]$, заданные формулами а) $\displaystyle\int_{-1}^{1} \frac{f(x)g(x)\,dx}{\sqrt{1-x^2}}$ б) $\displaystyle\int_{0}^{+\infty} f(x)g(x)e^{-x}dx$

[1] т. е. позволяет перевести любой флаг в любой

в) $\displaystyle\int\limits_{-\infty}^{+\infty} f(x)g(x)e^{-x^2}\,dx$

г) $\displaystyle\int\limits_{-1}^{1} f(x)g(x)\,dx$ являются евклидовыми, и сравните результаты ортогонализации стандартного мономиального базиса $\{x^\nu\}$ в этих евклидовых структурах с семействами многочленов д) Лаггера $L_n(x) = e^x \dfrac{d^n}{dx^n}\left(e^{-x}x^n\right)$

е) Эрмита $E_n(x) = e^{x^2}\dfrac{d^n}{dx^n}\,e^{-x^2}$ ж) Лежандра $P_n(x) = \dfrac{d^n}{dx^n}(1-x^2)^n$

з) Чебышева $T_n(x) = \cos(n\arccos x)$

Задача 14.20. Найдите $\min\displaystyle\int\limits_{-1}^{1} P^2(x)\,dx$ по всем приведённым многочленам P степени k. Если общий случай не получается, решите задачу для $k = 2,\ 3,\ 4$.

Задача 14.21. Найдите ближайший к $\sin x$ кубический многочлен в пространстве гладких функций на $[-\pi,\pi]$ со со скалярным произведением $\displaystyle\int\limits_{-\pi}^{\pi} P(x)Q(x)\,dx.$

Задача 14.22. Покажите, что скалярное произведение $(A,B) = \operatorname{tr}(AB^t)$ задаёт евклидову структуру на пространстве $\mathrm{Mat}_n(\mathbb{R})$ и найдите ортогональные дополнения к подпространствам а) бесследных
б) симметричных
в) верхнетреугольных г) кососимметричных матриц.

Задача 14.23 (параметризация Кэли). Докажите, что отображение $K \longmapsto (E-K)(E+K)^{-1}$ задаёт биекцию между вещественными кососимметричными матрицами и вещественными ортогональными матрицами без собственного значения -1.

Задача 14.24. Для k точек $p_1, p_2, \dots, p_k$ евклидова пространства обозначим через $D_{p_1,p_2,\dots,p_k}$ симметричную $k\times k$ матрицу с $d_{ij} = |\overrightarrow{p_ip_j}|^2$, через $C_{p_1,p_2,\dots,p_k}$ — матрицу размера $(k+1)\times(k+1)$, полученную приписыванием к D сверху и слева единичной строки и единичного столбца и нуля в левом верхнем углу, а через $G_{w_1,w_2,\dots,w_m}$ — матрицу Грама набора векторов w_i. Покажите, что:
а) $\det G_{\overrightarrow{p_0p_1},\overrightarrow{p_0p_2},\cdots,\overrightarrow{p_0p_n}} = \frac{(-1)^{n+1}}{2^n}\det C_{p_0,p_1,\dots,p_n}$ (размер у матриц разный!)
б) $p_0, p_1, \dots, p_n \in \mathbb{R}^n$ лежат в одной гиперплоскости $\iff \det C_{p_0,p_1,\dots,p_n} = 0$
в) $p_0, p_1, \dots, p_{n+1} \in \mathbb{R}^n$ тогда и только тогда лежат на одной сфере или в одной гиперплоскости, когда $\det D_{p_0,p_1,\dots,p_{n+1}} = 0$
г) симплекс $[p_0, p_1, \dots, p_n]$ с предписанными длинами сторон $\ell_{ij} = |p_ip_j|$ существует тогда и только тогда, когда все главные миноры[1] матрицы $\left(\ell_{ij}^2\right)$ всех

[1] т. е. определители всевозможных квадратных подматриц, главная диагональ которых содержится в главной диагонали исходной матрицы

порядков $2 \leqslant r \leqslant (n+1)$ отличны от нуля и имеют знак $(-1)^{r-1}$

д) квадрат радиуса шара, описанного вокруг симплекса $[p_0, p_1, \dots, p_n]$, равен

$$R^2 = -\frac{1}{2}\,\frac{\det D_{p_0,p_1,\dots,p_n}}{\det C_{p_0,p_1,\dots,p_n}}\,.$$

Задача 14.25 (отражения). Для фиксированного вектора e единичной длины отображение $\sigma_e : v \mapsto v - 2(v,e)\,e$ называется *отражением* в гиперплоскости $e^{\perp}$. Покажите, что это ортогональный линейный оператор, и опишите его собственные векторы и собственные значения.

Задача 14.26. Покажите, что любой ортогональный оператор на n-мерном евклидовом пространстве является композицией не более n отражений в гиперплоскостях (см. зад. 14.25) и что ортогональный оператор собственный тогда и только тогда, когда он является композицией чётного числа отражений.

Задача 14.27. Обозначим через τ_v, σ_π и $\varrho_{v,\varphi}$, соответственно, сдвиг на вектор v, отражение в плоскости π и поворот вокруг оси с направляющим вектором v на угол φ против ЧС, если глядеть вдоль v. Выясните, какие из написанных ниже равенств справедливы, и для всех таких равенств выразите параметры движения в правой части, через параметры движений из левой

а) $\sigma_{\pi_1}\circ\sigma_{\pi_2} = \varrho_{v,\varphi}$ б) $\sigma_{\pi_1}\circ\sigma_{\pi_2} = \tau_v$ в) $\sigma_\pi\circ\varrho_{u,\varphi}\circ\sigma_\pi = \varrho_{v,\psi}$ г) $\varrho_{u,\varphi}\circ\varrho_{w,\psi} = \tau_v\circ\varrho_{v,\vartheta}$

д) $\varrho_{u,\varphi}\circ\sigma_\pi\circ\varrho_{u,-\varphi} = \sigma_{\pi_2}$ е) $\varrho_{u,\varphi}\circ\sigma_{\pi_1} = \sigma_{\pi_2}$ ж) $\tau_{u_2}\circ\sigma_{\pi_2}\circ\tau_{u_1}\circ\sigma_{\pi_1} = \tau_v\circ\varrho_{v,\varphi}$, где $u_i \parallel \pi_i$.

Задача 14.28. В произвольном аффинном пространстве (над любым полем) заданы точки $p_1, p_2, \dots, p_k$. Прямая, соединяющая одну из точек p_i с (равновесным) барицентром c_i остальных точек, называется *медианой*. Покажите, что все медианы пересекаются в одной точке c, и найдите все отношения $\overrightarrow{p_i c} : \overrightarrow{c c_i}$.

Задача 14.29 (барицентрические координаты). В n-мерном аффинном пространстве A заданы $(n+1)$ точек $a_0, a_1, \dots, a_n$, не лежащие в одной аффинной гиперплоскости. Покажите, что сопоставление каждому набору весов

$$(\lambda_0, \lambda_1, \dots, \lambda_n) \quad \text{с} \quad \sum \lambda_i = 1$$

барицентра $c = \sum \lambda_i a_i$ точек a_i с весами λ_i является биекцией между такими наборами весов и точками $c \in A$. Нарисуйте все точки $c \in \mathbb{R}^2$, веса (α, β, γ) которых относительно данного $\triangle\, ABC$ удовлетворяют условиям: а) $\alpha, \beta, \gamma > 0$ б) $\alpha, \beta > 0$, $\gamma < 0$ в) $\alpha = \beta$ г) $\alpha, \beta > 1/3$, $\gamma > 0$ д) $\alpha \geqslant \beta$ е) $\alpha \geqslant \beta \geqslant \gamma$ и напишите условия на веса, задающие треугольники:

ж) на которые $\triangle\, ABC$ разрезается своими медианами (их всего 6)

з) гомотетичные $\triangle\, ABC$ относительно его центра тяжести с коэффициентами 3 и 1/3.

Задача 14.30. Покажите, что выпуклая оболочка компакта компакт.

Задача 14.31 (теорема Хелли). Докажите, что если в некотором наборе выпуклых фигур $K_1, K_2, \dots, K_m \subset \mathbb{R}^n$ любые $(n+1)$ фигур имеют общую точку, все и все m фигур имеют общую точку[1], а также приведите примеры, показывающие, что условие выпуклости нельзя отбросить, а число $n+1$ нельзя уменьшить.

Задача 14.32. Верна ли теорема Хелли для бесконечного набора а) компактных б) не компактных выпуклых фигур?

Задача 14.33. Полупространством в аффинном пространстве A над вещественным векторным пространством V называется множество решений x линейного неравенства $\xi(x) \geqslant c$, где $c \in \mathbb{R}$, $\xi \in V^*$. Покажите, что любое покрытие аффинного пространства $\mathbb{R}^n$ полупространствами содержит подпокрытие, состоящее из $n+1$ полупространств.

Задача 14.34 (теорема Юнга). Докажите, что любая плоская клякса диаметром[2] $\leqslant 1$ закрывается блюдцем радиуса $1/\sqrt{3}$, и придумайте обобщение этого факта на кляксы бо́льших размерностей.

Задача 14.35. Рассмотрим евклидово расстояние $\varrho(p,q) = |\overrightarrow{pq}|$ на $\mathbb{R}^n$ как функцию двух переменных $\varrho : \mathbb{R}^n \times \mathbb{R}^n \longrightarrow \mathbb{R}$. Докажите, что она дифференцируема, и ее производная $\varrho'(p,q) : \mathbb{R}^n \times \mathbb{R}^n \longrightarrow \mathbb{R}$ в точке (p,q) действует на касательный вектор $(\overrightarrow{v}, \overrightarrow{w})$ по формуле:

$$\varrho'(p,q)[\overrightarrow{v}, \overrightarrow{w}] = \frac{(\overrightarrow{pq}\,,\ \overrightarrow{w} - \overrightarrow{v})}{\varrho(p,q)} = |\overrightarrow{w}|\cos(\varphi) - |\overrightarrow{v}|\cos(\psi)\ ,$$

где φ — угол между векторами $\overrightarrow{w}$ и $\overrightarrow{pq}$, а ψ — между $\overrightarrow{v}$ и $\overrightarrow{pq}$.

[1] один из способов — индукция по m, начиная с $m = n+2$, но будьте внимательны: возможно, что не все $(n+2)$ точки, лежащие в пересечениях всех сочетаний из $(n+1)$ фигур, служат вершинами своей выпуклой оболочки (в любом случае полезно сначала отдельно разобраться с $n = 2, 3$)

[2] *диаметром* ограниченной фигуры называется точная верхняя грань расстояний между её точками

§15. Группы

15.1. Группы преобразований. Модельные примеры неабелевых групп — это группы преобразований. Напомним (см. n° 1.6), что непустой набор G взаимно однозначных отображений множества X в себя называется *группой преобразований* множества X, если вместе с каждым отображением $g \in G$ в G лежит и обратное к нему отображение g^{-1}, а вместе с каждыми двумя отображениями $f, g \in G$ в G лежит и их композиция fg. Эти условия гарантируют, что тождественное преобразование Id_X тоже лежит в G, поскольку $\mathrm{Id}_X = g^{-1}g$ для любого $g \in G$.

Если группа G конечна, число элементов в ней обозначается $|G|$ и называется *порядком* группы G. Для упрощения обозначений мы пишем gx вместо $g(x)$ для $g \in G$, $x \in X$.

15.1.1. Орбиты. Со всякой группой преобразований G множества X связано бинарное отношение $x \underset{G}{\sim} y$ на X, означающее, что $y = gx$ для некоторого $g \in G$. Из определения группы преобразований вытекает, что это отношение является эквивалентностью: оно рефлексивно, поскольку $x = \mathrm{Id}_X x$, симметрично, поскольку $y = gx \iff x = g^{-1}y$, и транзитивно, поскольку из $y = gx$ и $z = hy$ вытекает, что $z = (hg)x$.

Класс эквивалентности точки $x \in X$ по отношению $\underset{G}{\sim}$ обозначается Gx и называется *орбитой* x под действием G. Он состоит из всех точек, которые можно получить из x, применяя всевозможные преобразования из группы G. Из общих свойств классов эквивалентности вытекает, что орбиты двух различных точек или не пересекаются или совпадают[1]. Множество всех орбит называется *фактором* множества X по действию группы G и обозначается X/G.

15.1.2. Пример: длина орбиты конечной группы. Количество точек в орбите (если оно конечно) называется её *длиной*. Все орбиты конечной группы имеют конечную длину. Чтобы связать $|Gx|$ с $|G|$ рассмотрим сюрьективное отображение[2]

$$\mathrm{ev}_x : G \xrightarrow{g \mapsto gx} Gx \,. \tag{15-1}$$

Слой этого отображения над точкой x называется *стабилизатором* точки x. Он состоит из всех преобразований, оставляющих x на месте и обозначается

$$\mathrm{Stab}_G(x) = \{g \in G \mid gx = x\} \tag{15-2}$$

Упражнение 15.1. Убедитесь, что $\mathrm{Stab}_G(x)$ является подгруппой в группе G.

Слой отображения (15-1) над любой другой точкой $y \in Gx$ состоит из всех преобразований, переводящих x в y и содержит столько же элементов, сколько

[1] это легко увидеть и непосредственно: если $gx = hy$ для некоторых $g, h \in G$, то $x = g^{-1}hy$ и $\forall f \in G$ $fx = fg^{-1}hy \in Gy$, т. е. $Gx \subset Gy$; противоположное включение $Gx \supset Gy$ следует из равенства $y = h^{-1}gx$

[2] при желании его можно воспринимать как «некоммутативное» *отображения вычисления*

$\mathrm{Stab}(x)$, поскольку отображения левого умножения на произвольным образом выбранное преобразование $f : x \mapsto y$ и на обратное к нему преобразование $f^{-1} : y \mapsto x$

$$L_f : \{g \in G \mid gx = x\} \xrightarrow{g \mapsto fg} \{h \in G \mid hx = y\}$$
$$L_{f^{-1}} : \{h \in G \mid hx = y\} \xrightarrow{g \mapsto f^{-1}g} \{g \in G \mid gx = x\}$$

обратны друг другу и, стало быть, биективны. Мы получаем следующий важный результат.

Теорема 15.1 (формула для длины орбиты)
Длина орбиты произвольной точки при действии на неё конечной группы преобразований G равна отношению порядка группы к порядку стабилизатора этой точки: $|G(x)| = |G| : |\mathrm{Stab}_G(x)|$. В частности, длины всех орбит и порядки стабилизаторов всех точек являются делителями порядка группы. □

Следствие 15.1
Стабилизаторы всех точек, лежащих в одной орбите конечной группы, имеют одинаковый порядок. □

Упражнение 15.2 (сопряжённость стабилизаторов). Покажите, что для произвольной (в том числе бесконечной) группы $G \subset \mathrm{Aut}\,(X)$ и любых двух точек x и $y = f(x)$, лежащих в одной орбите, *сопряжение элементом* f

$$\mathrm{Ad}_f : g \longmapsto fgf^{-1}$$

задаёт *изоморфизм групп*[1] $\mathrm{Ad}_f : \mathrm{Stab}_G(x) \xrightarrow{\sim} \mathrm{Stab}_G(y)$.

15.1.3. Группы фигур. Для любой фигуры $\Phi \subset \mathbb{R}^3$, отображения $\Phi \longrightarrow \Phi$, получающиеся ограничением на Φ всевозможных ортогональных линейных операторов $\mathbb{R}^3 \longrightarrow \mathbb{R}^3$, переводящих фигуру Φ в себя, образуют группу преобразований фигуры Φ. Мы будем называть эту группу *полной группой фигуры* Φ и обозначать O_Φ . Подгруппу $\mathrm{SO}_\Phi \subset \mathrm{O}_\Phi$, состоящую из отображений, индуцированных собственными ортогональными операторами $\mathbb{R}^3 \longrightarrow \mathbb{R}^3$, мы будем называть *собственной группой фигуры* Φ.

Если фигура $\Phi \subset \mathbb{R}^3$ содержится в некоторой плоскости $\Pi \subset \mathbb{R}^3$, то собственная группа фигуры Φ совпадает с полной: беря композицию любого несобственного движения из группы фигуры с отражением в плоскости Π, мы получаем собственное движение, которое действует на фигуру Φ точно также, как и исходное несобственное движение.

Упражнение 15.3. Изготовьте модели пяти *платоновых тел* — тетраэдра, октаэдра, куба, додекаэдра и икосаэдра (см. рис. 15◇4 – рис. 15◇6 ниже).

[1] т. е. биективно и переводит композицию отображений в композицию их образов

15.1.4. Пример: группы диэдров. Группа правильного плоского n-угольника, лежащего в пространстве $\mathbb{R}^3$ так, что его центр находится в нуле, обозначается D_n и называется *n-той группой диэдра*.

Простейший диэдр — *двуугольник* — возникает при $n = 2$. Это симметричная луночка с двумя сторонами, изображённая на рис. 15◇1. Группу D_2 такой луночки[1] иначе можно описать как с группу описанного вокруг луночки прямоугольника или как группу вписанного в неё ромба, если только они не квадраты.

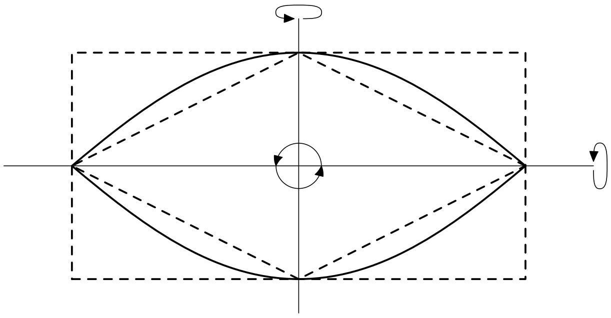


Рис. 15◇1. Группа двуугольника D_2.

Эта группа состоит из тождественного отображения и трёх поворотов на 180° вокруг перпендикулярных друг другу осей, одна из которых проходит через вершины луночки, другая — через середины её сторон, а третья перпендикулярна плоскости луночки и проходит её центр. Действительно, любое нетождественное преобразование диэдральной луночки должно менять местами либо её стороны, либо её вершины, либо то и другое сразу, а ровно это и происходит при трёх перечисленных выше поворотах.

Упражнение 15.4. Убедитесь, что $D_2 \simeq \mathbb{Z}/(2) \oplus \mathbb{Z}/(2)$.

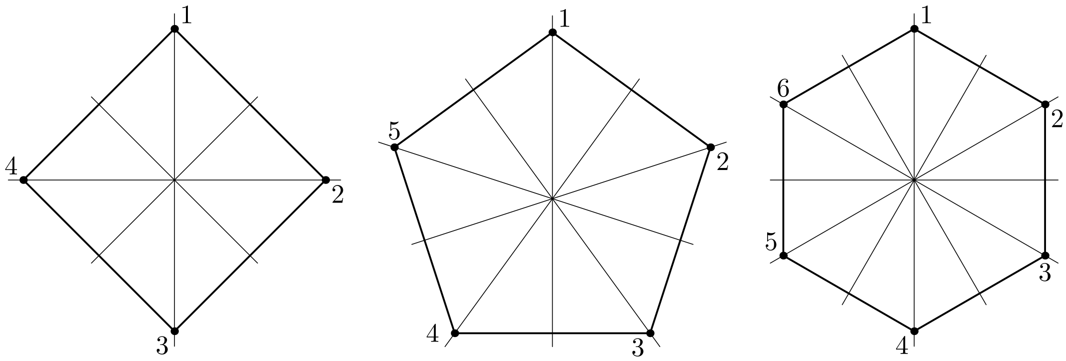


Рис. 15◇2. Оси диэдров для $n = 4, 5, 6$.

Для произвольного $n \geqslant 2$ группа диэдра D_n состоит из $2n$ движений: n поворотов вокруг центра многоугольника на углы $2\pi k/n$ с $k = 0, 1, \ldots, (n-1)$ (при $k = 0$ получается тождественное преобразование) и n осевых симметрий (т. е. поворотов на 180° в пространстве) относительно прямых, проходящих при нечётном n через вершину и середину противоположной стороны, а при чётном n — через пары противоположных вершин и через середины противоположных сторон (см. рис. 15◇2).

[1] диэдральная группа D_2 иногда ещё называется *четвертной группой Клейна* и обозначается $\mathfrak{V}_4$

В самом деле, n вершин диэдра образуют одну орбиту этой группы, и стабилизатор вершины состоит ровно из двух движений — тождественного, оставляющего две соседние вершины на месте, и осевой симметрии, меняющей их местами. По формуле для длины орбиты (теор. 15.1 на стр. 261) $|D_n| = 2n$, и значит, никаких других преобразований кроме перечисленных поворотов и отражений в D_n нет.

Например, *группа треугольника* D_3 состоит из шести движений: тождественного, двух поворотов τ, τ^{-1} на $\pm 120°$ вокруг центра треугольника и трёх осевых симметрий σ_{ij} относительно его медиан (см. рис. 15◇3).

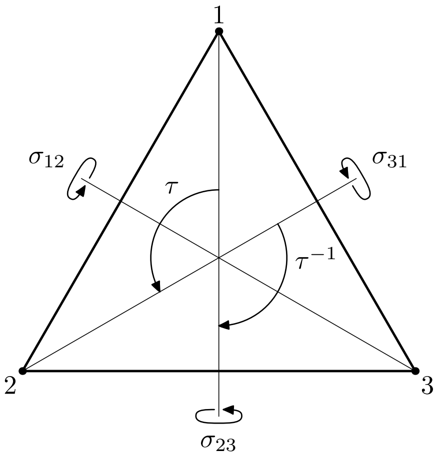


Рис. 15◇3. Группа треугольника.

Если занумеровать вершины треугольника числами 1, 2, 3 и сопоставить каждому движению из группы треугольника осуществляемую им перестановку вершин, мы получим отображение

$$D_3 \hookrightarrow S_3 = \mathrm{Aut}\left(\{1,\,2,\,3\}\right). \tag{15-3}$$

из группы D_3 в симметрическую группу S_3 . Поскольку векторы, идущие из центра треугольника в вершины, линейно порождают $\mathbb{R}^2$, оператор, оставляющий вершины треугольника на месте, действует на плоскость тождественно. Тем самым, отображение (15-3) инъективно, а так как порядок обеих групп равен 6, оно изоморфизм. При этом изоморфизме повороты на $\pm 120°$ отождествляются с циклическими перестановками $(2,\,3,\,1)$, $(3,\,1,\,2)$, а осевые симметрии — с транспозициями $\sigma_{23} = (1,\,3,\,2)$, $\sigma_{13} = (3,\,2,\,1)$, $\sigma_{12} = (2,\,1,\,3)$.

Упражнение 15.5. Составьте таблицы умножения для групп D_3, D_4 и D_5, аналогичные таблице (1-25) на стр. 16.

15.1.5. Пример: группа тетраэдра. Полная группа правильного тетраэдра с центром в нуле состоит из $24 = 4 \cdot 6$ движений, поскольку 4 вершины тетраэдра составляют одну орбиту этой группы, а стабилизатор вершины есть шестиэлементная группа треугольника (а именно, противолежащей этой вершине грани).

Собственная группа тетраэдра состоит из $12 = 4 \cdot 3$ движений: 4 вершины составляют одну орбиту и для собственной группы, но стабилизатор вершины в собственной группе состоит всего из трёх движений — тождественного и двух поворотов на углы $\pm 120°$ вокруг прямой, соединяющий вершину с центром противолежащей грани (отражения в плоскостях, проходящих через вершину и ось противолежащей грани, не являются собственными).

Полный список собственных движений таков: тождественное, $4 \cdot 2 = 8$ поворотов на углы $\pm 120°$ вокруг прямых, проходящих через вершину и центр противоположной грани, а также 3 поворота на 180° вокруг прямых, проходящих через середины противоположных рёбер (см. рис. 15◇4).

В несобственной группе, помимо перечисленных поворотов, имеется 6 отражений в плоскостях, проходящих через ребро и середину противоположного к нему ребра. Чтобы описать остальные 6 несобственных движений тетраэдра, занумеруем его вершины числами 1, 2, 3, 4 и рассмотрим вложение полной группы тетраэдра в симметрическую группу S_4, сопоставляющее движению тетраэдра осуществляемую им перестановку вершин. Как и для треугольника, это отображение инъективно[1].

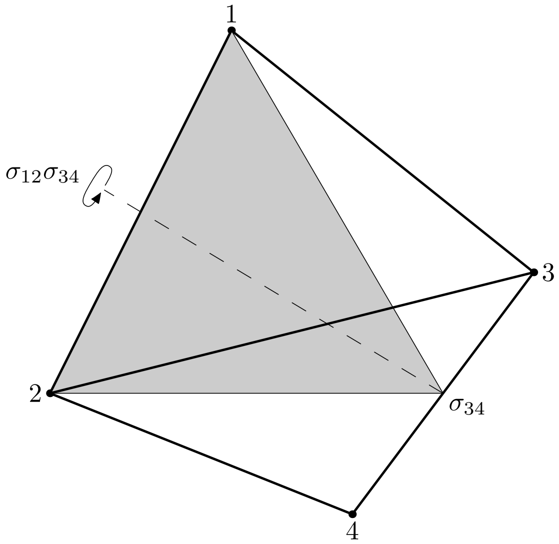


Рис. 15◇4. Плоскость симметрии σ_{34} и ось поворота на 180° (равного композиции $\sigma_{12}\sigma_{34}$).

Обозначим через σ_{ij} отражение тетраэдра в плоскости, проходящей через середину ребра $[i, j]$ и противоположное ребро. Шесть отражений σ_{ij} переходят в транспозиции букв i и j. Повороты на ±120°, представляющие собой всевозможные композиции $\sigma_{ij}\sigma_{jk}$ с попарно различными i, j, k, переходят в циклические перестановки букв i, j, k. Три вращения на ±180° относительно осей, соединяющих середины противоположных рёбер, это одновременные транспозиции непересекающихся пар букв:

$$\sigma_{12}\sigma_{34} = (2, 1, 4, 3)\,, \quad \sigma_{13}\sigma_{24} = (3, 4, 1, 2)\,, \quad \sigma_{14}\sigma_{23} = (4, 3, 2, 1)\,.$$

Упражнение 15.6. Убедитесь, что эти три поворота образуют вместе с тождественным четвертную группу Клейна $\mathfrak{V}_4 = D_2 = \mathbb{Z}/(2) \oplus \mathbb{Z}/(2)$.

В итоге, «недостающие» шесть несобственных преобразований должны отвечать шести циклическим перестановкам вершин:

$$|1234\rangle\,, \quad |1243\rangle\,, \quad |1324\rangle\,, \quad |1342\rangle\,, \quad |1423\rangle\,, \quad |1432\rangle\,.$$

Геометрически они реализуются поворотами на ±90° относительно прямых, проходящих через середины противоположных рёбер с последующим отражением в плоскости, проходящей через центр тетраэдра и перпендикулярной оси поворота.

Упражнение 15.7. Выразите эти 6 движений через отражения в плоскостях.

[1]векторы, идущие из центра тетраэдра в вершины, линейно порождают $\mathbb{R}^3$). Поскольку $|S_4| = 24$, это вложение изоморфизм

15.1.6. Пример: полная и собственная группы додекаэдра. Собственная группа додекаэдра (см. рис. 15◇5) состоит из $6 \cdot 4 = 24$ поворотов на углы $2\pi k/5$ (где $k = 1, 2, 3, 4$) вокруг осей, проходящих через центры противоположных граней додекаэдра, $10 \cdot 2 = 20$ поворотов на углы $\pm 2\pi/3$ вокруг осей, проходящих через противоположные вершины, 15 поворотов на 180° вокруг осей, проходящих через середины противоположных рёбер додекаэдра, и тождественного преобразования. В полной группе додекаэдра помимо этих 60 движений содержатся их композиции с центральной симметрией относительно центра додекаэдра.

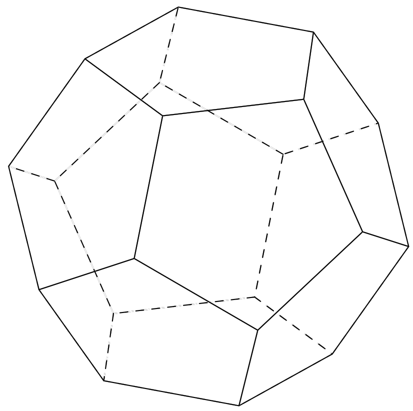


Рис. 15◇5. Додекаэдр.

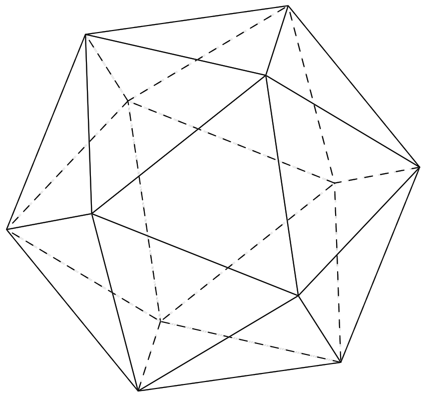


Рис. 15◇6. Икосаэдр.

Убедиться в том, что этими преобразованиями группы додекаэдра исчерпываются, можно ровно так же, как и выше — вычислив порядки обеих групп по формуле для длины орбиты. Например, центры граней додекаэдра образуют одну орбиту длины 12. Стабилизатор центра грани состоит из всех движений, переводящих эту грань в себя. В несобственной группе он состоит из 10 движений, составляющих группу пятиугольника — пяти собственных поворотов вокруг прямой, соединяющей центр грани с центром додекаэдра, и пяти несобственных отражений в плоскостях, проходящих через ось грани и центр додекаэдра. Соответственно в собственной группе порядок стабилизатора грани равен 5. Итак, собственная группа додекаэдра состоит из $12 \cdot 5 = 60$, а несобственная — из $12 \cdot 10 = 60$ движений.

Упражнение 15.8. Покажите что полные группы куба (см. рис. 15◇7), октаэдра (см. рис. 15◇8) и икосаэдра (см. рис. 15◇6) состоят, соответственно из 48, 48 и 120 движений, а собственные — из 24, 24 и 60.

15.2. Абстрактные группы. Множество G, на котором задана операция *композиции* $G \times G \longrightarrow G$, сопоставляющая каждой паре элементов $(g_1, g_2) \in G \times G$ некоторый элемент $g_1 g_2 \in G$, называется *группой*, если выполняются следующие три свойства:

$$\textit{ассоциативность}: \qquad \forall\, f,g,h \in G \quad (fg)h = f(gh) \tag{15-4}$$

$$\textit{наличие единицы}: \qquad \exists\, e \in G : \forall\, g \in G \quad eg = ge = g \tag{15-5}$$

$$\textit{наличие обратных}: \qquad \forall\, g \in G \quad \exists\, g^{-1} \in G : gg^{-1} = g^{-1}g = e \tag{15-6}$$

Группа, в которой выполняется дополнительное свойство

$$\textit{коммутативность}: \qquad \forall\, f,g \in G \quad fg = gf \tag{15-7}$$

называется *коммутативной* (или *абелевой*). Количество элементов в группе G (если оно конечно) называется *порядком* группы G и обозначается $|G|$.

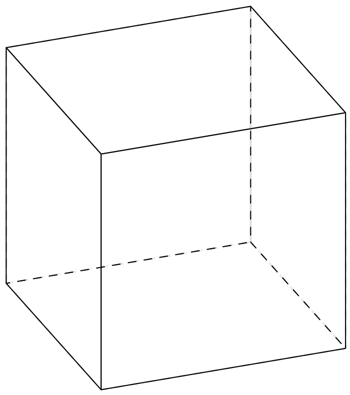


Рис. 15◇7. Куб.

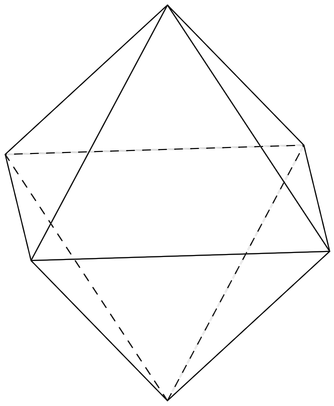


Рис. 15◇8. Октаэдр.

15.2.1. Комментарии к определению. Элемент e, существование которого постулируется в (15-5), автоматически единственен, поскольку для любых двух таких элементов e' и e'' имеем $e' = e'e'' = e''$.

Свойство (15-6) можно было бы ослабить до требования существования для каждого элемента $g \in G$ левого обратного f: $fg = e$ и правого обратного h: $gh = e$, не требуя, чтобы они совпадали друг с другом. Равенство $f = h$ будет выполняться автоматически, поскольку $f = fe = f(gh) = (fg)h = eh = h$. Это же вычисление показывает, что обратный элемент $g^{-1} = f = h$ определяется по g однозначно. Минимизировать условия, определяющие группу можно и дальше:

Упражнение 15.9. Проверьте, что в условии (15-5) достаточно требовать существования одной только левой единицы (т. е. такого элемента e, что $\forall g \in G$ $eg = g$), а в условии (15-6) — существования одного только левого обратного.

15.2.2. Подгруппы. Подмножество $H \subset G$ в группе G называется *подгруппой*, если оно образует группу относительно операции композиции, имеющейся в G. Это означает, что $h \in H \Rightarrow h^{-1} \in H$ и $h_1, h_2 \in H \Rightarrow h_1h_2 \in H$. При этом единичный элемент $e \in G$ автоматически окажется в H, так как $e = hh^{-1}$ для произвольного $h \in H$, и все свойства (15-4)–(15-6) очевидно будут выполнены.

Упражнение 15.10. Проверьте, что в любой группе G

а) $(g_1 g_2 \cdots g_k)^{-1} = g_k^{-1} \cdots g_2^{-1} g_1^{-1}$
б) пересечение любого множества подгрупп является подгруппой
в) $H \subset G$ подгруппа если и только если $h_1, h_2 \in H \Rightarrow h_1 h_2^{-1} \in H$.

15.2.3. Пример: циклические группы и подгруппы. Для любого элемента g произвольной группы G положим $g^0 = e$ и $g^{-n} = (g^{-1})^n$. Тогда все целые степени g^m составят в G подгруппу, которая называется *циклической подгруппой*, порождённой g и обозначается $\langle g \rangle$. Это наименьшая по включению подгруппа в G, содержащая g. Отметим, что она абелева и, будучи абелевой группой с одной образующей, группа $\langle g \rangle$ изоморфна либо $\mathbb{Z}$, либо $\mathbb{Z}/(n)$.

В самом деле, $\langle g \rangle$ является образом сюрьективного гомоморфизма

$$\varphi_g : \mathbb{Z} \longrightarrow G \,,$$

переводящего m в g^m. Если $\ker \varphi_g = 0$, то $\varphi_g : \mathbb{Z} \xrightarrow{\sim} \langle g \rangle$ является изоморфизмом. В этом случае говорят, что g имеет *бесконечный порядок* и пишут $\operatorname{ord} g = \infty$. Если $\ker \varphi_g \neq 0$, то $\ker \varphi_g = (n)$, где $n \in \mathbb{N}$ — наименьшая степень, для которой $g^n = e$, и $\langle g \rangle = \operatorname{im} \varphi_g = \mathbb{Z}/(n)$. В этом случае говорят, что *порядок* элемента g равен n и пишут $\operatorname{ord}(g) = n$.

Таким образом, *порядок* элемента g можно эквивалентными способами определить либо как наименьшее $n \in \mathbb{N}$, для которого $g^n = e$, либо как порядок $|\langle g \rangle|$ в циклической группы порождённой G.

Группа G называется *циклической*, если в ней существует элемент $g \in G$ такой, что все элементы группы являются его целыми степенями, т. е. $G = \langle g \rangle$. Элемент g называется в этом случае *образующей* циклической группы G.

Например, аддитивная группа целых чисел $\mathbb{Z}$ является циклической, и в качестве образующего элемента можно взять любой из двух элементов ± 1. Аддитивная группа вычетов $\mathbb{Z}/(10)$ также является циклической, и в качестве её образующего элемента можно взять любой из четырёх классов $[\pm 1]_6$, $[\pm 3]_6$ (обратите внимание, что остальные 6 классов не являются образующими).

Упражнение 15.11. Покажите, что мультипликативная группа ненулевых вычетов по модулю 7 является циклической и перечислите все её образующие элементы.

Лемма 15.1
Элемент $h = g^k$ тогда и только тогда является образующей циклической группы $G = \langle g \rangle$ порядка n, когда $\text{нод}(k, n) = 1$.

Доказательство. Поскольку $\langle h \rangle \subset \langle g \rangle$, совпадение $\langle h \rangle \subset \langle g \rangle$ равносильно тому, что $\operatorname{ord} h \geqslant n$. Равенство $h^m = g^{mk} = e$ означает, что mk делится на n. При $\text{нод}(n, k) = 1$ это возможно только при m делящемся на n, так что в этом случае $\operatorname{ord} h \geqslant n$. Если же $n = n_1 d$ и $k = k_1 d$ с $d > 1$, то $h^{n_1} = g^{kn_1} = g^{nk_1} = e$, т. е. $\operatorname{ord} h \leqslant n_1 < n$. $\square$

15.2.4. Пример: циклы в симметрической группе S_n. Перестановка

$$\tau \in S_n\,,$$

по кругу переводящая друг в друга какие-нибудь $m \geqslant 2$ различных элементов[1]

$$i_1 \to i_2 \to \cdots \to i_{m-1} \to i_m \to i_1 \tag{15-8}$$

и оставляющая на месте все остальные элементы, называется *циклом* длины m.

Упражнение 15.12. Покажите, что k-тая степень цикла длины m является циклом тогда и только тогда, когда $\text{нод}(k,m)=1$.

Цикл (15-8) часто бывает удобно обозначать

$$\tau = |i_1, i_2, \dots, i_m\rangle\;, \tag{15-9}$$

не смотря на то, что один и тот же цикл (15-8) имеет m *различных* записей (15-9), получающихся друг из друга циклическими перестановками элементов.

Упражнение 15.13. Сколько имеется в S_n различных циклов длины k?

Теорема 15.2

Каждая перестановка $g \in S_n$ является композицией непересекающихся циклов:

$$g = \tau_1\tau_2 \cdots \tau_k\,. \tag{15-10}$$

Любые два цикла этого разложения перестановочны: $\tau_i\tau_j = \tau_j\tau_i$, и разложение (15-10) единственно с точностью до перестановки циклов между собой.

Доказательство. Множество $X = \{1, 2, \dots, n\}$ является дизъюнктным объединением орбит циклической группы $\langle g\rangle$. Каждая орбита имеет вид

$$x \overset{g}{\longmapsto} g(x) \overset{g}{\longmapsto} g^2(x) \overset{g}{\longmapsto} g^3(x) \overset{g}{\longmapsto} \cdots \tag{15-11}$$

и является циклом: поскольку множество X конечно, в последовательности (15-11) будут повторения, а так как g переводит разные элементы в разные, первым из повторившихся элементов будет именно стартовый элемент x. Таким образом, перестановка g циклически действует на элементах каждой орбиты группы $\langle g\rangle$, т. е. является произведением непересекающихся циклов. Наоборот, если перестановка g является произведением непересекающихся циклов (15-10), то эти циклы являются орбитами действия циклической группы $\langle g\rangle$ на множестве X. Непересекающиеся циклы, очевидно, перестановочны. □

Упражнение 15.14. Покажите, что два цикла $\tau_1, \tau_2 \in S_n$ перестановочны ровно в двух случаях: либо когда они не пересекаются, либо когда $\tau_2 = \tau_1^s$, причём в этом случае оба цикла имеют равную длину, взаимно простую с s.

[1] числа $i_1, i_2, \dots, i_m$ могут быть любыми, не обязательно соседними или возрастающими

15.2.5. Цикловой тип перестановки. Написанный в порядке нестрогого убывания набор длин непересекающихся циклов, в которые раскладывается перестановка $g \in S_n$ (включая циклы длины один, отвечающие элементам, которые перестановка g оставляет на месте), представляет собою n-клеточную диаграмму Юнга. Эта диаграмма называется *цикловым типом* (или *диаграммой циклов*) перестановки g и обозначается $\lambda(g)$.

Например, перестановка

$$g = (6,\,5,\,4,\,1,\,8,\,3,\,9,\,2,\,7) = |1,6,3,4\rangle|2,5,8\rangle|7,9\rangle = \begin{array}{|c|c|c|c|}\hline 1 & 6 & 3 & 4 \\ \hline 2 & 5 & 8 \\ \cline{1-3} 7 & 9 \\ \cline{1-2} \end{array}$$

имеет цикловой тип $\begin{array}{|c|c|c|c|}\hline \; & \; & \; & \; \\ \hline \; & \; & \; \\ \cline{1-3} \; & \; \\ \cline{1-2} \end{array}$, т. е. $\lambda(6,\,5,\,4,\,1,\,8,\,3,\,9,\,2,\,7) = (4,\,3,\,2)$. Единственной перестановкой циклового типа $\lambda = (1,\,1,\,\dots\,,\,1)$ (один столбец высоты n) является тождественная перестановка Id. Диаграмму $\lambda = (n)$ (одна строка длины n) имеют $(n-1)!$ циклов максимальной длины n.

Упражнение 15.15. Сколько перестановок в симметрической группе S_n имеют заданный цикловой тип, содержащий для каждого $i = 1,\,2,\,\dots\,,\,n$ m_i циклов длины i ?

15.2.6. Пример: порядок и знак перестановки. Порядок перестановки $g \in S_n$ равен наименьшему общему кратному длин непересекающихся циклов, из которых она состоит. Например, порядок перестановки

$$(3,\,12,\,7,\,9,\,10,\,4,\,11,\,1,\,6,\,2,\,8,\,5) = |1,\,3,\,7,\,11,\,8\rangle|2,\,12,\,5,\,10\rangle|4,\,9,\,6\rangle \in S_{12}$$

равен $5 \cdot 4 \cdot 3 = 60$. Представление перестановок в виде произведений независимых циклов упрощает многие вычисления. Например, из правила ниточек (см. n° 10.2.1) вытекает, что знак цикла длины ℓ равен $(-1)^{\ell-1}$. Поэтому перестановка чётна, если и только если чётно число её циклов чётной длины.

Упражнение 15.16. Найдите чётность $g = (6,\,5,\,4,\,1,\,8,\,3,\,9,\,2,\,7) \in S_9$ и вычислите g^{15}.

15.3. Гомоморфизмы. Отображение групп $\varphi : G_1 \longrightarrow G_2$ называется *гомоморфизмом*, если оно переводит композицию в композицию, т. е. для любых $g, h \in G_1$ в группе G_2 выполняется соотношение $\varphi(gh) = \varphi(g)\varphi(h)$.

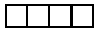
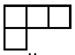
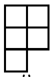
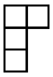
Упражнение 15.17. Убедитесь, что композиция гомоморфизмов тоже является гомоморфизмом.

Термины *эпиморфизм*, *мономорфизм* и *изоморфизм* применительно к отображению групп далее по умолчанию будут подразумевать, что это отображение является *гомоморфизмом* групп.

Нам уже встречалось несколько изоморфизмов групп. Например, группа треугольника изоморфна симметрической группе S_3, а полная группа тетраэдра изоморфна симметрической группе S_4 (оба изоморфизма сопоставляют движению фигуры осуществляемую им перестановку вершин).

15.3.1. Пример: изоморфизм собственной группы куба с S_4. Занумеруем диагонали куба цифрами 1, 2, 3, 4 (на рис. 15◇9 они проставлены на концах соответствующей диагонали) и сопоставим каждому вращению куба осуществляемую им перестановку диагоналей. Полученный гомоморфизм

$$\psi_{\text{куб}} : \mathrm{SO}_{\text{куб}} \xrightarrow{\sim} S_4 \,. \tag{15-12}$$

переводит 6 поворотов на $\pm 90°$ в 6 циклов длины 4 циклового типа , 8 поворотов на $\pm 120°$ — в 8 циклов длины 3 циклового типа , 3 поворота на $\pm 180°$ вокруг осей, проходящих через центры противоположных граней, — в 3 пары независимых транспозиций циклового типа , а 6 поворотов на $180°$ вокруг осей, проходящих через середины противоположных рёбер, — в 6 простых транспозиций циклового типа . Так как собственная группа куба по упр. 15.8 исчерпывается этими 24 поворотами, а S_4 — перечисленными перестановками, гомоморфизм (15-12) биективен.

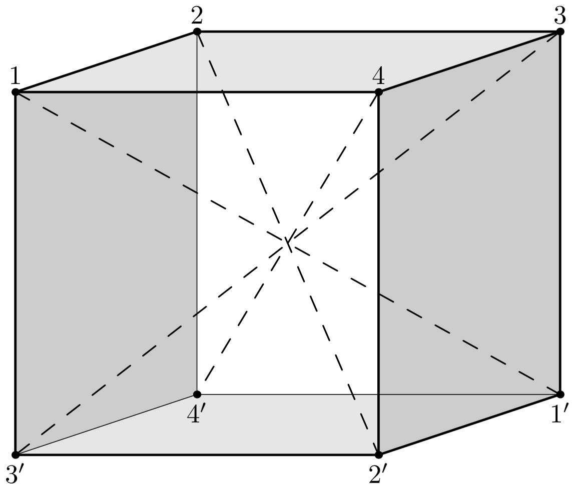


Рис. 15◇9. 4 диагонали и 3 пары противоположных граней куба.

15.3.2. Свойства гомоморфизмов. Любой гомоморфизм групп

$$\varphi : G_1 \longrightarrow G_2$$

переводит единицу e_1 группы G_1 в единицу e_2 группы G_2. В самом деле,

$$\varphi(e_1)\,\varphi(e_1) = \varphi(e_1 e_1) = \varphi(e_1)$$

и, умножая обе части на $\varphi(e_1)^{-1} \in G_2$, получаем $\varphi(e_1) = e_2$.

Далее, для любого $g \in G$ выполняется равенство $\varphi(g^{-1}) = \varphi(g)^{-1}$, поскольку

$$\varphi\left(g^{-1}\right)\varphi(g) = \varphi\left(g^{-1}g\right) = \varphi(e_1) = e_2 \,.$$

Следовательно, образ любого гомоморфизма $G_1 \longrightarrow G_2$ является *подгруппой* в группе G_2.

Полный прообраз единицы $e_2 \in G_2$ называется *ядром* гомоморфизма φ и обозначается

$$\ker\varphi \overset{\text{def}}{=} \varphi^{-1}(e_2) = \{g \in G_1 \mid \varphi(g_1) = e_2\} \,.$$

Ядро является подгруппой в G_1, поскольку из равенств $\varphi(g) = e_2$ и $\varphi(h) = e_2$ вытекает равенство $\varphi(gh) = \varphi(g)\varphi(h) = e_2 e_2 = e_2$, а из равенства $\varphi(g) = e_2$ — равенство $\varphi(g^{-1}) = \varphi(g)^{-1} = e_2^{-1} = e_2$.

Предложение 15.1
Каждый непустой слой любого гомоморфизма групп $\varphi : G_1 \longrightarrow G_2$ находится во взаимно однозначном соответствии с ядром этого гомоморфизма.

Доказательство. Пусть $\varphi(g_1) = g_2$. Если $h \in \ker\varphi$, т. е. $\varphi(h) = e_2$, то $\varphi(g_1 h) = \varphi(g_1)\varphi(h) = g_2$. Поэтому отображение левого умножения на g_1: $h \mapsto g_1 h$ переводит $\ker\varphi$ в слой $\varphi^{-1}(g_2)$. Наоборот, если $g \in \varphi^{-1}(g_2)$, т. е. $\varphi(g) = g_2$, то $\varphi(g_1^{-1}g) = \varphi(g_1)^{-1}\varphi(g) = e_2$, и значит, отображение левого умножения на g_1^{-1}: $g \mapsto g_1^{-1}g$ переводит слой φ над g_2 в $\ker\varphi$. Таким образом, мы имеем два отображения[1]

$$\varphi^{-1}(e_2) \underset{g_1^{-1}g \leftarrow g}{\overset{h \mapsto g_1 h}{\rightleftarrows}} \varphi^{-1}(g_2)\,,$$

которые, очевидно, обратны друг другу. По предл. 1.4 оба они биективны. □

Следствие 15.2
Для того, чтобы гомоморфизм групп $G_1 \xrightarrow{\varphi} G_2$ был инъективен, необходимо и достаточно, чтобы его ядро исчерпывалось единичным элементом. □

Следствие 15.3
Для любого гомоморфизма конечных групп $G_1 \xrightarrow{\varphi} G_2$ выполнено равенство

$$|\mathrm{im}\,(\varphi)| = |G_1|/|\ker(\varphi)|\,. \tag{15-13}$$

В частности, порядок ядра и порядок образа являются делителями порядка группы $|G_1|$. □

15.3.3. Пример: эпиморфизм $S_4 \twoheadrightarrow S_3$. Занумеруем три отрезка, соединяющие центры противоположных граней куба (на рис. 15◇9 — прозрачные, светлые и тёмные) цифрами 1, 2, 3 и сопоставим каждому вращению куба осуществляемую им перестановку этих отрезков. Получим гомоморфизм собственной группы куба в симметрическую группу S_3.

$$\varphi : \mathrm{SO}_{\text{куб}} \longrightarrow S_3 \tag{15-14}$$

Его ядро состоит из вращений, оставляющих на месте каждую из трёх перпендикулярных осей, проходящих через центры противоположных граней. Кроме тождественного преобразования, таких вращений имеется ровно три — повороты на $\pm 180°$ вокруг каждой из этих осей. Вместе с тождественным преобразованием они образуют группу, изоморфную группе двуугольника D_2 из примера n° 15.1.4. Поэтому $|\ker\varphi| = 4$, и по (15-13) $|\mathrm{im}\,\varphi| = 24/4 = 6 = |S_3|$.

Таким образом, φ эпиморфен, и прообраз каждой перестановки из S_3 должен состоять ровно из четырёх поворотов куба. Это действительно так: 8 поворотов на $\pm 120°$ вокруг диагоналей перейдут в два различных цикла длины

[1]это рассуждение поучительно сравнить с доказательством формулы для длины орбиты (теор. 15.1 на стр. 261)

3, а 6 поворотов на 180° вокруг осей, проходящих через середины противоположных рёбер и 6 поворотов на $\pm 90^\circ$ перейдут в три цикла длины 2.

Принимая во внимание изоморфизм (15-14) собственной группы с симметрической группой S_4, мы заключаем, что имеется сюрьективный гомоморфизм

$$S_4 \twoheadrightarrow S_3 \tag{15-15}$$

ядром которого являются 3 перестановки

$$(2,1,4,3)\,, \quad (3,4,1,2)\,, \quad (4,3,2,1)$$

циклового типа $\boxplus$ и тождественное отображение.

Упражнение 15.18. Явно опишите образ и прообраз каждой перестановки при гомоморфизме (15-15) .

15.3.4. Знакопеременные группы. Множество всех чётных перестановок составляет ядро знакового гомоморфизма

$$\mathrm{sgn} : S_n \twoheadrightarrow \{\pm 1\}\,,$$

и, тем самым, является подгруппой в S_n порядка $n!/2$. По историческим причинам[1] эта подгруппа называется n-той *знакопеременной группой* (или *группой чётных перестановок*) и обозначается[2]

$$A_n \overset{\text{def}}{=} \ker(\mathrm{sgn}) \subset S_n\,.$$

15.3.5. Пример: эпиморфизм$\mathbf{SO}_{\text{дод}} \twoheadrightarrow A_5$. На поверхности додекаэдра (см. рис. 15◇10) имеется ровно 5 кубов с вершинами в вершинах додекаэдра.

Упражнение 15.19. Убедитесь, что восьмивершинный шестигранник, образованный показанными на рис. 15◇10 диагоналями двенадцати граней додекаэдра, является кубом, и что таких кубов действительно 5.

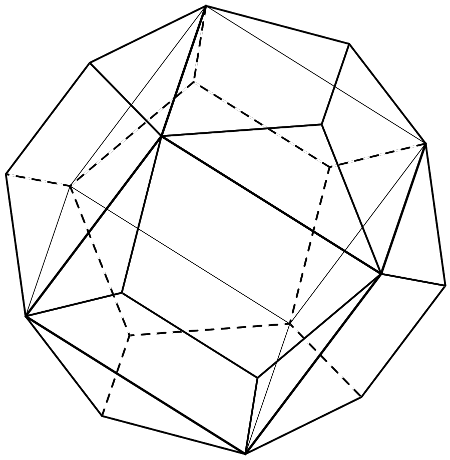


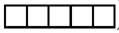
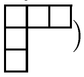
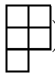
Рис. 15◇10. Один из пяти кубов, лежащих на додекаэдре.

Занумеруем эти кубы цифрами 1, 2, 3, 4, 5 и сопоставим каждому движению из группы додекаэдра осуществляемую им перестановку кубов. Мы получим гомоморфизм из группы додекаэдра в симметрическую группу S_5:

$$\psi_{\text{дод}} : \mathrm{SO}_{\text{дод}} \longrightarrow S_5 \tag{15-16}$$

Легко видеть (ср. с (n° 15.1.6)), что образами 60 поворотов при этом будут в точности 60 чётных перестановок: $6 \cdot 4 = 24$

[1]которые мы обсудим в следующем томе, когда будем изучать теорию Галуа
[2]использованная в обозначении буква «A» как раз и происходит из *alternate*

поворота на углы $2\pi k/5$ с $k = 1, 2, 3, 4$ вокруг осей, проходящих через центры противоположных граней додекаэдра, реализуют всевозможные циклы длины 5 (т. е. все 24 перестановки циклового типа ), $10 \cdot 2 = 20$ поворотов на углы $\pm 2\pi/3$ вокруг осей, проходящих через противоположные вершины додекаэдра, реализуют всевозможные циклы длины 3 (т. е. все 20 перестановок циклового типа ), 15 поворотов на 180° вокруг осей, проходящих через середины противоположных рёбер додекаэдра, реализуют всевозможные пары независимых транспозиций (т. е. все 10 перестановок циклового типа ); наконец, тождественное преобразование перейдёт в тождественную перестановку. Согласно n° 15.1.6, собственная группа додекаэдра исчерпывается шестьюдесятью перечисленными поворотами, а значит, гомоморфизм (15-16) является изоморфизмом между собственной группой додекаэдра и знакопеременной группой A_5.

Отметим, что в отличие от примера n° 15.1.5 переход от собственной группы додекаэдра к полной не добавляет новых перестановок кубов. В самом деле, гомоморфизм $\mathrm{O}_{\text{дод}} \longrightarrow S_5$ из полной группы додекаэдра в S_5, заданный тем же правилом, что и раньше, имеет нетривиальное ядро — центральная симметрия додекаэдра оставляет на месте каждый из кубов (в силу их центральной симметричности). Поэтому образ этого гомоморфизма совпадает с образом предыдущего гомоморфизма (15-16) и равен A_5, а прообраз каждой чётной перестановки кубов в $\mathrm{O}_{\text{дод}}$ состоит ровно из двух элементов: одного из перечисленных выше поворотов и композиции этого поворота с центральной симметрией додекаэдра.

Упражнение 15.20. Покажите, что симметрическая группа S_5 не изоморфна полной группе додекаэдра.

15.4. Действие группы на множестве. Пусть G — группа, а X — множество. Обозначим через $\mathrm{Aut}\,(X)$ группу всех взаимно однозначных отображений из X в себя.

Гомоморфизм $G \xrightarrow{\varphi} \mathrm{Aut}\,(X)$ называется *действием* группы G на множестве X или *представлением* группы G автоморфизмами множества X. Если понятно, о каком действии идёт речь, то результат применения отображения $\varphi(g) : X \longrightarrow X$ к точке $x \in X$ обозначается просто через gx.

Поскольку образ $\varphi(G) \subset \mathrm{Aut}\,(X)$ является группой преобразований, к нему применимо всё сказанное в n° 15.1.2 и n° 15.1.2. В частности, множество X распадается в дизъюнктное объединение орбит $Gx = \{gx \mid g \in G\}$ и в случае, когда группа G конечна, длина каждой орбиты Gx связана с порядком стабилизатора $\mathrm{Stab}_G(x) = \{g \in G \mid gx = x\}$ формулой $|Gx| \cdot |\mathrm{Stab}_G(x)| = |G|$. В частности, порядки стабилизаторов всех точек одной орбиты одинаковы.

Действие называется *свободным*, если каждый отличный от единицы элемент группы действует на X без неподвижных точек. Действие называется *транзитивным*, если любую точку множества X можно перевести в любую другую точку каким-нибудь преобразованием из группы G. Действие называется *точным* (или *эффективным*), если каждый отличный от единицы элемент группы действует на X нетождественным образом, т. е. если $\ker\varphi = 0$. Точное представление отождествляет G с группой преобразований $\varphi(G) \subset \mathrm{Aut}\,(X)$. Замечательно, что каждая группа обладает такой реализацией.

15.4.1. Пример: левое регулярное действие. Обозначим через X множество элементов группы G. Отображение $L : G \longrightarrow \mathrm{Aut}\,(X)$, сопоставляющее элементу $g \in G$ преобразование $L_g : X \xrightarrow{x\mapsto gx} X$ левого умножения на g, называется *левым регулярным действием* группы G на себе.

Это действие свободно и транзитивно. Первое означает, что равенство $gx = x$ возможно только при $g = e$, второе — что для любых $x, y \in G$ уравнение $y = gx$ разрешимо относительно g (оба этих факта устанавливаются умножением обеих частей соответствующего равенства справа на $x^{-1} \in G$).

Будучи свободным, левое регулярное действие точно. Тем самым, любая абстрактная группа может быть реализована как некоторая группа преобразований подходящего множества.

Например, левые регулярные представления числовых групп реализуют аддитивную группу $\mathbb{R}$ группой сдвигов $L_v : x \longmapsto x + v$ числовой прямой, а мультипликативную группу $\mathbb{R}^*$ — группой гомотетий $L_\lambda : x \longmapsto \lambda x$ проколотой прямой $\mathbb{R}^* = \mathbb{R} \smallsetminus \{0\}$.

Упражнение 15.21 (правое регулярное действие). Покажите, что сопоставление элементу $g \in G$ отображения $R_g : X_G \xrightarrow{x\mapsto xg^{-1}} X_G$ правого умножения на g^{-1} задаёт свободное транзитивное действие[1] группы G на себе.

15.4.2. Пример: присоединённое действие. Отображение

$$\mathrm{Ad} : G \longrightarrow \mathrm{Aut}\,(G)\,, \tag{15-17}$$

сопоставляющее элементу $g \in G$ автоморфизм Ad_g сопряжения элементом g

$$\mathrm{Ad}_g : G \xrightarrow{h\mapsto ghg^{-1}} G\,, \tag{15-18}$$

называется *присоединённым действием* группы G на себе. В отличие от левого сдвига L_g из предыдущего примера преобразование сопряжения Ad_g является *гомоморфизмом* из G в G.

Упражнение 15.22. Убедитесь в этом и проверьте, что отображение (15-17) тоже является гомоморфизмом групп.

Другое важное отличие присоединённого действия от регулярного заключается в том, что присоединённое действие, вообще говоря, не свободно и не точно. Например, если группа G абелева, все внутренние автоморфизмы (15-18) исчерпываются тождественным отображением, и ядро присоединённого действия в этом случае совпадает со всей группой.

[1] появление g^{-1} не случайно: проверьте, что сопоставление элементу $g \in G$ отображения правого умножения на g является не гомоморфизмом, а антигомоморфизмом (т. е. оборачивает порядок сомножителей в произведениях)

В общем случае $\ker(\mathrm{Ad})$ образовано такими $g \in G$, что $ghg^{-1} = h$ для всех $h \in G$. Последнее равенство равносильно равенству $gh = hg$ и означает, что g *коммутирует* со всеми элементами группы.

Подгруппа элементов, перестановочных со всеми элементами группы G называется *центром* группы G и обозначается

$$Z(G) = \{g \in G \mid \ \forall\, h \in G \ \ gh = hg\}\,.$$

Таким образом, ядро присоединённого действия — это центр группы G.

Образ присоединённого действия называется *группой внутренних автоморфизмов* группы G и обозначается $\mathrm{Int}(G) = \mathrm{Ad}_G = \mathrm{im}\,(\mathrm{Ad}) \subset \mathrm{Aut}\,(G)$. Автоморфизмы, не попавшие в образ присоединённого действия, называются *внешними*.

15.4.3. Пример: действие перестановок букв на словах. Зафиксируем какой-нибудь k-буквенный алфавит $A = \{a_1, a_2, \dots, a_k\}$ и рассмотрим множество X всех n-буквенных слов w, которые можно написать с его помощью. Иначе X можно воспринимать как множество всех отображений

$$w : \{1,\, 2,\, \dots\,,\, n\} \longrightarrow A\,.$$

Сопоставим каждой перестановке $\sigma \in S_n$ преобразование $w \mapsto w\sigma^{-1}$, которое переставляет буквы в словах так, как предписывает[1] σ. Таким образом, мы получили действие симметрической группы S_n на множестве слов.

Орбита слова $w \in X$ под действием этой группы состоит из всех слов, где каждая буква алфавита встречается столько же раз, сколько в слове w. Стабилизатор $\mathrm{Stab}(w)$ слова w, в котором буква a_i встречается m_i раз (для каждого $i = 1, \dots, k$), состоит из перестановок между собою одинаковых букв и имеет порядок $|\mathrm{Stab}(w)| = m_1! \cdot m_2! \cdot \,\cdots\, \cdot m_k!$. Таким образом, длина орбиты такого слова равна мультиномиальному коэффициенту

$$|S_n w| = \frac{|S_n|}{|\mathrm{Stab}(w)|} = \frac{n!}{m_1! \cdot m_2! \cdot \,\cdots\, \cdot m_k!} = \binom{n}{m_1 \dots m_k}\,.$$

Этот пример лишний раз показывает, что разные орбиты могут иметь разную длину, и порядки стабилизаторов точек из разных орбит могут быть разными.

15.4.4. Пример: классы сопряжённости в симметрической группе. Перестановка $\mathrm{Ad}_g(\sigma) = g\sigma g^{-1}$, сопряжённая перестановке $\sigma = (\sigma_1, \sigma_2, \dots, \sigma_n) \in S_n$, для каждого $i = 1, 2, \dots, n$ переводит $g(i)$ в $g(\sigma_i)$. Например, при сопряжении цикла $\tau = |i_1, i_2, \dots, i_k\rangle \in S_n$ перестановкой $g = (g_1, g_2, \dots, g_n)$ получится цикл $|g(i_1),\, g(i_2),\, \dots\,,\, g(i_k)\rangle$.

---

[1] т. е. переводит слово $w = a_{\nu_1} a_{\nu_2} \,\dots\, a_{\nu_n}$ в слово $a_{\nu_{\sigma^{-1}(1)}} a_{\nu_{\sigma^{-1}(2)}} \,\dots\, a_{\nu_{\sigma^{-1}(n)}}$, на i-том месте которого стоит та буква, номер которой в исходном слове w переводится перестановкой σ в номер i

Предложение 15.2

Орбиты присоединённого действия симметрической группы S_n на себе взаимно однозначно соответствуют n-клеточным диаграммам Юнга. Орбита, отвечающая диаграмме λ, состоит из всех перестановок циклового типа λ. Если диаграмма λ имеет m_i строк длины i (для каждого $i = 1, 2, \dots, n$), то порядок централизатора $C(\lambda)$ любой перестановки циклового типа λ равен

$$z_\lambda = 1^{m_1} \cdot m_1! \cdot 2^{m_2} \cdot m_2! \cdot \,\cdots\, \cdot n^{m_n} \cdot m_n! = \prod_{\alpha=1}^{n} m_\alpha!\alpha^{m_\alpha}$$

и длина присоединённой орбиты такой перестановки равна $n! \cdot z_\lambda^{-1}$.

Доказательство. Сопоставим произвольному заполнению диаграммы λ веса n неповторяющимися числами от 1 до n перестановку $\sigma \in S_n$ циклового типа λ, которая является произведением независимых циклов, слева направо циклически переставляющих элементы каждой строки заполнения. Действие внутреннего автоморфизма Ad_g на такую перестановку σ состоит в применении отображения g ко всем элементам заполнения, т. е. в замене каждого числа i числом g_i. Ясно, что таким образом можно получить любое заполнение диаграммы λ, т. е. присоединённая орбита состоит в точности из перестановок заданного циклового типа. Это доказывает первые два утверждения.

Вторые два утверждения следуют из того, что два заполнения диаграммы λ тогда и только тогда дают одну и ту же перестановку σ, когда они отличаются друг от друга независимыми циклическими перестановками элементов в строках и произвольными перестановками между собою строк одинаковой длины как единого целого. □

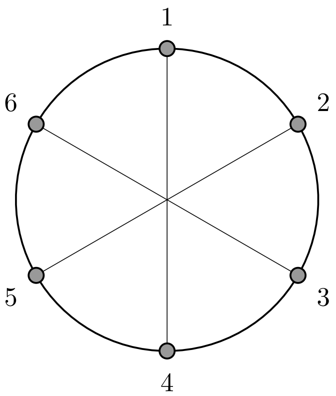
15.4.5. Пример: перечисление орбит. Подсчёт числа элементов в факторе X/G конечного множества X по действию конечной группы G наталкивается на очевидную трудность: поскольку длины у орбит могут быть разные, число орбит «разного типа» придётся подсчитывать по отдельности, заодно уточняя по ходу дела, что именно имеется в виду под «типом орбиты». Разом преодолеть обе эти трудности позволяет

Теорема 15.3 (формула Полиа – Бернсайда)

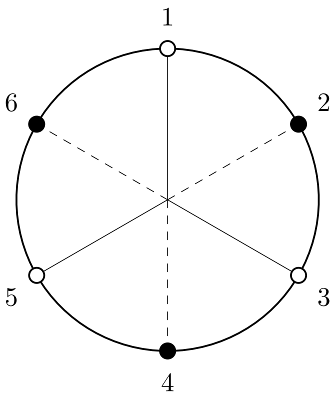
Пусть конечная группа G действует на конечном множестве X. Для каждого $g \in G$ обозначим через $X^g = \{x \in X \mid gx = x\} = \{x \in X \mid g \in \mathrm{Stab}(x)\}$ множество неподвижных точек преобразования g. Тогда $|X/G| = |G|^{-1} \sum\limits_{g\in G} |X^g|$.

Доказательство. Обозначим через $F \subset G \times X$ множество всех пар (g, x), таких что $gx = x$. Иначе F можно описать как $F = \bigsqcup\limits_{x\in X} \mathrm{Stab}(x) = \bigsqcup\limits_{g\in G} X^g$. Первое из этих описаний получается из рассмотрения проекции $F \longrightarrow X$, второе — из рассмотрения проекции $F \longrightarrow G$. Согласно второму описанию, $|F| = \sum\limits_{g\in G} |X^g|$.

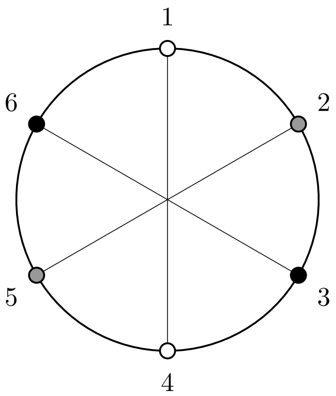
С другой стороны, из первого описания мы заключаем, что $|F| = |G| \cdot |X/G|$. В самом деле, стабилизаторы всех точек, принадлежащих одной орбите, имеют одинаковый порядок, и сумма этих порядков по всем точкам орбиты равна произведению порядка стабилизатора на длину орбиты, т. е. $|G|$. Складывая по всем орбитам, получаем $|F| = |G| \cdot |X/G| = \sum\limits_{g \in G} |X^g|$. $\square$



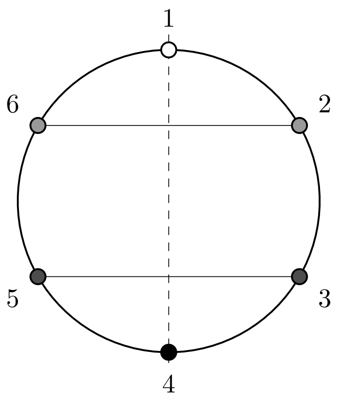
τ-инваринтные бусы



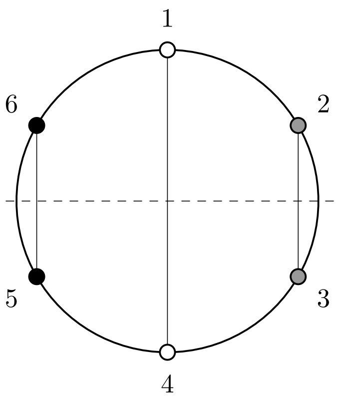
τ^2-инваринтные бусы



τ^3-инваринтные бусы



σ_{14}-симметричные бусы



$\overline{\sigma}_{14}$-симметричные бусы

Рис. 15◇11. Симметричные ожерелья из шести бусин.

15.4.6. Пример: ожерелья. Предположим у нас имеются одинаковые по форме бусины n различных цветов (количество бусин каждого цвета неограничено). Сколько различных ожерелий одинаковой формы можно сделать из 6 бусин? Ответом на этот вопрос является количество орбит группы диэдра D_6 на множестве всех раскрасок вершин правильного шестиугольника в n цветов.

Группа D_6 состоит из 12 элементов: тождественного преобразования e, двух поворотов $\tau^{\pm 1}$ на $\pm 60°$, двух поворотов $\tau^{\pm 2}$ на $\pm 120°$, центральной симметрии τ^3, трёх отражений σ_{14}, σ_{23}, σ_{36} относительно больших диагоналей и трёх отражений $\overline{\sigma}_{14}$, $\overline{\sigma}_{23}$, $\overline{\sigma}_{36}$ относительно срединных перпендикуляров к сторонам.

Единица оставляет на месте все n^6 раскрасок. Раскраски, симметричные относительно остальных преобразований, показаны на рис. 15◇11 ниже (одинаковым оттенкам серого отвечают одинаковые цвета). Беря на этих рисунках все допустимые сочетания цветов, получаем, соответственно, n, n^2, n^3, n^4 и n^3 раскрасок. По теор. 15.3 искомое число 6-бусинных ожерелий равно

$$\frac{1}{12} \cdot \left(n^6 + 3\,n^4 + 4\,n^3 + 2\,n^2 + 2\,n\right)$$

Упражнение 15.23. Подсчитайте количество ожерелий из 7, 8, 9, и 10 бусин.

Задачи для самостоятельного решения к §15

Задача 15.1. Докажите, что множество G с ассоциативной операцией композиции $G \times G \longrightarrow G$ является группой тогда и только тогда, когда $\forall\, a, b \in G$ уравнения $ax = b$ и $ya = b$ имеют единственные решения.

Задача 15.2 (группа кватернионных единиц). Определим на множестве

$$Q_8 = \{\pm e,\, \pm i,\, \pm j,\, \pm k\}$$

композицию так, что e является единицей, «минус на минус даёт плюс», и

$$\begin{array}{ccc} & i^2 = j^2 = k^2 = -e & \\ ij = k & jk = i & ki = j \\ ji = -k & kj = -i & ik = -j \end{array}$$

Покажите, что Q_8 является группой. Изоморфны ли Q_8 и D_4?

Задача 15.3. Перечислите все подгруппы в группах диэдров D_4 и D_6.

Задача 15.4. Покажите, что любая подгруппа циклической группы тоже циклическая.

Задача 15.5. Докажите следующие свойства порядков элементов группы G:
а) Если $g^m = \mathrm{Id}$, то $\mathrm{ord}\,(g)$ конечен и нацело делит m
б) $\forall\, f, g \in G$ $\mathrm{ord}\,(f) = \mathrm{ord}\,(gfg^{-1})$ в) $\forall\, n \in \mathbb{N}$ $\mathrm{ord}\,(g^n) = \mathrm{ord}\,(g)/\text{нод}(n, \mathrm{ord}\,(g))$
г) Если $fg = gf$, то $\mathrm{ord}\,(fg)$ нацело делит нок$(\mathrm{ord}\,(f), \mathrm{ord}\,(g))$.

Задача 15.6. Чему может быть равен $\mathrm{ord}\,(fg)$, если $\mathrm{ord}\,(gf) = n$?

Задача 15.7. Что можно сказать о чётности порядка произвольной нечётной перестановки?

Задача 15.8. Вычислите 100-ю степень перестановки $(3,\,5,\,4,\,1,\,2)$.

Задача 15.9. Сколько элементов $\mathfrak{S}_5$ неподвижно при сопряжении перестановкой $(3,\,5,\,1,\,2,\,4)$?

Задача 15.10. Покажите, что из любого элемента нечётного порядка в любой группе можно извлечь квадратный корень.

Задача 15.11 (инволютивные перестановки). Перестановка $\sigma \in S_n$ называется *инволютивной* (или просто *инволюцией*), если $\sigma^2 = \mathrm{Id}$. Покажите, что
а) перестановка инволютивна тогда и только тогда, когда в её цикловом типе встречаются только циклы длины 1 и циклы длины 2
б) любой цикл $\tau \in S_n$ длины $\geqslant 3$ является композицией двух инволюций.

Задача 15.12 (задача Н. Н. Константинова). В городе N разрешаются лишь простые двусторонние обмены квартир[1], причём в течение одного дня каждому жителю разрешается сделать не более одного обмена. Можно ли за два дня осуществить любой, сколь угодно сложный обмен?

Задача 15.13. Из игры «15» выковыряли фишки «1» и «2», поменяли их местами и засунули обратно. Удастся ли вернуть такую позицию в исходное положение, следуя правилам игры?

Задача 15.14. Покажите, что группа, все элементы которой имеют порядок два, абелева.

Задача 15.15. Приведите несколько различных примеров бесконечных групп, в которых каждый элемент имеет конечный порядок.

Задача 15.16. Говорят, что группа G порождается элементами $g_1, g_2, \ldots, g_k \in G$, если любой элемент G является произведением элементов g_i (возможно, с повторениями). Порождается ли а) группа S_n циклами $|1, 2\rangle$ и $|1, 2, 3, \ldots, n\rangle$?
б) знакопеременная группа A_n 3-циклами $|1, 2, 3\rangle$, $|1, 2, 4\rangle$, …, $|1, 2, n\rangle$?

---

[1] когда A въезжает в квартиру, принадлежавшую B, а B — в квартиру, принадлежавшую A; все более сложные обмены, скажем, когда A въезжает в квартиру, принадлежавшую B, B — в квартиру, принадлежавшую C, а уже C — в квартиру, принадлежавшую A, запрещены

Задача 15.17. Покажите, что любая конечная группа, порождённая двумя различными и отличными от единицы инволюциями[1], изоморфна группе диэдра.

Задача 15.18. Какие перестановки а) вершин тетраэдра б) диагоналей куба можно получить собственными движениями этих фигур?

Задача 15.19. Для каждого из пяти платоновых тел найдите длины орбит всех точек этого тела при действии на них собственной и несобственной группы тела и явно перечислите все орбиты, длина которых меньше порядка группы.

Задача 15.20. Найдите порядок собственной и несобственной группы 4-мерного а) куба б) кокуба[2] в) тетраэдра г) октаплекса[3].

Задача 15.21 (прямое произведение групп). Покажите, что произведение

$$F \times H = \{(f,h) \mid f \in F\,,\ h \in H\}$$

групп F и H является группой[4] относительно операции

$$(f_1,h_1)\cdot(f_2,h_2) \stackrel{\text{def}}{=} (f_1\cdot f_2\,,\,h_1\cdot h_2)$$

и докажите, что группа G изоморфна прямому произведению двух своих подгрупп $F,H \subset G$ если и только если выполнены следующие три условия:

1) $F \cap H = \{e\}$, где $e \in G$ — единичный элемент группы G;
2) $fh = hf \ \ \forall\, f \in F$ и $\forall\, h \in H$;
3) любой элемент $g \in G$ представим в виде $g = fh$ с $f \in F$ и $h \in H$.

Задача 15.22. При каких n группа диэдра D_n изоморфна $\mathbb{Z}/(2)\times\mathbb{Z}/(n)$?

Задача 15.23. Может ли прямое произведение $D_m \times \mathbb{Z}/(n)$ быть изоморфно D_{mn} ?

Задача 15.24. У каких платоновых тел полная группа изоморфна прямому произведению собственной группы на группу знаков $\{\pm 1\}$?

Задача 15.25. Выясните, какие из перечисленных групп изоморфны друг другу:
а) D_8 , $D_4 \times \mathbb{Z}/(2)$, $Q_8 \times \mathbb{Z}/(2)$
б) S_4 , D_{12} , $D_6 \times \mathbb{Z}/(2)$, $D_3 \times \mathbb{Z}/(2) \times \mathbb{Z}/(2)$, $D_3 \times \mathbb{Z}/(4)$, $Q_8 \times \mathbb{Z}/(3)$, $D_4 \times \mathbb{Z}/(3)$

Задача 15.26. Ясно, что конечные группы G и H, содержащие разное количество элементов порядка k (для какого-нибудь $k \in \mathbb{N}$), не могут быть изоморфны. Пусть при всех k число элементов порядка k в конечных группах G и H одинаково. Верно ли, что $G \simeq H$ для а) любых б) абелевых конечных групп G и H ?

[1] напомним, что *инволюцией* называется элемент с квадратом единица
[2] см. зад. 14.15
[3] см. зад. 14.16
[4] эта группа называется *прямым произведением* групп F и H

Задача 15.27. Симметрическая группа S_n стандартно действует на

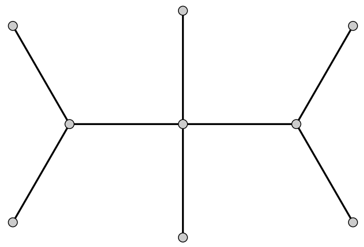
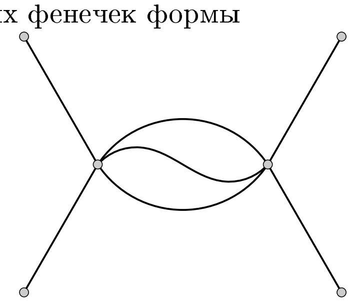
$$X = \{1,\, 2,\, \dots\,,\, n\}\,.$$

Опишите орбиты диагонального[1] действия S_n на а) X^2 б) X^3 (для $n \geqslant 3$) в) X^m (для $n \geqslant m$)

Задача 15.28. Собственная группа куба $\mathfrak{S}_4$ действует на множествах V (вершин) и E (рёбер) куба. Опишите орбиты диагонального действия $\mathfrak{S}_4$ на а) $V \times V$ б) $V \times E$ в) $E \times E \times E$

Задача 15.29. Сколько различных с виду бус получится из а) 4 б) 7 в) 8 г) 9 одинаковых по форме бусин n разных цветов[2]?

Задача 15.30. Сколько разных на вид верёвочных фенечек формы

а)  б) 

можно связать из неразличимых по длине и форме кусочков верёвок n различных цветов[3]?

Задача 15.31. Конечная группа транзитивно действует на множестве, содержащем более одного элемента. Верно ли, что всегда найдётся элемент группы, действующий без неподвижных точек?

[1]если G действует на множествах $X_1, X_2, \dots, X_m$, то *диагональное* действие G на $X_1 \times X_2 \times \dots \times X_m$ задаётся правилом $g : (x_1, x_2, \dots, x_m) \mapsto (gx_1, gx_2, \dots, gx_m)$

[2]запас бусин каждого из цветов неограничен

[3]запас нитей каждого из цветов неограничен

§16. Смежные классы

16.1. Теорема Лагранжа. С каждой подгруппой $H \subset G$ связано разбиение группы G в дизъюнктное объединение подмножеств вида

$$gH \overset{\text{def}}{=} \{gh \mid h \in H\}, \tag{16-1}$$

называемых *левыми смежными классами* (или *левыми сдвигами*) подгруппы H в группе G.

Предложение 16.1
Любые два смежных класса g_1H и g_2H либо не пересекаются либо совпадают. Последнее равносильно любому из условий: $g_1^{-1}g_2 \in H$, $g_2^{-1}g_1 \in H$.

Доказательство. Если $g_1h_1 = g_2h_2 \in g_1H \cap g_2H$, то оба элемента

$$g_1^{-1}g_2 = h_1h_2^{-1} \quad \text{и} \quad g_2^{-1}g_1 = h_2h_1^{-1}$$

лежат в H. С другой стороны, если хоть один из этих элементов лежит в H, то в H лежит и обратный к нему второй элемент, и тогда

$$g_1H = g_2\left(g_2^{-1}g_1\right)H \subset g_2H \quad \text{и} \quad g_2H = g_1\left(g_1^{-1}g_2\right)H \subset g_1H,$$

т. е. $g_1H = g_2H$. □

Упражнение 16.1. Зададим на группе G бинарное отношение $\underset{H}{\sim}$, полагая $g_1 \underset{H}{\sim} g_2$ тогда и только тогда, когда $g_1 = g_2h$ для некоторого $h \in H$. Покажите, что это эквивалентность, и получите отсюда другое доказательство предл. 16.1.

16.1.1. Индекс подгруппы. Множество левых смежных классов подгруппы $H \subset G$ обозначается G/H, а число элементов в нём (если оно конечно) называется *индексом* подгруппы H в группе G и иногда обозначается

$$[G:H] \overset{\text{def}}{=} |G/H|.$$

Теорема 16.1 (теорема Лагранжа об индексе подгруппы)
Порядок и индекс любой подгруппы H в произвольной конечной группе G нацело делят порядок группы и $[G:H] = |G| : |H|$.

Доказательство. Отображения левого умножения на обратные друг другу элементы $g_2g_1^{-1}$ и $g_1g_2^{-1}$:

$$g_1H \underset{L_{g_1g_2^{-1}}}{\overset{L_{g_2g_1^{-1}}}{\rightleftarrows}} g_2H$$

являются взаимно обратными биекциями. Поэтому все смежные классы состоят из одинакового числа элементов, равного $|eH| = |H|$. □

Упражнение 16.2. Ограничение правого регулярного представления из упр. 15.21 на подгруппу $H \subset G$ задаёт действие $R : H \hookrightarrow \mathrm{Aut}\,(X_G)$ подгруппы H на X_G правыми умножениями. Покажите, что орбиты этого действия суть левые смежные классы подгруппы H, и $\forall\, x \in X_G \;\; \mathrm{Stab}_H(x) = \{e\}$. Получите отсюда новые доказательства предл. 16.1 и теор. 16.1.

Следствие 16.1
Порядок любого элемента конечной группы нацело делит порядок группы.

Доказательство. Порядок элемента $g \in G$ равен порядку порождённой им циклической подгруппы $\langle g \rangle \subset G$. □

16.1.2. Правые смежные классы. Аналогичным образом можно рассмотреть разбиение группы G в дизъюнктное объединение *правых смежных классов* (или *правых сдвигов*)

$$Hg \overset{\text{def}}{=} \{hg \mid h \in H\}. \tag{16-2}$$

подгруппы $H \subset G$. Симметрично тому, как это было в упр. 16.2, правые смежные классы подгруппы H являются орбитами точного действия подгруппы H на множестве X_G левыми сдвигами:

$$L : H \hookrightarrow \mathrm{Aut}\,(X_G)\,,$$

при котором элемент $h \in H$ действует преобразованием $L_h : x \mapsto hx$.

Поскольку равенство $hx = x$ влечёт равенство $h = e$, стабилизаторы всех точек $x \in X_G$ состоят только из тождественного преобразования. Поэтому длины всех орбит левого регулярного действия подгруппы H на X_G равны $|H|$, и мы получаем «правую» версию теоремы Лагранжа: число правых смежных классов любой подгруппы H в любой конечной группе G равно $|G| : |H|$.

Упражнение 16.3. Сформулируйте и докажите для правых смежных классов аналог предл. 16.1.

16.2. Фактор группы. Попытка определить умножение на множестве левых смежных классов G/H неабелевой группы G формулой

$$(g_1H)\cdot(g_2H) \overset{\text{def}}{=} (g_1g_2)H\,, \tag{16-3}$$

вообще говоря, некорректна: различные записи $g_1H = f_1H$ и $g_2H = f_2H$ одних и тех же классов могут приводить к *различным* классам $(g_1g_2)H \neq (f_1f_2)H$.

Упражнение 16.4. Возьмем в качестве G группу треугольника S_3, а в качестве $H \subset G$ подгруппу второго порядка, состоящую из тождественного отображения и транспозиции σ_{12}. Покажите, что формула (16-3) в этом случае некорректна.

Умножение (16-3) иначе можно охарактеризовать как единственное возможное умножение левых смежных классов G/H, для которого *отображение факторизации* $G \xrightarrow{g \mapsto gH} G/H$, сопоставляющее каждому элементу группы задаваемый им левый смежный класс, является гомоморфизмом групп. Поэтому, если формула (16-3) корректна, подгруппа $H \subset G$ оказывается ядром гомоморфизма групп. Ядра гомоморфизмов групп обладают специальным дополнительным свойством, выделяющим их среди всех прочих подгрупп. А именно, если $\varphi : G_1 \longrightarrow G_2$ — гомоморфизм и $H = \ker \varphi$, то для любого $g \in G$ и любого $h \in H$ элемент ghg^{-1} лежит в H, поскольку

$$\varphi\left(ghg^{-1}\right) = \varphi(g)\varphi(h)\varphi\left(g^{-1}\right) = \varphi(g)e\varphi(g)^{-1} = e\,.$$

Тем самым, для любого $g \in G$ мы имеем включение $gHg^{-1} \subset H$. Беря в нём g^{-1} вместо g, получаем включение $g^{-1}Hg \subset H$, эквивалентное включению $H \subset gHg^{-1}$. Таким образом, $gHg^{-1} = H$ для всех $g \in G$.

Определение 16.1
Подгруппа $H \subset G$ называется *нормальной* (или *инвариантной*), если для любого $g \in G$ выполняется равенство $gHg^{-1} = H$, или (что то же самое) $gH = Hg$. Мы будем писать $H \lhd G$ вместо $H \subset G$, если H — нормальная подгруппа.

Предложение 16.2
Для того, чтобы правило $g_1H \cdot g_2H = (g_1g_2)H$ корректно определяло на G/H структуру группы, необходимо и достаточно, чтобы подгруппа H была нормальна в G.

Доказательство. Необходимость вытекает из предыдущего: если определение групповой структуры корректно, то отображение факторизации $G \twoheadrightarrow G/H$ является гомоморфизмом групп с ядром H, и значит, H нормальна.

Наоборот, пусть H нормальна, и пусть $f_1H = g_1H$ и $f_2H = g_2H$. Как мы видели в предл. 16.1, эти равенства означают, что элементы $h_1 = g_1^{-1}f_1$ и $h_2 = g_2^{-1}f_2$ оба лежат в H. Из нормальности H вытекает тогда, что элемент $g_2^{-1}h_1g_2$ тоже лежит в H. Умножая его справа на $h_2 \in H$, мы также получим элемент из H, т. е. $g_2^{-1}\left(g_1^{-1}f_1\right)g_2\left(g_2^{-1}f_2\right) = g_2^{-1}g_1^{-1}f_1f_2 = (g_1g_2)^{-1}(f_1f_2) \in H$. Следовательно, $(g_1g_2)H = (f_1f_2)H$, и произведение классов определено корректно. Все требуемые определением группы свойства этого произведения автоматически наследуются из G: ассоциативность умножения в G/H вытекает из ассоциативности в G

$$\begin{aligned}(g_1H \cdot g_2H) \cdot g_3H = (g_1g_2)H \cdot g_3H = ((g_1g_2)g_3)H = \\ = (g_1(g_2g_3))H = g_1H \cdot (g_2g_3)H = g_1H \cdot (g_2H \cdot g_3H)\,,\end{aligned}$$

единичным элементом в G/H является класс $eH = H$, обратным к классу gH является класс $g^{-1}H$. □

Определение 16.2
Множество смежных классов[1] G/H нормальной подгруппы $H \subset G$, наделённое групповой структурой (16-3), называется *фактором* (или *фактор группой*)

[1]мы не уточняем о каких смежных классах — левых или правых — идёт речь, поскольку у нормальной подгруппы левые смежные классы совпадают с правыми: $\forall g\in G \ \ gH = Hg$

группы G по нормальной подгруппе H. Гомоморфизм групп $G \xrightarrow{g \mapsto gH} G/H$ называется *гомоморфизмом факторизации*. Вложение нормальной подгруппы H в группу G обозначается символом $H \lhd G$.

Следствие 16.2
Любой гомоморфизм групп $G_1 \xrightarrow{\varphi} G_2$ является композицией эпиморфизма факторизации $G_1 \twoheadrightarrow G_1/\ker\varphi$ и мономорфизма $G_1/\ker\varphi \hookrightarrow G_2$, переводящего смежный класс $g\ker\varphi \in G_1/\ker\varphi$ в элемент $\varphi(g) \in G_2$.

Доказательство. Следствие утверждает, что слой $\varphi^{-1}(g_2)$ гомоморфизма φ над произвольной точкой $g_2 \in G_2$ является левым сдвигом ядра $\ker\varphi$ на какой-нибудь элемент $g_1 \in \varphi^{-1}(g_2)$. Это действительно так, поскольку

$$\varphi(f) = \varphi(g_1) \iff \varphi(g_1^{-1}f) = \varphi(g_1^{-1})\varphi(f) = e \iff g_1^{-1}f \in \ker\varphi\,,$$

а последнее условие означает, что $f \in g\ker\varphi$. □

16.2.1. Геометрический смысл нормальности. Согласно предыдущему, нормальность подгруппы $H \subset G$ означает существование гомоморфизма φ : $G \longrightarrow G'$ из группы G в какую-нибудь группу G', такой что $H = \ker\varphi$. Если группа G' реализована как группа преобразований какого-нибудь множества X (а такая реализация, как мы видели в n° 15.4.1, всегда существует — например, при помощи левого регулярного действия на себе), то мы имеем представление $G \longrightarrow \operatorname{Aut} X$ исходной группы G преобразованиями множества X, такое что H является ядром этого представления. Таким образом, подгруппа $H \subset G$ нормальна тогда и только тогда, когда имеется действие группы G на некотором множестве X, такое что H — это совокупность всех преобразований из G, которые оставляют на месте каждую точку X.

Например, собственная группа куба $\mathrm{SO}_{\text{куб}}$ действует на трёх отрезках, соединяющих центры противоположных граней куба. Ядро этого действия — диэдральная группа D_2, состоящая из тождественного преобразования и трёх поворотов на 180° вокруг проходящих через эти отрезки осей. Тем самым, $D_2 \subset \mathrm{SO}_{\text{куб}}$ нормальна, и $\mathrm{SO}_{\text{куб}}/D_2 \simeq S_3$.

Упражнение 16.5. Переговорите предыдущий абзац на языке перестановок, отождествив собственную группу куба с симметрической группой S_4.

16.2.2. Пример: аффинная группа и группа сдвигов. Для любого аффинного пространства A над векторным пространством V биективные аффинные отображения[1] $A \longrightarrow A$ образуют группу преобразований пространства A. Эта группа называется *аффинной группой* пространства A и обозначается $\mathrm{GA}(A)$. Отображение D, сопоставляющее аффинному отображению F его дифференциал DF

$$D : \mathrm{GA}(A) \longrightarrow \mathrm{GL}(V)$$

[1] см. n° 14.6.4

является сюрьективным гомоморфизмом групп. Его ядро $\ker D$ состоит из параллельных переносов. Тем самым, параллельные переносы образуют $\mathrm{GA}(A)$ нормальную подгруппу, изоморфную аддитивной группе векторного пространства V.

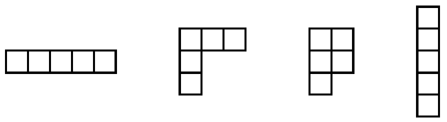
Упражнение 16.6. Покажите, что $F\tau_v F^{-1} = \tau_{DF(v)}$ для любого $F \in \mathrm{GA}(A)$ и любого $v \in V$.

16.3. Простые группы. Группа G называется *простой*, если она не содержит нормальных подгрупп, отличных от $\{e\}$ и G. Например, любая группа простого порядка проста, поскольку по теореме Лагранжа вообще не содержит никаких подгрупп кроме $\{e\}$ и G. Согласно предложению (сл. 15.2) простота группы G равносильна тому, что всякий гомоморфизм $G \longrightarrow G'$ либо является вложением, либо отображает всю группу G в единицу $e' \in G'$.

Одним из крупных достижений математики XX века было создание полного списка всех конечных простых групп. Этот список открывает бесконечная серия знакопеременных групп A_n с $n \geqslant 5$.

Предложение 16.3
Знакопеременная группа A_5 проста.

Доказательство. Пусть $H \lhd A_5$. Тогда вместе с каждой перестановкой $g \in H$ в подгруппу H войдут и все перестановки сопряжённые g в A_5. Как мы видели в n° 15.4.4, орбита перестановки g относительно присоединённого действия полной симметрической группе S_5 состоит из всех перестановок того же циклового типа, что и g. Поскольку g чётна, её диаграмма Юнга имеет чётное число строк чётной длины. Всего имеется 4 таких диаграммы веса 5:

 , (16-4)

отвечающие, соответственно, циклам длины 5, циклам длины 3, парам независимых транспозиций и тождественному преобразованию.

Если отождествить A_5 с группой вращений додекаэдра, как в n° 15.3.5, то эти классы превратятся, соответственно, в повороты на углы $2\pi k/5$ вокруг осей, проходящих через центры противоположных граней, повороты на углы $\pm 2\pi/3$ вокруг осей, проходящих через противоположные вершины, и повороты на $180°$ вокруг осей, проходящих через середины противоположных рёбер.

Поскольку любые две упорядоченные пары противоположных вершин додекаэдра переводятся друг в друга подходящим вращением, все повороты на $\pm 2\pi/3$ сопряжены между собою не только в S_5, но и в A_5. По тем же причинам сопряжены между собою в A_5 и все пары независимых транспозиций. А вот вращения пятого порядка очевидным образом распадаются на два разных класса: 12 сопряжённых вращений на углы $\pm\pi/5$ и 12 сопряжённых вращений на углы $\pm 2\pi/5$.

Упражнение 16.7. Покажите, что при действии группы S_5 на себе сопряжениями, стабилизатор любого цикла длины 5 не содержит нечётных перестановок, а стабилизаторы перестановок всех остальных перечисленных в (16-4) цикловых типов содержат нечётную перестановку. Выведите отсюда не использующее изоморфизм с группой додекаэдра доказательство того, что класс сопряжённости цикла длины 5 в S_5 распадается в A_5 на два класса, а остальные три класса из (16-4) остаются классами сопряжённости и в A_5.

Таким образом, в знакопеременной группе A_5 имеется ровно 5 классов сопряжённости: класс единицы, содержащий 1 элемент, класс циклов длины 3, содержащий 20 элементов, класс пар независимых транспозиций, содержащий 15 элементов, и два класса циклов длины 5, содержащие по 12 элементов. Поскольку $e \in H$, и любой из четырёх оставшихся классов либо входит в H целиком, либо не пересекается с H, порядок подгруппы H равен

$$|H| = 1 + 12\varepsilon_1 + 12\varepsilon_2 + 20\varepsilon_3 + 15\varepsilon_4\ , \tag{16-5}$$

где каждый из коэффициентов ε_k равен либо 1, либо 0. С другой стороны, по теор. 16.1 $|H|$ является делителем $|A_5| = 60$.

Упражнение 16.8. Убедитесь, что правая часть формулы (16-5) делит $60 = 3\cdot 4\cdot 5$ ровно в двух случаях: когда все $\varepsilon_k = 1$ или когда все $\varepsilon_k = 0$.

Таким образом, нормальные подгруппы в A_5 исчерпываются единичной подгруппой и всей группой A_5, что и требовалось установить. □

Упражнение 16.9. Докажите, что все знакопеременные группы A_n с $n > 5$ тоже просты.

16.4. p-группы. Группа порядка p^n, где $p \in \mathbb{N}$ — простое, называется *p-группой*. Поскольку все подгруппы p-группы также являются p-группами, длина любой орбиты p-группы при любом её действии на любом множестве либо делится на p, либо равна единице. Мы получаем простое, но полезное

Предложение 16.4

Пусть p-группа G действует на конечном множестве X, число элементов в котором не делится на p. Тогда G имеет на X неподвижную точку. □

Следствие 16.3

Любая p-группа имеет нетривиальный центр.

Доказательство. Рассмотрим присоединённое действие группы на себе. Центр группы представляет собой множество неподвижных точек этого действия. Поскольку и число элементов в группе, и длины всех орбит, содержащих более одной точки, делятся на p, кроме одноточечной орбиты e должны быть и другие одноточечные орбиты. □

Упражнение 16.10. Покажите, что любая группа G порядка p^2 (где p простое) абелева.

16.4.1. Силовские подгруппы. Пусть G — произвольная конечная группа. Запишем её порядок в виде $|G| = p^n m$, где p — простое, $n \geqslant 1$, и m взаимно просто с p. Всякая подгруппа $\mathfrak{S} \subset G$ порядка $|\mathfrak{S}| = p^n$ называется *силовской p-подгруппой* в G. Количество силовских p-подгрупп в G обозначается через $N_p(G)$.

Теорема 16.2 (теорема Силова)
Для любого простого p, делящего $|G|$, силовские p-подгруппы в G существуют. Все они сопряжены друг другу, и любая p-подгруппа в G содержится в некоторой силовской p-подгруппе.

Доказательство. Пусть $|G| = qm$, где $q = p^n$ и m взаимно просто с p. Обозначим через $\mathscr{E}_q$ множество q-элементных подмножеств в G и рассмотрим действие G на $\mathscr{E}_q$, индуцированное левым регулярным действием G на себе. Стабилизатор точки $F \in \mathscr{E}$ состоит из всех элементов $g \in G$, левое умножение на которые переводит множество $F \subset G$ в себя: $\mathrm{Stab}(F) = \{g \in G \mid gF \subset F\}$.

Лемма 16.1
$|\mathrm{Stab}(F)|$ делит $|F|$, и равенство $|\mathrm{Stab}(F)| = |F|$ равносильно тому, что F является правым смежным классом подгруппы $\mathrm{Stab}(F) \subset G$.

Доказательство. $\mathrm{Stab}(F)$ свободно действует на F, и каждая орбита этого действия состоит из $|\mathrm{Stab}(F)|$ точек, т. к. $g_1 x \neq g_2 x$ при $g_1 \neq g_2$. Поскольку F является дизъюнктным объединением орбит, $|F|$ делится на $|\mathrm{Stab}(F)|$. Равенство $|\mathrm{Stab}(F)| = |F|$ означает, что все точки F составляют одну орбиту, т. е. $F = \{gx \mid g \in \mathrm{Stab}(F)\} = \mathrm{Stab}(F) \cdot x$ есть правый сдвиг подгруппы $\mathrm{Stab}(F)$ на элемент $x \in F$. □

Лемма 16.2
$|\mathscr{E}_q| = \binom{p^n m}{p^n} \equiv m \pmod p$ (в частности, $|\mathscr{E}_q|$ не делится на p).

Доказательство. Класс вычетов $\binom{p^n m}{p^n} \pmod p$ равен коэффициенту при x^{p^n} в биноме $(1+x)^{p^n m}$, раскрытом над полем $\mathbb{F}_p = \mathbb{Z}/(p)$. Поскольку $(a+b)^p = a^p + b^p$ над $\mathbb{F}_p$, получаем

$$\begin{aligned}(1+x)^{p^n m} = \left((1+x)^p\right)^{p^{n-1}m} = (1+x^p)^{p^{n-1}m} = \\ = \left((1+x^p)^p\right)^{p^{n-2}m} = \left(1+x^{p^2}\right)^{p^{n-2}m} = \ \dots \\ \dots = \left(1+x^{p^n}\right)^m = 1 + mx^{p^n} + \text{ старшие степени}\end{aligned}$$

что и требовалось. □

Вернёмся к доказательству теоремы Силова. Согласно лем. 16.1, порядок $|\mathrm{Stab}(F)|$ стабилизатора произвольно взятой точки $F \in \mathscr{E}_q$ является делителем $q = p^n$. Если $|\mathrm{Stab}(F)| < q$, длина орбиты точки F делится на p. Поскольку $|\mathscr{E}_q|$

не делится на p, найдётся $F_s \in \mathscr{E}_q$ со стабилизатором порядка $|\mathrm{Stab}(F_s)| = q = |F_s|$. Тем самым, подгруппа $P = \mathrm{Stab}(F_s) \subset G$ — силовская.

Для доказательства остальных утверждений заметим, что длина орбиты GF_s рана m, так что стабилизатор любой точки этой орбиты — силовская p-подгруппа. Произвольная p-подгруппа $H \subset G$, действуя на GF_s, имеет по предл. 16.4 неподвижную точку $F \in GF_s$ и, тем самым, содержится в силовской p-подгруппе $\mathrm{Stab}(F)$. В частности, если H сама является силовской, мы получим равенство $H = \mathrm{Stab}(F)$, т. е. любая силовская подгруппа является стабилизатором некоторой точки из орбиты GF_s. Так как стабилизаторы всех точек одной орбиты сопряжены, все силовские подгруппы сопряжены. □

Следствие 16.4 (дополнение к теореме Силова)
В условиях теоремы Силова число N_p силовских p-подгрупп в G делит m и сравнимо с единицей по модулю p.

Доказательство. Обозначим множество силовских p-подгрупп в G через $\mathscr{S}$ и рассмотрим действие G на $\mathscr{S}$, индуцированное присоединённым действием G на себе. По теореме Силова это действие транзитивно, откуда $|\mathscr{S}| = |G|/|\mathrm{Stab}(P)|$, где $P \in \mathscr{S}$ — произвольно взятая силовская p-подгруппа. Поскольку $P \subset \mathrm{Stab}(P)$, порядок $|\mathrm{Stab}(P)|$ делится на $|P| = p^n$, а значит $|\mathscr{S}|$ делит $|G|/p^n = m$, что доказывает первое утверждение.

Для доказательства второго утверждения достаточно проверить, что P, действуя сопряжениями на $\mathscr{S}$, имеет там ровно одну неподвижную точку, а именно, саму себя. Тогда порядки всех остальных P-орбит будут делиться на p, и мы получим $|\mathscr{S}| \equiv 1 \pmod p$.

Пусть силовская подгруппа $H \in \mathscr{S}$ неподвижна при сопряжении подгруппой P. Это означает, что $P \subset \mathrm{Stab}(H) = \{g \in G \mid gHg^{-1} \subset H\}$. Поскольку $H \subset \mathrm{Stab}(H) \subset G$, порядок $|\mathrm{Stab}(H)| = p^n m'$, где $m'|m$ и взаимно просто с p. Таким образом, и P и H являются силовскими p-подгруппами в $\mathrm{Stab}(H)$, причём H нормальна в $\mathrm{Stab}(H)$. Так как все силовские подгруппы сопряжены, $H = P$, что и требовалось. □

16.4.2. Строение небольших групп часто удаётся полностью выяснить при помощи теоремы Силова и дополнения к ней.

Например, пусть $|G| = 15$. Тогда в G есть ровно одна силовская подгруппа $H_3 \simeq \mathbb{Z}/(3)$ порядка 3 и ровно одна силовская подгруппа $H_5 \simeq \mathbb{Z}/(5)$ порядка 5. Следовательно, обе они нормальны. Поскольку H_3 и H_5 к тому же ещё и просты $H_3 \cap H_5 = e$. Поэтому элементы ab с $a \in H_3$, $b \in H_5$ все различны. Наконец, $ab = ba$, т. к. $aba^{-1}b^{-1} \in H_5 \cap H_3 = e$. Следовательно, $G = \mathbb{Z}/(3) \times \mathbb{Z}/(5)$.

Ещё пример: опишем все группы G порядка 10. В G имеется ровно одна силовская подгруппа $H_5 \simeq \mathbb{Z}/(5)$ порядка 5, и она, тем самым, нормальна. Кроме того, в G может быть либо 1, либо 5 силовских подгрупп порядка 2, каждая из которых тривиально пересекается с H_5. Если подгруппа второго порядка одна, то мы, как и выше, получим $G \simeq \mathbb{Z}/(5) \times \mathbb{Z}/(2)$. Если двухэлементных подгрупп 5, обозначим одну из них через H_2 и посмотрим её присоединенное действие на нормальной подгруппе H_5.

Упражнение 16.11. Убедитесь, что группа $\mathrm{Aut}(\mathbb{Z}/(5)) \simeq \mathbb{Z}/(4)$ представляет собою циклическую группу, порождённую автоморфизмом, переводящим класс $[1] \in \mathbb{Z}/(5)$ в класс $[2] \in \mathbb{Z}/(5)$.

Присоединённое действие $H_2 \longrightarrow \mathrm{Aut}(H_5)$ переводит элемент $b \neq e$ из H_2 либо в тождественный эндоморфизм H_5, либо в автоморфизм второго порядка, каковой имеется ровно один — переводящий образующий элемент $a \in H_5$ в a^{-1}. В первом случае подгруппа H_2 коммутирует с подгруппой H_5, откуда $G = H_2 \times H_5 \simeq \mathbb{Z}/(5) \times \mathbb{Z}/(2)$. Во втором случае $bab^{-1} = a^{-1}$ и группа $G \simeq D_5$ — подгруппа H_5 представляет собой подгруппу поворотов, пять силовских подгрупп второго порядка порождаются пятью отражениями, сопряжёнными между собою посредством поворотов, и сопряжение любым отражением изменяет образующий поворот на обратный.

Задачи для самостоятельного решения к §16

Задача 16.1. Докажите, что любая группа простого порядка циклическая.

Задача 16.2. Верно ли, что в группе чётного порядка всегда существует элемент порядка 2?

Задача 16.3. Покажите, что симметрическая группа S_n при $n \geqslant 3$ имеет тривиальный центр: $Z(S_n) = \{e\}$ (в частности, присоединённое действие симметрической группы на себе является точным).

Задача 16.4. Пусть произведение любых двух левых смежных классов некоторой подгруппы H также является левым смежным классом подгруппы H. Покажите, что H нормальна.

Задача 16.5. Две нормальные подгруппы пересекаются по единице. Покажите, что их элементы коммутируют друг с другом.

Задача 16.6. Перечислите все нормальные подгруппы групп: а) D_3 б) D_4 в) Q_8 и опишите фактор группы по каждой из них.

Задача 16.7. Перечислите все подгруппы симметрической группы S_4, выясните, какие из них нормальны, и опишите соответствующие фактор группы.

Задача 16.8. Рассмотрим группу G всех движений евклидовой плоскости $\mathbb{R}^2$ и обозначим через σ_ℓ и $T_{p,\alpha}$ осевую симметрию относительно прямой ℓ и поворот на угол α вокруг точки $p \in \mathbb{R}^2$. Убедитесь, что $g\sigma_\ell g^{-1} = \sigma_{g(\ell)}$ и $gT_{p,\alpha}g^{-1} = T_{g(p),\alpha}$ для любого собственного движения $g \in G$. Что изменится, если движение g будет несобственным?

Задача 16.9 (простота группы SO_3). Рассмотрим группу $SO_3(\mathbb{R})$ всех вращений евклидова векторного пространства $\mathbb{R}^3$ и для каждой пары $v \in \mathbb{R}^3$, $\varphi \in \mathbb{R}$ обозначим через $R_{v,\varphi} \in SO_3(\mathbb{R})$ поворот вокруг оси, содержащей вектор v на угол φ по ЧС, если смотреть в направлении вектора v. Покажите, что $FR_{v,\varphi}F^{-1} = R_{Fv,\varphi}$ для любого $F \in SO_3$, и выведите отсюда, что группа SO_3 проста.

Задача 16.10. Приведите пример двух неизоморфных групп G_1 и G_2 и их нормальных подгрупп $H_1 \lhd G_1$ и $H_2 \lhd G_2$, таких что $G_1/H_1 \simeq G_2/H_2$.

Задача 16.11. Известно, что любая подгруппа конечной группы G нормальна. Верно ли, что G абелева?

Задача 16.12. Докажите, что любая группа порядка $2p$, где p — нечётное простое число, либо является циклической, либо изоморфна группе диэдра D_p.

Задача 16.13. Покажите, что число подгрупп группы G, сопряженных данной подгруппе $H \subset G$, равно индексу её *нормализатора* $N(H) = \{g \in G \mid gHg^{-1} = H\}$.

Задача 16.14. Перечислите классы сопряжённых элементов с указанием числа элементов в каждом классе для знакопеременных групп а) $\mathfrak{A}_3$ б) $\mathfrak{A}_4$ в) $\mathfrak{A}_6$. Какие классы сопряжённости в S_n распадаются на несколько классов сопряжённости в A_n?

Задача 16.15. Покажите, что подгруппа внутренних автоморфизмов нормальна в группе всех автоморфизмов.

Задача 16.16. Докажите, что внутренние автоморфизмы знакопеременной группы A_5 составляют подгруппу индекса 2 в группе всех автоморфизмов группы A_5.

Задача 16.17*. Постройте внешний автоморфизм симметрической группы[1] S_6.

Задача 16.18. Опишите группы автоморфизмов следующих групп:
а) $\mathbb{Z}/(n)$ б) $\mathbb{Z}/(2) \times \mathbb{Z}/(2)$ в) D_3 г) D_4 д) Q_8 (см. зад. 15.2).
У каких из этих групп все автоморфизмы являются внутренними?

Задача 16.19. Докажите, что любая подгруппа, индекс которой равен наименьшему простому числу, делящему порядок группы нормальна (в частности, любая подгруппа индекса 2 нормальна, в группе нечётного порядка любая подгруппа индекса 3 нормальна и т. д.).

Задача 16.20. Перечислите (с точностью до изоморфизма) все группы порядка $\leqslant$ 15.

[1]подсказка: найдите в S_6 два разных класса сопряжённости, состоящие из одинакового числа элементов, и попытайтесь «переставить» их друг с другом подходящим автоморфизмом

§17. Ортогональная геометрия над произвольным полем

17.1. Билинейные формы. Пусть V — векторное пространство над произвольным полем $\Bbbk$. Отображение

$$\beta : V \times V \xrightarrow{(u,w)\mapsto\beta(u,w)} \Bbbk\,,$$

линейное по каждому из двух аргументов при фиксированном другом, называется *билинейной формой* на пространстве V. Билинейные формы на V образуют векторное подпространство в пространстве всех функций $V \times V \longrightarrow \Bbbk$.

Примером билинейной формы является скалярное произведение на вещественном евклидовом пространстве из n° 14.1.

Пусть на пространствах V_1 и V_2 заданы билинейные формы β_1 и β_2. Линейное отображение $V_1 \xrightarrow{f} V_2$ называется *изометрическим* (или *гомоморфизмом билинейных форм*), если $\beta_1(v,w) = \beta_2(f(v), f(w))\ \forall\, v, w \in V_1$. Билинейные формы β_1 и β_2 называются *изоморфными*, если между пространствами V_1 и V_2 имеется изометрический изоморфизм.

17.1.1. Матрицы Грама. Как и в евклидовом пространстве, у любого набора векторов $v_1, v_2, \dots, v_m$ на пространстве V с билинейной формой β имеется *матрица Грама*, представляющая собою таблицу значений формы на парах векторов из этого набора[1]: $B_v = \big(\beta(v_\mu, v_\nu)\big)$. Если один набор векторов линейно выражается через другой как $w = v\,C_{vw}$, то матрица Грама B_w пересчитывается через матрицу Грама B_v по формуле

$$B_w = C_{vw}^t G_v C_{vw}\ , \tag{17-1}$$

где C_{vw}^t обозначает матрицу, транспонированную к C_{vw}.

Упражнение 17.1. Докажите это.

Пусть форма α на пространстве U имеет в базисе u матрицу Грама A, форма β на W имеет в базисе w матрицу B, а линейный изоморфизм $f : U \xrightarrow{\sim} W$ имеет в базисах u и w матрицу F_{wu}. Изометричность F равносильна равенству $\alpha\,(u_i, u_j) = \beta\,(f(u_i), f(u_j))$, которое утверждает, что матрица A равна матрице Грама формы β в базисе $f(u) = w\,F_{wu}$. Таким образом, f является изоморфизмом форм α и β тогда и только тогда, когда $A = F_{wu}^t B F_{wu}$. В частности, изоморфность двух форм на одном и том же пространстве V означает, что их матрицы Грама A и B, записанные в одном и том же базисе, связаны соотношением $A = C^t B C$ для некоторого $C \in \mathrm{GL}(V)$.

Для каждого базиса $e = (e_1, e_2, \dots, e_n)$ в V отображение $\beta \mapsto B_e$, сопоставляющее каждой билинейной форме её матрицу Грама в базисе e, является изоморфизмом пространства билинейных форм с пространством квадратных матриц

[1] здесь и далее для обозначений матриц Грама билинейных форм $\alpha, \beta, \gamma, \dots$ мы используем соответствующие большие буквы A, B, Γ, …

размера $n \times n$. В самом деле, это отображение линейно, и для любой матрицы $B \in \mathrm{Mat}_n(\Bbbk)$ существует единственная билинейная форма β с $B_e = B$. Значение такой формы на любой паре векторов $u = \sum\limits_i x_i e_i$ и $w = \sum\limits_j y_j e_j$ однозначно определяется по билинейности через её значения на базисных векторах:

$$\beta(u,w) = \beta\Big(\sum_i x_i e_i\,,\,\sum_j y_j e_j\Big) = \sum_{ij} b_{ij} x_i y_j = x^t B y \tag{17-2}$$

где $b_{ij} = \beta(e_i, e_j)$ суть элементы матрицы Грама B, а через x^t и y обозначены, соответственно, строка и столбец координат векторов $u = ex$ и $w = eu$.

Предложение 17.1
Пространство билинейных форм на n-мерном векторном пространстве имеет размерность n^2. □

17.1.2. Корреляции. Каждая билинейная форма определяет два линейных отображения

$$\begin{aligned} L_\beta \,:\, V &\xrightarrow{v\mapsto\beta(v,*)} V^* \\ R_\beta \,:\, V &\xrightarrow{v\mapsto\beta(*,v)} V^* \end{aligned} \tag{17-3}$$

называемые *левой* и *правой корреляциями* билинейной формы β.

Предложение 17.2
Отображения $L : \beta \mapsto L_\beta$ и $R : \beta \mapsto R_\beta$ являются изоморфизмами пространства билинейных форм на V с пространством линейных операторов $V \longrightarrow V^*$. Композиция $LR^{-1} = RL^{-1} : \mathrm{Hom}(V, V^*) \xrightarrow{\sim} \mathrm{Hom}(V, V^*)$ переводит оператор $\varphi : V \longrightarrow V^*$ в двойственный оператор $\varphi^* : V^{**} = V \longrightarrow V^*$.

Доказательство. Зафиксируем базис e в V и двойственный базис e^* в V^* и сопоставим каждой билинейной форме β на V её матрицу Грама B_e в базисе e, а каждому оператору $\varphi : V \longrightarrow V^*$ его матрицу $\varPhi_{e^*e}$, в j-том столбце которой стоит столбец координат вектора $\varphi(e_j)$ в базисе e^*. Все утверждения немедленно вытекают из того, что матрицы операторов R_β и L_β суть B_e и B_e^t соответственно. □

Предложение 17.3 (критерии невырожденности)
Следующие условия на билинейную форму $\beta : V \times V \longrightarrow \Bbbk$ с матрицей Грама B_e в некотором базисе $e = (e_1, e_2, \dots, e_n)$ пространства V эквивалентны:

1) $\det B_e \neq 0$

2) для любого ненулевого $u \in V$ $\exists\, w \in V : \beta(u,w) \neq 0$

3) левая корреляция $L_\beta : V \longrightarrow V^*$ является изоморфизмом

4) любой функционал $\xi : V \longrightarrow \Bbbk$ представим в виде $\xi(v) = \beta(u_\xi, v)$ для некоторого $u_\xi \in V$

5) для любого ненулевого $w \in V$ $\exists\, u \in V : \beta(u, w) \neq 0$

6) правая корреляция $R_\beta : V \longrightarrow V^*$ является изоморфизмом

7) любой функционал $\xi : V \longrightarrow \Bbbk$ представим в виде $\xi(v) = \beta(v, w_\xi)$ для некоторого $w_\xi \in V$.

В частности, если условие (1) выполнено для какого-то базиса e, то оно выполнено и для любого другого базиса, а векторы u_ξ и w_ξ в (4) и (7), если существуют, то единственны.

Доказательство. Поскольку $\dim V = \dim V^*$, условия (2) и (4), означающие, соответственно, что $\ker L_\beta = 0$ и что $\operatorname{im} L_\beta = V^*$, равносильны условию (3). По той же причине эквивалентны друг другу и условия (5), (6), (7). Поскольку матрицы операторов L_β и R_β в двойственных друг другу базисах e и e^* суть B_e^t и B_e, невырожденность операторов L_β и R_β равносильна тому, что $\det B_e^t = \det B_e \neq 0$. □

17.1.3. Ядра и ортогоналы. Билинейная форма β, удовлетворяющая условиям предл. 17.3 называется *невырожденной*. В противном случае форма называется *вырожденной*.

Отметим, что если форма β вырождена, то *обе* её корреляции имеют ненулевые ядра

$$\ker L_\beta = \{u \in V \mid \beta(u, v) = 0 \;\; \forall\, v \in V\}$$
$$\ker R_\beta = \{u \in V \mid \beta(v, u) = 0 \;\; \forall\, v \in V\},$$

называемые, соответственно, *левым* и *правым* ядром билинейной формы β. Вообще говоря, это *разные* подпространства в V. Но размерность у них одинакова, поскольку матрицы L_β и R_β транспонированы друг другу.

Невырожденные формы ведут себя во многом похоже на скалярное произведение. Например, для любого базиса $e = (e_1, e_2, \dots, e_n)$ пространства V прообразы векторов двойственного базиса $e^* = (e_1^*, e_2^*, \dots, e_n^*)$ пространства V^* относительно левой и правой корреляций дадут два базиса в V

$$^{\vee}e = (^{\vee}e_1, {}^{\vee}e_2, \dots, {}^{\vee}e_n) \quad \text{и} \quad e^{\vee} = (e_1^{\vee}, e_2^{\vee}, \dots, e_n^{\vee}) \tag{17-4}$$

двойственные слева и *справа* к исходному базису e относительно формы β в том смысле, что

$$\beta\left(^{\vee}e_i, e_j\right) = \beta\left(e_i, e_j^{\vee}\right) = \begin{cases} 1 & \text{при } i = j \\ 0 & \text{при } i \neq j\,. \end{cases} \tag{17-5}$$

Они выражаются через базис e по формулам ${}^{\vee}e = e\,B_e^{-1\,t}$ и $e^{\vee} = e\,B_e^{-1}$. Знание двойственного базиса позволяет раскладывать произвольный вектор $v \in V$ по базису e как

$$v = \sum_{\nu} \beta\,({}^{\vee}e_{\nu}, v) \cdot e_{\nu} = \sum_{\nu} \beta\,(v, e_{\nu}^{\vee}) \cdot e_{\nu} \tag{17-6}$$

(в чём легко убедиться применив к обеим частям функционалы $\beta\,({}^{\vee}e_{\nu}, *)$ и $\beta\,(*\,, e_{\nu}^{\vee})$ соответственно).

Для подпространства $U \subset V$ обозначим через

$$\begin{aligned} {}^{\perp}U &= \{v \in V \mid \beta(v,u) = 0 \;\; \forall\, u \in U\}\,, \\ U^{\perp} &= \{v \in V \mid \beta(u,v) = 0 \;\; \forall\, u \in U\} \end{aligned}$$

левый и *правый ортогоналы* к U. Отметим, что это, вообще говоря, *разные* подпространства в V.

Предложение 17.4

Если ограничение формы β на конечномерное подпространство $U \subset V$ невырождено, то $V = {}^{\perp}U \oplus U = U \oplus U^{\perp}$. Для произвольного вектора $v \in V$ его левая ортогональная проекция $v_{л} \in U$ вдоль ${}^{\perp}U$ и правая ортогональная проекция $v_{п} \in U$ вдоль $U^{\perp}$ однозначно определяются тем, что

$$\beta(v,w) = \beta(v_{л}, w) \quad \text{и} \quad \beta(w,v) = \beta(w, v_{п}) \qquad \forall\, w \in U\;, \tag{17-7}$$

и вычисляются через пары двойственных относительно формы β базисов пространства U по формулам

$$v_{л} = \sum_{\nu} \beta\,(v, u_{\nu}^{\vee}) \cdot u_{\nu} \quad \text{и} \quad v_{п} = \sum_{\nu} \beta\,({}^{\vee}u_{\nu}, v) \cdot u_{\nu}\,. \tag{17-8}$$

Доказательство. Мы докажем утверждения про левый ортогонал, для правого ортогонала всё аналогично. Поскольку ограничение формы β на U невырождено, для любого $v \in V$ ограничение на U функционала левого скалярного умножения на v: $u \longmapsto \beta(v,u)$ допускает представление в виде левого скалярного умножения на некоторый вектор $v_{л} \in U$, который однозначно определяется по v. Тогда для любого $u \in U$ мы имеем равенство $\beta(v,u) = \beta(v_{л}, u)$, которое равносильно равенству $\beta(v - v_{л}, u) = 0$. Тем самым, любой вектор $v \in V$ допускает единственное представление в виде $v = v_{л} + (v - v_{л})$ с $v_{л} \in U$ и $v - v_{л} \in {}^{\perp}U$, т. е. $V = U \oplus {}^{\perp}U$. Наконец, поскольку $\beta(v, u_i^{\vee}) = \beta(v_{л}, u_i^{\vee})$, разложение вектора $v_{л}$ по формуле (17-6) имеет вид $v_{л} = \sum_{\nu} \beta\,(v_{л}, u_{\nu}^{\vee}) \cdot u_{\nu} = \sum_{\nu} \beta\,(v, u_{\nu}^{\vee}) \cdot u_{\nu}\,.$ $\square$

17.1.4. (Косо) симметричные формы. Билинейная форма β называется *симметричной*, если

$$\forall\, v, w \in V \quad \beta(v,w) = \beta(w,v)$$

и *кососимметричной*, если

$$\forall\, v, w \in V \quad \beta(v,w) = -\beta(w,v)$$

(Косо) симметричность формы означает (косо) симметричность её матрицы Грама в каком-нибудь (а значит, и в любом) базисе.

Упражнение 17.2. Покажите, что если $\forall\, v \in V\ \beta(v,v) = 0$, то форма β кососимметрична, а если $\operatorname{char}(\Bbbk) \neq 2$, то верно и обратное.

Произвольная билинейная форма β однозначно представляется в виде суммы симметричной и кососимметричной форм:

$$\beta(v,w) = \beta_+(v,w) + \beta_-(v,w)\,, \quad \text{где}$$
$$\beta_+(v,w) = (\beta(v,w) + \beta(w,v))/2\,, \quad \beta_-(v,w) = (\beta(v,w) - \beta(w,v))/2\,,$$

Тем самым, пространство билинейных форм на V является прямой суммой подпространств симметричных и кососимметричных форм.

Упражнение 17.3. Вычислите размерности этих подпространств при $\dim V = n$.

Если форма β на V (косо) симметрична, то левый ортогонал к любому подпространству $U \subset V$ совпадает с правым:

$${}^\perp U = U^\perp = \{ w \in V \mid \beta(w,u) = \pm\beta(u,w) = 0 \ \ \forall\, u \in U \}$$

В частности, левое и правое ядра (косо) симметричной формы равны друг другу и называются просто *ядром* (косо) симметричной формы β:

$$\ker\beta = {}^\perp V = V^\perp = \{ w \in V \mid \beta(w,v) = \pm\beta(v,w) = 0 \ \forall\, v \in V \}\,.$$

Предложение 17.5
Ограничение (косо) симметричной формы β на любое дополнительное к её ядру подпространство $U \subset V$ невырождено.

Доказательство. Пусть $U \subset V$ таково, что $V = \ker\beta \oplus U$. Если $w \in U$ лежит в ядре ограничения $\beta|_U$, т. е. удовлетворяет $\forall\, u \in U$ соотношению $\beta(w,u) = 0$, то записывая произвольный вектор $v \in V$ в виде $v = e + u$ с $e \in \ker\beta$, $u \in U$ мы получим $\beta(w,v) = \beta(w,e) + \beta(w,u) = 0$, т. е. $w \in U \cap \ker\beta = 0$. □

Упражнение 17.4. Покажите, что для произвольных форм предложение неверно. Точнее, проверьте, что если $V = \ker L_\beta \oplus U = \ker R_\beta \oplus W$, то ограничение левой корреляции $V \xrightarrow{L_\beta} V^*$ на подпространство U устанавливает изоморфизм U с W^*, а не с U^*.

Всюду далее мы предполагаем, что $\operatorname{char}(\Bbbk) \neq 2$.

17.2. Симметричные билинейные и квадратичные формы. Зафиксируем в векторном пространстве V над полем $\Bbbk$ некоторый базис $e_1, e_2, \dots, e_n$ и будем обозначать через $(x_1, x_2, \dots, x_n)$ координаты векторов $v \in V$ в этом базисе. Каждый многочлен $f \in \Bbbk[x_1, x_2, \dots, x_n]$ определяет тогда функцию

$$V \xrightarrow{f} \Bbbk \,:\, a = \sum \alpha_i e_i \longmapsto f(a) = f(\alpha_1, \alpha_2, \dots, \alpha_n)\,,$$

значение которой на векторе $a = \sum \alpha_i e_i$ равно результату подстановки $x = \alpha$ в многочлен f.

Упражнение 17.5. Покажите, что сопоставление многочлену f описанной выше функции $a \mapsto f(a)$ является гомоморфизмом из кольца $\Bbbk[x_1, x_2, \dots, x_n]$ в кольцо функций $V \xrightarrow{\Bbbk}$, причём образ этого гомоморфизма не зависит от выбора базиса (хотя сам гомоморфизм существенно от него зависит). Докажите, что этот гомоморфизм инъективен[1] тогда и только тогда, когда поле $\Bbbk$ бесконечно.

Функции $q : V \longrightarrow \Bbbk$, задаваемые однородными многочленами второй степени, называются *квадратичными формами* на пространстве V.

Упражнение 17.6. Покажите, что свойство функции $q : V \longrightarrow \Bbbk$ быть квадратичной формой не зависит от выбора базиса.

Если $\operatorname{char}(\Bbbk) \neq 2$, квадратичную форму q удобно записывать в виде

$$q(x) = \sum_{i,j} x_i q_{ij} x_j = x \cdot Q \cdot x^t\,, \tag{17-9}$$

где суммирование происходит по всем парам индексов $1 \leqslant i, j \leqslant n$ и коэффициенты q_{ij} организованы в симметричную матрицу $Q = (q_{ij})$ размера $n \times n$ так, что при $i \neq j$ величина $q_{ji} = q_{ij}$ равна *половине*[2] фактического коэффициента при $x_i x_j$, получающегося после приведения подобных слагаемых. Из такой записи видно, что квадратичная форма $q : V \longrightarrow \Bbbk$, задаваемая многочленом (17-9) является ограничением на диагональ $\Delta = \{(v, v)\} \subset V \times V$ *симметричной билинейной* формы $\widetilde{q} : V \times V \longrightarrow \Bbbk$ с матрицей Грама Q, т. е.

$$q(v) = \widetilde{q}(v, v)\,.$$

Билинейная форма $\widetilde{q}$ называется *поляризацией* многочлена q. Отображение, сопоставляющее симметричной билинейной форме $\widetilde{q}(u, w)$ квадратичную форму $q(v) = \widetilde{q}(v, v)$ является линейным изоморфизмом пространства симметричных билинейных форм с пространством квадратичных форм. В самом деле, поляризация $\widetilde{q}$ однозначно восстанавливается по квадратичному многочлену q по формулам

$$\widetilde{q}(v, w) = \big(q(v + w) - q(v) - q(w)\big)/2 = \big(q(v + w) - q(v - w)\big)/4\,. \tag{17-10}$$

[1] т. е. разным многочленам отвечают разные функции на V

[2] над полем характеристики 2 многочлен $x_1 x_2$ в таком виде не записывается

Упражнение 17.7. Проверьте это и покажите, что $\widetilde{q}(x,y) = \frac{1}{2}\sum\limits_i y_i \frac{\partial q(x)}{\partial x_i}$.

Мы будем называть матрицу Q из представления (17-9) *матрицей Грама* квадратичного многочлена q. Поскольку ранг матрицы не меняется при её умножении на обратимую матрицу, ранг матрицы Грама не зависит от выбора базиса. Он называется *рангом квадратичной формы* q.

Теорема 17.1 (теорема Лагранжа)
Для любой симметричной билинейной формы $\widetilde{q}$ на пространстве V над любым полем $\Bbbk$ характеристики $\operatorname{char}(\Bbbk) \neq 2$ в V существует базис с диагональной матрицей Грама.

Доказательство. Если $\dim V = 1$ или $\widetilde{q}$ тождественно равна 0, то матрица Грама уже диагональна. Если $\widetilde{q} \not\equiv 0$, то отвечающий форме $\widetilde{q}$ квадратичный многочлен $q(v) = \widetilde{q}(v,v)$ согласно (17-10) тоже не является тождественным нулём, и найдётся вектор $e \in V$, такой что $\widetilde{q}(e,e) \neq 0$. Возьмем его в качестве первого вектора искомого базиса. Поскольку ограничение формы $\widetilde{q}$ на одномерное пространство $\Bbbk \cdot e$ невырождено, V по предл. 17.4 распадается в прямую ортогональную сумму $(\Bbbk \cdot e) \oplus e^{\perp}$, где $e^{\perp} = \{\, v \in V \mid \widetilde{q}(e,v) = 0 \,\}$. По индукции, в $e^{\perp}$ существует базис с диагональной матрицей Грама. Добавляя к нему e, получаем нужный базис в V. $\square$

Следствие 17.1
Всякая квадратичная форма над любым полем $\Bbbk$ характеристики $\operatorname{char}(\Bbbk) \neq 2$ линейной обратимой заменой переменных приводится к виду $\sum a_i x_i^2$.

Следствие 17.2
Над алгебраически замкнутым полем $\Bbbk$ характеристики $\operatorname{char}(\Bbbk) \neq 2$ две квадратичные формы тогда и только тогда переводятся одна в другую линейной обратимой заменой координат, когда их матрицы Грама имеют одинаковый ранг.

Доказательство. Над алгебраически замкнутым полем ненулевые диагональные элементы матрицы Грама преобразуются в единицы заменой базисных векторов по формуле $e_i \mapsto e_i/\sqrt{q(e_i)}$. Количества единиц и нулей на главной диагонали такой матрицы равны рангу формы и размерности её ядра и не зависят от выбора базиса. Поэтому любые две формы одинакового ранга обратимой линейной заменой координат приводятся к одинаковому виду $\sum x_i^2$. $\square$

17.2.1. Определитель Грама. Над алгебраически незамкнутым полем отнормировать ортогональный базис до ортонормального, вообще говоря, невозможно. Простейшим инвариантом, доставляющим препятствие к этому, является определитель $\det Q_e$ матрицы Грама Q формы q в произвольном базисе e. При переходе к другому базису определитель Грама умножается на квадрат определителя матрицы перехода. Поэтому с точностью до умножения на ненулевой квадрат из поля $\Bbbk$ определитель Грама не зависит от выбора базиса. В частности, форма, определитель Грама которой не является квадратом, не имеет ортонормального базиса.

Мы будем обозначать класс определителя Грама по модулю умножения на ненулевые квадраты через $\det q \in \Bbbk/\Bbbk^{*2}$ и писать $a \sim b$, если $a = \lambda^2 b$ для ненулевого $\lambda \in \Bbbk$.

Квадратичная форма q называется *вырожденной*, если $\det q = 0$. Формы с $\det q \neq 0$ называются *невырожденными*.

17.2.2. Пример: квадратичные формы от двух переменных. По теореме Лагранжа ненулевая квадратичная форма от двух переменных

$$q(x) = a\,x_1^2 + 2\,b\,x_1x_2 + c\,x_2^2 = (x_1, x_2)\begin{pmatrix} a & b \\ b & c \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \not\equiv 0$$

подходящей линейной заменой координат приводятся либо к виду $\alpha t^2 = 0$ с $\alpha \neq 0$, либо к виду $\alpha t_1^2 + \beta\,t_2^2$, где $\alpha \neq 0$ и $\beta \neq 0$.

В первом случае форма q вырождена: $\det q \sim ac - b^2 \sim \alpha \cdot 0 = 0$ и пропорциональна полному квадрату линейной формы $t = t(x_1, x_2)$. Такая форма зануляется вдоль одномерного подпространства $\operatorname{Ann}(t) \subset V$ и отлична от нуля на всех остальных векторах.

Во втором случае $\det q \sim ac - b^2 \sim \alpha\beta \neq 0$ и форма q невырождена. Если существует ненулевой вектор $v = (\vartheta_1, \vartheta_2)$, такой что $q(v) = \alpha\vartheta_1^2 + \beta\vartheta_2^2 = 0$, то

$$-\det q \sim -\alpha\beta \sim -\beta/\alpha = (\vartheta_1/\vartheta_2)^2$$

является полным квадратом[1], и в этом случае

$$\alpha t_1^2 + \beta\,t_2^2 = \alpha\left(t_1 + \frac{\vartheta_1}{\vartheta_2}t_2\right)\left(t_1 - \frac{\vartheta_1}{\vartheta_2}t_2\right)$$

является произведением двух непропорциональных линейных форм.

Таким образом, есть два типа невырожденных форм от двух переменных:

1) неприводимые формы q, у которых $-\det q$ не квадрат, и $q(v) \neq 0$ при $v \neq 0$

2) произведения $q = \xi_1\xi_2$ непропорциональных линейных форм; в этом случае $-\det q$ квадрат, и q тождественно зануляется на двух одномерных подпространствах $\operatorname{Ann}(\xi_1) \neq \operatorname{Ann}(\xi_2)$ и отлична от нуля на всех остальных векторах.

Формы первого типа называются *анизотропными*, а второго типа — *гиперболическими*. Отметим, что над алгебраически замкнутым полем $\Bbbk$ анизотропных форм от $\geqslant 2$ переменных не бывает.

[1] отметим, что $\vartheta_2 \neq 0$ в силу равенства $\alpha\vartheta_1^2 + \beta\vartheta_2^2 = 0$

17.2.3. Изотропные и анизотропные подпространства. Подпространство $U \subset V$ называется *анизотропным* для квадратичной формы q, если $q(v) = \widetilde{q}(v,v) \neq 0$ для любого ненулевого $v \in V$.

Например, вещественное евклидово пространство является анизотропным по отношению к евклидовому скалярному произведению.

В n° 17.2.2 мы видели, что двумерное подпространство U анизотропно, если и только если $-\det(q|_U)$ не квадрат в $\Bbbk$.

Подпространство $U \subset V$ называется *изотропным* для квадратичной формы q, если ограничение $q|_U \equiv 0$ или, что то же самое, $\widetilde{q}(u_1, u_2) = 0 \ \forall\, u_1, u_2 \in U$. Ненулевые векторы v, порождающие одномерные изотропные подпространства, называются *изотропными векторами*. Для таких векторов $q(v) = \widetilde{q}(v,v) = 0$.

Согласно n° 17.2.2, ненулевая квадратичная форма от двух переменных вырождена тогда и только тогда, когда у неё имеется ровно одно одномерное изотропное подпространство, а невырожденная квадратичная форма от двух переменных либо анизотропна, либо имеет ровно два различных одномерных изотропных подпространства.

Предложение 17.6

Размерность изотропного подпространства U в пространстве V с невырожденной симметричной билинейной формой β не превышает $\dim V/2$.

Доказательство. Поскольку форма β невырождена, оператор корреляции

$$R_\beta : V \xrightarrow{v \mapsto \beta(\,*\,,v)} V^*$$

является изоморфизмом. Изотропность $U \subset V$ означает, что $R_\beta(U) \subset \mathrm{Ann}\,(U)$. Поэтому $\dim U = \dim R_\beta(U) \leqslant \dim \mathrm{Ann}\, U = \dim V - \dim U$. □

17.2.4. Пример: $2n$-мерное гиперболическое пространство H_{2n} определяется как прямая сумма $V^* \oplus V$ $(\dim V = n)$, наделённая симметричной билинейной формой $h\big((\xi_1, v_1), (\xi_2, v_2)\big) = \xi_1(v_2) + \xi_2(v_1)$, которая ограничивается в тождественно нулевые формы на подпространства V и V^*, а на любой паре паре вектор-ковектор равна свёртке $h(\xi, v) = h(v, \xi) = \langle \xi, v \rangle$.

Базис H_{2n}, составленный из векторов $e_1, e_2, \dots, e_n, e_1^*, e_2^*, \dots, e_n^*$ каких-нибудь двойственных базисов V и V^*, называется *гиперболическим базисом*. Матрица Грама такого базиса имеет вид

$$\begin{pmatrix} 0 & E \\ E & 0 \end{pmatrix},$$

где 0 и E — нулевая и единичная $n \times n$-матрицы.

Тем самым, форма h невырождена и обладает изотропными подпространствами половинной размерности, так что оценка из предл. 17.6 является точной.

Векторы $p_i = e_i + e_i^*$ и $q_i = e_i - e_i^*$ образуют ортогональный базис формы h со скалярными квадратами $h(p_i, p_i) = 2$, $h(q_i, q_i) = -2$.

Отметим, что прямая ортогональная сумма $H_{2m} \oplus H_{2k}$ изометрически изоморфна $H_{2(m+k)}$.

Лемма 17.1
Всякое m-мерное изотропное подпространство U в пространстве V с невырожденной симметричной формой β содержится в некотором $2m$-мерном гиперболическом подпространстве $W \subset V$, и любой базис в U дополняется до гиперболического базиса в W.

Доказательство. Выберем в U базис $u_1, u_2, \dots, u_m$, дополним его до базиса в V и рассмотрим двойственный базис относительно невырожденной формы β. Первые m векторов $u_1^\vee, u_2^\vee, \dots, u_m^\vee$ этого двойственного базиса таковы, что

$$\beta\left(u_i, u_j^\vee\right) = \begin{cases} 1 & \text{при } i = j \\ 0 & \text{при } i \neq j\,, \end{cases} \tag{17-11}$$

причём добавление к любому из векторов $u_j^\vee$ любой линейной комбинации векторов u_i не нарушает этого свойства. Заменяя каждый $u_j^\vee$ на

$$w_j = u_j^\vee - \frac{1}{2} \sum_\nu \beta\left(u_j^\vee, u_\nu^\vee\right) u_\nu\,,$$

получим набор векторов $w_1, w_2, \dots, w_m$, также удовлетворяющий (17-11) и порождающий изотропное подпространство, поскольку $\forall\, i,j\ \beta(w_i, w_j) = \beta(u_i^\vee, u_j^\vee) - \frac{1}{2}\,\beta(u_i^\vee, u_j^\vee) - \frac{1}{2}\,\beta(u_j^\vee, u_i^\vee) = 0\,.$ □

Теорема 17.2
Любое пространство V с невырожденной симметричной билинейной формой раскладывается в прямую ортогональную сумму гиперболического и анизотропного подпространства.

Доказательство. Индукция по $\dim V$. Если $\dim V = 1$ или в V нет изотропных векторов, то само V является анизотропным пространством. Если в V есть ненулевой изотропный вектор e, то по лем. 17.1 он содержится в некоторой гиперболической плоскости H_2. Поскольку ограничение формы на эту плоскость невырождено, пространство V раскладывается в ортогональную прямую сумму $V = H_2 \oplus H_2^\perp$. По индукции, $H_2^\perp = H_{2k} \oplus U$, где U анизотропно и ортогонально H_{2k}. Тогда $V = H_{2k+2} \oplus U$. □

Следствие 17.3
Любая квадратичная форма q от n переменных линейной обратимой координат приводится к виду $x_1 x_{i+1} + x_2 x_{i+2} + \dots + x_i x_{2i} + \alpha(x_{2i+1}, x_{2i+1} \dots, x_r)$, где $r = \operatorname{rk}(q)$ и $\alpha(x) \neq 0$ при $x \neq 0$. □

17.3. Изометрии невырожденной симметричной формы. Пусть на пространстве V задана невырожденная симметричная билинейная форма β. Если линейный оператор $f : V \longrightarrow V$ является изометрическим для β, то его матрица F в произвольном базисе пространства V связана с матрицей Грама B формы β в этом базисе соотношением $F^tBF = B$. Поэтому f обратим, и обратный оператор f^{-1} имеет матрицу $F^{-1} = B^{-1}F^tB$.

Таким образом, изометрические операторы любой невырожденной симметричной билинейной формы β образуют группу. Эта группа называется *ортогональной группой* формы β и обозначается O_β.

17.3.1. Пример: изометрии гиперболической плоскости. Оператор

$$H_2 \xrightarrow{f} H_2$$

имеющий в гиперболическом базисе e, e^* матрицу

$$F = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

является изометрическим оператором гиперболической формы, когда

$$\begin{pmatrix} a & c \\ b & d \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

что равносильно уравнениям $ac = bd = 0$ и $ad + bc = 1$, имеющим два семейства решений:

$$F_\lambda = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix} \quad \text{и} \quad \widetilde{F}_\lambda = \begin{pmatrix} 0 & \lambda \\ \lambda^{-1} & 0 \end{pmatrix}, \quad \text{где } \lambda \in \Bbbk \smallsetminus \{0\} \text{ любое.} \tag{17-12}$$

Если основное поле $\Bbbk = \mathbb{R}$, то оператор F_λ с $\lambda > 0$ называется *гиперболическим поворотом*, поскольку траектория каждого ненулевого вектора $v = (x, y)$ при действии на него операторов F_λ с $\lambda \in (0, \infty)$ представляет собой гиперболу $xy = \mathrm{const}$. Если положить $\lambda = e^t$ и перейти к ортогональному базису

$$p = (e + e^*)/\sqrt{2}\,, \quad q = (e - e^*)/\sqrt{2}\,,$$

то оператор F_λ запишется в этом базисе матрицей

$$\begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} \end{pmatrix} \cdot \begin{pmatrix} e^t & 0 \\ 0 & e^{-t} \end{pmatrix} \cdot \begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} \end{pmatrix} = \begin{pmatrix} \operatorname{ch} t & \operatorname{sh} t \\ \operatorname{sh} t & \operatorname{ch} t \end{pmatrix}$$

аналогичной матрице поворота евклидовой плоскости. При $\lambda < 0$ оператор F_λ является композицией гиперболического поворота с центральной симметрией относительно нуля. В обоих случаях операторы F_λ собственные и лежат в $\mathrm{SL}(\mathbb{R}^2)$, т. е. сохраняют площадь. Операторы $\widetilde{F}_\lambda$ несобственные и являются композициями гиперболических поворотов с отражением относительно оси гиперболы. Они сохраняют абсолютную величину площади, но меняют ориентацию.

17.3.2. Отражения. С каждым анизотропным вектором $e \in V$ связано прямое ортогональное разложение $V = \Bbbk \cdot e \oplus e^{\perp}$, где $e^{\perp} = \{v \in V \mid \beta(e,v) = 0\}$. Линейный оператор

$$V \xrightarrow{\sigma_e} V \,:\, v \longmapsto \sigma_e(v) \overset{\text{def}}{=} v - 2\,\frac{\beta(e,v)}{\beta(e,e)} \cdot e \tag{17-13}$$

тождественно действует на $e^{\perp}$ и переводит e в $-e$. Поэтому $\sigma_e \in \mathrm{O}_\beta$ и $\sigma_e^2 = 1$. Оператор (17-13) называется *отражением в гиперплоскости* $e^{\perp}$ (см. рис. 17◇1).

Упражнение 17.8. Убедитесь, что для любой изометрии $V \xrightarrow{f} V$ и любого анизотропного $e \in V$ выполняется равенство $f \circ \sigma_e \circ f^{-1} = \sigma_{f(e)}$.

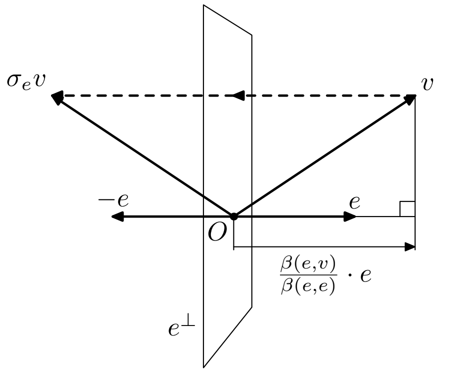


Рис. 17◇1. Отражение σ_e.

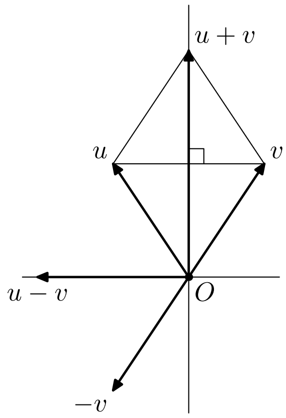


Рис. 17◇2. Отражения в ромбе.

Лемма 17.2
В пространстве с невырожденной симметричной билинейной формой β для любых двух различных анизотропных векторов u, v с равными скалярными квадратами $\beta(u,u) = \beta(v,v) \neq 0$ существует отражение, переводящее u либо в v либо в $-v$.

Доказательство. Если u и v коллинеарны, то искомым отражением является $\sigma_v = \sigma_u$. Если u и v неколлинеарны, то хотя бы одна из двух диагоналей натянутого на них ромба (см. рис. 17◇2) анизотропна. В самом деле, эти диагонали ортогональны между собою: $\beta(u+v, u-v) = \beta(u,u) - \beta(v,v) = 0$, и если бы они обе имели нулевые скалярные квадраты, то ограничение формы на их линейную оболочку, совпадающую с линейной оболочкой векторов u и v, было бы нулевым, что не так. Отражение σ_{u-v} переводит u в v, а отражение σ_{u+v} переводит u в $-v$. □

Упражнение 17.9. Покажите, что если пространство V анизотропно, то всегда существует отражение, переводящее u в точности в v.

Теорема 17.3
Всякая изометрия n-мерного пространства с невырожденной симметричной формой является композицией $\leqslant 2n$ отражений.

Доказательство. Индукция по n. Ортогональная группа одномерного пространства состоит из тождественного оператора E и отражения $-E$. Рассмотрим изометрию $f : V \xrightarrow{\sim} V$ n-мерного пространства. Выберем в V какой-нибудь анизотропный вектор v и обозначим через σ отражение, переводящее $f(v)$ либо в v, либо в $-v$. Композиция σf переводит v в $\pm v$, а значит, переводит в себя $(n-1)$-мерную гиперплоскость $v^{\perp}$. По индукции, действие σf на $v^{\perp}$ является композицией $\leqslant 2(n-1)$ отражений. Продолжим гиперплоскости в $v^{\perp}$, относительно которых происходили эти отражения, до гиперплоскостей в V, добавив к ним вектор v. Тогда композиция $(2n-2)$ отражений в этих расширенных гиперплоскостях совпадает σf на $v^{\perp}$, и σf либо равен этой композиции, либо получается из неё применением ещё одного отражения в гиперплоскости $v^{\perp}$, переводящего v в $-v$. Но тогда $f = \sigma\sigma f$ является композицией $\leqslant 2n$ отражений. □

Упражнение 17.10. Докажите, что любая изометрия n-мерного анизотропного пространства является композицией $\leqslant n$ отражений.

Теорема 17.4 (лемма Витта)
Пусть на пространствах U, V, W заданы какие-то невырожденные симметричные билинейные формы. Если существует изометрический изоморфизм прямой ортогональной суммы $U \oplus V$ с прямой ортогональной суммой $U \oplus W$, то существует изометрический изоморфизм V с W.

Доказательство. Индукция по $\dim U$. Если $U = 0$, доказывать нечего. Если $\dim U = 1$, то $U = \Bbbk \cdot u$, где u анизотропен. Пусть имеется изометрический изоморфизм ортогональных прямых сумм

$$f : \Bbbk \cdot u \oplus V \xrightarrow{\sim} f\Bbbk \cdot u \oplus W\,.$$

Рассмотрим отражение σ второго пространства, переводящее $f(u)$ в $\pm u$. Изометрический изоморфизм σf переводит $\Bbbk\cdot u$ в $\Bbbk\cdot u$, а значит, изоморфно отображает ортогональное дополнение к u в первом пространстве на ортогональное дополнение к u во втором и, тем самым, даёт нужный изометрический изоморфизм $\sigma f : V \xrightarrow{\sim} W$.

Если $\dim U > 1$, то выберем в U какой-нибудь анизотропный вектор u и рассмотрим ортогональное разложение $U = \Bbbk\cdot u \oplus u^{\perp}$. Применяя предположение индукции к $U = \Bbbk \cdot u$ получим изометрический изоморфизм $u^{\perp} \oplus V$ с $u^{\perp} \oplus W$. Второй раз применяя индуктивное предположение с $U = u^{\perp}$, получаем искомую изометрию V с W. □

Следствие 17.4
Построенное в теореме (теор. 17.2) разложение пространства V с невырожденной симметричной билинейной формой в прямую ортогональную сумму гиперболического и анизотропного подпространств единственно в том смысле, что

для любых двух таких разложений $V = H_{2k} \oplus U = H_{2m} \oplus W$ анизотропные подпространства U и W изометрически изоморфны, а гиперболические пространства имеют равные размерности $2k = 2m$.

Доказательство. Пусть $m \geqslant k$, так что $H_{2m} = H_{2k} \oplus H_{2(m-k)}$. Тождественное отображение $\mathrm{Id}_V : H_{2k} \oplus U \xrightarrow{\sim} H_{2k} \oplus H_{2(m-k)} \oplus W$ является изометрическим изоморфизмом. По лемме Витта существует изометрический изоморфизм $U \xrightarrow{\sim} H_{2(m-k)} \oplus W$. Поскольку в U нет изотропных векторов, гиперболическое подпространство $H_{2(m-k)}$ нулевое. Таким образом, $k = m$ и U изометрически изоморфно W. □

Следствие 17.5

Пусть подпространства U, W в в пространстве V с невырожденной симметричной билинейной формой таковы, что ограничения формы на U и на W невырождены и существует изометрический изоморфизм $\varphi : U \xrightarrow{\sim} W$. Тогда φ продолжается (многими способами) до изометрического автоморфизма всего пространства V, совпадающего с φ на подпространстве U.

Доказательство. Достаточно показать, что в условиях теоремы ортогоналы $U^\perp$ и $W^\perp$ изометрически изоморфны: тогда для любого изометрического изоморфизма $\psi : U^\perp \longrightarrow \sim W^\perp$, отображение

$$U \oplus U^\perp = V \xrightarrow{(u,u') \mapsto (\varphi(h'),\psi(u'))} V = W \oplus W^\perp$$

даст требуемое продолжение. По условию, отображения

$$\eta : U \oplus U^\perp \xrightarrow{(u,u') \mapsto u+u'} V$$
$$\zeta : U \oplus W^\perp \xrightarrow{(u,w') \mapsto \varphi(u)+w'} V$$

являются изометрическими изоморфизмами. Поэтому композиция

$$\zeta^{-1}\eta : U \oplus U^\perp \xrightarrow{\sim} U \oplus W^\perp$$

тоже является изометрическим изоморфизмом. По лемме Витта $U^\perp$ и $W^\perp$ изометрически изоморфны. □

Следствие 17.6

Ортогональная группа любой невырожденной симметричной билинейной формы транзитивно действует на гиперболических и на изотропных подпространствах данной размерности.

Доказательство. Утверждение про гиперболические подпространства вытекает из предыдущего следствия. Утверждение про изотропные подпространства сводится к утверждению про гиперболические подпространства при помощи лем. 17.1. □

17.3.3. Пример: квадратичные формы над $\mathbb{F}_p$, $p \neq 2$. Зафиксируем какой-нибудь не квадрат $\varepsilon \in \mathbb{F}_p$. В n° 4.4.4 мы видели, что ненулевые квадраты образуют в мультипликативной группе поля $\mathbb{F}_p = \mathbb{Z}/(p)$ подгруппу индекса 2. Поэтому любой ненулевой элемент $\mathbb{F}_p$ умножением на подходящий ненулевой квадрат может быть сделан равным либо 1, либо ε. Из теор. 17.1 вытекает тогда, что всякая квадратичная форма над $\mathbb{F}_p$ обратимой линейной заменой переменных приводится к виду

$$q(x) = \sum x_i^2 + \varepsilon \sum x_j^2 \tag{17-14}$$

(наборы переменных в первой и второй сумме не пересекаются).

Далее, уравнение

$$ax_1^2 + bx_2^2 = c \tag{17-15}$$

разрешимо в $\mathbb{F}_p$ при любых ненулевых a, b и любом c. В самом деле, когда x_1 и x_2 независимо друг от друга пробегают $\mathbb{F}_p$, функции $a\,x_1^2$ и $c - b\,x_2^2$ принимают по $(p+1)/2$ различных значений. Поэтому эти множества значений пересекаются по какому-то элементу $a\,x_1^2 = c - b\,x_2^2$.

Из разрешимости уравнения (17-15) вытекает, что для любой невырожденной квадратичной формы q на двумерном пространстве существует вектор e с $q(e) = 1$, а значит, координаты, в которых форма имеет вид $x_1^2 + x_2^2$ или $x_1^2 + \varepsilon x_2^2$. Это позволяет сделать вторую сумму в (17-14) состоящей из не более, чем одного слагаемого.

Таким образом, квадратичная форма q ранга r над полем $\mathbb{F}_p$ изоморфна форме $x_1^2 + \dots + x_{r-1}^2 + x_r^2$, если $\det q$ квадрат, или форме $x_1^2 + \dots + x_{r-1}^2 + \varepsilon x_r^2$, если $\det q$ не квадрат.

Другое следствие разрешимости уравнения (17-15) состоит в том, что невырожденная квадратичная форма $ax_1^2 + bx_2^2 + cx_3^2 + \ \cdots$ от $\geqslant 3$ переменных всегда имеет ненулевой изотропный вектор — например, вектор $(\alpha_1, \alpha_2, 1, 0, \dots)$ с $a\alpha_1^2 + b\alpha_2^2 = -c$. Поэтому анизотропные формы над полем $\mathbb{F}_p$ бывают только в размерностях 1 и 2 и с точностью до изоморфизма исчерпываются невырожденными одномерными формами x^2 и εx^2 и двумерными формами

$$x_1^2 + x_2^2 \ (\text{при } p \equiv -1 \pmod 4) \quad \text{и} \quad x_1^2 + \varepsilon x_2^2 \ (\text{при } p \equiv 1 \pmod 4)\,.$$

Упражнение 17.11. Покажите, что форма $x_1^2 + x_2^2$ гиперболична при $p \equiv 1 \pmod 4$ и анизотропна при $p \equiv -1 \pmod 4$, а форма $x_1^2 + \varepsilon x_2^2$, наоборот, анизотропна при $p \equiv 1 \pmod 4$ и гиперболична при $p \equiv -1 \pmod 4$.

Таким образом, квадратичная форма над полем $\mathbb{F}_p$ либо гиперболична, либо является прямой ортогональной суммой гиперболической формы и одной из четырёх перечисленных выше анизотропных форм.

17.3.4. Пример: вещественные квадратичные формы. В силу теор. 17.1, всякая вещественная квадратичная форма q от n вещественных переменных линейной заменой координат преобразуется к виду

$$q(x) = x_1^2 + x_2^2 + \cdots + x_p^2 - x_{p+1}^2 - x_{p+2}^2 - \cdots - x_{p+m}^2 \,. \tag{17-16}$$

Для этого достаточно построить в $\mathbb{R}^n$ какой-нибудь базис $e_1, e_2, \ldots, e_n$ с диагональной матрицей Грама, а затем поделить каждый e_i с $q(e_i) \neq 0$ на $\sqrt{|q(e_i)|}$.

Числа p и m называются *положительным* и *отрицательным индексами инерции* квадратичной формы q, а их разность $p-m$ — просто *индексом* формы q. Пару чисел (p, m) также называют *сигнатурой* формы β. Сумма $p+m = \operatorname{rk} q$ не зависит от выбора базиса, в котором q имеет вид (17-16). Покажем, что каждый из индексов p, m также не зависит от этого выбора.

Заменяя V на фактор $V/\ker q$, мы можем считать, что форма q невырождена. Тогда она раскладывается в ортогональную прямую сумму гиперболической и анизотропной формы.

Двумерная вещественная форма сигнатуры $(1,1)$ гиперболична, поскольку $x_1^2 - x_2^2 = (x_1 + x_2)(x_1 - x_2) = 2y_1y_2$, где $y_{1,2} = (x_1 \pm x_2)/\sqrt{2}$. Поэтому над полем $\mathbb{R}$ в каждой размерности с точностью до изоморфизма имеются ровно две неизоморфные анизотропные формы: *положительно определённая* (или *евклидова*), для которой $\beta(v, v) > 0 \ \forall\ v \neq 0$, и *отрицательно определённая*, для которой $\beta(v, v) < 0 \ \forall\ v \neq 0$. Их матрицы Грама в подходящих базисах равны E и $-E$.

В частности, форма (17-16) является ортогональной прямой суммой гиперболической формы h размерности $2\min(p, m)$ и анизотропной формы α размерности $|p - m|$, которая положительно определена, если $p > m$ и отрицательно определена, если $p < m$. Из единственности разложения в ортогональную прямую сумму гиперболической и анизотропной формы вытекает, что числа $p-m$ и $\min(p, m)$ не зависят от способа разложения, а числа p и m однозначно по ним восстанавливаются. Мы доказали

Следствие 17.7

Две квадратичных формы с вещественными коэффициентами тогда и только тогда переводятся друг в друга обратимой линейной заменой переменных, когда они имеют одинаковый ранг и индекс. □

Упражнение 17.12. Докажите, что положительный индекс инерции формы q равен наибольшей из размерностей подпространств, на которые q ограничивается в положительно определённую форму, а отрицательный — наибольшей из размерностей подпространств, на которые q ограничивается в отрицательно определённую форму.

17.3.5. Отыскание сигнатуры вещественной формы часто оказывается возможным без явного построения ортогонального базиса. А именно, рассмотрим матрицу Грама формы q в произвольном базисе и обозначим через Δ_i её *главный угловой минор*, стоящей в первых i строках и первых i столбцах.

Этот минор является определителем Грама ограничения формы q на линейную оболочку V_i первых i базисных векторов $e_1, e_2, \dots, e_i$. Он зануляется, если $q|_{V_i}$ вырождена, и имеет знак $(-1)^{m_i}$, если $q|_{V_i}$ невырождена и имеет отрицательный индекс инерции m_i. Таким образом, читая слева направо последовательность

$$\Delta_1, \Delta_2, \dots, \Delta_{\dim V}\,, \tag{17-17}$$

можно проследить за последовательным изменением сигнатуры формы $q|_{V_i}$ при переходе от V_i к V_{i+1} или за появлением у формы q изотропных векторов.

Пусть, например, в последовательности главных угловых миноров квадратичной формы q на $\mathbb{R}^4$

$$\Delta_1 < 0\,, \quad \Delta_2 = 0\,, \quad \Delta_3 < 0\,, \quad \Delta_4 > 0\,.$$

Так как ограничение $q|_{V_2}$ вырождено, в V_2 имеется изотропный вектор. Поэтому невырожденная форма $q|_{V_3}$ является суммой гиперболической плоскости сигнатуры $(1,1)$ и одномерного анизотропного пространства, т. е. имеет сигнатуру $(2,1)$ или $(1,2)$. Поскольку $\Delta_3 < 0$, сигнатура равна $(1,2)$. Из $\Delta_4 > 0$ вытекает, что полная сигнатура q на всём пространстве равна $(2,2)$.

Когда ни один из главных угловых миноров не обращается в нуль, ограничение формы на каждое из пространств V_i невырождено, и знак у Δ_{i+1} отличается от знака Δ_i тогда и только тогда, когда $m_{i+1} = m_i + 1$. Поэтому полный отрицательный индекс инерции m формы q равен числу перемен знака в последовательности $1, \Delta_1, \Delta_2, \dots, \Delta_{\dim V}$. Это наблюдение называется *критерием Сильвестра*.

17.4. Невырожденные кососимметричные формы. Прямая сумма $V^* \oplus V$, наделённая кососимметричной билинейной формой

$$\omega\big(\,(\xi_1, v_1)\,,\,(\xi_2, v_2)\,\big) = \langle \xi_1, v_2 \rangle - \langle \xi_2, v_1 \rangle\,, \tag{17-18}$$

называется *симплектическим пространством* и обозначается Ω_{2n}, где $n = \dim V$. Это кососимметрический аналог гиперболического пространства из n° 17.2.4. В базисе, составленном из векторов $e_1, e_2, \dots, e_n, e_1^*, e_2^*, \dots, e_n^*$ каких-нибудь двойственных базисов V и V^*, матрица Грама формы ω имеет вид

$$J = \begin{pmatrix} 0 & E \\ -E & 0 \end{pmatrix}. \tag{17-19}$$

Матрица J называется *симплектической единицей* и удовлетворяет соотношениям $J^2 = -E$, $\det J = 1$. В частности, форма ω невырождена. Базис, в котором матрица Грама невырожденной кососимметричной формы имеет вид (17-19), называется *симплектическим базисом* этой формы. Прямая ортогональная сумма $\Omega_{2m} \oplus \Omega_{2k}$ изометрически изоморфна $\Omega_{2(m+k)}$.

Теорема 17.5
Любое пространство V с невырожденной кососимметричной формой ω изометрически изоморфно симплектическому пространству (в частности, $\dim V$ чётна).

Доказательство. В качестве первого базисного вектора возьмём произвольный ненулевой вектор $e_1 \in V$. Поскольку ω невырождена, существует $w \in V$, такой что $\omega(e_1, w) = a \neq 0$. Положим $e_2 = w/a$. Матрица Грама ограничения ω на двумерное подпространство $U \subset V$, порождённое векторами e_1, e_2, равна

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Тем самым, $\omega|_U$ невырождена, $V = U \oplus U^{\perp}$, и мы можем воспользоваться индукцией по размерности. □

Упражнение 17.13. Убедитесь непосредственно, что определитель кососимметричной квадратной матрицы нечётного размера равен нулю.

17.4.1. Симплектическая группа $\mathbf{Sp}_{\boldsymbol{\omega}}(\boldsymbol{V})$. Изометрические линейные преобразования $V \xrightarrow{F} V$ невырожденной симплектической формы ω на V называются *симплектическими* и образуют группу $\mathrm{Sp}_\omega(V)$, называемую *симплектической группой* формы ω. Сопоставление оператору его матрицы в симплектическом базисе изоморфно отображает группу $\mathrm{Sp}_\omega(V)$ на *группу симплектических матриц* $\mathrm{Sp}_{2n}(\Bbbk) = \{F \in \mathrm{Mat}_{2n}(\Bbbk) \mid F^t \cdot J \cdot F = J\}$, где $2n = \dim V$.

17.4.2. Лагранжевы подпространства. Максимальные изотропные подпространства $L = L^{\perp}$ формы ω имеют размерность $n = \dim V/2$ и называются *лагранжевыми*. Точно также, как в лем. 17.1, проверяется, что любое изотропное подпространство U невырожденной кососимметричной формы ω содержится в некотором в некотором симплектическом подпространстве W размерности $2\dim U$ и любой базис U достраивается до симплектического базиса в W. Из этого следует, что любое изотропное подпространство содержится в некотором лагранжевом изотропном подпространстве[1], а любой базис U достраивается до симплектического базиса в V. В частности, симплектическая группа транзитивно действует на изотропных подпространствах данной размерности (в частности, на лагранжевых подпространствах).

17.4.3. Пфаффиан. Рассмотрим при $i < j$ элементы a_{ij} кососимметричной матрицы $A = (a_{ij})$ размера $(2n) \times (2n)$, как независимые переменные, и покажем, что существует единственный многочлен $\mathrm{Pf}(A) \in \mathbb{Z}[a_{ij}]$, такой что

$$\mathrm{Pf}(A)^2 = \det(A) \quad \text{и} \quad \mathrm{Pf}(J') = 1\,,$$

[1] можно, к примеру, представить $W^{\perp}$ как $L \oplus L^*$; тогда $U \oplus L$ будет лагранжевым подпространством, содержащим U

где J' — блочно диагональная матрица, составленная из 2×2-блоков $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$. Многочлен $\mathrm{Pf}(A)$ называется *пфаффианом* кососимметричной матрицы A и явно выражается через матричные элементы по формуле

$$\mathrm{Pf}(A) = \sum_{\substack{\{i_1,j_1\}\sqcup\dots\sqcup\{i_n,j_n\}= \\ =\{1,2,\dots,2n\}}} \mathrm{sgn}\big(i_1j_1i_2j_2\dots i_nj_n\big) \cdot a_{i_1j_1}a_{i_2j_2}\,\cdots\,a_{i_nj_n}\,, \tag{17-20}$$

где суммирование происходит по всем разбиениям множества $\{1, 2, \dots, 2n\}$ в объединение n непересекающихся пар $\{i_\nu, j_\nu\}$, порядок которых не существенен, а sgn означает знак соответствующей перестановки[1].

Будем воспринимать A как матрицу Грама кососимметричной формы на координатном векторном пространстве K^{2n} над полем $K = \mathbb{Q}(a_{ij})$ рациональных функций от переменных a_{ij} с коэффициентами в $\mathbb{Q}$. Она, очевидно, невырождена и по теор. 17.5 обладает симплектическим базисом $e_1, e_2, \dots, e_n, e_1^*, e_2^*, \dots, e_n^*$. Перегруппировывая базисные векторы по парам $e_1,\ e_1^*,\ e_2,\ e_2^*,\ \dots,\ e_n,\ e_n^*$, получаем базис с матрицей Грама J'. Это означает, что $A = C \cdot J' \cdot C^t$ для некоторой невырожденной матрицы C, элементы которой суть отношения полиномов от a_{ij} с рациональными коэффициентами. Поскольку $\det J' = 1$, мы имеем равенство $\det(A) = \det(C)^2$.

С другой стороны, *определим* для любой кососимметричной матрицы B многочлен $\mathrm{Pf}(B)$ формулой (17-20)

$$\mathrm{Pf}(B) \overset{\text{def}}{=} \sum_{\substack{\{i_1,j_1\}\sqcup\dots\sqcup\{i_n,j_n\}= \\ =\{1,2,\dots,2n\}}} \mathrm{sgn}\big(i_1j_1i_2j_2\dots i_nj_n\big) \cdot b_{i_1j_1}b_{i_2j_2}\,\cdots\,b_{i_nj_n}$$

и рассмотрим грассманов многочлен $\beta = (\xi\, B) \wedge \xi^t = \sum\limits_{ij} b_{ij}\xi_i \wedge \xi_j$ от переменных $\xi = (\xi_1, \xi_2, \dots, \xi_n)$. Так как чётные мономы $\xi_i \wedge \xi_j$ попарно перестановочны,

$$\beta^n = \beta \wedge \beta \wedge \dots \wedge \beta = n! \cdot \mathrm{Pf}(B) \cdot \xi_1 \wedge \xi_2 \wedge\,\cdots\,\wedge \xi_{2n}\,.$$

Если перейти от координат ξ к координатам η, через которые ξ выражаются как $\xi = \eta\, C$, где матрица C та же, что и выше, многочлен β перепишется в виде $\beta = (\xi\, B) \wedge \xi^t = (\eta\, CB) \wedge (\eta\, C)^t = (\eta\, CBC^t) \wedge \eta^t = (\eta\, B') \wedge \eta^t$ и будет соответствовать матрице $B' = CBC^t$ в том смысле, что

$$\beta^n = n! \cdot \mathrm{Pf}(B') \cdot \eta_1 \wedge \eta_2 \wedge\,\cdots\,\wedge \eta_{2n}\,.$$

Поскольку $\xi_1 \wedge \xi_2 \wedge\,\cdots\,\wedge \xi_{2n} = \det C \cdot \eta_1 \wedge \eta_2 \wedge\,\cdots\,\wedge \eta_{2n}$, многочлены $\mathrm{Pf}(B)$ и $\mathrm{Pf}(B') = \mathrm{Pf}(CBC^t)$ связаны соотношением $\mathrm{Pf}(CBC^t) = \mathrm{Pf}(B) \cdot \det C$. Полагая в нём $B = J'$, получаем $\mathrm{Pf}(A) = \det(C) \cdot \mathrm{Pf}(J) = \det C$. Поэтому

$$\det(A) = \det{}^2(C) = \mathrm{Pf}^2(A)\,,$$

[1] убедитесь, что правая часть не меняется ни при перестановках пар друг с другом, ни при перестановке элементов в каждой паре

что доказывает существование многочлена Pf и формулу (17-20). Единственность вытекает из того, что $x^2 - \det A = \bigl(x - \mathrm{Pf}(A)\bigr)\bigl(x + \mathrm{Pf}(A)\bigr)$ в целостном кольце $\mathbb{Z}[a_{ij}][x]$, так что уравнение $x^2 = \det A$ имеет ровно два решения $x = \pm\mathrm{Pf}(A)$, и условие $\mathrm{Pf}(J') = 1$ однозначно фиксирует знак.

Задачи для самостоятельного решения к §17

Задача 17.1. Обозначим через W пространство квадратичных форм от двух переменных (x_0, x_1) с базисом $(\,x_0^2\,,\,2\,x_0x_1\,,\,x_1^2\,)$. Свяжем с матрицей $A \in \mathrm{GL}_2(\Bbbk)$ оператор $S_A^2 : W \longrightarrow W$, переводящий $f(x_0, x_1)$ в $f\left((x_0, x_1)\cdot A\right)$. Напишите его матрицу и выразите её след и определитель через $\operatorname{tr} A$ и $\det A$.

Задача 17.2. Существует ли на $\mathbb{R}^7$ квадратичная форма с главными угловыми минорами а) $\Delta_1 > 0\,,\ \Delta_2 = 0\,,\ \Delta_3 > 0\,,\ \Delta_4 < 0\,,\ \Delta_5 = 0\,,\ \Delta_6 < 0\,,\ \Delta_7 > 0$
б) $\Delta_1 > 0\,,\ \Delta_2 = 0\,,\ \Delta_3 > 0\,,\ \Delta_4 < 0\,,\ \Delta_5 = 0\,,\ \Delta_6 < 0\,,\ \Delta_7 < 0$
в) $\Delta_1 > 0\,,\ \Delta_2 = 0\,,\ \Delta_3 > 0\,,\ \Delta_4 < 0\,,\ \Delta_5 = 0\,,\ \Delta_6 < 0\,,\ \Delta_7 < 0$
Если да, то какую сигнатуру может иметь эта форма?

Задача 17.3. Симметричная билинейная форма β на $\mathbb{R}^5$ имеет в матрицу Грама

$$\begin{pmatrix} -12 & 14 & -5 & -3 & 8 \\ 14 & -17 & 2 & 5 & -8 \\ -5 & 2 & -12 & 3 & 6 \\ -3 & 5 & 3 & -3 & 1 \\ 8 & -8 & 6 & 1 & -6 \end{pmatrix}$$

Найдите ранг и сигнатуру ограничения формы β на пространство решений системы

$$\begin{cases} 2\,x_1 + 2\,x_2 - 3\,x_3 - 4\,x_4 - 7\,x_5 = 0 \\ -x_1 - x_2 + 2\,x_3 + 2\,x_4 + 4\,x_5 = 0 \end{cases}$$

и напишите уравнение гиперплоскости, ортогональное[1] отражение в которой переводит друг в друга прямые с направляющими векторами $(3,0,2,3,6)$ и $(0,3,-11,-12,-18)$, а также найдите ортогональные проекции этих векторов на эту гиперплоскость.

Задача 17.4. Запишем характеристический многочлен матрицы $X \in \mathrm{Mat}_n(\mathbb{R})$ в виде $\det(tE - X) = t^n + \sigma_1(X)\,t^{n-1} + \sigma_2(X)\,t^{n-2} + \cdots$. Покажите, что $\sigma_2(X)$ является квадратичной формой на пространстве $\mathrm{Mat}_n(\mathbb{R})$ и вычислите её ранг и сигнатуру. Если общий случай вызывает затруднения, решите задачу для $n = 2, 3, 4$.

[1] в этой задаче всюду имеется в виду ортогональность относительно формы β

Задача 17.5. Найдите сигнатуру квадратичной формы $\operatorname{tr}\left(A^2\right)$ на пространстве $\operatorname{Mat}_n(\mathbb{R})$. Если общий случай вызывает затруднения, решите задачу для $n = 2, 3, 4$.

Задача 17.6. Убедитесь, что функция $A \mapsto \det A$ является квадратичной формой на пространстве $\operatorname{Mat}_2(\Bbbk)$ и покажите, что её поляризация равна $\widetilde{\det}(A, B) = \operatorname{tr}(AB^\vee)/2$, где $B^\vee$ — присоединённая к B матрица. Какова сигнатура этой формы при $\Bbbk = \mathbb{R}$? Гиперболична ли она над полем $\Bbbk = \mathbb{F}_p$?

Задача 17.7. Рассмотрим кольцо $K = \mathbb{F}_3[x]/(x^3 - x + 1)$ как трёхмерное векторное пространство над полем $\mathbb{F}_3$ с симметричной билинейной формой $\operatorname{tr}(ab)$ (след оператора умножения на ab: $K \xrightarrow{x \mapsto abx} K$). Напишите матрицу Грама этой формы в базисе $\{1, \vartheta, \vartheta^2\}$, где $\vartheta = x \pmod{x^3 - x + 1}$, и выясните, содержит ли K гиперболическую плоскость (если да, то укажите гиперболический базис этой плоскости, если нет — объясните, почему).

Задача 17.8. Обозначим через W пространство однородных грассмановых многочленов степени 2 от четырёх переменных ξ_1, ξ_2, ξ_3, ξ_4 и зададим на W билинейную форму $p : W \times W \longrightarrow \Bbbk$ правилом

$$\omega_1 \wedge \omega_2 = p(\omega_1, \omega_2) \cdot \xi_1 \wedge \xi_2 \wedge \xi_3 \wedge \xi_4 \,.$$

Напишите матрицу Грама формы p в базисе $\xi_{ij} = \xi_i \wedge \xi_j$ $(1 \leqslant i < j \leqslant 4)$ и убедитесь, что эта форма симметрична и невырождена. Какова её сигнатура над полем $\Bbbk = \mathbb{R}$?

Задача 17.9. Покажите, что следующие условия на пространство W с невырожденной симметричной билинейной формой эквивалентны друг другу:

а) W изометрически изоморфно гиперболическому пространству

б) $\dim W$ чётна и в W есть изотропное подпространство размерности $\dim W/2$

в) W является прямой суммой изотропных подпространств.

Задача 17.10. Покажите, что правило $F \mapsto \begin{pmatrix} F^{-1t} & 0 \\ 0 & F \end{pmatrix}$ задаёт инъективный гомоморфизм групп[1] $\operatorname{GL}_n(\Bbbk) \hookrightarrow \operatorname{Sp}_{2n}(\Bbbk)$.

Задача 17.11. Докажите, что любой симплектический оператор $F \in \operatorname{Sp}_{2n}(\Bbbk)$ имеет возвратный характеристический многочлен $\chi_F(t) = t^{2n}\chi_F\left(t^{-1}\right)$ и единичный определитель $\det F = 1$.

Задача 17.12. Напишите явные формулы для пфаффианов 2-го, 4-го и 6-го порядка.

Задача 17.13*. Фиксируем любое $n \in \mathbb{N}$ и любое чётное $m \leqslant n$. Покажите, что для кососимметричной матрицы A размера $n \times n$ и произвольной матрицы C из m

[1] на бескоординатном языке оператор $F \in \operatorname{GL}(V)$ действует на $V^* \oplus V$ парой операторов $V \xrightarrow{F} V$ и $V^* \xrightarrow{F^{-1t}} V^*$

строк и n столбцов имеет место полиномиальное тождество[1]

$$\mathrm{Pf}(CAC^t) = \sum_{\#I=m} \mathrm{Pf}(A_I) \cdot \det(C_I)$$

где суммирование идёт по всем наборам $I = (i_1, i_2, \dots, i_m)$ строго возрастающих индексов, C_I означает минор m-того порядка, стоящий в I-столбцах, а $A_I = \left(a_{i_\mu i_\nu}\right)_{i_\mu, i_\nu \in I}$ обозначает квадратную $m \times m$-подматрицу, стоящую в пересечениях строк и столбцов с номерами из I.

Задача 17.14. Приведите пример пространства V с невырожденной билинейной формой β и подпространства $U \subset V$ с невырожденным ограничением $\beta|_U$ и $U^\perp \neq {}^\perp U$.

Задача 17.15. Пусть несимметричная билинейная форма на пространстве V ограничивается в невырожденную форму на конечномерном подпространстве $U \subset V$. Постройте изометрический изоморфизм между ${}^\perp U$ и $U^\perp$.

Задача 17.16. Приведите пример пространства V с вырожденной билинейной формой β и подпространства $U \subset V$, дополнительного к ядру левой корреляции

$$L_\beta : V \xrightarrow{v \mapsto \beta(v,*)} V^*$$

и такого что ограничение $\beta|_U$ вырождено.

Задача 17.17* (канонический оператор). Пусть $\Bbbk = \mathbb{C}$. Свяжем с каждой невырожденной (несимметричной) билинейной формой $\beta : V \times V \longrightarrow \mathbb{C}$ линейный оператор $V \xrightarrow{\varkappa} V$, определяемый равенством $\beta(v, w) = \beta(w, \varkappa v) \quad \forall\, v, w \in V$ (мы будем называть его *каноническим* или *оператором Серра* формы β).

а) Убедитесь, что канонический оператор существует, единственен и является изометрическим изоморфизмом формы β (в частности, невырожден).

б) Выразите матрицу канонического оператора через матрицу Грама формы β и покажите, что канонический оператор имеет возвратный характеристический многочлен $\chi_\varkappa(t) = t^{\dim V} \chi_\varkappa\left(t^{-1}\right)$.

в) Докажите, то формы β и β' изоморфны (т. е. $\beta' = C \cdot \beta \cdot C^t$ для некоторого $C \in \mathrm{GL}(V)$) тогда и только тогда, когда их канонические операторы $\varkappa$ и $\varkappa'$ подобны (т. е. $\varkappa' = D \cdot \varkappa \cdot D^{-1}$ для некоторого $D \in \mathrm{GL}(V)$)

г) Докажите, что при $\lambda \neq \pm 1$ канонический оператор вместе с каждым элементарным делителем $(t - \lambda)^m$ имеет элементарный делитель $(t - 1/\lambda)^m$

д) Покажите, что две жордановы цепочки оператора $\varkappa$ с собственными значениями λ, μ двусторонне ортогональны[2] относительно β, если $\lambda\mu \neq 1$ или если у них разная длина.

[1] т. е. равенство в кольце многочленов с целыми коэффициентами от независимых матричных элементов $a_{ij} = -a_{ji}$ и $c_{\alpha\beta}$

[2] т. е. $\beta(v, w) = \beta(w, v) = 0$ для любого v из линейной оболочки одной цепочки и любого w из линейной оболочки другой

Задача 17.18* (невырожденные билинейные формы над $\mathbb{C}$). Будем называть пространство V с невырожденной билинейной формой β *неразложимым*, если если оно не является прямой двусторонне ортогональной суммой двух ненулевых подпространств[1]. Покажите, что

а) любое пространство с невырожденной билинейной формой является прямой суммой двусторонне ортогональных неразложимых подпространств

б) неразложимое пространство с невырожденной билинейной формой над полем $\mathbb{C}$ изометрически изоморфно либо $2k$-мерному пространству $W_{2k}(\lambda)$, форма на котором в подходящем базисе имеет блочную матрицу Грама

$$\begin{pmatrix} 0 & I \\ I_\lambda & 0 \end{pmatrix}, \quad \text{где} \quad I = \begin{pmatrix} 0 & & 1 \\ & \iddots & \\ 1 & & 0 \end{pmatrix} \quad \text{и} \quad I_\lambda = \begin{pmatrix} 0 & & & \lambda \\ & & \lambda & 1 \\ & \iddots & \iddots & \\ \lambda & 1 & & 0 \end{pmatrix}$$

либо m-мерному пространству U_m, форма на котором в подходящем базисе имеют матрицу Грама:

$$\begin{pmatrix} & & & & 1 \\ & 0 & & -1 & 1 \\ & & 1 & -1 & \\ & \iddots & 1 & & \\ \iddots & \iddots & & & 0 \end{pmatrix}.$$

в) канонический оператор (см. зад. 17.17) формы на пространстве $W_{2k}(\lambda)$ имеет две жордановы цепочки длины k с собственными значениями λ и λ^{-1} (и форма невырожденно спаривает их линейные оболочки друг с другом, ограничиваясь при этом на каждую в тождественно нулевую форму), а канонический оператор формы на пространстве U_m имеет одну жорданову цепочку длины m с собственным значением $(-1)^{m-1}$.

---

[1]т.е. $V \neq U \oplus W$, где $U, W \neq 0$ и $\beta(u,w) = \beta(w,u) = 0$ для любых $u \in U$ и $w \in W$

§18. Проективное пространство

18.1. Проективизация векторного пространства. Над любым полем $\Bbbk$ с каждым $(n+1)$-мерным векторным пространством V помимо $(n+1)$-мерного аффинного пространства $\mathbb{A}(V)$ связано ещё одно точечное пространство — n-*мерное проективное пространство*

$$\mathbb{P}_n = \mathbb{P}(V)$$

(*проективизация* V). По определению, точками $\mathbb{P}(V)$ являются одномерные векторные подпространства в V. Иначе можно сказать, что точки $\mathbb{P}(V)$ — это ненулевые векторы из V, рассматриваемые с точностью до пропорциональности, или проходящие через начало координат прямые в $\mathbb{A}(V)$.

Чтобы видеть эти прямые как «обычные» точки, внутрь $\mathbb{A}(V)$ следует поместить экран (см. рис. 18◇1) — не содержащую начала координат аффинную гиперплоскость U_ξ, задаваемую в $\mathbb{A}(V)$ линейным уравнением $\xi(x) = 1$, где $\xi \in V^*$ — какая-нибудь ненулевая линейная форма на V.

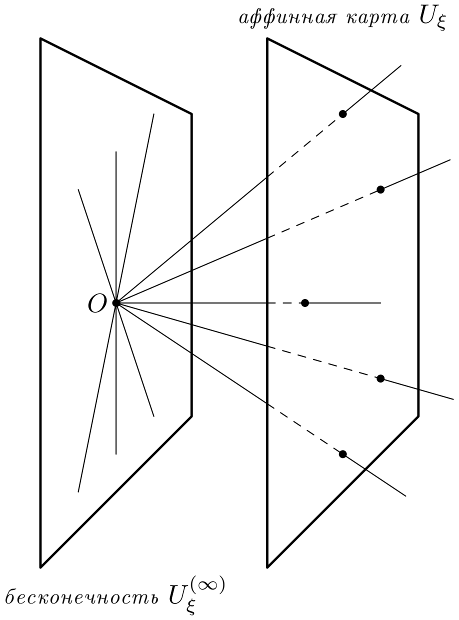


Рис. 18◇1. Проективный мир.

Всякий такой экран U_ξ называется *аффинной картой* на $\mathbb{P}(V)$. В карте U_ξ видны только такие одномерные подпространства, которые порожденны векторами $v \in V$ с $\xi(v) \neq 0$. Таким образом, дополнение $U_\xi^{(\infty)} \overset{\text{def}}{=} \mathbb{P}_n \setminus U_\xi$ состоит из одномерных подпространств, лежащих в n-мерном векторном подпространстве $\operatorname{Ann}(\xi) \subset V$, которое представляет собою параллельную копию гиперплоскости U_ξ, проходящую через нуль. Одномерные подпространства из $\operatorname{Ann}(\xi)$ составляют, тем самым, $(n-1)$-мерное проективное пространство $\mathbb{P}_{n-1} = \mathbb{P}(\operatorname{Ann}(\xi))$. Оно называется *бесконечно удалённой гиперплоскостью* карты U_ξ и обозначается $U_\xi^{(\infty)}$. Точки $U_\xi^{(\infty)}$ можно воспринимать как *направления* в аффинной карте U_ξ.

Из сказанного вытекает, что n-мерное проективное пространство $\mathbb{P}_n$ разбивается в объединение непересекающихся аффинных пространств всех промежуточных размерностей:

$$\mathbb{P}_n = U_\xi \sqcup U_\xi^{(\infty)} = \mathbb{A}^n \sqcup \mathbb{P}_{n-1} = \mathbb{A}^n \sqcup \mathbb{A}^{n-1} \sqcup \mathbb{P}_{n-2} = \cdots = \mathbb{A}^n \sqcup \mathbb{A}^{n-1} \sqcup \ldots \sqcup \mathbb{A}^0$$

(где $\mathbb{A}^0 = \mathbb{P}_0$ — это одна точка). Отметим, что это даёт геометрическое объяснение формулы суммирования геометрической прогрессии: над полем из q элементов дизъюнктное объединение аффинных пространств всех размерностей от 0 до n это $q^{n+1} - 1$ ненулевых векторов большего пространства с точностью до умножения на $q-1$ ненулевых элементов поля:

$$\frac{q^{n+1}-1}{q-1} = q^n + q^{n-1} + \cdots + q + 1\,.$$

18.1.1. Глобальные однородные координаты. Зафиксируем в V координаты $x_0, x_1, \dots, x_n$ относительно какого-нибудь базиса $e_0, e_1, \dots, e_n$. Два ненулевых вектора $v = (x_0, x_1, \dots, x_n)$ и $w = (y_0, y_1, \dots, y_n)$ тогда и только тогда задают одну и ту же точку $p \in \mathbb{P}_n$, когда их координаты пропорциональны. Это равносильно равенству отношений $x_\mu : x_\nu = y_\mu : y_\nu$ для всех $0 \leqslant \mu \neq \nu \leqslant n$ (где мы допускаем и равенства вида $0 : x = 0 : y$ и $x : 0 = y : 0$). Иначе говоря, точкам $p \in \mathbb{P}_n$ корректно соответствуют не сами координаты, а только отношения $(x_0 : x_1 : \dots : x_n)$ между ними. Эти отношения называется *однородными координатами* точки p в базисе $\{e_0, e_1, \dots, e_n\} \subset V$.

18.1.2. Локальные аффинные координаты. Рассмотрим на $\mathbb{P}_n = \mathbb{P}(V)$ аффинную карту $U_\xi = \{(x_0, x_1, \dots, x_n) \in \mathbb{A}(V) \mid \xi(x) = 1\}$, отвечающую какому-нибудь ненулевому ковектору $\xi \in V^*$. Тогда любые n линейных форм

$$\xi_1, \xi_2, \dots, \xi_n \in V^*\,,$$

которые образуют вместе с ξ базис $\xi, \xi_1, \xi_2, \dots, \xi_n$ пространства V^*, задают внутри карты U_ξ *локальные аффинные координаты* $t_i = \xi_i|_{U_\xi}$. Чтобы вычислить их значения в точке $p = (p_0 : p_1 : \dots : p_n)$, следует сначала выбрать в одномерном подпространстве, отвечающем точке p, вектор $v = p/\xi(p) \in U_\xi$, а затем вычислить значения n линейных форм ξ_i на этом векторе. Отметим, что получающиеся таким образом n чисел $t_i(p) = \xi_i(v) = \xi_i(p)/\xi(p)\,,\ 1 \leqslant i \leqslant n\,,$ зависят от однородных координат точки p *нелинейно*.

18.1.3. Пример: проективная прямая $\mathbb{P}_1 = \mathbb{P}(\Bbbk^2)$ покрывается двумя аффинными картами $U_0 = U_{x_0}$ и $U_1 = U_{x_1}$, представляющими собою аффинные прямые с уравнениями $x_0 = 1$ и $x_1 = 1$ (см. рис. 18◇2).

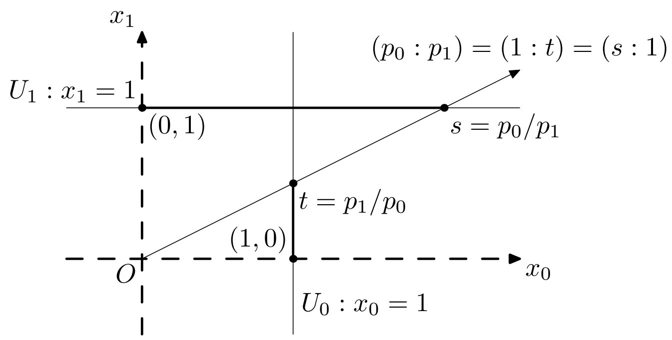


Рис. 18◇2. Стандартные карты на $\mathbb{P}_1$.

В карте U_0 видны все проходящие через начало координат прямые, кроме вертикальной. Проективная точка

$$(p_0 : p_1) \in \mathbb{P}_1$$

с $p_0 \neq 0$ видна в U_0 как аффинная точка $(1, p_1/p_0)$. В качестве локальной аффинной координаты в карте U_0 можно взять ограничение на U_0 линейной формы x_1. Если обозначить её через $t = x_1|_{U_0}$, то $t(p_0 : p_1) = p_1/p_0$.

Карта U_1 покрывает все точки $(x_0 : x_1)$, у которых $x_1 \neq 0$, и в качестве локальной координаты в U_1 годится ограничение $s = x_0|_{U_1}$. Тогда $s(p_0 : p_1) =$

p_0/p_1. Единственной бесконечно удалённой точкой для карты U_1 является горизонтальная координатная ось $(1:0)$.

Координаты s и t одной и той же точки $(x_0 : x_1) \in \mathbb{P}_1$, видимой сразу в обеих картах, связаны соотношением $s = 1/t$. Таким образом, $\mathbb{P}_1$ можно воспринимать как результат склейки двух аффинных координатных прямых $\mathbb{A}^1$ (одна —с координатой s, другая — с координатой t) вдоль дополнения до нуля по следующему правилу: точка с координатой s на одной прямой приклеивается к точке с координатой $t = 1/s$ на другой.

Над полем $\Bbbk = \mathbb{R}$ эта склейка совпадает со склейкой окружности диаметра 1 из двух параллельных касательных прямых (см. рис. 18◇3), каждая из которых проектируется на окружность из точки, диаметрально противоположной точке своего касания с нею.

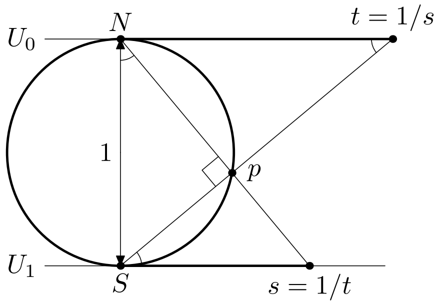


Рис. 18◇3. $\mathbb{P}_1(\mathbb{R}) \simeq S^1$.

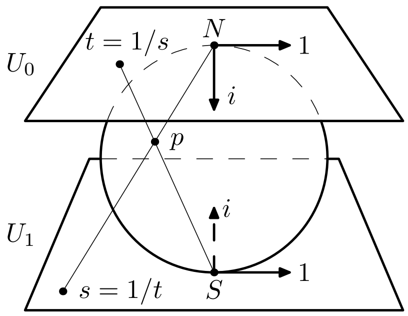


Рис. 18◇4. $\mathbb{P}_1(\mathbb{C}) \simeq S^2$.

Аналогичным образом, над полем $\Bbbk = \mathbb{C}$ склейка $\mathbb{P}_1 = \mathbb{P}(\mathbb{C}^2)$ из двух аффинных прямых $\mathbb{A}^1 = \mathbb{C}$ ничем не отличается от склеивания сферы диаметра 1 из двух параллельных касательных плоскостей, проходящих через северный и южный полюса сферы и ориентированных согласованным образом[1] (см. рис. 18◇4). Каждая из них рассматривается как поле $\mathbb{C}$ и проектируется на сферу из противоположного к точке касания полюса, рис. 18◇4 показывает, что комплексные числа s и t имеют противоположные аргументы, а рис. 18◇3 — что у них обратные модули.

Упражнение 18.1. Если вы знакомы с началами топологии, покажите, что

а) вещественная плоскость $\mathbb{P}_2 = \mathbb{P}\left(\mathbb{R}^3\right)$ гомеоморфна ленте Мёбиуса с заклеенной диском границей[2]

б) вещественное пространство $\mathbb{P}_3 = \mathbb{P}\left(\mathbb{R}^4\right)$ гомеоморфно собственной ортогональной группе $\mathrm{SO}_3(\mathbb{R})$ вращений евклидова пространства $\mathbb{R}^3$.

18.1.4. Стандартное аффинное покрытие $\mathbb{P}_n$ состоит из $(n+1)$ аффинных карт $U_\nu = U_{x_\nu}$, задаваемых в $\mathbb{A}^{n+1}$ уравнениями $x_\nu = 1$. Для каждого $\nu = 0, 1, \dots, n$ в качестве стандартных локальных аффинных координат на U_ν

[1] верхний репер $(1, i)$ получился из нижнего репера $(1, i)$ параллельным переносом вдоль меридиана, перпендикулярного плоскости чертежа

[2] границей ленты Мёбиуса, так же как и границей круга, является окружность, по которой их и можно приклеить друг к другу

берутся n форм $t_i^{(\nu)} = x_i|_{U_\nu}$, где $0 \leqslant i \leqslant n$ и $i \neq \nu$, которые выражаются через однородные координаты по формуле $t_i^{(\nu)}(x_0 : x_1 : \ \dots : x_n) = x_i/x_\nu$.

Таким образом, пространство $\mathbb{P}_n$ (над любым полем) можно представлять себе как результат склейки $(n+1)$ различных копий $U_0, U_1, \dots, U_n$ n-мерного аффинного координатного пространства $\Bbbk^n$. Склейка карты U_μ с картой U_ν происходит вдоль их пересечения внутри $\mathbb{P}_n$, состоящего из точек x, у которых обе однородные координаты x_μ и x_ν не обращаются в 0. В локальных аффинных координатах на U_μ и U_ν это подмножество задаётся, соответственно, неравенствами $t_\nu^{(\mu)} \neq 0$ и $t_\mu^{(\nu)} \neq 0$. Правило склейки таково: точка $t^{(\mu)} \in U_\mu$ склеивается с точкой $t^{(\nu)} \in U_\nu$, когда $t_\nu^{(\mu)} = 1/t_\mu^{(\nu)}$ и $t_i^{(\mu)} = t_i^{(\nu)}/t_\mu^{(\nu)}$ для $i \neq \mu, \nu$. Правые части этих равенств называются *функциями перехода* от локальных координат $t^{(\nu)}$ к локальным координатам $t^{(\mu)}$.

18.2. Задание фигур уравнениями. В отличие от аффинной геометрии, на проективном пространстве $\mathbb{P}(\Bbbk^{n+1})$ с фиксированной системой однородных координат $x = (x_0, x_1, \dots, x_n)$ отличные от констант многочлены от x *не задают* никаких функций: подставляя в многочлен f вместо x координаты пропорциональных векторов v и λv, задающих одну и ту же точку в $\mathbb{P}_n$, мы получим различные значения $f(v) \neq f(\lambda v)$.

Тем не менее, *однородный* многочлен $f \in \Bbbk[x_0, x_1, \dots, x_n]$ степени d корректно определяет в $\mathbb{P}_n$ фигуру

$$V(f) \overset{\text{def}}{=} \{ v \in V \mid f(v) = 0 \} \qquad (18\text{-}1)$$

которая называется *проективной гиперповерхностью* степени d. В самом деле, поскольку $f(\lambda v) = \lambda^d f(v)$, равенства

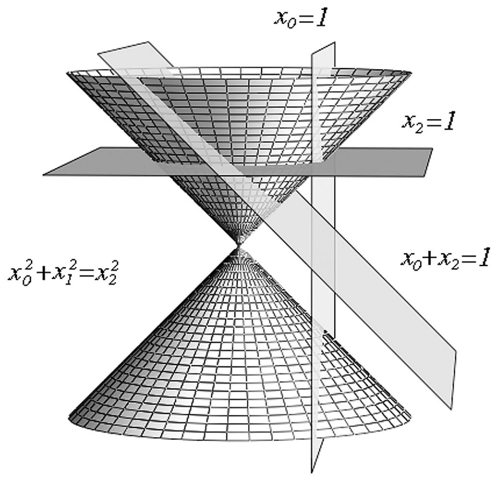


Рис. 18◇5. Конус.

$$f(v) = 0 \quad \text{и} \quad f(\lambda v) = 0$$

эквивалентны друг другу. Говоря геометрически, уравнение $f(v) = 0$ задаёт в аффинном пространстве $\mathbb{A}(V)$ конус с вершиной в нуле: вместе с каждой точкой $P \neq O$ он содержит всю прямую OP, и проективная гиперповерхность $V(f) \subset \mathbb{P}(V)$ состоит из точек, отвечающих этим прямым OP. Конус, задаваемый уравнением $f = 0$ в аффинном пространстве $\mathbb{A}(V)$ называется *аффинным конусом* над проективной гиперповерхностью $V(f) \subset \mathbb{P}(V)$.

18.2.1. Пример: гладкая коника. Посмотрим как выглядит в различных аффинных картах кривая C, заданная в однородных координатах на плоскости $\mathbb{P}_2 = \mathbb{P}(\mathbb{R}^3)$ уравнением второй степени

$$x_0^2 + x_1^2 = x_2^2 \qquad (18\text{-}2)$$

В стандартной карте U_{x_0}, где $x_0 = 1$, в локальных координатах

$$t_1 = x_1|_{U_{x_0}} = x_1/x_0 \quad \text{и} \quad t_2 = x_2|_{U_{x_0}} = x_2/x_0$$

уравнение (18-2) превращается в уравнение гиперболы $t_2^2 - t_1^2 = 1$. В стандартной карте U_{x_2}, где $x_2 = 1$, с локальными аффинными координатами

$$t_0 = x_0|_{U_{x_2}} = x_0/x_2 \quad \text{и} \quad t_1 = x_1|_{U_{x_2}} = x_1/x_2$$

мы получим уравнение окружности $t_0^2 + t_1^2 = 1$. В карте $U_{x_0+x_2}$, где $x_0 + x_2 = 1$, в локальных аффинных координатах

$$t = x_1|_{U_{x_0+x_2}} = x_0/(x_0 + x_2) \quad \text{и} \quad u = (x_2 - x_0)|_{U_{x_0+x_2}} = (x_2 - x_0)/(x_0 + x_2)$$

мы получим уравнение параболы $t^2 = u$ (надо перенести x_1^2 в (18-2) слева направо и поделить обе части на $(x_2 - x_0)^2$).

Таким образом, аффинные эллипс, гипербола и парабола суть изображения одной и той же проективной кривой (18-2) в различных картах. Облик C в карте $U_\xi \subset \mathbb{P}_2$ определяется тем, как располагается по отношению к C бесконечно удалённая прямая $\mathbb{P}_1 = \mathbb{P}(\operatorname{Ann}\xi)$ этой карты: эллипс, парабола и гипербола возникают, соответственно, когда эта прямая не пересекается с C, касается C и пересекается с C в двух различных точках (см. рис. 18◇5).

18.2.2. Проективное замыкание аффинной гиперповерхности

$$S = \{(t_1, t_2, \dots, t_n) \in \mathbb{A}^n \mid f(t) = 0\}$$

заданной в аффинном координатном пространстве $\mathbb{A}^n = \mathbb{A}(\Bbbk^n)$ с координатами $(t_1, t_2, \dots, t_n)$ произвольным (неоднородным) многочленом $f \in \Bbbk[t_1, t_2, \dots, t_n]$, — это проективная гиперповерхность

$$\overline{S} = V(\overline{f}) \subset \mathbb{P}_n$$

заданная в проективном пространстве $\mathbb{P}_n = \mathbb{P}(\Bbbk^{n+1})$ с однородными координатами $(x_0, x_1, \dots, x_n)$ однородным многочленом $\overline{f} \in \Bbbk[x_0, x_1, \dots, x_n]$ степени $\deg \overline{f} = \deg f$, пересечение которой со стандартной аффинной картой U_0 с координатами $t_i = x_i|_{U_0}$ совпадает с S. Последнее означает, что

$$f(t_1, t_2, \dots, t_n) = \overline{f}(1, t_1, t_2, \dots, t_n)\,.$$

Это соотношение (вместе с условием $\deg \overline{f} = \deg f$) определяет однородный многочлен $\overline{f}$ однозначно: следует заменить в f переменные t_i на x_i и приписать к каждому моному такую степень x_0, чтобы многочлен сделался однородным. Если

$$\begin{aligned} f(t_1, t_2, \dots, t_n) &= \\ &= f_0 + f_1(t_1, t_2, \dots, t_n) + f_2(t_1, t_2, \dots, t_n) + \dots + f_d(t_1, t_2, \dots, t_n)\,, \end{aligned}$$

где каждый $f_i \in \Bbbk[t_1, t_2, \dots, t_n]$ однороден степени i, то

$$\overline{f}(x_0, x_1, \dots, x_n) = f_0 \cdot x_0^d + f_1(x_1, x_2, \dots, x_n) \cdot x_0^{d-1} + \dots + f_d(x_1, x_2, \dots, x_n).$$

Дополнение $\overline{S} \smallsetminus S = \overline{S} \cap U_0^{(\infty)}$ в однородных координатах $(x_1 : x_2 : \dots : x_n)$ на бесконечно удалённой гиперплоскости $x_0 = 0$ задаётся уравнением

$$f_d(x_1, x_2, \dots, x_n) = 0.$$

В аффинной геометрии векторы $v \in \Bbbk^n$, удовлетворяющие уравнению $f_d(v) = 0$, называются *асимптотическими направлениями* аффинной гиперповерхности $S \subset \mathbb{A}^n$. В проективной геометрии асимптотические направления превращаются в обычные точки гиперповерхности $\overline{S}$, ничем не отличающиеся от остальных точек, кроме того, что их не видно в карте U_0.

Например, проективным замыканием аффинной кубической кривой $x_1 = x_2^3$ является проективная кривая $x_0^2 x_1 = x_2^3$, которая имеет на бесконечности ровно одну точку $(0 : 1 : 0)$, видимую в аффинной карте U_1 как остриё полукубической параболы $x_0^2 = x_2^3$.

18.2.3. Пространство гиперповерхностей. Обозначим через

$$S^d V^* \subset \Bbbk[x_1, x_2, \dots, x_n]$$

векторное пространство однородных многочленов степени d от координат на векторном пространстве V. Поскольку пропорциональные уравнения задают одну и ту же проективную гиперповерхность $S \subset \mathbb{P}_n$, гиперповерхности степени d в $\mathbb{P}(V)$ являются точками проективного пространства $\mathbb{P}(S^d V^*)$, которое называется *пространством гиперповерхностей* степени d.

Упражнение 18.2. Какова размерность пространства гиперповерхностей степени d в $\mathbb{P}_n$?

Поскольку уравнение $f(p) = 0$ при фиксированном $p \in \mathbb{P}(V)$ является *линейным* уравнением на $f \in S^d V^*$, гиперповерхности степени d, проходящие через заданную точку p, образуют проективную в пространстве всех гиперповерхностей гиперплоскость.

Проективные подпространства $\mathbb{P}(U) \subset \mathbb{P}(S^d V^*)$ называются *линейными системами* гиперповерхностей. Если векторное подпространство $U \subset S^d V^*$ линейно порождается уравнениями $f_1, f_2, \dots, f_m$, то гиперповерхности из линейной системы $\mathbb{P}(U)$, порождённой гиперповерхностями $V(f_1), V(f_2), \dots, V(f_m)$, задаются уравнениями вида

$$\lambda_1 f_1 + \lambda_2 f_2 + \dots + \lambda_m f_m = 0,$$

где $\lambda_1, \lambda_2, \dots, \lambda_m \in \Bbbk$ — некоторые константы. Любая такая гиперповерхность обязательно содержит пересечение $V(f_1) \cap V(f_2) \cap \dots \cap V(f_m)$.

По старинной традиции, одномерные и двумерные линейные системы фигур называются, соответственно, *пучками* и *связками* таковых фигур.

Упражнение 18.3. Докажите, что в любом пучке гиперповерхностей (над любым полем) всегда найдётся гиперповерхность, проходящая через любую наперёд заданную точку.

18.2.4. Пример: наборы точек на $\mathbb{P}_1$ и кривая Веронезе. Фиксируем двумерное векторное пространство $U \simeq \Bbbk^2$ с координатами x_0, x_1 и рассмотрим проективную прямую $\mathbb{P}_1 = \mathbb{P}(U)$. Всякое конечное множество точек

$$p_1, p_2, \dots, p_d \in \mathbb{P}_1 = \mathbb{P}(U)$$

(среди которых допускаются и совпадающие) является алгебраической гиперповерхностью d-той степени, задаваемой однородным многочленом[1]

$$f(x_0, x_1) = \prod_{\nu=1}^{d} \det(x, p_\nu) = \prod_{\nu=1}^{d} (p_{\nu,1}x_0 - p_{\nu,0}x_1)\ , \quad \text{где } p_\nu = (p_{\nu,0} : p_{\nu,1})\ . \tag{18-3}$$

Эта формула аналогична разложению неоднородного многочлена от одной переменной на линейные множители, отвечающие его корням на аффинной прямой $\mathbb{A}_1$, и мы будем называть точки $p_\nu \in \mathbb{P}_1$ *корнями* однородного многочлена f от переменных x_0, x_1. Из (18-3) вытекает, что однородный многочлен степени d от двух переменных имеет не более d различных корней на $\mathbb{P}_1$, а если поле $\Bbbk$ алгебраически замкнуто, то таковых корней, с учётом кратностей[2], имеется ровно d. Таким образом, над алгебраически замкнутым полем $\Bbbk$ имеется биекция между всевозможными конфигурациями из d-точек на $\mathbb{P}_1$ и точкам проективного пространства $\mathbb{P}_d = \mathbb{P}(S^dU^*)$ однородных многочленов степени d от x_0, x_1 с точностью до пропорциональности.

Конфигурации, в которых все d точек слипаются в одну, образуют (над любым полем) алгебраическую кривую $C_d \subset \mathbb{P}_d = \mathbb{P}(S^dU^*)$, которая называется *кривой Веронезе* степени d (а также *рациональной нормальной кривой* степени d). Эта кривая является образом *отображения Веронезе*

$$\mathbb{P}_1^\times = \mathbb{P}\left(U^*\right) \xrightarrow{v_d} \mathbb{P}_d = \mathbb{P}\left(S^dU^*\right)\ , \tag{18-4}$$

переводящего линейную форму $\varphi \in U^*$, задающую одну точку $p \in \mathbb{P}(U)$, в её d-ю степень $\varphi^d \in S^d(U^*)$, задающую d точек, собравшихся в одной точке p. Если записывать формы $\varphi \in U^*$ и $f \in S^d(U^*)$ в виде

$$\varphi(x) = \alpha_0 x_0 + \alpha_1 x_1 \quad \text{и} \quad f(x) = \sum_\nu a_\nu \cdot \binom{d}{\nu} x_0^{d-\nu} x_1^\nu$$

и использовать отношения коэффициентов $(\alpha_0 : \alpha_1)$ и $(a_0 : a_1 : \ \dots\ : a_d)$ в качестве однородных координат на $\mathbb{P}_1^\times = \mathbb{P}(U^*)$ и на $\mathbb{P}_d = \mathbb{P}(S^dU^*)$ соответственно,

[1] такие многочлены часто называют *бинарными формами*

[2] под кратностью корня p понимается максимальная степень линейной формы $\det(t, p)$, на которую делится f

кривая Веронезе будет задаваться параметрическим уравнением

$$(\alpha_0 : \alpha_1) \longmapsto (a_0 \colon a_1 \colon \ \dots \ : a_d) = \left(\alpha_0^d : \alpha_0^{d-1}\alpha_1 : \alpha_0^{d-2}\alpha_1^2 : \dots : \alpha_1^d\right) \ . \tag{18-5}$$

Таким образом, C_d состоит из всех точек $(a_0 \colon a_1 \colon \ \dots \ : a_d) \in \mathbb{P}_d$, координаты которых составляют геометрическую прогрессию. Это условие равносильно тому, что

$$\operatorname{rk}\begin{pmatrix} a_0 & a_1 & a_2 & \dots & a_{d-2} & a_{d-1} \\ a_1 & a_2 & a_3 & \dots & a_{d-1} & a_d \end{pmatrix} = 1 \ ,$$

и может быть выражено системой однородных уравнений второй степени — обращением в нуль всех 2×2-миноров этой матрицы.

Например, кривая $C_2 \subset \mathbb{P}_2$ образована всеми квадратными трёхчленами $a_0x_0^2 + 2a_1x_0x_1 + a_2x_1^2$, которые являются полными квадратами. Она задаётся известным из школы уравнением

$$D/4 = -\det\begin{pmatrix} a_0 & a_1 \\ a_1 & a_2 \end{pmatrix} = a_1^2 - a_0a_2 = 0 \tag{18-6}$$

и допускает следующее параметрическое задание:

$$a_0 = \alpha_0^2 \ , \quad a_1 = \alpha_0\alpha_1 \ , \quad a_2 = \alpha_1^2 \ . \tag{18-7}$$

Пересечение кривой (18-5) с произвольной гиперплоскостью, заданной уравнением $\sum A_\nu a_\nu = 0$, состоит корней $(\alpha_0 : \alpha_1) \in \mathbb{P}_1$ однородного многочлена $\sum A_\nu \cdot \alpha_0^{d-\nu}\alpha_1^\nu$ степени d, каковых имеется не более d. Поэтому при $2 \leqslant m \leqslant d$ никакие $m+1$ точек кривой C_d не лежат в одном $(m-1)$-мерном подпространстве. Над алгебраически замкнутым полем пересечение кривой C_d с любой гиперплоскостью состоит в точности из d точек — именно поэтому мы и сказали выше, что *степень* кривой C_d равна d.

18.3. Подпространства. Проективизация $\mathbb{P}(U) \subset \mathbb{P}(V)$ векторного подпространства $U \subset V$ называется *проективным подпространством.*

Например, прямая $(a, b) \subset \mathbb{P}(V)$, проходящая через две различные точки $a, b \in \mathbb{P}(V)$, — это проективизация двумерного подпространства, порождённого непропорциональными векторами $a, b \in V$. Точки прямой (a, b) — это всевозможные линейные комбинации $p = \lambda a + \mu b$. Отношение $(\lambda : \mu)$ можно воспринимать как внутреннюю однородную координату на прямой (a, b) в базисе a, b. При этом точки $p = (\lambda : \mu)$, у которых $\lambda + \mu \neq 0$, будут видны в любой аффинной карте U_ξ, проходящей через концы векторов[1] a, b, как барицентрические комбинации

$$p = \frac{\lambda}{\lambda+\mu}\, a + \frac{\mu}{\lambda+\mu}\, b \,,$$

[1]т. е. такой, что $\xi(a) = \xi(b) = 1$

(делить на $\lambda+\mu$ нужно для того, чтобы $\xi(p)=1$), а точка $p=(-1:1)=b-a$, отвечающая направляющему вектору $\overrightarrow{ab}$ аффинной прямой (a,b), является для любой такой карты бесконечно удалённой точкой.

Более общим образом, минимальное проективное подпространство в $\mathbb{P}(V)$, содержащее точки $a_1, a_2, \dots, a_m \in \mathbb{P}(V)$ — это проективизация $\mathbb{P}(U) \subset \mathbb{P}(V)$ подпространства U, порождённого векторами $a_1, a_2, \dots, a_m \in V$. Она состоит из всех точек вида

$$\lambda_1 a_1 + \lambda_2 a_2 + \dots + \lambda_m a_m \in \mathbb{P}(V) \tag{18-8}$$

и представляет собою пересечение всех проективных подпространств, содержащих все точки a_i.

Упражнение 18.4. Покажите, что если поле $\Bbbk$ бесконечно, то любой конечный набор точек в $\mathbb{P}(V)$ можно одновременно увидеть в одной аффинной карте.

Если аффинная карта U_ξ содержит все точки a_i, т. е. $\xi(a_i)=1$ для всех i (чего можно добиться, заменяя a_i на $a_i/\xi(a_i)$, если все $\xi(a_i)\neq 0$), то значение ξ на точке (18-8) равно сумме коэффициентов $\xi(p)=\sum\lambda_i$. Таким образом, точка p видна в карте U_ξ тогда и только тогда, когда $\sum\lambda_i\neq 0$, и в этом случае она видна в ней как барицентрическая комбинация

$$p/\xi(p) = \sum \frac{\lambda_i}{\sum\lambda_i}\, p_i\,.$$

Упражнение 18.5. Рассмотрим произвольную аффинную карту $U_\xi \subset \mathbb{P}_n$ и произвольное k-мерное проективное подпространство $K \subset \mathbb{P}_n$. Покажите, что либо $K\cap U_\xi=\varnothing$, либо $K\cap U_\xi$ является k-мерным аффинным подпространством в U_ξ.

Из сл. 7.1, оценивающего размерность пересечения пары векторных подпространств, получается

Предложение 18.1

Для любых двух проективных подпространств $K, L \subset \mathbb{P}_n$

$$\dim(K\cap L) \geqslant \dim K + \dim L - n\,.$$

В частности, любые два подпространства дополнительных размерностей d и $n-d$ имеют в $\mathbb{P}_n$ непустое пересечение.

Доказательство. Пусть $K=\mathbb{P}(U)$, $L=\mathbb{P}(W)$ и $\mathbb{P}_n=\mathbb{P}(V)$. Тогда по сл. 7.1

$$\begin{aligned}\dim(K\cap L) &= \dim\mathbb{P}(U\cap W) = \\ &= \dim(U\cap W) - 1 \geqslant \dim(U)+\dim(W)-\dim(V)-1 = \\ &= \dim\mathbb{P}(U)+1+\dim\mathbb{P}(W)+1-n-2 = \dim K+\dim L-n\end{aligned}$$

Последнее утверждение вытекает из того, что нульмерное проективное пространство (проективизация одномерного векторного) это точка, т. е. непустое множество. □

18.3.1. Проективная двойственность. Проективные пространства

$$\mathbb{P}_n = \mathbb{P}(V) \quad \text{и} \quad \mathbb{P}_n^\times \overset{\text{def}}{=} \mathbb{P}(V^*)$$

называются *двойственными*. Геометрически, каждое из них представляет собою пространство гиперплоскостей в другом, ибо ненулевые линейные формы с точностью до пропорциональности это гиперплоскости.

Канонический изоморфизм $V^{**} \simeq V$ устанавливает биекцию $\mathbb{P}_n^{\times\times} \simeq \mathbb{P}(V)$, и взаимно однозначное соответствие $U \rightleftarrows \mathrm{Ann}\,(U)$ между подпространствами в V и их аннуляторами в V^* на геометрическом языке означает сопоставление k-мерному подпространству $K \subset \mathbb{P}_n$ $(n-k-1)$-мерного подпространства $K^\times \subset \mathbb{P}_n^\times$, которое можно описать либо как пересечение всех тех гиперплоскостей в $\mathbb{P}_n^\times$, что изображаются точками подпространства K, либо как множество точек в $\mathbb{P}_n^\times$, изображающих все проходящие через K гиперплоскости в $\mathbb{P}_n$.

Например, прямые ℓ на $\mathbb{P}_2$ задаются точками $\ell^\times \in \mathbb{P}_2^\times$, и каждая точка p на $\mathbb{P}_2$ двойственна прямой $p^\times = \{\ell^\times \in \mathbb{P}_2^\times \mid p \in \ell\}$, точки которой составляют пучок проходящих через p прямых $\ell \subset \mathbb{P}_2$. При этом прямая $(p_1, p_2) \subset \mathbb{P}_2$ двойственна точке пересечения прямых $p_1^\times \cap p_2^x \subset \mathbb{P}_2^\times$ (является единственной общей точкой двух пучков прямых, проходящих через p_1 и p_2) и т. д.

Таким образом, проективная двойственность позволяет переформулировать геометрические задачи на $\mathbb{P}_n$ в геометрические задачи на $\mathbb{P}_n^\times$ с обращением включений ($L_1 \subset L_2 \leftrightarrow L_1^\times \supset L_2^\times$) и линейной инцидентности (подпространства $L_1, L_2, \ldots, L_r$ порождают m-мерное подпространство, если и только если подпространства $L_1^\times, L_2^\times, \ldots, L_r^\times$ пересекаются по $(n-m-1)$-мерному подпространству). Например, три точки в $\mathbb{P}_3$ коллинеарны тогда и только тогда, когда три двойственные им плоскости пересекаются по прямой.

18.3.2. Дополнительные подпространства и проектирование. Подпространства

$$K = \mathbb{P}(U) \quad \text{и} \quad L = \mathbb{P}(W)$$

пространства $\mathbb{P}_n = \mathbb{P}(V)$ называются *дополнительными*, если $K \cap L = \varnothing$ и $\dim K + \dim L = n - 1$. Например, любые две непересекающиеся прямые в $\mathbb{P}_3$ дополнительны.

На языке линейной алгебры дополнительность означает, что соответствующие векторные пространства $U, W \subset V$ трансверсальны: $U \cap V = \{0\}$, и

$$\dim U + \dim W = \dim K + 1 + \dim L + 1 = (n+1) = \dim V\ ,$$

т. е. $V = U \oplus W$. В этом случае любой вектор $v \in V$ имеет единственное разложение $v = u + w$ с $u \in U$ и $w \in W$. Если v не содержится ни в U, ни в W, обе компоненты этого разложения отличны от нуля. Поэтому для любой точки $p \notin K \sqcup L$ существует единственная проходящая через p прямая (q, r) с $q \in K$ и $r \in L$. Действительно, точки $q = u$ и $r = w$ задают такую прямую, и наоборот, если вектор v, представляющий точку p, оказался в двумерной линейной оболочке ненулевых векторов $u \in U$ и $w \in W$, то одномерные подпространства, натянутые на u и w должны содержать компоненты разложения вектора v в силу единственности его разложения по U и W.

Таким образом, для любой пары дополнительных подпространств $K, L \subset \mathbb{P}_n$ определено отображение *проектирования на* L *из* K

$$\pi_L^K : (\mathbb{P}_n \setminus K) \longrightarrow L \,,$$

тождественно действующее на L и переводящее каждую точку $p \in \mathbb{P}_n \setminus (K \sqcup L)$ в точку пересечения с L единственной прямой, проходящей через p и пересекающей и K и L.

Например, пространство $\mathbb{P}_3$ можно спроектировать из точки на любую не проходящую через эту точку плоскость, а также из любой прямой на любую не пересекающую её прямую.

В однородных координатах $(x_0 : x_1 : \ \dots : x_n)$, согласованных с разложением $V = U \oplus W$ так, что $(x_0 : x_1 : \ \dots : x_m)$ являются координатами в K, а $(x_{m+1} : x_{m+2} : \ \dots : x_n)$ — в L, проекция π_L^K просто удаляет первые $(m+1)$ координат x_ν с $0 \leqslant \nu \leqslant m$.

18.3.3. Пример: проектирование коники на прямую. Рассмотрим проекцию $\pi_L^p : C \longrightarrow L$ коники C, заданной уравнением $x_0^2 + x_1^2 = x_2^2$, на прямую L, заданную уравнением $x_0 = 0$, из лежащей на C точки $p = (1 : 0 : 1)$.

В стандартной аффинной карте U_2, где $x_2 = 1$, она выглядит как на рис. 18◊6.

Каждая проходящая через p и какую-нибудь точку $t \in \ell$ прямая $\ell_t = (pt)$ пересекает C ещё ровно в одной отличной от p точке $q = q(t)$, причём однородные координаты точек $q = (q_0 : q_1 : q_2)$ и $t = (0 : t_1 : t_2)$ *рационально* выражаются друг друга:

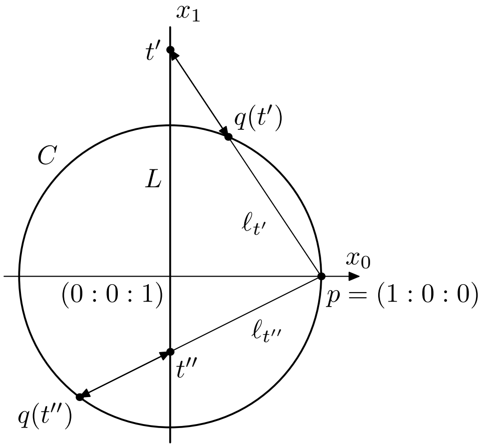


Рис. 18◊6. Проектирование коники.

$$\begin{aligned} (t_1 : t_2) &= (\, q_1 : (q_2 - q_0)\,) \\ (q_0 : q_1 : q_2) &= (\, (t_1^2 - t_2^2) : 2\, t_1 t_2 : (t_1^2 + t_2^2)\,) \end{aligned} \tag{18-9}$$

Упражнение 18.6. Проверьте эти формулы и обратите внимание, что вторая из них, когда $(t_1 : t_2)$ пробегает $\mathbb{Z} \times \mathbb{Z}$, дает полный список целочисленных решений уравнения Пифагора $q_0^2 + q_1^2 = q_2^2$.

Если сопоставить самой точке $p \in C$ бесконечно удалённую точку $(1 : 0 : 0)$, в которой прямая ℓ пересекает касательную к C в точке p прямую $x_0 = x_2$, мы получим *бирациональную биекцию* между точками прямой ℓ и точками коники C, задаваемую формулами (18-9).

Отметим, что обратимые линейные замены координат

$$\begin{cases} a_0 = x_2 + x_0 \\ a_1 = x_1 \\ a_2 = x_2 - x_0 \end{cases} \qquad \begin{cases} x_0 = (a_0 - a_2)/2 \\ x_1 = a_1 \\ x_0 = (a_0 + a_2)/2 \end{cases}$$

отождествляют конику C с коникой Веронезе $a_1^2 = a_0 a_2$ из n° 18.2.4, и параметризации (18-9) и (18-7) превращаются при этом друг в друга.

18.4. Линейные проективные преобразования. Любой линейный изоморфизм векторных пространств $F : U \xrightarrow{\sim} W$ корректно определяет биективное отображение $\overline{F} : \mathbb{P}(U) \xrightarrow{\sim} \mathbb{P}(W)$, которое называется *проективным линейным преобразованием* или *проективным изоморфизмом*.

Упражнение 18.7. Рассмотрим на $\mathbb{P}_2$ две прямые ℓ_1, ℓ_2 и точку $p \notin \ell_1 \cup \ell_2$. Убедитесь, что проекция из p задаёт проективный изоморфизм $\gamma_p : \ell_1 \xrightarrow{\sim} \ell_2$.

Лемма 18.1
Если $\dim U = \dim W = n+1$, то для любых двух упорядоченных наборов из $(n+2)$ точек $\{p_0, p_1, \dots, p_{n+1}\} \in \mathbb{P}(U)$ и $\{q_0, q_1, \dots, q_{n+1}\} \in \mathbb{P}(W)$, в каждом из которых которых никакие $(n+1)$ точек не лежат в одной гиперплоскости, существует единственный с точностью до пропорциональности линейный изоморфизм $F : U \xrightarrow{\sim} W$, такой что $\overline{F}(p_i) = q_i$ при всех i.

Доказательство. Зафиксируем некоторые векторы u_i и w_i, представляющие точки p_i и q_i, и возьмём $\{u_0, u_1, \dots, u_n\}$ и $\{w_0, w_1, \dots, w_n\}$ в качестве базисов в U и W. Для того, чтобы точки $p_0, p_1, \dots, p_n$ переводились преобразованием $\overline{F}$ в точки $q_0, q_1, \dots, q_n$, необходимо и достаточно, чтобы оператор F задавался в этих базисах диагональной матрицей с какими-нибудь ненулевыми константами $\lambda_0, \lambda_1, \dots, \lambda_n$ на главной диагонали. Равенство $\overline{F}(p_{n+1}) = q_{n+1}$ означает, что $F(u_{n+1}) = \lambda_{n+1} w_{n+1}$ для некоторого ненулевого $\lambda_{n+1} \in \mathbb{k}$. Переписывая это равенство в виде системы уравнений на координаты векторов

$$\begin{aligned} u_{n+1} &= x_0 u_0 + x_1 u_1 + \cdots + x_n u_n \\ w_{n+1} &= y_0 w_0 + y_1 w_1 + \cdots + y_n w_n \end{aligned} \tag{18-10}$$

получаем соотношения $y_i = \lambda_{n+1} \lambda_i x_i$ $(0 \leqslant i \leqslant n)$. Поскольку в разложении (18-10) все координаты x_i отличны от нуля[1] диагональные элементы матрицы F определяются из этих соотношений однозначно с точностью до умножения на ненулевую константу: $(\lambda_0, \lambda_1, \dots, \lambda_n) = \lambda_{n+1}^{-1} \cdot (y_1/x_1, y_2/x_2, \dots, y_n/x_n)$. □

Следствие 18.1
Два оператора тогда и только тогда задают одинаковые проективные изоморфизмы, когда они пропорциональны.

[1]в противном случае точка p_{n+1} оказалась бы в одной гиперплоскости с n базисными векторами, дополнительными к тому, вдоль которого обнулилась координата

18.4.1. Проективная линейная группа. Линейные проективные автоморфизмы пространства $\mathbb{P}(V)$ образуют группу, которая в силу лем. 18.1 изоморфна фактору полной линейной группы $\mathrm{GL}(V)$ по подгруппе гомотетий

$$H = \{\lambda \cdot \mathrm{Id} \mid \lambda \neq 0\} \subset \mathrm{GL}(V)\,.$$

Эта фактор группа обозначается $\mathrm{PGL}(V) = \mathrm{GL}(V)/H$ и называется *проективной линейной группой*. Выбор в V базиса отождествляет полную линейную группу $\mathrm{GL}(V)$ с группой невырожденных матриц GL_{n+1}. Проективная линейная группа $\mathrm{PGL}(V)$ отождествится при этом с группой PGL_{n+1} классов пропорциональности невырожденных матриц.

18.4.2. Пример: дробно линейные преобразования прямой. Группа проективных автоморфизмов прямой $\mathrm{PGL}_2(\Bbbk)$ образована классами пропорциональности невырожденных матриц

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\,.$$

Такая матрица действует на $\mathbb{P}_1$ по правилу

$$(x_0 : x_1) \xmapsto{\overline{A}} (\,(ax_0 + bx_1) : (cx_0 + dx_1)\,)\,.$$

В стандартной аффинной карте $U_1 \simeq \mathbb{A}^1$ с аффинной координатой $t = x_0/x_1$, это действие имеет вид дробно линейного преобразования

$$t \longmapsto \frac{at+b}{ct+d}\,.$$

В такой записи особенно хорошо видно, что пропорциональные матрицы действуют на $\mathbb{P}_1$ одинаково.

Единственное по лем. 18.1 дробно линейное преобразование, переводящее три заданных различных точки q, r, s в точки ∞, 0, 1 имеет вид

$$t \longmapsto \frac{t-r}{t-q} \cdot \frac{s-r}{s-q} \tag{18-11}$$

18.4.3. Двойное отношение. Правая часть равенства (18-11) называется *двойным отношением*[1] точек q, r, s, t и обозначается $[q, r, s, t]$. В однородных координатах двойное отношение четырёх точек выражается через попарные определители векторов, представляющих эти точки:

$$[p_1,\, p_2,\, p_3,\, p_4] = \frac{(p_1 - p_3)\,(p_2 - p_4)}{(p_1 - p_4)\,(p_2 - p_3)} = \frac{\det(p_1, p_3) \cdot \det(p_2, p_4)}{\det(p_1, p_4) \cdot \det(p_2, p_3)}\,. \tag{18-12}$$

[1] по-английски *cross-ratio*

Из определения сразу следует, что двойное отношение четырёх различных точек может принимать любые значения кроме ∞, 0 и 1 и что две упорядоченных четвёрки точек тогда и только тогда переводятся одна в другую дробно линейным преобразованием прямой, когда их двойные отношения одинаковы. Поскольку замена однородных координат является таким преобразованием, правая часть равенства (18-12) не зависит от выбора однородных координат, а средняя часть (выражающая двойное отношение через разности аффинных координат точек) не зависит ни от выбора аффинной карты, ни от выбора локальной аффинной координаты в ней при условии, что карта содержит все четыре точки (т. е. значения p_1, p_2, p_3, p_4 конечны).

Выясним, как изменяется двойное отношение при перестановках точек. Из формулы (18-12) очевидно, что подгруппа Клейна $\mathfrak{V}_4 \subset S_4$, состоящая из тождественного преобразования и одновременных транспозиций непересекающихся пар точек, не меняет двойного отношения:

$$[p_1, p_2, p_3, p_4] = [p_2, p_1, p_4, p_3] = [p_3, p_4, p_2, p_1] = [p_4, p_3, p_2, p_1] \tag{18-13}$$

Поэтому действие S_4 на множестве значений двойного отношения пропускается через эпиморфизм на группу треугольника $S_4 \twoheadrightarrow S_4/\mathfrak{V}_4 = S_3 = D_3$, состоящую из тождественного отображения, трёх отражений (представленных в S_4 транспозициями $(1,2)$, $(1,3)$ и $(1,4)$) и двух поворотов (представленных в S_4 циклами $|1,2,3\rangle$ и $|1,3,2\rangle$). Обозначая двойные отношения (18-13) через ϑ, получаем из определения (18-12) соотношения:

$$\begin{aligned}
&[p_1, p_2, p_3, p_4] = [p_2, p_1, p_4, p_3] = [p_3, p_4, p_2, p_1] = [p_4, p_3, p_2, p_1] = \vartheta\\
&[p_2, p_1, p_3, p_4] = [p_1, p_2, p_4, p_3] = [p_3, p_4, p_1, p_2] = [p_4, p_3, p_1, p_2] = \frac{1}{\vartheta}\\
&[p_3, p_2, p_1, p_4] = [p_2, p_3, p_4, p_1] = [p_1, p_4, p_2, p_3] = [p_4, p_1, p_2, p_3] = \frac{\vartheta}{\vartheta - 1}\\
&[p_4, p_2, p_3, p_1] = [p_2, p_4, p_1, p_3] = [p_3, p_1, p_2, p_4] = [p_1, p_3, p_2, p_4] = 1 - \vartheta\\
&[p_2, p_3, p_1, p_4] = [p_3, p_2, p_4, p_1] = [p_1, p_4, p_3, p_2] = [p_4, p_1, p_3, p_2] = \frac{\vartheta - 1}{\vartheta}\\
&[p_3, p_1, p_2, p_4] = [p_1, p_3, p_4, p_2] = [p_2, p_4, p_1, p_3] = [p_4, p_2, p_1, p_3] = \frac{1}{1 - \vartheta}\,.
\end{aligned} \tag{18-14}$$

Отметим, что есть три специальных значения $\vartheta = -1,\, 2,\, 1/2$, которые не меняются при транспозициях $(1,2)$, $(1,3)$ и $(1,4)$ соответственно и циклически переставляются двумя поворотами, а также два специальных значения ϑ, равные двум корням уравнения[1] $x^2 - x + 1 = 0$, которые не меняются при поворотах и переставляются между собой транспозициями точек. При всех остальных значениях ϑ мы получаем шесть различных значений двойного отношения.

[1] т. е. отличным от -1 кубическим корням из единицы в поле $\Bbbk$

18.4.4. Гармонические пары точек. Четвёрка точек $\{a, b; c, d\} \in \mathbb{P}_1$ называется *гармонической*, если их двойное отношение

$$[a, b, c, d] = -1\,.$$

При выполнении этого условия говорят также, что пары точек (a, b) и (c, d) *гармоничны* по отношению друг к другу.

Геометрически гармоничность означает, что в карте, для которой точка a лежит на бесконечности, точка b находится в центре тяжести точек c и d.

Алгебраически гармоничность равносильна тому, что изменение порядка точек в одной из пар не меняет двойного отношения, или тому, что двойное отношение не меняется при перемене пар местами — из (18-14) вытекает, что оба эти условия равносильны между собой.

Таким образом, гармоничность двух пар точек по отношению другу является *симметричным* отношением на парах *неупорядоченных* точек.

18.4.5. Пример: четырёхвешинник. С каждой четвёркой точек

$$a, b, c, d \in \mathbb{P}_2,$$

никакие 3 из которых не коллинеарны, связана конфигурация из трёх пар прямых, соединяющих пары этих точек (см. рис. 18◇7) и называемых *сторонами* четырёххвершинника $abcd$. Обозначим точки пересечения этих прямых через $x = (ab) \cap (cd)$, $y = (ac) \cap (bd)$, $z = (ad) \cap (bc)$. Тогда в каждом из трёх пучков прямых с центрами в точках x, y, z пара сторон четырёхвершинника гармонична по отношению к паре сторон треугольника xyz.

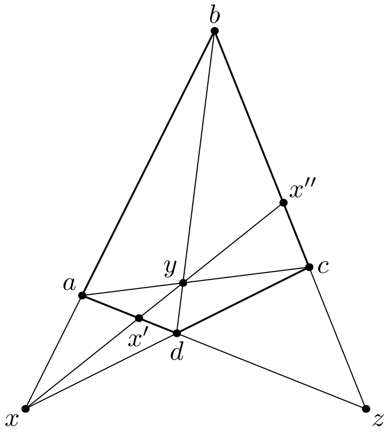


Рис. 18◇7. 4-вешинник.

Чтобы проверить это, запараметризуем пучок прямых, проходящих через точку x, точками прямой (ad) или точками прямой (bc) и покажем, что прямая (xy) пересекает прямые (ad) и (bc) по таким точкам x', x'', что $[a, d, z, x'] = [b, c, z, x''] = -1$.

Поскольку центральные проекции из x и из y являются дробно линейными изоморфизмами между прямыми (ad) и (bc), мы имеем следующие равенства двойных отношений соответственных точек:

$$[a, d, z, x'] = [b, c, z, x''] = [d, a, z, x']\,.$$

Коль скоро результате перестановки первых двух точек двойное отношение не поменялось, оно равно -1.

Задачи для самостоятельного решения к §18

Задача 18.1. При каком условии на три прямые ℓ_0, ℓ_1, ℓ_2 на проективной плоскости $\mathbb{P}_2 = \mathbb{P}(V)$ в пространстве V можно выбрать базис так, чтобы каждая прямая ℓ_i была бесконечно удалённой для стандартной аффинной карты U_i ?

Задача 18.2. На прямых (AB), (BC), $(CA) \subset \mathbb{P}_2$ взяли точки

$$A' = (1:0:0) \in (BC)\,, \quad B' = (0:1:0) \in (AC)\,, \quad C' = (0:0:1) \in (AB)\,.$$

Оказалось, что прямые (AA'), (BB') и (CC') пересекаются в точке $(1:1:1)$. Найдите координаты вершин $\triangle\, ABC$.

Задача 18.3. Покажите, что подмножество в $\mathbb{P}(V)$ тогда и только тогда имеет вид $\mathbb{P}(W)$ для некоторого $(k+1)$-мерного векторного подпространства W, когда во всех аффинных картах, имеющих с ним непустое пересечение, оно видно как k-мерное аффинное подпространство.

Задача 18.4. Пусть основное поле конечно и состоит из q элементов. Сколько всего имеется а) точек, прямых, … , k-мерных аффинных подпространств в $\mathbb{A}^n$? б) точек, прямых, … , k-мерных проективных подпространств в $\mathbb{P}_n$?

Задача 18.5. Кривые а) $y = x^2$ б) $y = x^3$ в) $y^2 + (x-1)^2 = 1$ г) $y^2 = x^2(x+1)$ заданы в стандартной карте U_0 на $\mathbb{P}_2 = \mathbb{P}(\mathbb{R}^3)$. Напишите их уравнения в картах U_1 и U_2 и нарисуйте все эти 12 аффинных кривых.

Задача 18.6. Вложим евклидову плоскость $\mathbb{R}^2$ в комплексную проективную плоскость $\mathbb{P}_2 = \mathbb{P}(\mathbb{C}^3)$ в качестве точек с вещественными координатами, лежащих в стандартной аффинной карте U_0. Найдите в $\mathbb{P}_2$ две различных точки, лежащие на всех кривых второй степени, видных в $\mathbb{R}^2$ как окружности, и покажите, что любая кривая второй степени в $\mathbb{P}_2$, проходящая через эти две точки и имеющая хотя бы 3 неколлинеарные точки в $\mathbb{R}^2$, будет видна в $\mathbb{R}^2$ как окружность.

Задача 18.7 (инволюции на прямой). Отличный от тождественного проективный автоморфизм σ называется *инволюцией*, если $\sigma^2 = \mathrm{Id}$.
а) Покажите, что над алгебраически замкнутым полем любая инволюция на $\mathbb{P}_1$ имеет ровно две различных неподвижных точки.
б) Пусть инволюция σ на $\mathbb{P}_1$ имеет неподвижные точки p и q. Покажите, что отличные от p и q точки a и b находятся в инволюции σ (т. е. $\sigma(a) = b$) тогда и только тогда, когда пары точек a, b и p, q гармоничны друг другу (т. е. $[\,a, b, p, q\,] = -1$).

Задача 18.8 (теорема Дезарга). Даны $\triangle\, A_1B_1C_1$ и $\triangle\, A_2B_2C_2$ на $\mathbb{P}_2$. Докажите, что три точки пересечения пар их поименованных одинаковыми буквами сторон коллинеарны тогда и только тогда, когда три прямые, проходящие через пары поименованных одинаковыми буквами вершин, пересекаются в одной точке (треугольники с такими свойствами называются *перспективными*).

Задача 18.9 (перекрёстная ось[1]). На $\mathbb{P}_2$ даны две прямые $\ell_1 \neq \ell_2$. Линейный проективный изоморфизм $\varphi : \ell_1 \xrightarrow{\sim} \ell_2$ переводит три заданных точки a_1, b_1, c_1 на ℓ_1 в три заданных точки a_2, b_2, c_2 на ℓ_2.

а) Опишите ГМТ пересечения прямых $(x, \varphi(y)) \cap (y, \varphi(x))$, где $x \neq y$ независимо пробегают ℓ_1.
б) Одной линейкой постройте $\varphi(x)$ для произвольно заданной точки $x \in \ell_1$.
в) Решите двойственную задачу: одной линейкой постройте образ данной прямой ℓ из пучка прямых, проходящих через данную точку $p_1 \in \mathbb{P}_2$, при проективном изоморфизме этого пучка с пучком прямых, проходящих через другую данную точку $p_2 \in \mathbb{P}_2$, если известно действие этого изоморфизма на какие-нибудь три прямые.
г) Одной линейкой постройте образ $\varphi(x)$ произвольной точки $x \in \ell \subset \mathbb{P}_2$ при линейном проективном автоморфизме $\psi : \ell \xrightarrow{\sim} \ell$, если известно действие ψ на какие-нибудь три точки.

Задача 18.10. Докажите, что над бесконечным полем $\Bbbk$ никакие $m+1$ точек кривой Веронезе $C_d \subset \mathbb{P}_d$ не лежат в одном $(m-1)$-мерном подпространстве (для всех $1 \leqslant m \leqslant d$).

Задача 18.11. Спроектируйте кубику Веронезе $C_3 \subset \mathbb{P}_3 = \mathbb{P}\left(S^3U^*\right)$ из n° 18.2.4
а) из точки t_0^3 на плоскость $\left(3\,t_0^2t_1,\, 3\,t_0t_1^2,\, t_1^3\right)$
б) из точки $3\,t_0^2t_1$ на плоскость $\left(t_0^3,\, 3\,t_0t_1^2,\, t_1^3\right)$
в) из точки $t_0^3 + t_1^3$ на плоскость $\left(t_0^3,\, 3\,t_0^2t_1,\, 3\,t_0t_1^2\right)$.
Напишите параметрические и «внешние» уравнения тех кривых, которые при этом получатся, в каждой из трёх стандартных аффинных карт на плоскости – образе проекции и нарисуйте все девять аффинных кривых, которые при этом получатся.

Задача 18.12 (плоские рациональные кривые). Предположим, что поле $\Bbbk$ алгебраически замкнуто. Плоская кривая $C \subset \mathbb{P}_2$ называется *рациональной*, если существуют однородные многочлены $p_0(t_0 : t_1)$, $p_1(t_0 : t_1)$, $p_2(t_0 : t_1)$ одинаковой степени, не имеющие общего делителя и такие, что отображение

$$\mathbb{P}_1 \longrightarrow \mathbb{P}_2 : \ (t_0 : t_1) \longmapsto (p_0(t_0 : t_1) : p_1(t_0 : t_1) : p_2(t_0 : t_1))$$

корректно определено и является биекцией между $\mathbb{P}_1$ и C всюду за исключением, может быть, конечного множества точек.
а) Пересекая C прямыми, покажите, что $\deg C = \deg p_i$.
б) Покажите, что любая плоская рациональная кривая степени d является проекцией кривой Веронезе $C_d \subset \mathbb{P}_d$ на подходящую плоскость $\mathbb{P}_2 \subset \mathbb{P}_d$.
в) Выведите из зад. 18.11, что гладкая (без самопересечений и заострений[1]) плоская кубическая кривая не рациональна.

Задача 18.13 (рациональная нормальная кривая). Покажите, что любые две из описываемых далее кривых $C \subset \mathbb{P}_n$ переводятся друг в друга подходящим линейным изоморфизмом. а) Кривая Веронезе $C = C_n \subset \mathbb{P}(S^nU^*)$.

[1]формальные определения таковы: точка p кривой $C = V(f) \subset \mathbb{P}_2$ называется *особой*, если она является кратным корнем (в смысле n° 18.2.4) ограничения многочлена f на любую проходящую через p прямую; кривая называется *гладкой*, если у неё нет особых точек; покажите, что у проекций из п.п. (б) и (в) зад. 18.11 есть особые точки (над алгебраически замкнутым полем)

б) Зафиксируем любой линейно независимый набор однородных многочленов n-той степени $f_0, f_1, \dots, f_n \in \Bbbk[t_0, t_1]$. Кривая C есть образ отображения

$$\mathbb{P}_1 \longrightarrow \mathbb{P}_n \,:\, (t_0 : t_1) \longmapsto (f_0(t_0,t_1) : f_1(t_0,t_1) : \cdots : f_n(t_0,t_1)) \,.$$

в) Зафиксируем $n+1$ точек $p_0, p_1, \dots, p_n \in \mathbb{P}_1$. Пусть $p_\nu = (\alpha_\nu : \beta_\nu)$. Положим $\det(p_\nu, t) = \alpha_\nu t_1 - \beta_\nu t_0$. Кривая C есть образ отображения

$$\mathbb{P}_1 \longrightarrow \mathbb{P}_n \,:\, t = (t_0 : t_1) \longmapsto \left(\frac{1}{\det(p_0,t)} : \frac{1}{\det(p_1,t)} : \cdots : \frac{1}{\det(p_n,t)} \right) .$$

г) Зафиксируем $n{+}3$ точки $p_1, p_2, \dots, p_n$, a, b, $c \in \mathbb{P}_n$, никакие $(n{+}1)$ из которых не лежат в одной гиперплоскости, и обозначим через $\ell_i \simeq \mathbb{P}_1$ пучок гиперплоскостей в $\mathbb{P}_n$, проходящих через все точки p_ν кроме p_i. Для всех $i \neq j$ зададим линейный проективный изоморфизм $\psi_{ij} : \ell_j \xrightarrow{\sim} \ell_i$ так, чтобы 3 гиперплоскости пучка ℓ_j, проходящие через точки a, b, c, переходили в аналогичные 3 гиперплоскости пучка ℓ_i. Кривая C есть ГМТ пересечения соответственных гиперплоскостей $C = \bigcup\limits_{H \in \ell_1} H \cap \psi_{21}(H) \cap \ldots \cap \psi_{n1}(H)$.

Задача 18.14. Покажите, что через любые $n+3$ точки в $\mathbb{P}_n$, никакие $n+1$ из которых не лежат в одной гиперплоскости, проходит единственная рациональная нормальная кривая.

Задача 18.15 (проективная эквивалентность $(n+3)$ точек на $\mathbb{P}_n$). Набор из $n+3$ точек на $\mathbb{P}_n$ называется *линейно общим*, если никакие $n+1$ точек этого набора не лежат в одной гиперплоскости. Согласно зад. 18.14 через любой линейно общий набор точек можно провести рациональную нормальную кривую C, которую можно биективно отобразить на $\mathbb{P}_1$ одним из способов, перечисленных в зад. 18.13. Будем называть двойным отношением четырёх точек в рассматриваемом наборе из $n+3$ точек двойное отношение их образов на $\mathbb{P}_1$.

а) Покажите, что это определение корректно в том смысле, что любые два отождествления C с $\mathbb{P}_1$ отличаются друг от друга дробно линейным автоморфизмом $\mathbb{P}_1$ (сохраняющим все двойные отношения).

б) Покажите, что два линейно общих набора из $n+3$ точек на $\mathbb{P}_n$ тогда и только тогда переводятся друг в друга некоторым линейным проективным автоморфизмом, когда двойные отношения любых двух четвёрок соответственных точек в этих наборах одинаковы.

§19. Квадрики

Всюду в этом параграфе предполагается, что $\mathrm{char}(\Bbbk) \neq 2$.

19.1. Проективные квадрики. Проективная гиперповерхность

$$Q = V(q) = \{v \in \mathbb{P}(V) \mid q(v) = 0\}\,,$$

заданная однородным многочленом второй степени $q \in S^2V^*$ называется *проективной квадрикой*. Две квадрики называются *изоморфными* (или *проективно эквивалентными*), если одна переводится в другую линейным проективным автоморфизмом.

Согласно сл. 17.3 уравнение квадрики $V(q) \subset \mathbb{P}_n = \mathbb{P}(V)$ в подходящих однородных координатах имеет вид

$$x_0x_1 + x_2x_3 + \cdots + x_{2m}x_{2m+1} + \alpha(x_{2m+2}, \dots, x_r) = 0\,, \tag{19-1}$$

где форма $\alpha(x)$ анизотропна (т. е. $\alpha(x) \neq 0$ при $x \neq 0$). Число входящих в уравнение переменных равно рангу $\mathrm{rk}\, q$ квадратичной формы q, а линейная оболочка остальных $n - r$ базисных векторов, координаты вдоль которых не задействованы в (19-1), составляет ядро формы q. Число $2(m+1)$ в уравнении (19-1) равно размерности гиперболического ортогонального слагаемого формы q и по сл. 17.4 не зависит от выбора координат, где форма q имеет вид (19-1).

19.1.1. Гладкие квадрики. Квадрики с нулевым ядром, т. е. с $r = n$ или, что то же самое, с $\det q \neq 0$, называются *невырожденными* или *гладкими*.

Линейные проективные изоморфизмы $\overline{F} : \mathbb{P}(V) \xrightarrow{\sim} \mathbb{P}(V)$, индуцированные изометрическими изоморфизмами $F \in \mathrm{O}_q$ невырожденной квадратичной формы q, переводят квадрику $Q = V(q)$ в себя и называются *автоморфизмами* проективной квадрики. Согласно сл. 17.6 группа проективных автоморфизмов квадрики Q транзитивно действует на точках квадрики, а также лежащих на квадрике проективных подпространствах любой фиксированной размерности. Размерность максимального проективного подпространства, лежащего на невырожденной квадрике Q, заданной уравнением

$$x_0x_1 + x_2x_3 + \cdots + x_{2m}x_{2m+1} + \alpha(x_{2m+2}, \dots, x_n) = 0\,,$$

равна m, и через каждую точку квадрики Q проходит лежащее на Q подпространство такой размерности. Мы будем называть число m *планарностью* неособой квадрики Q. Если форма $q(x_0, x_1, \dots, x_n) = \alpha(x_0, x_1, \dots, x_n)$ анизотропна, то квадрика Q пуста, а её планарность равна -1. Неособые квадрики разной планарности проективно не эквивалентны.

19.1.2. Гладкие квадрики над замкнутым полем. Поскольку над алгебраически замкнутым полем $\Bbbk$ имеется ровно одна анизотропная форма x^2, n-мерная гладкая квадрика $Q_n \subset \mathbb{P}_{n+1}$ над алгебраически замкнутым полем единственна и в подходящих координатах она задаётся при чётном $n = 2m$ уравнением

$$x_0x_1 + x_2x_3 + \cdots + x_{2m}x_{2m+1} = 0\,, \tag{19-2}$$

при нечётном $n = 2m+1$ уравнением

$$x_0x_1 + x_2x_3 + \cdots + x_{2m}x_{2m+1} = x_{2m+2}^2\,. \tag{19-3}$$

Через каждую точку обеих квадрик (19-2) и (19-3) проходит m-мерное проективное подпространство, лежащее на квадрике, и подпространств большей размерности на этих квадриках нет.

19.1.3. Пример: гладкие вещественные квадрики. Поскольку над полем $\Bbbk = \mathbb{R}$ в каждой размерности k имеется единственная с точностью до знака анизотропная форма $\alpha_k(x_1, x_2, \dots, x_k) = \sum\limits_{i=1}^{k} x_i^2$, гладкая n-мерная вещественная квадрика в $\mathbb{P}_{n+1} = \mathbb{P}(\mathbb{R}^{n+2})$ в подходящих координатах имеет вид

$$x_0x_1 + x_2x_3 + \cdots + x_{2m}x_{2m+1} = x_{2m+2}^2 + x_{2m+3}^2 + \cdots + x_{n+1}^2\,, \tag{19-4}$$

где $-1 \leqslant m \leqslant n/2$. Мы будем называть такую квадрику *m-планарной* и обозначать $Q_{n,m}$. Иначе m-планарную квадрику $Q_{n,m}$ можно охарактеризовать как квадрику сигнатуры $(n+2-m, m)$ или как как квадрику индекса $n+2-2m$. В координатах Лагранжа уравнение квадрики $Q_{n,m}$ имеет вид

$$t_0^2 + t_1^2 + \cdots + t_m^2 = t_{m+1}^2 + t_{m+2}^2 + \cdots + t_{n+1}^2\,. \tag{19-5}$$

Переход от гиперболических координат x_ν к лагранжевым координатам t_ν задаётся формулами $x_{2i} = t_{m+i} + t_i$, $x_{2i+1} = t_{m+i} - t_i$ при $0 \leqslant i \leqslant m$ и $x_j = t_j$ при $2m+2 \leqslant j \leqslant n+2$.

Квадрики разной планарности проективно неэквивалентны, так как через каждую точку m-планарной квадрики проходит m-мерное проективное подпространство, лежащее на квадрике, и подпространств большей размерности на $Q_{n,m}$ нет. В частности, (-1)-планарная квадрика

$$x_0^2 + x_1^2 + \cdots + x_n^2 = 0$$

пуста. Непустая не содержащая прямых квадрика планарности нуль

$$t_0^2 = t_1^2 + t_2^2 + \cdots + t_n^2$$

называется *эллиптической*. Квадрики большей планарности называются *гиперболическими*.

19.1.4. Пример: квадрики на $\mathbb{P}_1$. Над произвольным полем $\Bbbk$ характеристики $\operatorname{char}(\Bbbk) \neq 2$ уравнение (19-1) на проективной прямой $\mathbb{P}_1$ имеет либо вид $x_0^2 = 0$ (если q вырождена), либо вид $x_0x_1 = 0$ (если форма q невырождена и $-\det q$ квадрат), либо вид $x_0^2 - a\,x_1^2$, где $a \in \Bbbk$ не квадрат (если форма q невырождена и $-\det q$ не квадрат).

Вырожденная квадрика $x_0^2 = 0$ называется *двойной точкой*, ибо состоит из единственной точки $(0 : 1)$, а её уравнение представляет собой квадрат линейной формы, обращающейся в этой точке в нуль.

Неособая гиперболическая квадрика $x_0x_1 = 0$ имеет планарность 0 и состоит из двух различных точек. Неособая анизотропная квадрика $x_0^2 - a\,x_1^2$ планарности -1 пуста, и над алгебраически замкнутым полем $\Bbbk$ таких квадрик нет.

Следствие 19.1
Для пересечения произвольной квадрики Q с произвольной прямой ℓ имеется ровно четыре альтернативных возможности: либо $\ell \subset Q$, либо $\ell \cap Q$ является двойной точкой, либо $\ell \cap Q$ состоит из двух различных точек, либо $\ell \cap Q = \varnothing$. Над алгебраически замкнутым полем последний случай не реализуется. □

19.1.5. Пример: квадрики на $\mathbb{P}_2$. Плоские квадрики называются *кониками*. На плоскости уравнение (19-1) может принимать вид

$$x_0^2 = 0 \qquad (\operatorname{rk} q = 1) \tag{19-6}$$

$$x_0x_1 = 0 \qquad (\operatorname{rk} q = 2,\ i = 0) \tag{19-7}$$

$$x_0^2 - a\,x_1^2 = 0 \qquad (\operatorname{rk} q = 2,\ i = -1,\ a \in \Bbbk \text{ не квадрат}) \tag{19-8}$$

$$x_0x_1 = x_2^2 \qquad (\operatorname{rk} q = 3,\ i = 0,\ V(q) \neq \varnothing) \tag{19-9}$$

$$\alpha(x_0, x_1, x_2) = 0 \qquad (\operatorname{rk} q = 3,\ i = -1,\ \alpha(x) \text{ анизотропна},\ V(q) = \varnothing) \tag{19-10}$$

Коника (19-6) ранга 1 называется *двойной прямой*. Её уравнение — это квадрат линейной формы, зануляющейся на двумерном ядре квадратичной формы q. Геометрически такая коника представляет собою прямую — проективизацию ядра квадратичной формы q.

Непустая коника (19-7) ранга 2 называется *распавшейся коникой* и представляет собой пару различных прямых, пересекающихся точке $(0 : 0 : 1)$, которая является проективизацией одномерного ядра формы q.

Вырожденная коника (19-8) называется *двойной точкой*. Она состоит из единственной точки $p = (0 : 0 : 1) \in \mathbb{P}_2$, которая является проективизацией одномерного ядра квадратичной формы q. Название «двойная точка» связано с тем, что пересечение этой коники с любой проходящей через p прямой, будучи рассмотрено как квадрика на этой прямой, представляет собою двойную точку p в смысле классификации из n° 19.1.4. Отметим, что над алгебраически замкнутым полем одноточечной коники (19-8) не существует.

Гладкая коника (19-10) пуста и над алгебраически замкнутым полем также не встречается.

Непустая *гладкая коника* (19-9) это *коника Веронезе* C_2 из (18-6). Её удобно представлять себе следующим образом. Рассмотрим плоскость $\mathbb{P}_2 = \mathbb{P}(S^2U^*)$, точки которой суть классы пропорциональных квадратичных форм

$$x_0t_0^2 + 2\,x_2\,t_0t_1 + x_1t_1^2 = 0$$

на прямой $\mathbb{P}_1 = \mathbb{P}(U)$ с однородной координатой $(t_0 : t_1)$. Гладкая коника $C_2 \subset \mathbb{P}_2$ состоит из нулевых вырожденных квадрик $(\alpha_0t_0 + \alpha_1t_1)^2$. Она задаётся уравнением

$$\det\begin{pmatrix} x_0 & x_2 \\ x_2 & x_1 \end{pmatrix} = x_0x_1 - x_2^2 = 0\,. \tag{19-11}$$

и имеет рациональную параметризацию

$$(\alpha_0 : \alpha_1) \longmapsto (x_0 : x_1 : x_2) = (\alpha_0^2 : \alpha_1^2 : \alpha_0\alpha_1)\,. \tag{19-12}$$

Предложение 19.1
Непустая гладкая коника C пересекает произвольную плоскую кривую, заданную однородным уравнением степени d, не более, чем по $2\,d$ точкам, либо целиком содержится в этой кривой в качестве компоненты.

Доказательство. Приведём уравнение C к виду (19-11) и запараметризуем C по формулам (19-12). Значения параметра $\alpha = (\alpha_0 : \alpha_1)$, при которых C пересекает кривую, заданную уравнением $f(x) = 0$, суть корни однородного многочлена $f(x(\alpha))$, который либо имеет степень $2\,d$, либо равен нулю тождественно. □

Предложение 19.2
Через любые 5 точек на $\mathbb{P}_2$ можно провести конику. Если никакие 4 из пяти точек не коллинеарны, то такая коника единственна, а если никакие 3 не коллинеарны, то она невырождена.

Доказательство. Классы пропорциональных квадратичных форм на трёхмерном пространстве V образуют пятимерное проективное пространство $\mathbb{P}_5 = \mathbb{P}(S^2V^*)$. Поскольку при фиксированном p уравнение $q(p) = 0$ линейно по q, коники, проходящие через данную точку $p \in \mathbb{P}_2$, образуют в этом $\mathbb{P}_5$ гиперплоскость. Поскольку любые 5 гиперплоскостей в $\mathbb{P}_5$ имеют непустое пересечение, требуемая коника существует. Если какие-то три из точек коллинеарны, то коника содержит проходящую через них прямую, и потому распадается на эту прямую и прямую, проходящую через две другие точки. Если никакие три из точек не коллинеарны, всякая проходящая через них коника автоматически неособа и единственна по предл. 19.1. □

19.1.6. Особые точки. Обозначим через $\widehat{q} : V \xrightarrow{v \mapsto \widetilde{q}(\,*\,,v)} V^*$, оператор *корреляции* (см. n° 17.1.2) квадратичной формы q, переводящий вектор $v \in V$ в линейную форму $\widehat{q}(v) \, : \, w \longmapsto \widetilde{q}(w, v)$. Форма q невырождена тогда и только тогда, когда $\widehat{q}$ изоморфизм. Проективное подпространство

$$\operatorname{Sing} Q = \mathbb{P}(\ker q) \subset \mathbb{P}(V)$$

называется *множеством особых точек* (или *вершинным пространством*) квадрики Q. Например, вершинными пространствами двойной точки из n° 19.1.4 и двойной точки (19-8) являются сами эти точки, вершинным пространством двойной прямой (19-6) тоже является сама эта прямая, а вершинным пространством распавшейся коники (19-7) является точка пересечения пары прямых, из которых она состоит.

Вершинное пространство любой особой квадрики всегда лежит на этой квадрике. В частности, особая квадрика никогда не пуста. Особые точки квадрики имеют следующую инвариантную геометрическую характеризацию.

Лемма 19.1
Точка $a \in Q$ тогда и только тогда особая, когда любая проходящая через a прямая либо целиком лежит на Q либо пересекает Q по двойной точке a.

Доказательство. Если точка $a \in \operatorname{Sing} Q$, то $\widetilde{q}(a, b) = 0$ для любой точки b, и единственным ненулевым элементом матрицы Грама ограничения q на прямую (a, b) в базисе a, b может быть только $\widetilde{q}(b, b) = q(b)$. Если этот элемент нулевой, прямая изотропна и лежит на Q, если он не нулевой, уравнение квадрики $Q \cap (a, b) \subset \mathbb{P}_1 = (a, b)$ координатах $(x_0 : x_1)$ относительно базиса a, b имеет вид $q(b)x_1^2$ и задаёт двойную точку a. Наоборот, если $a \in Q$ неособа, то найдётся точка b дополняющая изотропный вектор a до гиперболической плоскости, и тогда $Q \cap (a, b)$ будет гиперболической квадрикой на (a, b), т. е. парой разных точек. □

Следствие 19.2
Квадрики разного ранга не могут быть проективно эквивалентны (над произвольным полем).

Теорема 19.1
Пересечение $Q' = L \cap Q$ квадрики $Q\mathbb{P}(V)$ с любым дополнительным к $\operatorname{Sing} Q$ проективным подпространством $L \subset \mathbb{P}(V)$ представляет собой невырожденную квадрику в L, и квадрика Q является *линейным соединением*[1] этой неособой квадрики Q' и вершинного пространства $\operatorname{Sing} Q$.

Доказательство. Первое утверждение следует из предл. 17.5. Второе — из лем. 19.1, согласно которой прямая, соединяющая произвольные две точки $a \in$

[1] т. е. объединением всех прямых, пересекающих как Q', так и $\operatorname{Sing} Q$

$\operatorname{Sing} Q$ и $b \in L$ либо целиком лежит на квадрике Q и, в частности, пересекает L по точке $b \in L \cap Q$, либо вообще не пересекает Q нигде, кроме a. $\square$

Следствие 19.3

Размерность максимального проективного подпространства, целиком лежащего на квадрике (19-1), равна $n+1-r+i$. В частности, квадрики одинакового ранга, имеющие разное значение i в представлении (19-1), проективно не эквивалентны.

19.2. Касательное пространство к квадрике. Прямая ℓ, проходящая через точку $p \in Q$, называется *касательной* к Q в p, если ℓ либо лежит на Q целиком, либо пересекает Q по двойной точке p. Объединение всех прямых, касающихся Q в точке p называется *касательным пространством* к квадрике Q в точке $p \in Q$ и обозначается T_pQ. Согласно лем. 19.1, точка $p \in Q \subset \mathbb{P}_n$ особа тогда и только тогда, когда $T_pQ = \mathbb{P}_n$ совпадает со всем пространством.

Лемма 19.2

Прямая $\ell = (ab)$ касается квадрики Q, заданной уравнением $q(x) = 0$, в точке $a \in Q$ тогда и только тогда, когда $\widetilde{q}(a,b) = 0$.

Доказательство. Пусть $\ell = \mathbb{P}(U)$. Матрица Грама ограничения $q|_U$ имеет в базисе $\{a,b\}$ вид

$$\begin{pmatrix} 0 & \widetilde{q}(a,b) \\ \widetilde{q}(b,a) & \widetilde{q}(b,b) \end{pmatrix},$$

и $\det q|_U = 0 \iff \widetilde{q}(a,b) = \widetilde{q}(b,a) = 0$. $\square$

Следствие 19.4

Видимый из точки $b \notin Q$ контур квадрики[1] Q высекается из квадрики гиперплоскостью $\operatorname{Ann} \widehat{q}(b) = \{x \mid \widetilde{q}(b,x) = 0\}$. $\square$

Следствие 19.5

Если точка $p \in Q$ неособа, то $T_pQ = \{x \in \mathbb{P}_n \mid \widetilde{q}(p,x) = 0\}$ является гиперплоскостью в $\mathbb{P}_n$. $\square$

Замечание 19.1. Для точки p, лежащей на квадрике Q, заданной уравнением $q(x) = 0$, линейное уравнение $\widetilde{q}(p,x) = 0$, задающее касательное пространство T_pQ к Q в точке p, может быть записано как

$$\sum_{i=0}^{n} \frac{\partial q}{\partial x_i}(p) \cdot x_i = 0\,.$$

В частности, точка p особа, если и только если частные производные

$$\frac{\partial q}{\partial x_i}(p) = 0 \quad \forall\, i\,.$$

[1] т. е. ГМТ касания с Q всевозможных касательных, опущенных на Q из b

Упражнение 19.1. Покажите, что $\operatorname{Sing} Q = \bigcap\limits_{p \in Q} T_p Q$.

19.2.1. Пример: гиперболическая квадрика в $\mathbb{P}_3$, задаётся уравнением $x_0 x_3 = x_1 x_2$, которое можно воспринимать как условие обращения в нуль детерминанта 2×2-матрицы. А именно, рассмотрим два 2-мерных векторных пространства U_- и U_+ и положим $W = \operatorname{Hom}(U_-, U_+)$. Классы пропорциональных операторов $U_- \longrightarrow U_+$ ранга 1 образуют в $\mathbb{P}_3 = \mathbb{P}(W)$ *квадрику Сегре*

$$\begin{aligned} Q_s &= \{F : U_- \longrightarrow U_+ \mid \det F = 0\} = \\ &= \left\{ \begin{pmatrix} x_0 & x_1 \\ x_2 & x_3 \end{pmatrix} \;\middle|\; \det \begin{pmatrix} x_0 & x_1 \\ x_2 & x_3 \end{pmatrix} = x_0 x_3 - x_1 x_2 = 0 \right\}. \end{aligned} \tag{19-13}$$

Каждый оператор F ранга 1 имеет одномерный образ. Выбирая в нём базисный вектор v, видим, что действие F на произвольный вектор $u \in U_-$ происходит по правилу $F(u) = \xi(u) \cdot v$, где $\xi \in U_-^*$. Линейная форма ξ и вектор v определяются оператором F однозначно с точностью до пропорциональности как базисные векторы в одномерных пространствах $\operatorname{Ann} \ker F$ и $\operatorname{im} F$ соответственно. Наоборот, для любых ненулевых $v \in U_+$ и $\xi \in U_-^*$ оператор

$$\xi \otimes v \;:\; U_- \xrightarrow{u \mapsto \xi(u)\, v} U_+ \tag{19-14}$$

имеет ранг 1. Таким образом, *отображение Сегре*

$$\mathbb{P}(U_-^*) \times \mathbb{P}(U_+) \xhookrightarrow{s} \mathbb{P}(\operatorname{Hom}(U_-, U_+)), \tag{19-15}$$

переводящее пару $(\xi, v) \in \mathbb{P}(U_-^*) \times \mathbb{P}(U_+)$ в оператор (19-14) устанавливает биекцию между $\mathbb{P}_1 \times \mathbb{P}_1 = \mathbb{P}(U_-^*) \times \mathbb{P}(U_+)$ и квадрикой Сегре (19-13).

Предложение 19.3
Отображение Сегре (19-15) переводит два семейства координатных прямых $\mathbb{P}_1 \times v$ и $\xi \times \mathbb{P}_1$ на $\mathbb{P}_1 \times \mathbb{P}_1$ в два семейства прямых на квадрике Сегре таким образом, что в каждом из двух семейств прямые попарно скрещиваются, а любые две прямые из разных семейств пересекаются. Каждая точка квадрики является точкой пересечения пары прямых из различных семейств, и никаких других прямых на квадрике Сегре нет.

Доказательство. Зафиксируем в пространствах $U_\pm$ координаты и будем записывать операторы матрицами. Всякая 2×2-матрица ранга 1 имеет пропорциональные строки и столбцы, и матрицы с фиксированными отношениями

$$\begin{gathered} ([\text{строка } 1] : [\text{строка } 2]) = (t_0 : t_1) \\ ([\text{столбец } 1] : [\text{столбец } 2]) = (\xi_0 : \xi_1) \end{gathered}$$

составляют двумерные векторные подпространства в W, т.е. образуют два семейства прямых на квадрике Сегре. С другой стороны, оператор $\xi \otimes v$, отвечающий форме $\xi = (\xi_0 : \xi_1) \in U_-^*$ и вектору $v = (t_0 : t_1) \in U_+$, имеет матрицу

$$\xi \otimes v = \begin{pmatrix} t_0 \\ t_1 \end{pmatrix} \cdot \begin{pmatrix} \xi_0 & \xi_1 \end{pmatrix} = \begin{pmatrix} \xi_0 t_0 & \xi_1 t_0 \\ \xi_0 t_1 & \xi_1 t_1 \end{pmatrix} \tag{19-16}$$

в точности с предписанными отношениями между строками и столбцами. Тем самым, координатные прямые $\mathbb{P}_1 \times \mathbb{P}_1$ переходят в прямые на квадрике Сегре. В силу биективности отображения Сегре, все соотношения инцидентности между координатными прямыми на $\mathbb{P}_1 \times \mathbb{P}_1$ сохранятся и между их образами на квадрике. Остаётся показать, что никаких других прямых на Q_S нет. Но всякая прямая, лежащая на Q_S и проходящая через заданную точку $p \in Q_S$ содержится в конике $Q_S \cap T_x Q_S$, которая полностью исчерпывается парой пересекающихся в точке p образов координатных прямых. □

Упражнение 19.2. Покажите, что любые 9 точек, а также любые 3 прямые в $\mathbb{P}_3$ лежат на некоторой квадрике, причём квадрика, проходящая через три попарно непересекающиеся прямые, автоматически является гиперболической квадрикой Сегре.

19.2.2. Подпространства, лежащие на гладкой квадрике. Проективное подпространство $L = \mathbb{P}(W)$, лежащее на n-мерной гладкой квадрике

$$Q_n = V(q) \subset \mathbb{P}_{n+1} = \mathbb{P}(V)$$

является проективизацией изотропного подпространства $W \subset V$, размерность которого согласно предл. 17.6 не превышает $\dim V/2$. Поэтому на гладкой n-мерной квадрике $Q_n \subset \mathbb{P}_{n+1}$ нет проективных подпространств размерности большей, чем половина размерности квадрики.

Лемма 19.3

Сечение $\Pi \cap Q$ неособой квадрики Q произвольной гиперплоскостью Π либо является неособой квадрикой в Π, либо имеет единственную особую точку. Второе происходит, если и только если $\Pi = T_p Q$ для некоторой точки $p \in Q$, и в этом случае особая квадрика $\Pi \cap Q$ является конусом с вершиной в p над неособой квадрикой $Q' = \Pi' \cap Q$, которая высекается из Q любой не проходящей через p гиперплоскостью $\Pi' \subset T_p Q = \Pi$ и имеет на единицу меньшую планарность, чем Q.

Доказательство. Пусть $Q = V(q) \subset \mathbb{P}(V)$ и $\Pi = \mathbb{P}(W)$. Первое утверждение следует из оценки:

$$\begin{aligned}\dim\ker(\widehat{q}|_W) = \dim\bigl(W \cap \widehat{q}^{\,-1}(\operatorname{Ann} W)\bigr) \leqslant \dim \widehat{q}^{\,-1}(\operatorname{Ann} W) = \\ = \dim \operatorname{Ann} W = \dim V - \dim W = 1\,.\end{aligned}$$

Если ядро ограничения $\widehat{q}|_W$ не нулевое, а одномерное с базисом p, то $p \in Q \cap \Pi$ и $\mathrm{Ann}\,(\widehat{q}(p)) = W$, откуда $T_pQ = \Pi$. Наоборот, если $\Pi = T_pQ = \mathbb{P}(\mathrm{Ann}\,\widehat{q}(p))$, то вектор $p \in \mathrm{Ann}\,\widehat{q}(p)$ лежит в ядре ограничения $\widehat{q}$ на $\mathrm{Ann}\,\widehat{q}$.

Для любой не проходящей через p гиперплоскости $\Pi' = \mathbb{P}(U) \subset T_pQ$ ограничение $q|_U$ невырождено. Поэтому пространство V является ортогональной прямой суммой $V = U \oplus U^\perp$, причём ограничение $q|_{U^\perp}$ тоже невырождено. Поскольку $q|_{U^\perp}$ имеет изотропный вектор p, форма $q|_{U^\perp}$ гиперболическая. Тем самым, размерность гиперболической составляющей формы $q|_U$, задающей квадрику $Q' = \Pi' \cap Q$, на 2 меньше, чем у q. □

Следствие 19.6
Невырожденная квадрика либо пуста, либо не содержится ни в какой гиперплоскости.

Доказательство. Если непустая невырожденная квадрика содержится в гиперплоскости H, то $H = T_pQ$ для всех $p \in Q$ и $Q = Q \cap T_VQ$ должна быть особа. □

Следствие 19.7
Проективные подпространства размерности m на гладкой m-планарной квадрике $Q \subset \mathbb{P}_n$, проходящие через данную точку $p \in Q$, взаимно однозначно соответствуют всем $(m-1)$-мерным проективным подпространствам, лежащим на гладкой $(m-1)$-планарной квадрике $Q' \subset \mathbb{P}_{n-2}$, высекаемой из Q любой не проходящей через p гиперплоскостью $\mathbb{P}_{n-2} \subset T_pQ = \mathbb{P}_{n-1}$.

19.2.3. Пример: подпространства на квадриках Q_n м $Q_{n,m}$. Результат сл. 19.7 позволяет уточнить геометрию линейных подпространств максимальной размерности, лежащих на n-мерной неособой квадрике $Q_n \subset \mathbb{P}_{n+1}$ над алгебраически замкнутым полем и на m-планарной неособой вещественной n-мерной квадрике $Q_{n,m} \subset \mathbb{P}_{n+1}(\mathbb{R})$.

А именно, над алгебраически замкнутым полем $\Bbbk$ на нульмерной и одномерной гладких квадриках $Q_0 \subset \mathbb{P}_1$ и $Q_1 \subset \mathbb{P}_2$ лежат только 0-мерные подпространства. Следующие две квадрики — двумерная $Q_2 \subset \mathbb{P}_3$ и трёхмерная $Q_3 \subset \mathbb{P}_4$ — не содержат плоскостей, но каждая точка $p \in Q_2$ лежит на паре прямых, проходящих через p и две точки неособой квадрики $Q_0 \subset \mathbb{P}_1 \subset T_pQ_2 \smallsetminus \{p\}$, а через каждую точку $p \in Q_3$ проходит одномерное семейство прямых, образующих конус с вершиной p над гладкой коникой $Q_1 \subset \mathbb{P}_2 \subset T_pQ_4 \smallsetminus \{p\}$. Гладкая 4-мерная квадрика $Q_4 \subset \mathbb{P}_5$ не содержит 3-мерных подпространств, но через любую точку $p \in Q_4$ проходят два пучка[1] плоскостей, взаимно однозначно соответствующих двум семействам прямых на квадрике Сегре, и т. д.

[1]напомним, что *пучок* в этом контексте означает семейство фигур, образующих *прямую* в подходящем проективном пространстве фигур, ср. с (n° 18.2.3)

В вещественном случае на n-мерной эллиптической квадрике $Q_{n,0}$ нет прямых. Через каждую точку n-мерной 1-планарной квадрики $Q_{n,1}$ проходит целый конус прямых с основанием в $(n-2)$-мерной эллиптической квадрике $Q_{n-2,0} \subset \mathbb{P}_{n-1} \subset T_pQ_{n,1} \smallsetminus \{p\}$. Так, через каждую точку поверхности Сегре $Q_{2,1} \subset \mathbb{P}_3$ проходит ровно две прямые, образующие конус над двухточечной гиперболической квадрикой на $\mathbb{P}_1$. Плоскости, проходящие через каждую точку n-мерной 2-планарной квадрики $Q_{n,2}$ являются линейными соединениями этой точки со всевозможными прямыми, лежащими на $(n-2)$-мерной 1-планарной квадрике $Q_{n-2,1} \subset \mathbb{P}_{n-1} \subset T_pQ_{n,2} \smallsetminus \{p\}$ и т. д.

19.3. Пример: $\mathbf{Gr(2,4)} \subset \mathbb{P}_5$ и прямые в $\mathbb{P}_3$. Зафиксируем 4-мерное векторное пространство V с базисом e_1, e_2, e_3, e_4 и обозначим через $\Lambda^d V$ пространство однородных грассмановых многочленов степени d от переменных e_i. На шестимерном пространстве $\Lambda^2 V$ имеется билинейная форма $\widetilde{q}(\omega_1,\omega_2)$, определяемая равенством[1]

$$\omega_1 \wedge \omega_2 = \widetilde{q}(\omega_1,\omega_2) \cdot e_1 \wedge e_2 \wedge e_3 \wedge e_4 \,. \tag{19-17}$$

Поскольку $\omega_1 \wedge \omega_2 = \omega_2 \wedge \omega_1$ для грассмановых многочленов чётной степени, форма $\widetilde{q}$ симметрична. Задаваемая ею квадрика в $\mathbb{P}_5 = \mathbb{P}(\Lambda^2 V)$

$$P = \{\, \omega \in \Lambda^2 V \mid \omega \wedge \omega = 0 \,\} \tag{19-18}$$

называется *квадрикой Плюккера*. В мономиальном базисе $e_{ij} = e_i \wedge e_j$ пространства $\Lambda^2 V$ условие $\omega \wedge \omega = 0$ на грассманову квадратичную форму $\omega = \sum\limits_{i<j} x_{ij} e_{ij}$ записывается уравнением

$$x_{01}x_{23} - x_{02}x_{13} + x_{03}x_{12} = 0 \,. \tag{19-19}$$

Таким образом, плюккерова квадрика — это невырожденная гиперболическая квадрика в $\mathbb{P}_5$.

Квадрика Плюккера состоит из всех квадратичных форм $\omega \in \Lambda^2 V$, которые являются произведениями двух линейных форм. В самом деле, любая разложимая форма $\omega = u_1 \wedge u_2$ имеет нулевой квадрат $\omega \wedge \omega = u_1 \wedge u_2 \wedge u_1 \wedge u_2 = 0$. С другой стороны, произвольная форма $\omega \in \Lambda^2 V$ согласно упр. 10.7 записывается в подходящем базисе пространства V либо как $\omega = \xi_0 \wedge \xi_1 + \xi_2 \wedge \xi_3$, либо как $\omega = \xi_0 \wedge \xi_1$, и в первом случае ω не разложима, поскольку $\omega \wedge \omega = 2\,\xi_0 \wedge \xi_1 \wedge \xi_2 \wedge \xi_3 \neq 0$.

Напомним (см. n° 8.6.1), что множество всех 2-мерных векторных подпространств $U \subset V$ или, что то же самое, множество всех прямых

$$\ell = \mathbb{P}(U) \subset \mathbb{P}_3 = \mathbb{P}(V)$$

[1] отметим, что при выборе в V другого базиса $e' = eC$ подпространства $\Lambda^d(V)$, определённые как пространства однородных грассмановых многочленов степени d от e'_i, останутся тем же, а форма $\widetilde{q}' : \Lambda^2 V \times \Lambda^2 V \longrightarrow \Bbbk$, заданная равенством $\omega_1 \wedge \omega_2 = \widetilde{q}'(\omega_1,\omega_2) \cdot \varepsilon'_1 \wedge e'_2 \wedge e'_3 \wedge e'_4$ будет отличаться от формы $\widetilde{q}$ ненулевым постоянным множителем

называется *грассманианом* $\mathrm{Gr}(2,4)$. Из предыдущего вытекает, что плюккерова квадрика P является образом *отображения Плюккера*

$$\mathfrak{u} : \mathrm{Gr}(2,4) \xrightarrow{(a,b)\mapsto a\wedge b} \mathbb{P}_5 = \mathbb{P}(\Lambda^2 V)\,, \tag{19-20}$$

которое отправляет прямую $(a,b) \subset \mathbb{P}(V)$ в произведение $a\wedge b \in \Lambda^2 V$. Поскольку при выборе на той же прямой другого базиса $(a',b') = (a,b)\cdot C$ произведение $a'\wedge b' = a\wedge b\cdot \det C$ умножается на ненулевую константу, отображение (19-20) определено корректно.

Упражнение 19.3. Проверьте, что на координатном языке отображение (19-20) переводит подпространство, порождённое в $\Bbbk^4$ строками u, w матрицы

$$\begin{pmatrix} u_1 & u_2 & u_3 & u_4 \\ w_1 & w_2 & w_3 & w_4 \end{pmatrix}$$

в грассманову квадратичную форму $u\wedge w = \sum x_{ij}\, e_i\wedge e_j$, коэффициенты которой суть шесть 2×2-миноров этой матрицы:

$$x_{ij} = u_i w_j - u_j w_i = \det\begin{pmatrix} u_i & u_j \\ w_i & w_j \end{pmatrix}\,.$$

Лемма 19.4

Две прямые $\ell_1, \ell_2 \subset \mathbb{P}_3$ пересекаются тогда и только тогда, когда их образы при отображении Плюккера (19-20) ортогональны относительно плюккеровой квадрики, т. е. $\widetilde{q}(\mathfrak{u}(\ell_1), \mathfrak{u}(\ell_2)) = \mathfrak{u}(\ell_1)\wedge\mathfrak{u}(\ell_2) = 0$.

Доказательство. Пусть $\ell_1 = \mathbb{P}(U_1)$, $\ell_2 = \mathbb{P}(U_2)$. Если $U_1\cap U_2 = 0$, то $V = U_1\oplus U_2$ и существует базис $\{e_i\}\subset V$ такой, что U_1 натянуто на e_1, e_2 и U_2 натянуто на e_3, e_4. Тогда $\mathfrak{u}(U_1) = e_1\wedge e_2$, $\mathfrak{u}(U_2) = e_3\wedge e_4$ и $\mathfrak{u}(U_1)\wedge\mathfrak{u}(U_2) = e_1\wedge e_2\wedge e_3\wedge e_4 \neq 0$. Если $U_1\cap U_2 \neq 0$, то можно выбрать в U_1 и U_2 базисы (w, u_1) и (w, u_2) с общим вектором $w\in U_1\cap U_2$. Тогда $\mathfrak{u}(U_1)\wedge\mathfrak{u}(U_2) = w\wedge u_1\wedge w\wedge u_2 = 0$. □

Следствие 19.8

Плюккерово отображение(19-20) инъективно и задаёт биекцию между грассманианом $\mathrm{Gr}(2,4)$ и квадрикой Плюккера $P\subset\mathbb{P}_5$.

Доказательство. Для любых двух прямых $\ell_1 \neq \ell_2$ на $\mathbb{P}_3$ существует третья прямая ℓ, которая пересекает ℓ_1 и не пересекает ℓ_2. Тогда тогда $\mathfrak{u}(\ell_1)\wedge\mathfrak{u}(\ell) = 0$ и $\mathfrak{u}(\ell_2)\wedge\mathfrak{u}(\ell)\neq 0$, т. е. $\mathfrak{u}(\ell_1)\neq\mathfrak{u}(\ell_2)$. □

Следствие 19.9

Пересечение $P\cap T_pP$ плюккеровой квадрики с касательной плоскостью в точке $p = \mathfrak{u}(\ell)\in P$ состоит из плюккеровых образов $\mathfrak{u}(\ell')$ всех прямых $\ell'\subset\mathbb{P}_3$, пересекающих ℓ.

19.3.1. Связки и пучки прямых в $\mathbb{P}_3$. Множество прямых на $\mathbb{P}_3$ называется *связкой*, если оно изображается на квадрике Плюккера плоскостью $\pi \subset P$.

Всякая связка $\pi \subset P$ однозначно определяется какими-нибудь тремя своими неколлинеарными точками $p_i = \mathfrak{u}(\ell_i)$, $i = 1, 2, 3$. Такая связка является пересечением касательных пространств $\pi = P \cap T_{p_1}P \cap T_{p_2}P \cap T_{p_3}P$ и по лемме лем. 19.4 и следствию сл. 19.9 состоит из всех прямых, пересекающих три данные прямые ℓ_1, ℓ_2, ℓ_3, любые две из которых пересекаются между собой. Последнее означает, что прямые ℓ_i либо все три лежат в одной плоскости, либо все три пересекаются в одной точке. Но тогда и любая прямая из натянутой на ℓ_1, ℓ_2, ℓ_3 связки должна лежать в той же плоскости либо, соответственно, проходить через ту же точку.

Итак, существуют два геометрически разных типа связок прямых на $\mathbb{P}_3$ или, что то же самое, 2-мерных плоскостей на квадрике Плюккера. По традиции, они называются *α-связка* и *β-связка*. Первая состоит из всех прямых, проходящих через данную точку $a \in \mathbb{P}_3$ и переводится плюккеровым вложением в *α-плоскость* $\pi_\alpha(a) \subset P$. Вторая состоит из всех прямых, лежащих в данной плоскости $\Pi \in \mathbb{P}_3$ и переводится плюккеровым вложением в *β-плоскость* $\pi_\beta(\Pi) \subset P$. При этом любые две плоскости одного типа пересекаются в единственной точке

$$\pi_\beta(\Pi_1) \cap \pi_\beta(\Pi_2) = \mathfrak{u}(\,\Pi_1 \cap \Pi_2\,)$$
$$\pi_\alpha(a_1) \cap \pi_\alpha(a_2) = \mathfrak{u}(\,(a_1 a_2)\,)\ ,$$

а две плоскости $\pi_\beta(\Pi)$ и $\pi_\alpha(a)$ различных типов при $a \notin \Pi$ не пересекаются вовсе, а при $a \in \Pi$ пересекаются по прямой, изображающей на квадрике Плюккера пучок проходящих через точку a прямых на плоскости π.

Упражнение 19.4. Покажите, что каждая прямая на плюккеровой квадрике является пересечением α-плоскости и β-плоскости (иначе говоря, любой пучок прямых на $\mathbb{P}_3$ представляет собою множество всех прямых, лежащих в некоторой плоскости и проходящих там через одну точку).

19.3.2. Аффинные клетки $\mathrm{Gr}(2, 4)$**.** Зафиксируем какую-нибудь 3-мерную гиперплоскость $H \subset T_pP$, дополнительную к точке $p \in P$ в 4-мерном касательном пространстве T_pP к квадрике Плюккера $P \subset \mathbb{P}_5$. Особая квадрика $C = P \cap T_pP$ представляет собой простой конус с вершиной p над гиперболической квадрикой Сегре $G = H \cap P$, что приводит к следующей стратификации плюккеровой квадрики P замкнутыми подмножествами:

$$\begin{tikzcd}
 & & \pi_\alpha \arrow[dr, hook] & & \\
p \arrow[r, hook] & \pi_\alpha \cap \pi_\beta \arrow[ur, hook] \arrow[dr, hook] & & C \arrow[r, hook] & P \\
 & & \pi_\beta \arrow[ur, hook] & &
\end{tikzcd}$$

Беря в каждом страте дополнение до объединения всех содержащихся в нём стратов меньшей размерности, получаем разбиение квадрики $P \simeq \mathrm{Gr}(2,4)$ в дизъюнктное объединение открытых подмножеств, изоморфных аффинным пространствам:

$$\mathrm{Gr}(2,4) = \mathbb{A}^0 \sqcup \mathbb{A}^1 \sqcup \left(\mathbb{A}^2 \sqcup \mathbb{A}^2\right) \sqcup \mathbb{A}^3 \sqcup \mathbb{A}^4 ,$$

где $\mathbb{A}^0$ это точка p, $\mathbb{A}^1$ это проективная прямая $\pi_\alpha \cap \pi_\beta$ без точки p, два экземпляра $\mathbb{A}^2$ получаются выкидыванием проективной прямой $\pi_\alpha \cap \pi_\beta$ из проективных плоскостей π_α и π_β. Пространство $\mathbb{A}^3 = \mathbb{A}^1 \times \mathbb{A}^2$ является объединением аффинных прямых $\mathbb{A}^1$, остающихся после выкидывания вершины p из конуса над изоморфным $\mathbb{A}^2$ дополнением квадрики Сегре до креста, высекаемого из неё касательной плоскостью.

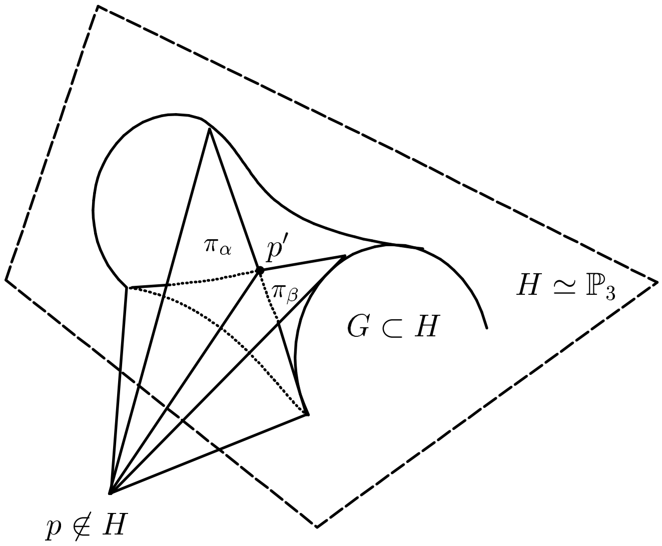


Рис. 19◇1. Конус $C = P \cap T_pP$.

Упражнение 19.5. Убедитесь в том, что проекция гладкой квадрики $Q \subset \mathbb{P}_n$ из любой точки $p \in Q$ на на любую не проходящую через p гиперплоскость H устанавливает бирациональную[1] биекцию между дополнением $Q \smallsetminus (Q \cap T_pQ)$ и аффинным пространством $\mathbb{A}^{n-1} = H \smallsetminus (H \cap T_pQ)$.

Последний, плотный в P открытый кусок $\mathbb{A}^4$ есть дополнение до $P \cap T_pP$.

Упражнение 19.6. Установите соответствие между только что описанными аффинными клетками и клетками Шуберта, обсуждавшимися в n° 8.6.1 (напомним, что клетки Шуберта на грассманиане $\mathrm{Gr}(2,4)$ определяются выбором базиса в пространстве V и нумеруются шестью диаграммами Юнга $(0,0)$, $(1,0)$, $(1,1)$, $(2,0)$, $(2,1)$, $(2,2)$, умещающимися в прямоугольнике 2×2 и описывающими комбинаторный тип расположения двумерного подпространства $U \subset V$ относительно координатных плоскостей выбранного базиса, ср. с зад. 8.1).

19.4. Поляритеты. Корреляция $\widehat{q}$, ассоциированная с невырожденной квадратичной формой q, индуцирует линейный проективный изоморфизм

$$\overline{q} : \mathbb{P}(V) \xrightarrow{\sim} \mathbb{P}(V^*)$$

который называется *полярным преобразованием* (или *поляритетом*) квадрики Q. Он переводит точку $p \in \mathbb{P}_n$ в гиперплоскость $L = \{x \in \mathbb{P}_n \mid \widetilde{q}(p,x) = 0\}$. Точка p и гиперплоскость L в этом случае называются *полюсом* и *полярой* друг

[1] в том смысле, что координаты соответственных точек рационально выражаются друг через друга

друга относительно квадрики Q. Геометрически, поляра точки, не лежащей на квадрике, — это гиперплоскость, высекающая видимый из этой точки контур квадрики, а поляра точки, лежащей на квадрике, — это гиперплоскость, касающаяся квадрики в этой точке. Таким образом, всякую квадрику Q можно охарактеризовать как геометрическое место точек, лежащих на своих полярах.

Поскольку условие $\widetilde{q}(a,b) = 0$ симметрично по a и b, точка a лежит на поляре точки b, если и только если точка b лежит на поляре точки a. Такие точки называются *сопряжёнными* относительно квадрики Q.

Упражнение 19.7. Рассмотрим полярное преобразование евклидовой плоскости $\mathbb{R}^2$ относительно какой-нибудь окружности. Циркулем и линейкой постройте поляру данной точки и полюс данной прямой (это особенно интересно, когда прямая не пересекает окружности или когда точка лежит внутри ограничиваемого окружностью круга).

Предложение 19.4
Пусть $a, b \notin Q$ и прямая (ab) пересекает Q в двух различных точках c, d. Точки a, b тогда и только тогда сопряжены относительно квадрики Q, когда они гармоничны по отношению к точкам c, d.

Доказательство. Ограничение квадрики Q на прямую $(ab) = (cd)$ задаётся в однородных координатах $(x_0 : x_1)$ относительно базиса (c, d) квадратичной формой $q(x) = \det(x,c)\det(x,d)$, поляризация которой имеет вид

$$\widetilde{q}(x,y) = \frac{1}{2}\bigl(\det(x,c)\det(y,d) + \det(y,c)\det(x,d)\bigr)\,.$$

Условие сопряжённости $\widetilde{q}(a,b) = 0$ равносильно тому, что

$$\det(a,c)\det(b,d) = -\det(b,c)\det(a,d)\,,$$

т. е. равенству $[a,b,c,d] = -1$. □

Предложение 19.5
Для неособой квадрики $G \subset \mathbb{P}_n$ и произвольной квадрики $Q \subset \mathbb{P}_n$ множество гиперплоскостей, полярных точкам $p \in Q$ относительно квадрики G, образуют квадрику в $Q_G^\times \subset \mathbb{P}_n^x$, того же ранга, что и квадрика Q. Если Q и G имеют в некоторых однородных координатах матрицы Грама A и B соответственно, то квадрика $Q_G^\times$ имеет в двойственных однородных координатах матрицу $B^{-1}AB^{-1}$.

Доказательство. Поляритет $\overline{q} : \mathbb{P}_n \xrightarrow{\sim} \mathbb{P}_n^\times$ гладкой квадрики $Q \subset \mathbb{P}_n$ переводит точку со столбцом координат x в точку двойственного пространства со строкой координат $x^t \cdot B$ и является проективным изоморфизмом. Полярные гиперплоскости $\xi = \widehat{q}(p)$ точек $p \in P$ задаются, таким образом, уравнением

$$0 = x^t \cdot A \cdot x = \bigl(\xi \cdot B^{-1}\bigr) \cdot A \cdot \bigl(\xi \cdot B^{-1}\bigr)^t = \xi \cdot B^{-1}AB^{-1} \cdot \xi^t\,,$$

что и утверждалось. □

Следствие 19.10
Касательные пространства к гладкой квадрике $Q \subset \mathbb{P}_n$ образуют гладкую квадрику $Q^\times \subset \mathbb{P}_n^\times$. Матрицы Грама квадрик Q и $Q^\times$ в двойственных базисах пространств $\mathbb{P}_n$ и $\mathbb{P}_n^\times$ обратны друг другу.

Доказательство. Положим в предыдущей теореме $G = Q$, т. е. $B = A$. Гиперплоскости, полярные точкам $p \in Q$ относительно квадрики Q, превратятся при этом в касательные пространства T_pQ. □

19.4.1. Поляритеты над незамкнутыми полями. Над алгебраически незамкнутыми полями имеются (в том числе и непропорциональные друг другу) квадратичные формы q, задающие *пустые* квадрики Q. Тем не менее, соответствующие таким квадрикам полярные преобразования вполне наблюдаемы геометрически и характеризуются тем, что никакая точка не лежит на своей поляре.

Упражнение 19.8. Опишите полярное преобразование евклидовой плоскости $\mathbb{R}^2$ относительно «мнимой» окружности $x^2 + y^2 = -1$.

Из лем. 18.1 и сл. 18.1 вытекает

Следствие 19.11
Два поляритета совпадают, если и только если задающие их квадратичные формы пропорциональны. □

Следствие 19.12
Над алгебраически замкнутым полем две квадрики совпадают тогда и только тогда, когда их уравнения пропорциональны.

Доказательство. Пусть $Q = Q'$. Поскольку при ограничении на любое дополнительное к $\operatorname{Sing} Q = \operatorname{Sing} Q'$ подпространство уравнения обеих квадрик не поменяются, можно считать обе квадрики невырожденными, а тогда всё следует из леммы сл. 19.11. □

19.5. Аффинные квадрики. Выберем в аффинном пространстве A над векторным пространством V какой-нибудь аффинный репер и отождествим A с координатным пространством $\Bbbk^n$. Фигура, задаваемая в A (неоднородным) многочленом второй степени от координат $(x_1, x_2, \ldots, x_n)$ пространства $\Bbbk^n$, называется *аффинной квадрикой*.

Упражнение 19.9. Покажите, что свойство фигуры $Q \subset A$ быть аффинной квадрикой не зависит от выбора координатного репера.

Две аффинных квадрики называются *аффинно эквивалентными* (или *изоморфными*), если они переводится друг в друга аффинным афтоморфизмом (см. n° 14.6.4 и n° 16.2.2).

Упражнение 19.10. Покажите, что при помощи подходящего выбора аффинных координат уравнение аффинной квадрики можно привести к одному из видов

$$a_1t_1^2 + a_2t_2^2 + \dots + a_kt_k^2 = c \quad \text{или} \quad a_1t_1^2 + a_2t_2^2 + \dots + a_kt_k^2 = t_{k+1}$$

которые алгебраически замкнутым полем упрощаются далее до одной из форм

$$t_1^2 + t_2^2 + \dots + t_k^2 = 0 \tag{19-21}$$

$$t_1^2 + t_2^2 + \dots + t_k^2 = 1 \tag{19-22}$$

$$t_1^2 + t_2^2 + \dots + t_k^2 = t_{k+1} \tag{19-23}$$

а над полем $\mathbb{R}$ — до одной из форм (где всюду $p \geqslant m$)

$$t_1^2 + \dots + t_p - t_{p+1}^2 - \dots - t_{p+m}^2 = 0 \tag{19-24}$$

$$t_1^2 + \dots + t_p - t_{p+1}^2 - \dots - t_{p+m}^2 = \pm 1 \tag{19-25}$$

$$t_1^2 + \dots + t_p - t_{p+1}^2 - \dots - t_{p+m}^2 = t_{p+m+1} \tag{19-26}$$

19.5.1. Проективные замыкания аффинных квадрик. Всякая аффинная квадрика $Q \subset \mathbb{A}^n$ может быть получена как изображение некоторой проективной квадрики $\overline{Q} \subset \mathbb{P}_n$ в некоторой аффинной карте $U_\xi \subset \mathbb{P}_n$. Например, можно реализовать Q в координатном пространстве $\Bbbk^n$ с координатами $(t_1, t_2, \dots, t_n)$ и вложить это пространство в качестве стандартной аффинной карты U_0 в проективное пространство $\mathbb{P}_n = \mathbb{P}(\Bbbk \cdot e_0 \oplus \Bbbk^n)$ с координатами $(x_0, x_1, \dots, x_n)$, такими что $t_i = x_i/x_0$, и взять в качестве $\overline{Q}$ проективное замыкание квадрики Q, как это описывалось в n° 18.2.2.

Легко видеть, что аффинные квадрики $\overline{Q}' \cap U_{\xi'}$ и $\overline{Q}'' \cap U_{\xi''}$ аффинно эквивалентны тогда и только тогда, когда существует проективный изоморфизм, одновременно переводящий квадрику $\overline{Q}'$ в квадрику $\overline{Q}''$, а бесконечно удалённую гиперплоскость $\mathbb{P}(\operatorname{Ann}\xi')$ карты $U_{\xi'}$ — в бесконечно удалённую гиперплоскость $\mathbb{P}(\operatorname{Ann}\xi'')$ карты $U_{\xi''}$. В самом деле, карты $U_{\xi'}$ и $U_{\xi''}$ являются аффинными пространствами над векторными пространствами $\operatorname{Ann}\xi'$ и $\operatorname{Ann}\xi''$. Зафиксируем два набора линейных форм $(\xi', \xi_1', \xi_2', \dots, \xi_n')$ и $(\xi'', \xi_1', \xi_2', \dots, \xi_n')$ в качестве однородных координат на $\mathbb{P}_n$ и используем $t_i' = \xi_i'|_{U_{\xi'}}$ и $t_i'' = \xi_i''|_{U_{\xi''}}$ в качестве локальных аффинных координат в картах $U_{\xi'}$ и $U_{\xi''}$. Всякий аффинный изоморфизм $F : U_{\xi'} \xrightarrow{\sim} U_{\xi''}$ однозначно задаётся своим дифференциалом $DF : \operatorname{Ann}\xi' \xrightarrow{\sim} \operatorname{Ann}\xi''$ и образом начальной точки аффинной координатной системы t' карты $U_{\xi'}$ $F(0, 0, \dots, 0) = (a_1, a_2, \dots, a_n) \in U_{\xi''}$. Такой аффинный автоморфизм индуцируется проективным автоморфизмом $\overline{F} : \mathbb{P}_n \xrightarrow{\sim} \mathbb{P}_n$, действующим на однородные координаты по правилу

$$\begin{pmatrix} \xi' \\ \xi_1' \\ \vdots \\ \xi_n' \end{pmatrix} \longmapsto \begin{pmatrix} \xi'' \\ \xi_1'' \\ \vdots \\ \xi_n'' \end{pmatrix} = \left(\begin{array}{c|ccc} 1 & 0 & \dots & 0 \\ \hline a_1 & & & \\ \vdots & & DF & \\ a_n & & & \end{array}\right) \cdot \begin{pmatrix} \xi' \\ \xi_1' \\ \vdots \\ \xi_n' \end{pmatrix}$$

Наоборот, любой проективный автоморфизм, переводящий $\operatorname{Ann}\xi'$ в $\operatorname{Ann}\xi''$ задаётся, с точностью до скалярного множителя, написанной выше матрицей и индуцирует аффинный изоморфизм $U_{\xi'} \xrightarrow{\sim} U_{\xi''}$ с дифференциалом DF, переводящий начальную точку $(1:0:\dots:0) \in U_{\xi'}$ в точку $(1:a_1:\dots:a_n) \in U_{\xi''}$.

Таким образом, с проективной точки зрения описание всех аффинных квадрик с точностью до аффинного изоморфизма представляет собой описание с точностью до проективного автоморфизма всевозможных взаимных расположений проективной квадрики и гиперплоскости, которая будет бесконечно удалённой для той карты, где мы собираемся наблюдать аффинный образ рассматриваемой проективной квадрики.

Если проективная квадрика $\overline{Q}$ невырождена и бесконечно удалённая гиперплоскость является её касательной плоскостью, то соответствующая аффинная квадрика Q называется *параболоидом*. Поскольку все касательные плоскости переводятся друг в друга автоморфизмами квадрики, аффинный тип параболоида Q однозначно определяется проективным типом проективной квадрики $\overline{Q}$. Так, над алгебраически замкнутым полем в $\mathbb{A}^n$ имеется ровно один параболоид, который в подходящих аффинных координатах задаётся уравнением (19-23) из упр. 19.10 (в котором надо положить $k = n$), а над полем $\mathbb{R}$ есть $[(n-1)/2]$ параболоидов различной планарности m, задаваемых уравнениями (19-26) из упр. 19.10 при различных $p \geqslant m$ и $p + m + 1 = n$.

Если невырожденная проективная квадрика $\overline{Q}$ пересекается с бесконечно удалённой гиперплоскостью по невырожденной квадрике R, то аффинный тип соответствующей аффинной квадрики определяется проективным типом квадрики R. Над алгебраически замкнутым полем такая квадрика единственна и задаётся уравнением (19-22) из упр. 19.10 (при $k = n$). Над полем $\mathbb{R}$ планарность квадрики R такая же или на единицу меньше, чем у квадрики $\overline{Q}$. Аффинные квадрики Q, получающиеся из различных вещественных проективных квадрик $\overline{Q}$ при двух геометрически различных выборах некасательной бесконечно удалённой гиперплоскости описываются уравнениями (19-25) из упр. 19.10

$$t_1^2 + \dots + t_p - t_{p+1}^2 - \dots - t_n^2 = \pm 1 \tag{19-27}$$

при различных $p \geqslant n/2$. Проективное замыкание $\overline{Q}$ такой квадрики задаётся уравнением

$$x_1^2 + \dots + x_p - x_{p+1}^2 - \dots - x_n^2 = \pm x_0^2 \tag{19-28}$$

и имеет планарность m при выборе в правой части знака минус и планарность $m+1$ при выборе в правой части знака плюс. Квадрика R, высекаемая бесконечно удалённой гиперплоскостью $x_0 = 0$, задаётся уравнением

$$x_1^2 + \dots + x_p - x_{p+1}^2 - \dots - x_n^2 = 0 \tag{19-29}$$

и имеет ту же планарность, что $\overline{Q}$, если в правой части предыдущей формулы выбирался знак минус, и на единицу меньшую планарность, чем $\overline{Q}$, если выбирался плюс. Поскольку квадрики (19-28) различной планарности заведомо проективно не эквивалентны, а квадрики

$$x_1^2 + \cdots + x_p - x_{p+1}^2 - x_{p+2}^2 - \cdots - x_n^2 = -x_0^2$$
$$x_1^2 + \cdots + x_p + x_{p+1}^2 - x_{p+2}^2 - \cdots - x_n^2 = x_0^2$$

пересекают бесконечно удалённую гиперплоскость по не эквивалентным квадрикам R разной планарности, все аффинные квадрики (19-27) попарно не эквивалентны, за единственным исключением: чётномерная чисто гиперболической квадрика

$$t_1^2 + \cdots + t_p - t_{p+1}^2 - \cdots - t_{2p}^2 = \pm 1$$

не меняется при смене знака в правой части и любое неособое гиперплоское сечение её проективного замыкания $\overline{Q}$ имеет ту же планарность, что и $\overline{Q}$.

Аффинные вещественные квадрики $\sum t_i^2 = 1$, для которых квадрика R пуста, называются *эллипсоидами*, остальные квадрики из списка (19-28) — гиперболоидами.

Аффинные квадрики Q, получающиеся из вырожденных проективных квадрик $\overline{Q}$ называются *конусами* и *цилиндрами* в зависимости от того, как бесконечно удалённая гиперплоскость пересекается с вершинным пространством квадрики $\overline{Q}$.

19.5.2. Пример: аффинные квадрики в $\mathbb{R}^3$. Неособая эллиптическая квадрика $Q_{2,0} \subset \mathbb{P}(\mathbb{R}^4)$ с однородным уравнением $x_0x_1 = x_2^2 + x_3^2$ видна в различных аффинных картах либо как *эллиптический параболоид* с аффинным уравнением $t_1^2 + t_2^2 = t_3$ (см. рис. 19◇3), либо как *двуполостный* (или *эллиптический*) *гиперболоид* с аффинным уравнением

$$t_1^2 + t_2^2 - t_3^2 = -1$$

(см. рис. 19◇4), либо *эллипсоид* с аффинным уравнением $t_1^2 + t_2^2 + t_3^2 = 1$ (см. рис. 19◇5).

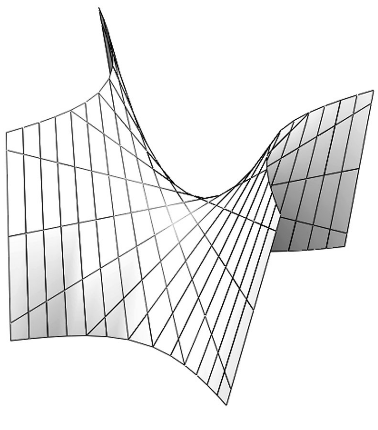


Рис. 19◇2. Гиперболический параболоид $t_1^2 - t_2^2 = t_3$.

Неособая гиперболическая квадрика Сегре

$$Q_{2,1} \subset \mathbb{P}_3(\mathbb{R})$$

с однородным уравнением $x_0x_1 = x_2x_3$ видна либо *гиперболический параболоид* с аффинным уравнением $t_1^2 - t_2^2 = t_3$ (см. рис. 19◇2), либо *однополостный* (или *гиперболический*) *гиперболоид* с аффинным уравнением $t_1^2 + t_2^2 - t_3^2 = 1$ (см. рис. 19◇6).

Особая квадрика ранга 2 с однородным уравнением $x_0x_1 = x_2^2$ может быть видна как *эллиптический конус* с аффинным уравнением $t_1^2 + t_2^2 - t_3^2 = 0$ (если поместить особую точку $(0 : 0 : 0 : 1)$ внутрь аффинной карты, см. рис. 19◇7) или, например, как *гиперболический цилиндр* с аффинным уравнением $t_1^2 - t_2^2 = 1$ (если особая точка на бесконечности, см. рис. 19◇8)

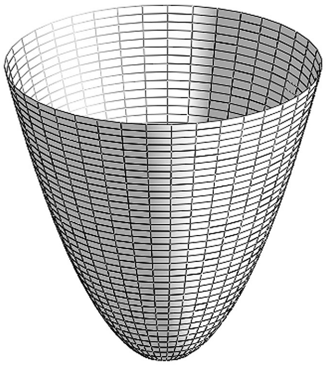


Рис. 19◇3. Эллиптический параболоид
$t_1^2 + t_2^2 = t_3$.

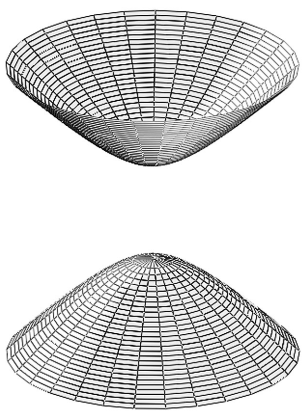


Рис. 19◇4. Двуполостный гиперболоид
$t_1^2 + t_2^2 - t_3^2 = -1$.

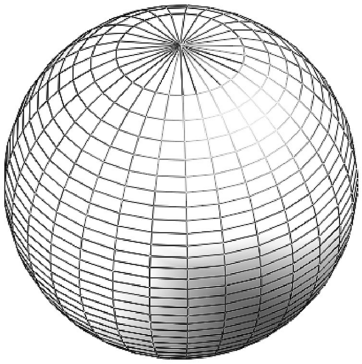


Рис. 19◇5. Эллипсоид
$t_1^2 + t_2^2 + t_3^2 = 1$.

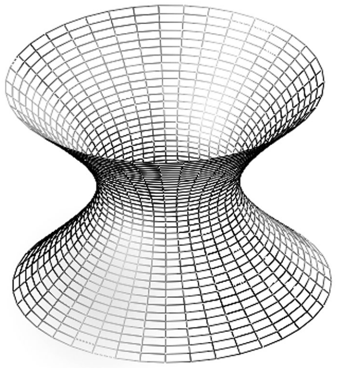


Рис. 19◇6. Однополостный гиперболоид
$t_1^2 + t_2^2 - t_3^2 = 1$.

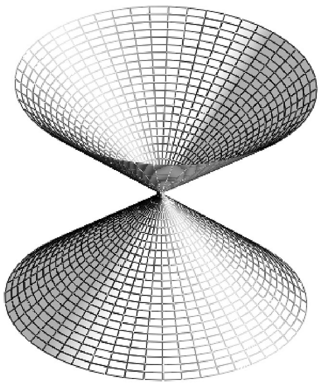


Рис. 19◇7. Эллиптический конус
$t_1^2 + t_2^2 - t_3^2 = 0$.

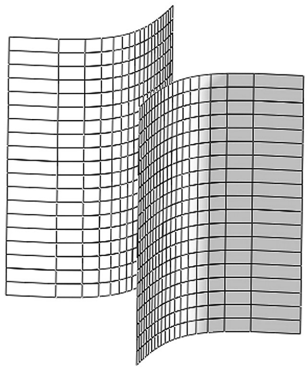


Рис. 19◇8. Гиперболический цилиндр
$t_1^2 - t_2^2 = 1$.

Задачи для самостоятельного решения к §19

Задача 19.1. Сколько коник касается пяти заданных прямых на плоскости, никакие три из которых не пересекаются в одной точке?

Задача 19.2. Напишите явное уравнение, задающее пучок коник[1], проходящих через точки $a = (1 : 0 : 0)$, $b = (0 : 1 : 0)$, $c = (0 : 0 : 1)$, $d = (1 : 1 : 1)$. Сколько в этом пучке вырожденных коник?

Задача 19.3. Пусть в обозначениях из n° 18.4.5 вершины a, b, c, d четырёхвершинника лежат на гладкой конике C. Покажите, что треугольник xyz автополярен[2] относительно C.

Задача 19.4. Покажите, что два треугольника на проективной плоскости тогда и только тогда перспективны (см. зад. 18.8), когда один из них полярен другому относительно некоторой коники.

Задача 19.5. Каково уравнение гладкой коники C в базисе (e_0, e_1, e_2), если треугольник $e_0e_1e_2$ а) вписан б) описан в) автополярен?

Задача 19.6 (двойное отношение на гладкой конике). Назовём двойным отношением $[a, b, c, d]$ четырёх точек гладкой коники C двойное отношение четырёх прямых $[(pa), (pb), (pc), (pd)]$ в пучке прямых с центром в некоторой пятой точке $p \in C$ или, что то же самое, двойное отношение проекций точек a, b, c, d из точки p на любую не проходящую через p прямую ℓ.

а) Покажите, что двойное отношение не зависит от выбора p и прямой ℓ.

б) Покажите, что две хорды C тогда и только сопряжены[3], когда пары их концов гармоничны на конике.

в) Отождествим гладкую конику $C \subset \mathbb{P}_2$ с коникой Веронезе, т.е. будем считать, что $\mathbb{P}_2 = \mathbb{P}(S^2U^*)$ есть пространство пар точек на $\mathbb{P}_1 = \mathbb{P}(U)$, а C — множество двойных точек. Покажите, что двойное отношение точек на $\mathbb{P}_1 = \mathbb{P}(U)$ равно двойному отношению соответствующих двойных точек на конике C.

Задача 19.7 (автоморфизмы гладкой коники). В условиях зад. 19.6 (в) будем называть *автоморфизмом* коники C преобразование двойных точек, вызванное дробно линейным преобразованием $\mathbb{P}_1 = \mathbb{P}(U)$. Для автоморфизма $\varphi : C \longrightarrow C$, заданного своим действием на некоторые три точки $a, b, c \in C$

а) (перекрёстная ось) опишите ГМТ пересечения прямых $(x\varphi(y)) \cap (y\varphi(x))$ по всем $x \neq y$ на C и постройте его одной линейкой б) одной линейкой отметьте какую-нибудь пару точек $p_1, p_2 \in C$ и нарисуйте прямую ℓ, не проходящую через них, так чтобы композиция проекции C на ℓ из p_1 а затем проекции ℓ обратно на C из p_2 совпала с φ в) одной линейкой постройте неподвижные точки φ.

[1] т.е. квадратичную форму от $(x_0 : x_1 : x_2)$, коэффициенты которой линейно зависят от $(\lambda : \mu)$, пробегающего $\mathbb{P}_1$

[2] т.е. каждая вершина является полюсом противолежащей стороны

[3] т.е. полюс прямой, высекающей одну из них, лежит на прямой, высекающей другую

Задача 19.8 (теорема Паскаля). Покажите, что шесть точек $p_1, p_2, \ldots, p_6$ тогда и только лежат на конике, когда коллинеарны три точки пересечения «пар противоположных сторон»

$$(p_1p_2) \cap (p_4p_5)\,, \quad (p_2p_3) \cap (p_5p_6)\,, \quad (p_3p_4) \cap (p_6p_1)\,.$$

Задача 19.9 (теорема Брианшона). Покажите, что шестиугольник описан около коники тогда и только тогда, когда три его главных диагонали пересекаются в одной точке.

Задача 19.10. Покажите, что два треугольника на $\mathbb{P}_2$ описаны около одной коники тогда и только тогда, когда они вписаны в одну конику.

Задача 19.11 (инволюции на гладкой конике). В условиях зад. 19.7 будем называть нетождественный автоморфизм $\sigma : C \xrightarrow{\sim} C$ с $\sigma^2 = \mathrm{Id}_C$ *инволюцией* на гладкой конике C. Покажите, что а) любая инволюция на C высекается пучком прямых[1] с центром вне C б) для любых двух различных точек $p, q \in C$ существует единственная инволюция, имеющая p и q неподвижными точками в) две разных инволюции коммутируют, если и только если пары их неподвижных точек гармоничны г) три разных инволюции тогда и только тогда составляют вместе с Id_C группу $\mathbb{Z}/(2) \times \mathbb{Z}/(2)$, когда прямые, соединяющие пары их неподвижных точек, образуют автополярный треугольник. д) Даны две различных инволюции $\sigma_1, \sigma_2 : C \longrightarrow C$. Сколько существует точек $p \in C$, таких что $\sigma_1(p) = \sigma_2(p)$?

Задача 19.12. Одной линейкой постройте две касательные к данной конике C из данной точки $p \notin C$.

Задача 19.13. Сколько общих касательных может быть у двух гладких коник?

Задача 19.14. Рассмотрим на пространстве $\mathrm{Mat}_{2\times 2}$ квадратичную форму $\det(X)$. Опишите полярное преобразование относительно этой формы.

Задача 19.15 (квадрика Сегре). В обозначениях из n° 19.2.1 покажите, что

а) операторы $\xi \otimes v : u \mapsto \xi(u) \cdot v$ со всевозможными $\xi \in U_-^*$, $u \in U_+$ линейно порождают пространство $\mathrm{Hom}(U_-, U_+)$

б) следующие три свойства оператора $F \in \mathrm{Hom}(U_-, U_+)$ эквивалентны:

(1) $F \in T_{\xi\otimes v}Q_S$ (2) $F(\mathrm{Ann}\,(\xi)) \subset \Bbbk \cdot v$ (3) $\exists\, \eta \in U_-^*,\ w \in U_+ : F = \xi \otimes w + \eta \otimes v$

в) действие проективного изоморфизма $\overline{F} : \mathbb{P}(U_-) \xrightarrow{\sim} \mathbb{P}(U_+)$, индуцированного невырожденным оператором $F \in \mathrm{Hom}(U_-, U_+)$, на произвольно заданную точку $p = \mathbb{P}(\mathrm{Ann}\,(\xi)) \in \mathbb{P}(U_-)$ допускает следующее описание: проведём в $\mathbb{P}_3 = \mathbb{P}(\mathrm{Hom}(U_-, U_+))$ плоскость π через F и прямолинейную образующую $L' = \xi \times \mathbb{P}(U_+) \subset Q_S$; она пересекает квадрику Сегре по распавшейся конике $\pi \cap Q_S = L' \cap L''$, где $L'' = \mathbb{P}(U_-^*) \times v \subset Q_S$ — прямая из другого семейства; тогда $F(p) = v$.

[1] т. е. $\forall\, \sigma\ \exists\, c_\sigma \in \mathbb{P}_2 : \forall\, a, b \in C\ \sigma(a) = b \iff (a, b) \ni c_\sigma$

Задача 19.16. Покажите, что через любые три заданные попарно скрещивающиеся прямые в $\mathbb{P}_3$ проходит единственная квадрика. Эта квадрика неособа и заметается всеми прямыми, пересекающими каждую из трёх заданных.

Задача 19.17. Даны четыре попарно скрещивающиеся прямые в пространстве
а) $\mathbb{P}(\mathbb{C}^4)$ б) $\mathbb{A}(\mathbb{C}^4)$ в) $\mathbb{P}(\mathbb{R}^4)$ г) $\mathbb{A}(\mathbb{R}^4)$
Сколько прямых пересекается со всеми четырьмя данными? Найдите все возможные ответы и выясните, какие из них устойчивы к малым шевелениям заданных четырёх прямых.

Задача 19.18. Покажите, что что пересечение неособой вещественной проективной квадрики Q сигнатуры (p,m) с касательной плоскостью T_xQ является линейным соединением точки x с неособой квадрикой сигнатуры $(p-1,m-1)$ в дополнительном к x подпространстве в T_xQ.

Задача 19.19. Выясните, из скольких точек состоит над полем из девяти элементов[1]
а) коника $x_0x_1 - x_1x_2 + x_0x_2 = 0$ на $\mathbb{P}_2(\mathbb{F}_9)$ б) квадрика $x_0^2 + x_1^2 + x_2^2 + x_3^2 = 0$ в $\mathbb{P}_3(\mathbb{F}_9)$

Задача 19.20. Какими могут быть ранг и сигнатура неособого гиперплоского сечения неособой вещественной проективной квадрики Q сигнатуры (p,m) ?

[1]напомним, что элементы поля $\mathbb{F}_9 = \mathbb{F}_3[x]/(x^2+1)$ имеют вид $a+ib$, где $a,b \in \mathbb{Z}/(3)$, и $i^2 \equiv -1 \pmod 3$

Раздел V
Комплексные и вещественные структуры

§20. Эрмитовы пространства

20.1. Эрмитова геометрия. Векторное пространство W над полем комплексных чисел $\mathbb{C}$ называется *эрмитовым* (или *унитарным*), если на нём задано билинейное относительно умножения на вещественные числа $\mathbb{R} \subset \mathbb{C}$ скалярное произведение $W \times W \longrightarrow \mathbb{C} \; : \; w_1, w_2 \mapsto (w_1, w_2)$, такое что $\forall \; w_1, w_2 \in W$ и $\forall \; z \in \mathbb{C}$ выполняются свойства:

$$\begin{aligned} (w_1, w_2) &= \overline{(w_2, w_1)} && \text{(эрмитова симметричность)} \\ (z\, w_1, w_2) &= z\,(w_1, w_2) = (w_1, \overline{z}\, w_2) && \text{(полуторалинейность)} \\ (w, w) &> 0 \quad \forall\, w \neq 0 && \text{(положительность).} \end{aligned} \tag{20-1}$$

Отметим, что в силу эрмитовой симметричности скалярный квадрат любого вектора

$$(w, w) = \overline{(w, w)}$$

является вещественным числом, и последнее свойство означает положительность этого вещественного числа для $w \neq 0$. Скалярное произведение со свойствами (20-1) называется *эрмитовой* (или *унитарной*) *структурой* на комплексном векторном пространстве W.

Координатное пространство $\mathbb{C}^n$ имеет *стандартную эрмитову структуру*

$$(z, w) = z_1\overline{w}_1 + z_2\overline{w}_2 + \,\cdots + z_n\overline{w}_n \tag{20-2}$$

где $z = (z_1, z_2, \dots, z_n)\,,\; w = (w_1, w_2, \dots, w_n) \in \mathbb{C}^n$. Аналогично, на пространстве непрерывных функций $[a, b] \longrightarrow \mathbb{C}$ имеется эрмитово скалярное произведение

$$(f, g) = \int\limits_a^b f(x)\overline{g}(x)\, dx \tag{20-3}$$

где под интегралом от комплекснозначной функции f по определению понимается комплексное число, действительная и мнимая части которого равны интегралам от вещественной и мнимой частей функции f, которые являются обычными вещественными функциями:

$$\int f\,dx = \int \mathrm{Re}\,(f)\,dx + i\cdot\int \mathrm{Im}\,(f)\,dx\,.$$

Разумеется, вместо отрезка можно рассматривать любое другое пространство, по которому можно интегрировать вещественные функции, например диск или какую-нибудь кривую в $\mathbb{C}$.

20.1.1. Эрмитова норма вектора. Пользуясь тем, что скалярный квадрат любого вектора в эрмитовом пространстве вещественен и положителен, определим *эрмитову норму* (или *длину*) вектора $w \in W$ формулой[1]

$$||w|| \overset{\text{def}}{=} \sqrt{(w,w)} \in \mathbb{R}_{\geqslant 0}\,. \tag{20-4}$$

Эрмитова структура однозначно восстанавливается по норме: из равенств

$$\begin{aligned}(w_1+w_2, w_1+w_2) &= ||w_1||^2 + ||w_2||^2 + 2\,\mathrm{Re}\,(w_1,w_2)\\ (w_1+iw_2, w_1+iw_2) &= ||w_1||^2 + ||w_2||^2 - 2i\,\mathrm{Im}\,(w_1,w_2)\,,\end{aligned}$$

вытекает, что

$$2(w_1,w_2) = ||w_1+w_2||^2 - ||w_1+iw_2||^2\,. \tag{20-5}$$

20.1.2. Матрицы Грама. Эрмитова симметричность скалярного произведения означает, что матрица Грама $G_w = \big((w_i,w_j)\big)$ любого набора векторов $w = (w_1, w_2, \dots, w_m)$ пространства W является *эрмитово симметричной*, т. е. сопрягается при транспонировании:

$$G^t = \overline{G}\,.$$

В следствие антилинейности эрмитова скалярного произведения по второму аргументу, при линейной замене набора векторов по формуле $w = v\,C_{vw}$ матрица Грама меняется по правилу

$$G_w = C_{vw}^t \cdot G_v \cdot \overline{C}_{vw}\,.$$

20.1.3. Ортогонализация Грама – Шмидта. Как и в евклидовом случае, из произвольного базиса $\{w_i\}$ эрмитова пространства W можно изготовить в *ортонормальный* базис $\{e_i\}$ с единичной матрицей Грама так, чтобы для каждого $k = 1, 2\ \dots, n$ линейная оболочка первых k базисных векторов в обоих базисах была одинакова. Векторы e_i такого ортонормального базиса находятся по рекурсивным формулам $e_1 = w_1/\sqrt{(w_1,w_1)}$ и $e_m = u_m/\sqrt{(u_m,u_m)}$, где

$$u_m = w_m - \sum_{\nu=1}^{m-1}(w_m, e_\nu) \quad (\text{при } m \geqslant 2)\,.$$

[1] мы используем обозначение $||w||$, чтобы отличать нормы *векторов* $w \in W$ от модулей комплексных *чисел* $z \in \mathbb{C}$ которые будем обозначать, как и раньше, через $|z| = \sqrt{z\cdot\overline{z}}$

Упражнение 20.1. Проверьте, что $e_1, e_2, \dots, e_n$ действительно обладает требуемыми свойствами.

Лемма 20.1

Определитель Грама $\det G_w$ любого набора векторов $w = (w_1, w_2, \dots, w_m)$ является вещественным неотрицательным числом и обращается в нуль тогда и только тогда, когда набор векторов линейно зависим.

Доказательство. Пусть $w = e\,C_{ew}$, где набор векторов $e = (e_1, e_2, \dots, e_n)$ составляет ортонормальный базис в линейной оболочке векторов w. Тогда $G_w = C_{ew}^t C_{ew}$. Если $n < m$, то ранг матрицы G_w строго меньше её размера, и $\det G_w = 0$. Если $n = m$, то $\det G_w = \det C \cdot \overline{\det C} = |\det C|^2$. $\square$

20.1.4. Неравенство Коши – Буняковского – Шварца. Из неотрицательности определителя Грама набора из двух векторов v, w

$$\det \begin{pmatrix} (v,v) & (v,w) \\ (w,v) & (w,w) \end{pmatrix} = ||v||^2||w||^2 - (v,w) \cdot \overline{(v,w)} \geqslant 0$$

вытекает эрмитова версия неравенства Коши – Буняковского – Шварца[1]

$$|(v,w)| \leqslant ||v|| \cdot ||w|| \,, \tag{20-6}$$

равенство в котором равносильно (комплексной) пропорциональности векторов v и w.

Следствие 20.1 (неравенство треугольника для нормы)

$||w_1|| + ||w_2|| \geqslant ||w_1 + w_2|| \quad \forall\, w_1, w_2 \in W$.

Доказательство.

$||w_1 + w_2||^2 = ||w_1||^2 + ||w_2||^2 + 2|(w_1,w_2)| \leqslant ||w_1||^2 + ||w_2||^2 + 2||w_1|| \cdot ||w_2||$. $\square$

20.1.5. Унитарная группа. Линейный оператор $F : W \longrightarrow W$ на эрмитовом пространстве W называется *унитарным*, если

$$||Fw|| = ||w|| \qquad \forall\, w \in W \;.$$

В силу (20-5), унитарный оператор F сохраняет скалярное произведение:

$$(Fv, Fw) = (v, w) \quad \forall\, v, w \in W \,.$$

Тем самым, матрица унитарного оператора в любом базисе связана с матрицей Грама этого базиса соотношением

$$F^t \cdot G \cdot \overline{F} = G \,. \tag{20-7}$$

[1] обратите внимание, что в его левой части стоит *модуль* скалярного произведения, которое в эрмитовом случае является *комплексным* числом

Переходя к определителям, получаем $|\det F| = 1$. В частности, унитарный оператор F всегда обратим, и

$$F^{-1} = \overline{G}^{-1}\overline{F}^t\overline{G} = G^{t\,-1}\overline{F}^t G^t\,.$$

В ортонормальном базисе эта формула редуцируется до $F^{-1} = \overline{F}^t$.

Унитарные операторы образуют *унитарную группу* пространства W, которая обозначается $\mathrm{U}(W)$. Записывая унитарные операторы матрицами в фиксированном ортонормальном базисе $e_1, e_2, \dots, e_n$, мы получаем изоморфизм унитарной группы с группой *унитарных матриц*

$$\mathrm{U}_n = \{F \in \mathrm{GL}_n(\mathbb{C}) \mid F^{-1} = \overline{F}^t\}\,.$$

Её подгруппа $\mathrm{SU}_n = \{F \in \mathrm{U}_n \mid \det F = 1\}$ называется *специальной унитарной* группой. Подчеркнём, что в отличие от евклидовой изометрии определитель унитарной матрицы вовсе не обязан равняться ± 1 и может принимать любое значение на единичной окружности $\mathrm{U}_1 = \{z \in \mathbb{C} \mid z\overline{z} = 1\}$. Поэтому в эрмитовом пространстве нет понятия *ориентации*, и эрмитовы операторы не разбиваются на два несвязных класса.

20.1.6. Эрмитов объём. Выберем какой-нибудь ортонормальный базис

$$e_1, e_2, \dots, e_n$$

эрмитова пространства W в качестве базиса единичного объёма и определим *эрмитов объём* n-мерного параллелепипеда, натянутого на векторы $v = e\,C_{ev}$ формулой

$$\mathrm{Vol}\,(v_1, v_2, \dots, v_n) = |\det C|\,.$$

Поскольку модуль определителя матрицы перехода между ортонормальными базисами равен единице, эрмитов объём не зависит от выбора эталонного ортонормального базиса, и квадрат эрмитова объёма, как и в евклидовом случае, равен определителю Грама:

$$\mathrm{Vol}^2(v_1, v_2, \dots, v_n) = |\det C_{ev}|^2 = \det C_{ev}^t \cdot \overline{\det C_{ev}} = \det G_v\,.$$

20.1.7. Ортогональное проектирование. В эрмитовом пространстве W для любого подпространства $U \subset W$ и любого вектора $w \in U$ имеется единственный вектор $\pi_U(w) \in U$, который называется *ортогональной проекцией* w на U и однозначно характеризуется любым из следующих эквивалентных друг другу свойств:

(1) разность $w - \pi_U(w)$ лежит в *ортогональном дополнении* к U, т. е. в

$$U^\perp = \{v \in W \mid (u, v) = 0 \ \ \forall\, u \in U\}$$

(2) вектор $\pi_U(w)$ это ближайший к w вектор подпространства U, т. е.

$$||w - \pi_U(w)|| < ||w - u|| \quad \text{для всех } u \neq \pi_U(w) \text{ из } U$$

(3) линейный функционал $u \mapsto (u, w)$ на подпространстве U представляется скалярным произведением с $\pi_U(w)$, т. е. $(u, w) = (u, \pi_U, w) \quad \forall\, u \in U$.

В самом деле, свойства (1) и (3) очевидно равносильны друг другу и позволяют однозначно построить $\pi_U(w)$ следующим образом. Выберем в U ортонормальный базис $u_1, u_2, \ldots, u_k$. Коэффициенты z_i разложения

$$u' = z_1u_1 + z_2u_2 + \cdots + z_ku_k$$

произвольного вектора $u' \in U$ суть скалярные произведения $z_i = (u', u_i)$, в чём легко убедиться скалярно умножив обе части равенства справа на u_i. Поскольку для вектора $\pi_U(w)$ по свойству (3) выполняются равенства

$$(\pi_U(w), u_i) = \overline{(u_i, \pi_U(w))} = \overline{(u_i, w)} = (w, u_i)\,,$$

разложение этого вектора по базису $u_1, u_2, \ldots, u_k$ имеет вид

$$\pi_U(w) = \sum_i (w, u_i) \cdot u_i\,. \tag{20-8}$$

Наоборот, вектор $\pi_U(w)$ определённый по этой формуле обладает свойством (3). Действительно, это свойство линейно по u, и его достаточно проверить для базисных векторов $u = u_i$ подпространства U. Скалярно умножая обе части равенства (20-8) справа на u_i, получаем $(\pi_U(w), u_i) = (w, u_i)$. Комплексно сопрягая обе части, приходим к требуемому соотношению $(u_i, w) = (u_i, \pi_U, w)$.

Экстремальное свойство (2) для вектора $\pi_U(w)$, такого что $w - \pi_U(w) \in U^\perp$, вытекает из того, что для любого $u \in U$

$$\begin{aligned} ||w - (\pi_U(w) + u)||^2 &= (\,(w - \pi_U(w)) - u\,,\, (w - \pi_U(w)) - u\,) = \\ &= ||w - \pi_U(w)||^2 + ||u||^2 \geqslant ||w - \pi_U(w)||^2\,, \end{aligned}$$

где равенство равносильно тому, что $u = 0$.

Следствие 20.2

$W = U \oplus U^\perp$, причём проекция произвольного вектора $w \in W$ на U вдоль $U^\perp$ является единственным ближайшим к w вектором подпространства U и задаётся формулой (20-8). □

20.1.8. Угол между комплексными прямыми. Разница между эрмитовой и евклидовой геометриями становится заметной при попытке определить *угол* между *комплексными* прямыми.

Напомним, что в евклидовом пространстве угол $\varphi = \widehat{vw} \in [0, \pi]$ между вещественными прямыми, натянутыми на векторы v и w, определялся нами из соотношения

$$\cos\varphi = \frac{(v,w)}{||v|| \cdot ||w||} = (\, v/||v||\, ,\, w/||w||\,)\ , \tag{20-9}$$

правая часть которого в евклидовом случае вещественна и в силу неравенства Коши – Буняковского – Шварца лежит на $[-1, 1]$. На геометрическом языке, векторы $v/||v||$ и $w/||w||$ являются единичными направляющими векторами рассматриваемых прямых, и в евклидовом пространстве каждый из них определяется этим свойством однозначно с точностью до умножения на ± 1. Выбор этих знаков есть выбор одного из четырёх углов, на которые разбивается двумя пересекающимися прямыми натянутая на них вещественная плоскость.

В комплексном случае правая часть (20-9) является *комплексным числом*, а каждая из «прямых» $\mathbb{C} \cdot v$, $\mathbb{C} \cdot w$ представляет собою двумерную вещественную плоскость. Эти две плоскости пересекаются только по нулю, а их линейная оболочка есть четырёхмерное вещественное пространство $\mathbb{R}^4 = \mathbb{C} \cdot v \oplus \mathbb{C} \cdot w$. Оно не разбивается этими плоскостями ни на какие связные компоненты, и на каждой из двух «прямых» $\mathbb{C} \cdot v$, $\mathbb{C} \cdot w$ имеется целая окружность базисных векторов единичной длины. Эти две окружности не пересекаются и лежат на компактной трёхмерной сфере векторов единичной длины

$$S^3 = \{\, u \in \mathbb{R}^4 = \mathbb{C} \cdot v \oplus \mathbb{C} \cdot w \mid ||u|| = 1\,\}\ .$$

Поэтому длины дуг[1], соединяющих точку на одной из окружностей с точкой на другой, ограничены снизу и достигают своего минимального значения. Иначе говоря, угол между вещественными прямыми $\mathbb{R} \cdot e_1$ и $\mathbb{R} \cdot e_2$, натянутыми на всевозможные $e_1 \in \mathbb{C} \cdot v$ и $e_2 \in \mathbb{C} \cdot w$ с $||e_1|| = ||e_2|| = 1$, достигает своего минимума на некоторой паре векторов e_1, e_2. Этот угол φ и называется углом между комплексными прямыми $\mathbb{C} \cdot v$ и $\mathbb{C} \cdot w$.

Замечательно, что он находится из простого алгебраического соотношения

$$\cos\psi = \frac{|(v,w)|}{||v|| \cdot ||w||} = |(\, v/||v||\, ,\, w/||w||\,)|\ , \tag{20-10}$$

которое формально совершенно аналогичного (20-9) и в евклидовом пространстве также даёт *наименьший* из двух смежных углов между двумя вещественными прямыми на вещественной плоскости.

Упражнение 20.2. Докажите это.

[1]имеются в виду дуги больших окружностей, высекаемых на сфере всевозможными вещественными двумерными плоскостями, проходящими через центр сферы

Отметим, что в силу эрмитовой версии неравенства Коши – Буняковского – Шварца правая часть (20-10) принадлежит $[0,1]$, так что угол φ между двумя комплексными прямыми всегда острый: $\varphi \in [\,0\,,\,\pi/2\,]$.

20.2. Сопряжение операторов. Линейные операторы F и F^*, действующие на эрмитовом пространстве W, называются *сопряжёнными*, если

$$\forall\, w_1, w_2 \in W \quad (F^* v, w) = (v, Fw)\,.$$

В терминах матриц это соотношение означает, что $F^{*t} \cdot G = G \cdot \overline{F}$, откуда

$$F^* = {G^{-1}}^t \cdot \overline{F}^t \cdot G^t = \overline{G^{-1}} \cdot \overline{F}^t \cdot \overline{G}\,. \tag{20-11}$$

В ортонормальном базисе это равенство редуцируется до

$$F^* = \overline{F}^t\,.$$

Таким образом, у каждого оператора F имеется ровно один сопряжённый оператор F^* и $F^{**} = F$.

Иначе говоря, операция сопряжения $F \longmapsto F^*$ является инволюцией на пространстве комплексно линейных эндоморфизмов $\mathrm{End}_{\mathbb{C}}(W)$ пространства W. Равенства

$$\begin{aligned}\bigl(v, (z_1 F_1 + z_2 F_2) w\bigr) = \overline{z}_1 (v, F_1 w) + \overline{z}_2 (v, F_2 w) = \\ = \overline{z}_1 (F_1^* v, w) + \overline{z}_2 (F_2^* v, w) = \bigl((\overline{z}_1 F_1^* + \overline{z}_2 F_2^*) v, w\bigr)\end{aligned}$$

показывают, что эта инволюция является *антилинейным* оператором, т. е.

$$(z_1 F_1 + z_2 F_2 + \,\cdots\, + z_m F_m)^* = \overline{z}_1 F_1^* + \overline{z}_2 F_2^* + \,\cdots\, + \overline{z}_m F_m^*$$

а из равенств $(v, FGw) = (F^* v, Gw) = (G^* F^* v, w)$ следует, что сопряжение является *антигомоморфизмом* алгебры $\mathrm{End}_{\mathbb{C}}(W)$, т. е.

$$(FG)^* = G^* F^*$$

Упражнение 20.3. Убедитесь, что унитарные операторы можно охарактеризовать как обратимые операторы, сопряжённые своим обратным:

$$F \in \mathrm{U}(W) \quad \iff \quad F^* = F^{-1}\,.$$

20.2.1. (Анти) самосопряжённые операторы. Операторы F, удовлетворяющие условию $F^* = F$ называются *самосопряжёнными* (или *эрмитовыми*), а операторы F, удовлетворяющие условию $F^* = -F^*$ называются *антисамосопряжёнными* (или *косоэрмитовыми*).

В ортонормированном базисе самосопряжённые операторы задаются *эрмитово симметричными* матрицами $F^t = \overline{F}$, а антисамосопряжённые — *эрмитово кососимметричными* матрицами $F^t = -\overline{F}$.

Множества (анти) самосопряжённых операторов

$$\mathrm{End}^+_{\mathbb{C}}(W) = \{F \mid F^* = F\} \tag{20-12}$$
$$\mathrm{End}^-_{\mathbb{C}}(W) = \{F \mid F^* = -F\} \tag{20-13}$$

являются *вещественными* векторными подпространствами в комплексном векторном пространстве $\mathrm{End}_{\mathbb{C}}(W)$ в том смысле, что линейные комбинации (анти) самосопряжённых операторов *с вещественными* коэффициентами также являются (анти) самосопряжёнными операторами. Умножение на комплексное число i задаёт вещественно линейный изоморфизм между этими пространствами

$$F^* = F \iff (iF)^* = -(iF)$$

(обратный изоморфизм задаётся умножением на $-i$).

Пространство $\mathrm{End}_{\mathbb{C}}(W)$, рассматриваемое как векторное пространство над полем вещественных чисел $\mathbb{R}$, является прямой суммой

$$\mathrm{End}_{\mathbb{C}}(W) = \mathrm{End}^+_{\mathbb{C}}(W) \oplus \mathrm{End}^-_{\mathbb{C}}(W) \quad (\text{как пространства над } \mathbb{R})\,.$$

Компоненты разложения $F = F_+ + F_-$ произвольного комплексно линейного оператора $W \xrightarrow{F} W$ в сумму самосопряжённого и антисамосопряжённого суть

$$F_+ = \frac{F + F^*}{2} \in \mathrm{End}^+_{\mathbb{C}}(W)\ , \quad F_- = \frac{F - F^*}{2} \in \mathrm{End}^-_{\mathbb{C}}(W)\ .$$

20.2.2. Сопряжение в евклидовом пространстве. На алгебре эндоморфизмов $\mathrm{End}_{\mathbb{R}}(V)$ вещественного евклидова пространства V формула

$$(F^*v, w) = (v, Fw) \quad \forall\, w_1, w_2 \in W$$

также корректно определяет операцию сопряжения $F \leftrightarrow F^*$. Эта операция является линейной инволюцией на пространстве $\mathrm{End}_{\mathbb{R}}(V)$ и антигомоморфизмом по отношению к композиции операторов. Матрица сопряжённого оператора в произвольном базисе связана с матрицей Грама этого базиса по формуле $F^* = G^{-1} \cdot F^t \cdot G$. В частности, в ортонормальном базисе $F^* = F^t$.

Упражнение 20.4. Для оператора $V \xrightarrow{F} V$ обозначим через $V^* \xleftarrow{F^\times} V^*$ двойственный оператор (см. n° 8.3), определяемый равенством $\langle F^\times \xi, v\rangle = \langle \xi, Fv\rangle$, где $\langle *, *\rangle : V^* \times V \longrightarrow \Bbbk$ это свёртка ковекторов и векторов, а поле $\Bbbk$ это $\mathbb{R}$ или $\mathbb{C}$. Рассмотрим правую корреляцию $R : V \longrightarrow V^*$, переводящую вектор $v \in V$ в функционал $(\,*\,,\, v) : u \mapsto (u, v)$. Покажите, что

а) в эрмитовом случае корреляция R является $\mathbb{R}$-линейным изоморфизмом вещественных векторных пространств, однако *антилинейна* по отношению к умножению на комплексные числа, т. е. $R(zv) = \overline{z}R(v)$

б) сопряжённый оператор $F^* = R^{-1}F^{\times}R$ (как в евклидовом, так и в эрмитовом случае[1]).

Пространство (вещественно) линейных эндоморфизмов евклидова пространства V раскладывается в прямую сумму

$$\mathrm{End}_{\mathbb{R}}(V) = \mathrm{End}^{+}_{\mathbb{R}}(V) \oplus \mathrm{End}^{-}_{\mathbb{R}}(V)\,, \quad F = (F + F^*)/2 + (F - F^*)/2\,,$$

подпространств $\mathrm{End}^{\pm}_{\mathbb{R}}(V) = \{F \mid F^* = \pm F\}$ (анти) самосопряжённых операторов. В ортонормальном базисе пространства V (анти) самосопряжённые операторы имеют в (косо) симметричные матрицы. Ортогональные операторы на евклидовом пространстве характеризуются как операторы, сопряжённые к своим обратным.

20.2.3. Пример: сопряжение дифференциальных операторов. Обозначим через V пространство бесконечно дифференцируемых функций

$$f : [a,b] \longrightarrow \mathbb{R}\,,$$

которые обращаются на концах отрезка в нуль вместе со всеми своими производными, и введём на V евклидову структуру

$$(f,g) = \int\limits_a^b f(t)g(t)\,dt\,.$$

Из формулы интегрирования по частям

$$\left(\frac{d}{dt}f\,,\,g\right) = \int\limits_a^b f'g\,dt = -\int\limits_a^b fg'\,dt = \left(f\,,\,-\frac{d}{dt}g\right)$$

вытекает, что оператор дифференцирования $d/dt \,:\, f \longrightarrow f'$ антисамосопряжён. Поскольку оператор умножения на любую заданную функцию, очевидно, самосопряжён, и сопряжение является антигомоморфизмом по отношению к композиции операторов, оператор, сопряжённый, к примеру, линейному дифференциальному оператору вида

$$t^3\frac{d^2}{dt^2} \,:\, f(t) \longmapsto t^3 f''(t)\,,$$

переводит f в $\left(t^3 f\right)'' = 6tf + 6t^2 f' + t^3 f''$, т. е. $\left[t^3\frac{d^2}{dt^2}\right]^* = t^3\frac{d^2}{dt^2} + 6t^2\frac{d}{dt} + 6t\,.$

Упражнение 20.5. Вычислите оператор, сопряжённый к оператору

$$L = a(t)\frac{d^2}{dt^2} + b(t)\frac{d}{dt} + c(t) \,:\, f \longmapsto af'' + bf + c$$

где $a, b, c \in V$.

[1]обратите внимание, что композиция двух антилинейных операторов линейна

20.3. Нормальные операторы Оператор F, действующий в эрмитовом пространстве W, называется *нормальным*, если он перестановочен со своим сопряжённым оператором, т. е. $F^* \cdot F = F \cdot F^*$.

Например, (анти) самосопряжённые и унитарные операторы, для которых F^* равен $\pm F$ и F^{-1} соответственно, все нормальны.

Теорема 20.1
Оператор F, действующий в эрмитовом пространстве W, нормален тогда и только тогда, когда он диагонализуем в ортонормальном базисе. При этом диагональная матрица для F с точностью до перестановки диагональных элементов не зависит от выбора диагонализующего ортонормального базиса.

Доказательство. Если оператор F диагонализуем в ортонормальном базисе, то сопряжённый к F оператор имеет в этом базисе сопряжённую диагональную матрицу $\overline{F}$, которая коммутирует с F. Поэтому F нормален. При этом диагональные элементы матрицы F — это собственные значения оператора, и каждое из них присутствует на диагонали столько раз, какова размерность соответствующего собственного подпространства. Это доказывает последнее утверждение.

Покажем теперь индукцией по $\dim W$, что нормальный оператор F диагонализуем в ортонормальном базисе. Если $\dim W = 1$, то доказывать нечего. При $\dim W > 1$ оператор F имеет ненулевое собственное подпространство $U \subset W$. Если $U \neq W$, то $W = U \oplus U^\perp$. Как мы видели в n° 13.3, из того, что F^* коммутирует с F, вытекает, что F^* переводит U в себя. Поэтому для всех $u \in U$ и любого $w \in U^\perp$ выполняется равенство $(Fw, u) = (w, F^*u) = 0$, т. е. $Fw \in U^\perp$, и оператор F переводит $U^\perp$ в себя. По индукции, $F|_{U^\perp}$ диагонализуем в некотором ортонормальном базисе пространства $U^\perp$. Добавляя к этому базису любой ортонормальный базис собственного подпространства U, получаем базис W, в котором матрица F диагональна. $\square$

Следствие 20.3
Самосопряжённые операторы — это диагонализуемые в ортонормальном базисе операторы с вещественными собственными значениями.

Следствие 20.4
Антисамосопряжённые операторы — это диагонализуемые в ортонормальном базисе операторы с чисто мнимыми собственными значениями.

Следствие 20.5
Унитарные операторы — это диагонализуемые в ортонормальном базисе операторы с собственными значениями, по модулю равными единице.

Упражнение 20.6. Покажите, что U_n является компактным линейно связным подмножеством в $\mathrm{Mat}_n(\mathbb{C})$.

20.4. Полярное разложение невырожденного линейного оператора на эрмитовом пространстве является непосредственным обобщением представления ненулевого комплексного числа $z \in \mathbb{C}$ в виде

$$z = \varrho \cdot e^{i\vartheta} \,, \tag{20-14}$$

где $\varrho = |z|$ вещественно и положительно, а $e^{i\vartheta} = \cos\vartheta + i\sin\vartheta \in \mathrm{U}_1$. Если воспринимать z как оператор умножения на z в одномерном эрмитовом координатном пространстве, то формула (20-14) представляет такой оператор в виде композиции самосопряжённого оператора $\varrho = \sqrt{zz^*}$ с положительным собственным значением и унитарного оператора $e^{i\vartheta} = z/\varrho$.

Лемма 20.2
Для любого линейного оператора F на эрмитовом пространстве W операторы FF^* и F^*F самосопряжены и имеют неотрицательные, а если F невырожден, то строго положительные собственные значения.

Доказательство. Первое утверждение очевидно. Из него следует, что все собственные значения FF^* и F^*F вещественны. Если $FF^*v = \lambda v \neq 0$, то $\lambda \cdot (v,v) = (\lambda v, v) = (FF^*v, v) = (F^*v, F^*v)$, откуда $\lambda = (F^*v, F^*v)/(v,v) > 0$. Аналогично, если $F^*Fv = \lambda v \neq 0$, то $\lambda \cdot (v,v) = (\lambda v, v) = (F^*Fv, v) = (Fv, Fv)$, и $\lambda = (Fv, Fv)/(v,v) > 0$. $\square$

Теорема 20.2 (полярное разложение)
Любой обратимый линейный оператор F, действующий на конечномерном эрмитовом пространстве W, допускает единственное разложение в композицию $F = S_1 I_1$ и единственное разложение в композицию $F = I_2 S_2$, в которых операторы U_1, U_2 унитарны, а операторы S_1 и S_2 самосопряжены и имеют положительные собственные числа.

Доказательство. Приведём FF^* и F^*F к диагональному виду и обозначим через $S_1 = \sqrt{FF^*}$, $S_2 = \sqrt{F^*F}$, диагональные операторы, получающиеся извлечением положительных квадратных корней из стоящих на диагонали положительных вещественных чисел. Полученные таким образом операторы $S_{1,2}$ тоже самосопряжены и имеют положительные собственные числа. Кроме того, S_1 коммутирует с FF^* и удовлетворяет соотношению $S_1^2 = FF^*$, а S_2 коммутирует с F^*F и удовлетворяет соотношению $S_1^2 = F^*F$. Положим $I_1 = S_1^{-1}F$ и $I_2 = FS_2^{-1}$. Равенства

$$\begin{aligned}
(I_1u, I_1w) &= (S_1^{-1}Fu, S_1^{-1}Fw) = (F^*S_1^{-2}Fu, w) = (F^*(FF^*)^{-1}Fv, w) = (u, w) \,, \\
(I_2u, I_2w) &= (FS_2^{-1}u, FS_2^{-1}w) = (u, S_2^{-1}F^*FS_2^{-1}w) = (v, F^*FS_2^{-2}w) = (u, w) \,.
\end{aligned}$$

показывают, что оба они унитарны. Это доказывает существование полярных разложений.

Докажем единственность разложения $F = S_1 I_1$ (единственность разложения $F = I_2 S_2$ устанавливается аналогично). Из равенства $I_1^* = I_1^{-1}$ вытекает, что $F^*F = S_1^2$. Поэтому оператор S_1 перестановочен с FF^*. Согласно лем. 13.3 самосопряжённые коммутирующие операторы S_1 и FF^* одновременно приводятся к диагональному виду. Поэтому действие оператора S_1 на каждом собственном подпространстве V_μ оператора FF^* с собственным значением μ задаётся в подходящем базисе диагональной матрицей с квадратом μE. Поскольку все собственные значения S_1 положительны, $S_1|_{V_\mu} = \sqrt{\mu} \cdot \mathrm{Id}_{V_\mu}$, а так как пространство W является прямой суммой пространств V_μ, действие оператора S_1 на W тем самым однозначно определено и этот оператор совпадает с построенным нами выше. Но тогда и $I_1 = FS_1^{-1}$ тоже совпадает с построенным выше. $\square$

20.4.1. Экспоненциальное накрытие унитарной группы. Для конечномерного эрмитова пространства W формула

$$|F| = \max_{||w||=1} ||Fw|| = \max_{w \neq 0} \frac{||Fw||}{||w||} \tag{20-15}$$

задаёт на пространстве линейных операторов $\mathrm{End}_{\mathbb{C}}(W)$, рассматриваемом как векторное пространство над полем $\mathbb{R}$, норму в смысле n° 14.7.1. В самом деле, функция $|F|$, очевидно, положительна, невырождена и однородна. Неравенство треугольника вытекает из неравенства треугольника для эрмитовой нормы:

$$|F + G| = \max_{||w||=1} ||Fw + Gw|| \leqslant \max_{||w||=1} \big(||Fw|| + ||Gw||\big) \leqslant \\ \leqslant \max_{||w||=1} ||Fw|| + \max_{||w||=1} ||Gw|| = |F| + |G| \,.$$

Лемма 20.3
$|FG| \leqslant |F| \cdot |G|$.

Доказательство.

$$|FG| = \max_{w \neq 0} \frac{||FGw||}{||w||} = \max_{Gw \neq 0} \left(\frac{||FGw||}{||Gw||} \cdot \frac{||Gw||}{||w||} \right) \leqslant \\ \leqslant \max_{Gw \neq 0} \frac{||FGw||}{||Gw||} \cdot \max_{w \neq 0} \frac{||Gw||}{||w||} \leqslant \max_{v \neq 0} \frac{||Fv||}{||v||} \cdot |G| = |F| \cdot |G| \,.$$

$\square$

Упражнение 20.7. Докажите, что для любой матрицы $A \in \mathrm{Mat}_n(\mathbb{C})$ экспоненциальный ряд $e^A = \sum\limits_{m \geqslant 0} A^m/m!$ абсолютно сходится по норме (20-15).

Теорема 20.3
Экспонента $A \mapsto e^A$ сюрьективно отображает (вещественное) векторное пространство косоэрмитовых матриц на группу унитарных матриц.

Доказательство. Поскольку $e^{CAC^{-1}} = Ce^A C^{-1}$, для вычисления экспоненты можно воспользоваться базисом, в котором матрица косоэрмитова оператора диагональна с чисто мнимыми собственными значениями. В этом базисе матрица e^A также будет диагональна с собственными значениями, по модулю равными единице, т. е. будет матрицей унитарного оператора. Наоборот, приводя произвольный унитарной оператор к диагональному виду, убеждаемся, что он может быть записан как e^A для некоторой диагональной матрицы A с чисто мнимыми диагональными элементами. $\square$

Замечание 20.1. Предыдущая теорема позволяет записать полярное разложение оператора F в виде $F = SI = Se^{iT}$, буквально совпадающем с полярным разложением (20-14) комплексного числа. Следует, однако, иметь в виду, что в отличие от унитарного оператора I, самосопряжённый оператор T, такой что $e^{iT} = I$, определён уже не однозначно, поскольку у экспоненциального отображения имеется период: например, $e^{2\pi i \mathrm{Id}} = \mathrm{Id}$. Впрочем, ровно такая же неоднозначность имеется и в формуле (20-14).

Замечание 20.2. Не следует думать, что экспонента является гомоморфизмом аддитивной группы косоэрмитовых матриц в мультипликативную унитарную группу. Если матрицы A и B не коммутируют, композиция $e^A e^B$, как правило, не равна e^{A+B}, и является экспонентой от бесконечного *ряда Кэмпбела – Хаусдорфа*, составленного из итерированных коммутаторов операторов A и B. Прочитать об этом можно в книге *Серр Ж. П. Алгебры Ли и группы Ли.* М. «Мир» 1969, гл. IV, §§ 7, 8.

Задачи для самостоятельного решения к §20

Задача 20.1. Приведите пример оператора на эрмитовом пространстве, у которого есть инвариантное подпространство, ортогонал к которому не переводится оператором в себя.

Задача 20.2. Докажите, что $(\ker F)^{\perp} = \operatorname{im} F^*$.

Задача 20.3. Пусть $V = V_1 \oplus V_2$ (сумма не обязательно ортогональная) и оператор F проектирует V на V_1 вдоль V_2. Покажите, что $V = V_1^{\perp} \oplus V_2^{\perp}$ и F^* проектирует V на $V_2^{\perp}$ вдоль $V_1^{\perp}$.

Задача 20.4 (гармонические многочлены). Введём на пространстве многочленов $\mathbb{R}[x, y, z]$ скалярное произведение так, чтобы базисные мономы $x^\alpha y^\beta z^\gamma$ составляли ортогональный базис со скалярными квадратами $\alpha!\beta!\gamma!$.
а) Найдите оператор, сопряженный *оператору Лапласа* $\Delta = \frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2} + \frac{\partial^2}{\partial z^2}$.

б) Покажите, что подпространство S^m однородных многочленов степени m раскладывается в прямую сумму вида

$$S^m = H_m \oplus \varrho^2 \cdot H_{m-2} \oplus \varrho^4 \cdot H_{m-4} \oplus \cdots ,$$

где $H_m = \{f \in S^m \mid \Delta f = 0\}$ — пространство *гармонических многочленов* степени m, а $\varrho^2 \stackrel{\text{def}}{=} x^2 + y^2 + z^2$.

Задача 20.5. На пространстве гладких периодических функций $\mathbb{R} \longrightarrow \mathbb{R}$ с периодом $T > 0$ со скалярным произведением $(f,g) = \int\limits_0^T f(x)g(x)\,dx$ вычислите операторы, сопряженные к операторам дифференцирования и умножения на функцию, а также оператор, сопряжённый к произвольному линейному дифференциальному оператору

$$L = a_k(x)\frac{d^k}{dx^k} + a_{k-1}(x)\frac{d^{k-1}}{dx^{k-1}} + \cdots + a_1(x)\frac{d}{dx} + a_0(x)$$

(с гладкими T-периодическими коэффициентами $a_0, a_1, \ldots, a_k$). Является ли самосопряжённым оператор $\sin^2\left(\frac{2\pi x}{T}\right)\frac{d^2}{dx^2} + \frac{2\pi}{T}\cos\left(\frac{4\pi x}{T}\right)\frac{d}{dx}$?

Задача 20.6. Самосопряжён ли дифференциальный оператор

$$x^2(x-1)^2\frac{d^2}{dx^2} + 2x(x-1)\frac{d}{dx}$$

на пространстве гладких функций на $[0,1]$, обращающихся на концах отрезка в нуль вместе со всеми производными, относительно скалярного произведения (20-3)?

Задача 20.7 (теорема Шура). Докажите, что любой оператор на эрмитовом пространстве записывается в подходящем ортонормальном базисе верхнетреугольной матрицей.

Задача 20.8. Докажите, что собственные векторы нормального оператора, имеющие различные собственные значения, ортогональны, и что любой ортонормированный набор собственных векторов можно дополнить до ортонормального базиса из собственных векторов.

Задача 20.9. Покажите, что для нормальности оператора F на эрмитовом пространстве необходимо и достаточно, чтобы любой собственный вектор оператора F был собственным и для F^*.

Задача 20.10. Покажите, что всякий обратимый оператор F, действующий в евклидовом (вещественном) векторном пространстве единственным образом раскладывается в композиции $F = S_1 I_1 = I_2 S_2$, где оба оператора I_ν ортогональны, а оба оператора S_ν самосопряжены и имеют положительные собственные числа.

Задача 20.11 (нормальные операторы). Докажите, что нормальность оператора F как в евклидовом, так и в эрмитовом пространстве равносильна каждому из следующих эквивалентных друг другу свойств: а) $||Fv|| = ||F^*v|| \quad \forall\, v \in V$
б) ортогонал к любому F-инвариантному подпространству F-инвариантен
в) всякое F-инвариантное подпространство F^*-инвариантно
г) компоненты разложения F в сумму самосопряжённого и антисамосопряжённого операторов перестановочны
д) компоненты полярного разложения оператора F перестановочны.

Задача 20.12. Найдите полярное разложение операторов:
а) $\begin{pmatrix} 2 & -1 \\ 2 & 1 \end{pmatrix}$ б) $\begin{pmatrix} 1 & 4 \\ 4 & 2 \end{pmatrix}$.

Задача 20.13. Докажите, что при любом $k \in \mathbb{N}$ уравнение $X^k = A$ с произвольным нормальным A разрешимо относительно X в области нормальных операторов. Для каких A все решения являются многочленами от A?

Задача 20.14. Докажите, что при любом $k \in \mathbb{N}$ уравнение $X^k = U$ с произвольным унитарным U всегда имеет в унитарной группе решение X, являющееся многочленом от U.

Задача 20.15. Рассмотрим координатное пространство $\mathbb{C}^n$ со стандартной эрмитовой структурой (20-2). Для эрмитова оператора A на $\mathbb{C}^n$ и r-мерного подпространства $L \subset \mathbb{C}^n$ с ортонормальным базисом $e_1, e_2, \dots, e_r$ положим

$$R_L(A) = \sum_{i=1}^{r} (Ae_i, e_i),$$

а) Покажите, что $R_L(A)$ не зависит от выбора ортонормального базиса в L.
б) Пусть A имеет различные собственные значения $\alpha_1 > \alpha_2 > \dots > \alpha_n$. Найдите $\max\limits_{L} R_L(A)$ по всем r-мерным подпространствам $L \subset \mathbb{C}^n$.

Задача 20.16. Покажите, что экспонента $K \longmapsto e^K$ переводит вещественные кососимметричные матрицы в собственные ортогональные. Эпиморфно ли это отображение?

Задача 20.17. Докажите, что группы $\mathrm{O}_n(\mathbb{R})$ и U_n компактны. Связны ли они?

§21. Комплексификация и овеществление

21.1. Овеществление. Всякое n-мерное комплексное векторное пространство W можно рассматривать и как векторное пространство над полем вещественных чисел $\mathbb{R} \subset \mathbb{C}$. Это вещественное векторное пространство называется *овеществлением* комплексного пространства W и обозначается $W_{\mathbb{R}}$.

Если векторы $e_1, e_2, \ldots, e_n$ составляют базис W над $\mathbb{C}$, то векторы

$$e_1, e_2, \ldots, e_n,\ ie_1, ie_2, \ldots, ie_n$$

образуют базис $W_{\mathbb{R}}$ над $\mathbb{R}$, поскольку единственность представления произвольного $w \in W$ в виде

$$w = \sum (x_\nu + i\, y_\nu) \cdot e_\nu \quad \text{с} \quad (x_\nu + i\, y_\nu) \in \mathbb{C}$$

равносильна единственности представления w в виде

$$w = \sum x_\nu \cdot e_\nu + \sum y_\nu \cdot ie_\nu \quad \text{с} \quad x_\nu,\, y_\nu \in \mathbb{R}\,.$$

Таким образом, $\dim_{\mathbb{R}} W_{\mathbb{R}} = 2 \dim_{\mathbb{C}} W$ (для избежания недоразумений здесь и далее мы пишем $\dim_{\mathbb{R}}$ и $\dim_{\mathbb{C}}$ для обозначения размерности векторных пространств над полями $\mathbb{R}$ и $\mathbb{C}$ соответственно). Отметим, в частности, что вещественные векторные пространства, возникающие как овеществления комплексных, всегда чётномерны.

21.1.1. Сравнение линейных групп. Все комплексно линейные операторы $W \xrightarrow{F} W$ составляют алгебру $\mathrm{End}_{\mathbb{C}}(W)$ над полем $\mathbb{C}$, а все вещественно линейные операторы $W_{\mathbb{R}} \xrightarrow{G} W_{\mathbb{R}}$ образуют алгебру $\mathrm{End}_{\mathbb{R}}(W_{\mathbb{R}})$ над полем $\mathbb{R}$, содержащую алгебру комплексно линейных эндоморфизмов в качестве подалгебры $\mathrm{End}_{\mathbb{C}}(W) \subset \mathrm{End}_{\mathbb{R}}(W_{\mathbb{R}})$. Если сопоставить операторам их матрицы в базисах

$$e_1, e_2, \ldots, e_n \tag{21-1}$$
$$e_1, e_2, \ldots, e_n,\ ie_1, ie_2, \ldots, ie_n \tag{21-2}$$

алгебра $\mathrm{End}_{\mathbb{C}}(W)$ отождествится с алгеброй $\mathrm{Mat}_n(\mathbb{C})$ комплексных матриц размера $n \times n$, а алгебра $\mathrm{End}_{\mathbb{R}}(W_{\mathbb{R}})$ — с алгеброй $\mathrm{Mat}_{2n}(\mathbb{R})$ вещественных матриц размера $(2n) \times (2n)$. Удобно записывать вещественные матрицы в блочном виде

$$G = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \tag{21-3}$$

в соответствии с разбиением базиса (21-2) на два набора по n векторов $\{e_\nu\}$ и $\{ie_\nu\}$. Вещественно линейный оператор G с матрицей (21-3) является комплексно линейным тогда и только тогда, когда $F(iw) = iF(w)$ для всех $w \in W_{\mathbb{R}}$. Ясно, что это условие достаточно проверять только на вещественных базисных векторах e_ν и ie_ν. Мы получаем:

Предложение 21.1 (условия Коши – Римана)
Вещественно линейный оператор (21-3) тогда и только тогда комплексно линеен, когда $C = B$ и $D = -A$. В базисе (21-1) пространства W над $\mathbb{C}$ такой оператор записывается комплексной $n \times n$-матрицей $A + iB$. □

21.1.2. Пример: комплексно дифференцируемые функции. Пусть

$$W = \mathbb{C}\,, \quad W_{\mathbb{R}} = \mathbb{R}^2\,,$$

комплексный базис (21-1) это $e = 1$, а ассоциированный вещественный базис (21-2) это $\{1, i\}$. Ненулевой комплексно линейный оператор $\mathbb{C} \xrightarrow{F} \mathbb{C}$ в этом случае является оператором умножения на какое-нибудь ненулевое комплексное число $z = a + ib$. В базисе $\{1, i\}$ такой оператор записывается 2×2-матрицей

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix}\,.$$

Произвольную функцию $\mathbb{C} = \mathbb{R}^2 \xrightarrow{f} \mathbb{R}^2 = \mathbb{C}$ можно воспринимать либо как функцию $w = f(z)$ одной комплексной переменной, либо положить $w = u + iv$, $z = x + iy$ с $x, y, u, v \in \mathbb{R}$ и думать про f как про пару функций от двух вещественных переменных

$$\begin{cases} u = u(x, y) \\ v = v(x, y)\,. \end{cases}$$

Напомним, что f называется *комплексно дифференцируемой* в точке $z_0 = x_0 + iy_0$, если её приращение (как функции от z) имеет вид

$$f(z_0 + \Delta z) = f(z_0) + \zeta \cdot \Delta z + o(\Delta z)\,, \qquad \text{где} \quad \zeta \in \mathbb{C}\,.$$

Аналогично, f называется *вещественно дифференцируемой*, если

$$\begin{pmatrix} u(x_0 + \Delta x, y_0 + \Delta y) \\ v(x_0 + \Delta x, y_0 + \Delta y) \end{pmatrix} = \begin{pmatrix} u(x_0, y_0) \\ v(x_0, y_0) \end{pmatrix} + \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \Delta x \\ \Delta y \end{pmatrix} + o(\Delta x, \Delta y)\,,$$

где $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{Mat}_{2\times 2}(\mathbb{R})\,.$

Нетрудно показать, что в обоих случаях линейные операторы, описывающие линейную часть приращения, выражаются через производные:

$$\zeta = f'(z_0) = \lim_{\Delta z \to 0} \frac{f(z_0 + \Delta z) - f(z_0)}{\Delta z}$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} \frac{\partial u}{\partial x}(x_0, y_0) & \frac{\partial v}{\partial x}(x_0, y_0) \\ \frac{\partial u}{\partial y}(x_0, y_0) & \frac{\partial v}{\partial y}(x_0, y_0) \end{pmatrix}$$

где $\frac{\partial u}{\partial x}(x_0, y_0) = \lim\limits_{\Delta x \to 0} \frac{u(x_0 + \Delta x, y_0) - f(x_0, y_0)}{\Delta x}$ и т. д.

Из предл. 21.1 вытекает, что пара вещественных непрерывно дифференцируемых функций двух вещественных переменных тогда и только тогда задаёт комплексно дифференцируемую функцию $\mathbb{C} \longrightarrow \mathbb{C}$, когда эти функции удовлетворяют дифференциальным *уравнениям Коши – Римана*

$$\frac{\partial u}{\partial x} = \frac{\partial v}{\partial y} \qquad \text{и} \qquad \frac{\partial u}{\partial y} = -\frac{\partial v}{\partial x}\,.$$

21.2. Комплексификация. Каждое векторное пространство V над полем вещественных чисел можно канонически расширить до векторного пространства над полем комплексных чисел, в которое V будет вкладываться в качестве подпространства «вещественных векторов» точно также, как поле $\mathbb{R}$ вкладывается в поле $\mathbb{C}$. Это комплексное векторное пространство обозначается $V_{\mathbb{C}} = \mathbb{C} \underset{\mathbb{R}}{\otimes} V$ и называется *комплексификацией* пространства V. Строится оно следующим образом.

Рассмотрим два экземпляра пространства V, один из которых обозначим через iV (векторы в нём тоже будут обозначаться через iv, чтобы не путать их с векторами из другого экземпляра) и образуем из этих двух пространств прямую сумму

$$V_{\mathbb{C}} = V \oplus iV\,. \tag{21-4}$$

Это векторное пространство над полем $\mathbb{R}$ размерности $\dim_{\mathbb{R}} V_{\mathbb{C}} = 2\dim_{\mathbb{R}} V$. Его векторы, по построению, имеют вид $w = v_1 + iv_2$, и равенство

$$v_1 + iv_2 = w_1 + iw_2\,,$$

по определению, означает пару равенств $v_1 = w_1$ и $v_2 = w_2$ в пространстве V. Зададим на $V_{\mathbb{C}}$ операцию умножения на комплексные числа $z = x + iy \in \mathbb{C}$ формулой:

$$(x + iy)\cdot(v_1 + iv_2) \stackrel{\text{def}}{=} (xv_1 - yv_2) + i(yv_1 + xv_2) \in V \oplus iV\,. \tag{21-5}$$

Упражнение 21.1. Проверьте, что такое умножение наделяет $V_{\mathbb{C}}$ структурой векторного пространства над полем $\mathbb{C}$.

Отметим, что каждый базис $e_1, e_2, \dots, e_n$ пространства V над $\mathbb{R}$ является одновременно базисом пространства $V_{\mathbb{C}}$ над $\mathbb{C}$, поскольку единственность представления векторов $v_1,\ v_2 \in V$ в виде

$$\begin{aligned} v_1 &= x_1e_1 + x_2e_2 + \cdots + x_ne_n \\ v_2 &= y_1e_1 + y_2e_2 + \cdots + y_ne_n \end{aligned} \qquad \text{с} \quad x_\nu, y_\nu \in \mathbb{R}$$

равносильна единственности представления вектора $w = v_1 + iv_2 \in V \oplus iV$ в виде

$$w = z_1e_1 + z_2e_2 + \cdots + z_ne_n \quad \text{с} \quad z_\nu = x_\nu + iy_\nu \in \mathbb{C}\,.$$

Таким образом, $\dim_{\mathbb{C}} V_{\mathbb{C}} = \dim_{\mathbb{R}} V$.

21.2.1. Комплексное сопряжение. На комплексифицированном пространстве $V_{\mathbb{C}}$ имеется вещественно линейная инволюция

$$V_{\mathbb{C}} \xrightarrow{\sigma} V_{\mathbb{C}} \,:\; w = v_1 + iv_2 \;\mapsto\; \overline{w} \stackrel{\text{def}}{=} v_1 - iv_2$$

которая называется *комплексным сопряжением*. По построению, $\sigma^2 = \mathrm{Id}_{V_{\mathbb{C}}}$, и вещественные подпространства V и iV из разложения (21-4) являются для этой инволюции собственными подпространствами с собственными значениями $+1$ и -1 соответственно. Векторы первого из них называются *вещественными*, а векторы второго — *чисто мнимыми*.

Подчеркнём, что по отношению к умножению на комплексные числа инволюция σ не линейна, а *антилинейна*, т. е. удовлетворяет соотношению

$$\sigma(zw) = \overline{z}\sigma(w) \;, \qquad \forall\, w \in V_{\mathbb{C}} \;, \quad \forall\, z \in \mathbb{C} \;.$$

21.2.2. Вещественная структура. Рассмотрим теперь произвольное векторное пространство W над полем $\mathbb{C}$. Всякий вещественно линейный комплексно антилинейный оператор $W_{\mathbb{R}} \xrightarrow{\sigma} W_{\mathbb{R}}$, такой что $\sigma^2 = \mathrm{Id}_W$, называется *вещественной структурой* (или *оператором комплексного сопряжения*) на комплексном пространстве W.

Комплексное векторное пространство W, оснащённое вещественной структурой, канонически представляется в виде комплексификации

$$W = \mathbb{C} \underset{\mathbb{R}}{\otimes} V$$

вещественного собственного подпространства $V \subset W_{\mathbb{R}}$ оператора σ, отвечающего собственному значению $+1$.

В самом деле, поскольку σ аннулируется многочленом $t^2 - 1 = (t+1)(t-1)$, его собственные значения равны ± 1, и вещественное пространство $W_{\mathbb{R}}$ является прямой суммой собственных подпространств, отвечающих эти собственным значениям (ср. с n° 13.2.2)

$$W_{\mathbb{R}} = V_+ \oplus V_- \;, \quad \text{где}$$
$$V_+ = \ker(\sigma - \mathrm{Id}) = \operatorname{im}(\sigma + \mathrm{Id}) \;, \quad V_- = \ker(\sigma + \mathrm{Id}) = \operatorname{im}(\sigma - \mathrm{Id}) \;.$$

Из комплексной антилинейности оператора σ вытекает, что умножения на i и на $-i$ являются взаимно обратными изоморфизмами между собственными подпространствами $V_{\pm}$, поскольку

$$v_+ \in V_+ \;\Rightarrow\; \sigma(v_+) = v_+ \;\Rightarrow\; \sigma(iv_+) = -i\sigma(v_+) = -iv_+ \;\Rightarrow\; iv_+ \in V_-$$
$$v_- \in V_- \;\Rightarrow\; \sigma(v_-) = -v_- \;\Rightarrow\; \sigma(-iv_-) = i\sigma(v_-) = -iv_- \;\Rightarrow\; -iv_- \in V_+ \;.$$

Таким образом, $W_{\mathbb{R}} = V \oplus iV$, где $V = V_+$, $iV = V_-$, и имеющееся в комплексном векторном пространстве W умножение векторов на комплексные числа происходит в точности по формуле (21-5).

Замечание 21.1. Подчеркнём, что на абстрактном векторном пространстве W над полем $\mathbb{C}$ имеется много разных вещественных структур, и никакого естественного предпочтения между ними *a priori* не существует. Иными словами у абстрактных векторов над полем $\mathbb{C}$ не бывает «вещественной части» и «мнимой части». А вот векторы в пространстве, которое является комплексификацией вещественного векторного пространства, по построению имеют вещественную и мнимую часть.

21.2.3. Пример: эрмитово сопряжение операторов. Инволюция эрмитова сопряжения $F \longmapsto F^*$ на комплексном векторном пространстве $\mathrm{End}_{\mathbb{C}}(W)$ комплексно линейных операторов на эрмитовом пространстве W, которую мы обсуждали в n° 20.2, задаёт на $\mathrm{End}_{\mathbb{C}}(W)$ вещественную структуру, вещественным и мнимым подпространствами которой являются эрмитовы и косоэрмитовы операторы соответственно, и разложение

$$\mathrm{End}_{\mathbb{C}}(W) = \mathrm{End}^+_{\mathbb{C}}(W) \oplus \mathrm{End}^-_{\mathbb{C}}(W)\,,$$

задаёт представление $\mathrm{End}_{\mathbb{C}}(W)$ в виде комплексификации вещественного векторного пространства эрмитовых операторов $\mathrm{End}^+_{\mathbb{C}}(W) = \{F \mid F^* = F\}$ путём добавления к нему вещественного пространства косоэрмитовых операторов $\mathrm{End}^-_{\mathbb{C}}(W) = \{F \mid F^* = -F\}$, каждый из которых является произведением эрмитова оператора на комплексное число i. Унитарные операторы играют в этой картине роль единичной окружности в поле комплексных чисел — это операторы, обратные к своим сопряжённым.

21.2.4. Комплексификация операторов. Всякий вещественно линейный оператор $F : V' \xrightarrow{F} V''$ между вещественными векторными пространствами продолжается по линейности до комплексно линейного оператора между их комплексификациями. Этот оператор обозначается через

$$F_{\mathbb{C}} V'_{\mathbb{C}} \longrightarrow V''_{\mathbb{C}}$$

и называется *комплексификацией* оператора F. По определению,

$$F_{\mathbb{C}}(v_1 + iv_2) \overset{\text{def}}{=} F(v_1) + iF(v_2) \quad \forall\, v_1, v_2 \in V'\,.$$

Упражнение 21.2. Убедитесь, что $F_{\mathbb{C}}(zw) = zF_{\mathbb{C}}(w)$ $\forall\, z \in \mathbb{C}$ и $\forall\, w \in V'_{\mathbb{C}}$.

Отметим, что в любом вещественном базисе $e_1, e_2, \dots, e_n \in V$ пространства $V_{\mathbb{C}}$ над полем $\mathbb{C}$ оператор $F_{\mathbb{C}}$ имеет в точности ту же (вещественную!) матрицу, что и исходный вещественный оператор F.

21.2.5. Комплексные собственные векторы. Поскольку поле $\mathbb{C}$ алгебраически замкнуто, оператор $F_{\mathbb{C}} : V_{\mathbb{C}} \longrightarrow V_{\mathbb{C}}$, полученный комплексификацией из вещественного оператора $F : V \longrightarrow V$ обязательно имеет в пространстве $V_{\mathbb{C}}$ собственный вектор. Если комплексный вектор $w = v_1 + iv_2 \in V_{\mathbb{C}}$ является собственным для $F_{\mathbb{C}}$ с комплексным собственным значением

$$\lambda = a + ib = \varrho \cdot (\cos\varphi + i \sin\varphi)\,,$$

то $F(v_1) + iF(v_2) = F_{\mathbb{C}}(v_1 + iv_2) = (a + ib)(v_1 + iv_2) = (av_1 - bv_2) + i(bv_1 + av_2)$. Таким образом, вещественная линейная оболочка векторов v_1, v_2 в V является инвариантным подпространством для F, и действие F на этом подпространстве в базисе $\{v_1, v_2\}$ задаётся матрицей

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \varrho \cdot \begin{pmatrix} \cos\varphi & \sin\varphi \\ -\sin\varphi & \cos\varphi \end{pmatrix} . \tag{21-6}$$

Поскольку матрицы операторов F и $\mathbb{F}_{\mathbb{C}}$ в любом вещественном базисе пространства $V_{\mathbb{C}}$ одинаковы, оператор $\mathbb{F}_{\mathbb{C}}$ имеет тот же самый характеристический многочлен, что и оператор F. Будучи многочленом с вещественными коэффициентами, он вместе с каждым комплексным корнем $\lambda = a + ib$ имеет также и сопряжённый комплексный корень $\overline{\lambda} = a - ib$. Из предыдущих формул видно, что вектор $w = v_1 + iv_2$ является собственным для $F_{\mathbb{C}}$ с собственным значением λ тогда и только тогда, когда сопряжённый вектор $\overline{w} = v_1 - iv_2$ является собственным для $F_{\mathbb{C}}$ с сопряжённым собственным значением $\overline{\lambda}$. Оба этих вектора соответствуют одному и тому же вещественному двумерному инвариантному подпространству $U = \mathbb{R} \cdot v_1 \oplus \mathbb{R} \cdot v_2 \subset V$, комплексификация которого является комплексной линейной оболочкой собственных векторов w и $\overline{w}$.

Упражнение 21.3. Покажите, что каждое собственное подпространство оператора $F_{\mathbb{C}}$, отвечающее вещественному собственному значению, является комплексификацией вещественного собственного пространства оператора F той же размерности и с тем же собственным значением.

Отметим, что из сказанного вытекает (независимо от сл. 13.7), что каждый вещественно линейный оператор на любом вещественном векторном пространстве обладает одномерным или двумерным инвариантным подпространством.

21.2.6. Комплексификация билинейной формы. Точно также как и линейный оператор, любую вещественно билинейную форму

$$V \times V \xrightarrow{\beta} \mathbb{R}$$

на вещественном векторном пространстве V можно продолжить по линейности до *комплексно билинейной* формы

$$V_{\mathbb{C}} \times V_{\mathbb{C}} \xrightarrow{\beta_{\mathbb{C}}} \mathbb{C} ,$$

значения которой на векторах комплексифицированного пространства вычисляются по правилу

$$\beta_{\mathbb{C}}(u_1 + iu_2, v_1 + iv_2) \overset{\text{def}}{=} \big(\beta(u_1, v_1) - \beta(u_2, v_2)\big) + i\,\big(\beta(u_1, v_2) + \beta(u_2, v_1)\big) .$$

Матрица Грама такой формы $\beta_{\mathbb{C}}$ в любом вещественном базисе пространства $V_{\mathbb{C}}$ совпадает с матрицей Грама формы β в том же базисе. Если форма β была (косо) симметричной, то такой же будет и её комплексификация $\beta_{\mathbb{C}}$.

Отметим, что специфический вещественный инвариант формы — её сигнатура — при комплексификации полностью утрачивается: все невырожденные симметричные $\mathbb{R}$-билинейные формы заданного ранга после комплексификации становятся эквивалентны друг другу над полем $\mathbb{C}$. В частности, евклидово скалярное произведение при комплексно билинейной комплексификации превращается в невырожденную комплексную форму, обладающую изотропными подпространствами размерности $[\dim V/2]$.

21.3. Эрмитово продолжение евклидовой структуры. Чтобы оставить возможность заниматься вещественной метрической геометрией в комплексифицированном пространстве $V_{\mathbb{C}}$, вещественно билинейные формы $\beta : V \times V \longrightarrow \mathbb{R}$ можно продолжать на $V_{\mathbb{C}}$ не комплексно билинейно, а линейно по первому аргументу и антилинейно по второму. Такое продолжение называется *эрмитовым* и обозначается $\beta_{\mathrm{H}} : V_{\mathbb{C}} \times V_{\mathbb{C}} \longrightarrow \mathbb{C}$. По определению,

$$\beta_{\mathrm{H}}(u_1 + iv_1, u_2 + iv_2) \stackrel{\text{def}}{=} \big(\beta(u_1, u_2) + \beta(v_1, v_2)\big) + i\,\big(\beta(u_1, v_2) - \beta(v_1, u_2)\big)\ . \quad (21\text{-}7)$$

Значения квадратичной формы ассоциированной с эрмитовым продолжением любой вещественной симметричной формы g автоматически получаются вещественными:

$$g_{\mathrm{H}}(u + iv, u + iv) = g(u, u) + g(v, v) \in \mathbb{R} \quad \forall\ (u + iv) \in V_{\mathbb{C}}\ ,$$

Замечательно, что квадратичная форма, ассоциированная с эрмитовым продолжением *косо*симметричной формы ω, также отлична от нуля, но является чисто мнимой:

$$\omega_{\mathrm{H}}(u + iv, u + iv) = 2i\,\omega(u, v) \in i \cdot \mathbb{R} \quad \forall\ (u + iv) \in V_{\mathbb{C}}\ .$$

Эрмитово продолжение $(*, *)_{\mathrm{H}}$ евклидовой структуры $(*, ast)$ на вещественном пространстве V задаёт на комплексифицированном пространстве $V_{\mathbb{C}}$ эрмитову структуру. Например, комплексификацией координатного пространства $V = \mathbb{R}^n$ является координатное пространство $V_{\mathbb{C}} = \mathbb{C}^n$, и эрмитовым продолжением стандартной евклидовой структуры $(x, y) = \sum x_\nu y_\nu$ является стандартная эрмитова структура $(z, w) = \sum z_\nu \overline{w}_\nu$. Аналогично, комплексификацией пространства вещественных непрерывных функций на отрезке $[a, b]$ с евклидовым скалярным произведением

$$(f, g) = \int\limits_a^b f(t)g(t)\,dt \quad (21\text{-}8)$$

является пространство непрерывных *комплекснозначных* функций на $[a, b]$, и эрмитово продолжение евклидовой структуры (21-8) задаётся формулой (20-3) на стр. 355.

21.3.1. Нормальные операторы в евклидовом пространстве. Комплексификация любого нормального оператора F на вещественном евклидовом пространстве V является нормальным оператором на эрмитовом пространстве $V_{\mathbb{C}}$, поскольку ортонормальные вещественные базисы евклидова пространства V, согласно формуле (21-7), остаются ортонормальными базисами эрмитова пространства $V_{\mathbb{C}}$, а матрица оператора $F_{\mathbb{C}}$ в таком базисе такая же, как у F.

Следствие 21.1
Самосопряжённый оператор F в евклидовом пространстве обладает ортонормированным базисом из собственных векторов.

Доказательство. По сл. 20.3 пространство $V_{\mathbb{C}}$ является ортогональной прямой суммой собственных подпространств оператора $\mathbb{F}_{\mathbb{C}}$, и все собственные значения оператора $\mathbb{F}_{\mathbb{C}}$ на этих подпространствах вещественны. По упр. 21.3 все эти подпространства являются комплексификациями вещественных собственных подпространств оператора F на V с теми же собственными значениями. Таким образом, пространство V является ортогональной прямой суммой собственных подпространств оператора $\mathbb{F}$. □

Следствие 21.2
Антисамосопряжённый оператор в евклидовом пространстве в подходящем ортонормированном базисе имеет блочно диагональную матрицу вида

$$\begin{pmatrix} A_1 & & & 0 \\ & A_2 & & \\ & & \ddots & \\ 0 & & & A_k \end{pmatrix}, \quad \text{где} \quad A_k = \begin{pmatrix} 0 & a_\nu \\ -a_\nu & 0 \end{pmatrix} \quad \text{и} \quad a_\nu \in \mathbb{R}$$

Доказательство. В силу того, что корни вещественного характеристического многочлена $\chi_F = \chi_{F_{\mathbb{C}}}$ разбиваются на пары комплексно сопряжённых, из сказанного в n° 21.2.5 и сл. 20.4 вытекает, что пространство $V_{\mathbb{C}}$ является ортогональной прямой суммой двумерных инвариантных подпространств оператора $\mathbb{F}_{\mathbb{C}}$, натянутых на пары комплексно сопряжённых собственных векторов с чисто мнимыми комплексно сопряжёнными собственными значениями $\pm ia_k$. Как мы видели в n° 21.2.5, каждое такое двумерное инвариантное подпространство является комплексификацией вещественного двумерного инвариантного подпространства оператора F в V, на котором F в подходящем базисе задаётся матрицей A_k. □

Упражнение 21.4. Получите из сл. 20.5 другое доказательство теор. 14.1 о приведении ортогонального оператора к блочно диагональному виду.

Упражнение 21.5. К какому виду приводится в подходящем ортонормальном базисе евклидова пространства произвольный нормальный оператор?

21.4. Комплексные структуры. Если $2n$-мерное вещественное векторное пространство $V = W_{\mathbb{R}}$ является овеществлением n-мерного комплексного векторного пространства W, то на пространстве V имеется вещественно линейный оператор умножения на i:

$$I : V \xrightarrow{v \mapsto iv} V ,$$

который удовлетворят условию $I^2 = -\mathrm{Id}_V$. Наоборот, если на произвольном вещественном векторном пространстве V задать вещественно линейный оператор I с $I^2 = -\mathrm{Id}_V$, то такой оператор позволяет определить операцию умножения векторов из V на комплексные числа по правилу

$$(x + iy) \cdot v \stackrel{\text{def}}{=} x \cdot v + y \cdot I(v) . \tag{21-9}$$

Поэтому всякий такой оператор I на вещественном векторном пространстве V называется *комплексной структурой* на V.

Упражнение 21.6. Проверьте прямым вычислением, что умножение на комплексные числа, определённое формулой (21-9), наделяет V структурой векторного пространства над полем $\mathbb{C}$ (отсюда вытекает, в частности, что $\dim V$ чётна).

Увидеть это без вычислений можно следующим геометрическим способом.

Поскольку оператор I аннулируется многочленом $t^2 + 1 = (t + i)(t - i)$, его собственные значения равны $\pm i$, и комплексифицированное пространство $V_{\mathbb{C}}$ распадается в прямую сумму двух собственных подпространств комплексифицированного оператора $V_{\mathbb{C}} \xrightarrow{I_{\mathbb{C}}} V_{\mathbb{C}}$:

$$\begin{aligned} V_{\mathbb{C}} &= W_+ \oplus W_- , \quad \text{где} \\ W_+ &= \ker(I_{\mathbb{C}} - i\,\mathrm{Id}_{V_{\mathbb{C}}}) = \operatorname{im}(I_{\mathbb{C}} + i\,\mathrm{Id}_{V_{\mathbb{C}}}) \\ W_- &= \ker(I_{\mathbb{C}} + i\,\mathrm{Id}_{V_{\mathbb{C}}}) = \operatorname{im}(I_{\mathbb{C}} - i\,\mathrm{Id}_{V_{\mathbb{C}}}) . \end{aligned}$$

Как мы видели в n° 21.2.5, для каждого собственного вектора w оператора $I_{\mathbb{C}}$ сопряжённый вектор $\overline{w}$ также будет собственным для $I_{\mathbb{C}}$, причём с сопряжённым собственным значением. Это означает, что оператор комплексного сопряжения является обратным к самому себе (антилинейным) изоморфизмом между комплексными собственными подпространствами $W_\pm$

$$W_+ \underset{\sim}{\overset{w \leftrightarrow \overline{w}}{\longleftrightarrow}} W_- .$$

В частности, $V_{\mathbb{C}} = W_+ \oplus \overline{W}_+$ и $\dim_{\mathbb{R}} V = \dim_{\mathbb{C}} V_{\mathbb{C}} = 2 \dim_{\mathbb{C}} W_+$ чётна.

Заметим теперь, что для любого комплексного прямого разложения $V_{\mathbb{C}}$ в сумму двух комплексно сопряжённых комплексных подпространств[1]

$$V_{\mathbb{C}} = U \oplus \overline{U} \tag{21-10}$$

[1] наличие такого разложения равносильно условиям $\dim_{\mathbb{R}} V = 2 \dim_{\mathbb{C}} U$ и $U \cap \overline{U} = 0$

взятие вещественной части

$$\mathrm{Re}\ :\ U \xrightarrow{w\mapsto \mathrm{Re}\, w=(w+\overline{w})/2} V \tag{21-11}$$

является вещественно линейным изоморфизмом, т. к. с точки зрения разложения (21-10) вещественные векторы $V = \{w \in V_{\mathbb{C}} \mid \overline{w} = w\}$ — это в точности все векторы вида $u+\overline{u}$. Перенося имеющееся в U умножение на i на пространство V посредством изоморфизма (21-11), мы получаем на V оператор $I = I_U$, который переводит вектор $v = \mathrm{Re}\,(u) \in V$ с $u \in U$ в вектор $\mathrm{Re}\,(iu) \in V$. По построению, $I^2 = -1$, подпространство U является $(+i)$-собственным для I, и умножение векторов из V на комплексные числа по правилу (21-9) задаёт на V структуру комплексного векторного пространства, $\mathbb{C}$-линейно изоморфного комплексному пространству U. Мы получаем

Предложение 21.2
Следующие данные на $2n$-мерном вещественном векторном пространстве V взаимно однозначно соответствуют друг другу:

1) структура векторного пространства над полем $\mathbb{C}$, для которой V является овеществлением;

2) вещественно линейный оператор $I : V \longrightarrow V$ с $I^2 = -E$

3) комплексное n-мерное подпространство $U \subset V_{\mathbb{C}}$, такое что $U \cap \overline{U} = 0$ (или, что равносильно, $V = U \oplus \overline{U}$).

Соответствие (1) $\Rightarrow$ (2) сопоставляет комплексной структуре оператор умножения на i. Соответствие (2) $\Rightarrow$ (3) сопоставляет I собственное $(+i)$-подпространство U комплексифицированного оператора $V_{\mathbb{C}} \xrightarrow{I_{\mathbb{C}}} V_{\mathbb{C}}$. Соответствие (3) $\Rightarrow$ (1) наделяет V комплексной структурой, индуцированной с комплексной структуры на пространстве U посредством вещественно линейного изоморфизма $\mathrm{Re}\ :\ U \xrightarrow{\sim} V$, переводящего $w \in U$ в $\mathrm{Re}\,(w) = (w+\overline{w})/2 \in V$. При этом изоморфизм (21-11) отождествляет оператор умножения на i в U с оператором I на V из данных (2). □

21.5. Келеровы тройки (I, g, ω). Эрмитово скалярное произведение $(\,*\,,\,*\,)$ на n-мерном комплексном векторном пространстве W индуцирует на овеществлённом пространстве $W_{\mathbb{R}}$ сразу три геометрических структуры:

- структуру евклидова пространства со скалярным произведением

$$g(v, w) = \mathrm{Re}\,(v, w)$$

- структуру симплектического пространства (см. n° 17.4) с невырожденной кососимметричной билинейной формой $\omega(v, w) = \mathrm{Im}\,(v, w)$

◦ комплексную структуру $I : w \longmapsto iw$.

В самом деле, разделяя вещественную и мнимую части эрмитова формы

$$(v, w) = g(v, w) + i\omega(v, w) \, ,$$

мы вследствие эрмитовой симметричности $(v, w) = \overline{(w, v)}$ получаем для вещественно значных билинейных форм g и ω соотношения

$$g(v, w) = g(w, v) \quad \text{и} \quad \omega(v, w) = -\omega(w, v) \, ,$$

причём $g(v, v) = (v, v) > 0$ для всех $v \neq 0$, в частности, g невырождена.

Из полуторалинейности эрмитова скалярного произведения вытекает равенство $(v, iw) = -i(v, w)$, которое означает, что

$$g(v, Iw) = \omega(v, w) \quad \text{и} \quad \omega(v, Iw) = -g(v, w) \, .$$

Иначе говоря, матрицы Грама G и Ω форм g и ω и матрица оператора I связаны равенством $GI = \Omega$, которое позволяет однозначно восстановить любой элемент тройки (I, g, ω) по двум другим. В частности, невырожденность G и I влечёт невырожденность кососимметричной формы ω.

Ещё одним следствием полуторалинейности эрмитова скалярного произведения является равенство $(v, iw) = -i(v, w)$, означающее, что

$$g(Iv, Iw) = g(v, w) \quad \text{и} \quad \omega(Iv, Iw) = \omega(v, w) \, ,$$

т. е. оператор комплексной структуры $I \in \mathrm{O}_g(W_{\mathbb{R}}) \cap \mathrm{Sp}_\omega(W_{\mathbb{R}})$ одновременно является ортогональным для g и симплектическим для ω.

Определение 21.1

Набор данных (I, g, ω) на $2n$-мерном вещественном пространстве V, состоящий из комплексной структуры I, евклидовой структуры g и невырожденной кососимметричной формы ω, называется *келеровой тройкой*, если комплекснозначная форма $(v, w) = g(v, w) + i\omega(v, w)$ задаёт эрмитово скалярное произведение на n-мерном комплексном векторном пространстве V_I, построенном по оператору I как это объяснялось в n° 21.4.

21.5.1. Келеровы тройки с заданным g. Для любой евклидовой структуры g на (чётномерном) вещественном пространстве V и любого оператора $I \in \mathrm{O}_g(V)$ с $I^2 = -1$ форма $g(v, Iw)$ автоматически невырождена и кососимметрична, поскольку $g(v, Iw) = g(Iv, I^2w) = -g(Iv, w) = -g(w, Iv)$. Поэтому комплекснозначная форма $(v, w) = g(v, w) - ig(v, Iw)$ автоматически эрмитово симметрична и положительно определена, а также полуторалинейна по отношению к комплексной структуре I , поскольку

$$\begin{aligned}(Iv, w) = g(Iv, w) + ig(v, w) = i\,(g(v, w) - ig(Iv, w)) = \\ = i\,(g(v, w) + ig(v, Iw)) = i(v, w)\end{aligned}$$

и $(v, Iw) = g(v, Iw) - ig(v, w) = -i\,(g(v, w) + ig(v, Iw)) = -i(v, w)$. Таким образом, (I, g, ω) с $\omega = g(v, I(w))$ является келеровой тройкой.

Предложение 21.3
Следующие данные на $2n$-мерном вещественном пространстве V с евклидовым скалярным произведением g эквивалентны:

1) келерова тройка (I, g, ω), в которой $\omega(v, w) = g(v, I(w))$

2) комплексная структура $I \in \mathrm{O}_g(V)$ на V

3) n-мерное комплексное подпространство $U \subset V_{\mathbb{C}}$ изотропное для $\mathbb{C}$-билинейного продолжения $g_{\mathbb{C}}$ формы g на $V_{\mathbb{C}}$

Связи между этими данными те же, что и в предл. 21.2.

Доказательство. Мы должны показать, что в терминах данных (3) из предложения предл. 21.2 условие $I \in \mathrm{O}_g(V)$ означает, что $(+i)$-собственное подпространство $U \subset V_{\mathbb{C}}$ комплексифицированного оператора $I_{\mathbb{C}}$ является максимальным изотропным подпространством $\mathbb{C}$-билинейной квадратичной формы $g_{\mathbb{C}}$.

Если $I \in \mathrm{O}_g(V)$, то $I_{\mathbb{C}} \in \mathrm{O}_{g_{\mathbb{C}}}(V_{\mathbb{C}})$, и для любого u, такого что $I_{\mathbb{C}}u = iu$, выполняется равенство $g_{\mathbb{C}}(u, u) = g_{\mathbb{C}}(I_{\mathbb{C}}u, I_{\mathbb{C}}u) = g_{\mathbb{C}}(iu, iu) = -g_{\mathbb{C}}(u, u)$, откуда $g_{\mathbb{C}}(u, u) = 0$.

Наоборот, для любого $g_{\mathbb{C}}$-изотропного подпространства U размерности

$$\dim_{\mathbb{C}} U = \frac{1}{2}\dim_{\mathbb{C}} V_{\mathbb{C}} = \frac{1}{2}\dim_{\mathbb{R}} V$$

пересечение $U \cap \overline{U} = 0$, так как у квадрики g нет вещественных изотропных векторов[1]. Тем самым, $V_{\mathbb{C}} = U \oplus \overline{U}$. Подпространство $\overline{U}$ также изотропно для $g_{\mathbb{C}}$, поскольку для любого вектора $v_1 + iv_2 \in U$ с $v_1, v_2 \in V$

$$\begin{aligned} g_{\mathbb{C}}(\overline{v_1 + iv_2}, \overline{v_1 + iv_2}) &= g(v_1, v_1) - g(v_2, v_2) - 2i\, g(v_1, v_2) = \\ &= \overline{g(v_1, v_1) - g(v_2, v_2) + 2i\, g(v_1, v_2)} = \overline{g_{\mathbb{C}}(v_1 + iv_2, v_1 + iv_2)} = 0 \end{aligned}$$

Из изотропности U и $\overline{U}$ вытекает, что оператор $I_{\mathbb{C}} : V_{\mathbb{C}} \longrightarrow V_{\mathbb{C}}$, такой что U и $\overline{U}$ суть его собственные $\pm i$ подпространства, является изометрией формы $g_{\mathbb{C}}$

$$\begin{aligned} g_{\mathbb{C}}(u_1 + \overline{u}_2, u_1 + \overline{u}_2) &= g_{\mathbb{C}}(u_1, \overline{u}_2) + g_{\mathbb{C}}(\overline{u}_1, u_2) = \\ &= g_{\mathbb{C}}(iu_1, -i\overline{u}_2) + g_{\mathbb{C}}(-i\overline{u}_1, iu_2) = g_{\mathbb{C}}(I_{\mathbb{C}}(u_1 + \overline{u}_2), I_{\mathbb{C}}(u_1 + \overline{u}_2)), \end{aligned}$$

что и требовалось проверить. □

[1] если $u_1 = \overline{u}_2$ для некоторых $u_1, u_2 \in U$, то $u_1 + u_2 \in U$ изотропен и вещественен, откуда $u_2 = -u_1 = iv$ для некоторого $v \in V$, и $0 = g_{\mathbb{C}}(u_1, u_1) = -g(v, v) \Rightarrow v = 0$

21.5.2. Изотропные грассманианы. Комплексные подпространства размерности n в $2n$-мерном пространстве образуют грассманиан $\mathrm{Gr}(n, 2n)$. Например, 2-мерные подпространства 4-мерного пространства $\mathbb{C}^4$ составляют грассманиан $\mathrm{Gr}(2,4)$, представляющий собою гладкую квадрику Плюккера в

$$\mathbb{P}_5 = \mathbb{P}(\Lambda^2\mathbb{C}^4)$$

(см. n° 19.3). Совокупность n-мерных подпространств, изотропных для фиксированной невырожденной квадратичной формы $g_\mathbb{C}$, или, что то же самое, семейство всех проективных подпространств максимальной размерности, заметающих гладкую комплексную проективную квадрику $V(g_\mathbb{C})$, образуют в $\mathrm{Gr}(n, 2n)$ замкнутое подмногообразие, которое называется *изотропным грассманианом* и обозначается $\mathrm{Gr}_{g_\mathbb{C}}(n, 2n)$.

Таким образом, продолжения данного евклидова скалярного произведения g на $\mathbb{R}^{2n}$ до келеровой тройки параметризуются точками (комплексного!) изотропного грассманиана $\mathrm{Gr}_{g_\mathbb{C}}(n, 2n)$.

Например, продолжения стандартного евклидова скалярного произведения на $\mathbb{R}^4$ до келеровой тройки на $\mathbb{C}^2$ образуют изотропный грассманиан

$$\mathrm{Gr}_{\mathrm{Segre}}(2,4) \subset \mathrm{Gr}(2,4)\,,$$

параметризующий прямолинейные образующие квадрики Сегре[1] в $\mathbb{P}_3$ и представляющий собою объединение двух непересекающихся коник Веронезе, высекаемых из квадрики Плюккера $\mathrm{Gr}(2,4) \subset \mathbb{P}_5$ двумя дополнительными 2-мерными плоскостями — проективизациями собственных подпростанств ходжевой инволюции $*$ на $\Lambda^2\mathbb{C}^4$, задаваемой евклидовым скалярным произведением g (см. n° 22.5 и зад. 24.7 ниже).

21.5.3. Келеровы тройки с заданным $\boldsymbol{\omega}$. Совершенно аналогично предыдущему, невырожденная кососимметричная форма ω на (чётномерном) вещественном пространстве V и любой оператор $I \in \mathrm{Sp}_\omega(V)$ с $I^2 = -1$ производят невырожденную симметричную[2] форму $-\omega(v, Iw)$. Таким образом, комплекснозначная форма

$$(v, w) = -\omega(v, Iw) + i\omega(v, w) \tag{21-12}$$

невырождена и эрмитово симметрична, а также полуторалинейна, поскольку

$$\begin{aligned}(Iv, w) = -\omega(v, w) + i\omega(Iv, w) = i\,(\omega(Iv, w) + i\omega(v, w)) = \\ = i\,(-\omega(v, Iw) + i\omega(v, w)) = i(v, w)\end{aligned}$$

и $(v, Iw) = \omega(v, w) + i\omega(v, Iw) = -i\,(-\omega(v, Iw) + i\omega(v, w)) = -i(v, w)$. Следовательно, (I, g, ω) с $g = -\omega(v, I(w))$ является келеровой тройкой тогда и только тогда, когда квадратичная форма $-\omega(v, Iv)$ положительно определена на V.

[1] $\mathbb{C}$-билинейное продолжение евклидова скалярного произведения на $\mathbb{R}^4$ является невырожденной комплексной билинейной формой, задающей в $\mathbb{P}_3 = \mathbb{P}(\mathbb{C}^4)$ квадрику Сегре

[2] симметричность проверяется выкладкой $\omega(v, Iw) = \omega(Iv, I^2w) = -\omega(Iv, w) = \omega(w, Iv)$

Чтобы геометрически прояснить последнее условие, рассмотрим комплексификацию $I_{\mathbb{C}} : V_{\mathbb{C}} \longrightarrow V_{\mathbb{C}}$ оператора I и обозначим через

$$\omega_{\mathbb{C}}(w_1, w_2) \quad \text{и} \quad \omega_{\mathrm{H}}(w_1, w_2) = \omega_{\mathbb{C}}(w_1, \overline{w}_2)$$

комплексно билинейное и полуторалинейное продолжения кососимметричной формы ω на $V_{\mathbb{C}}$. Тогда $V_{\mathbb{C}} = L \oplus \overline{L}$, где $L, \overline{L} \subset V_{\mathbb{C}}$ суть собственные $\pm i$-подпространства комплексифицированного оператора $I_{\mathbb{C}}$.

Предложение 21.4
Следующие данные на $2n$-мерном вещественном пространстве V с невырожденной кососимметричной билинейной формой ω эквивалентны:

1) келерова тройка (I, g, ω), в которой $g(v, w) = -\omega(v, Iw)$
2) комплексная структура $I \in \mathrm{Sp}_{\omega}(V)$ на V, такая что квадратичная форма $-\omega(v, Iw)$ положительно определена
3) n-мерное комплексное лагранжево подпространство $L \subset V_{\mathbb{C}}$ комплексно билинейной формы $\omega_{\mathbb{C}}$, такое что полуторалинейная форма $i\,\omega_{\mathrm{H}}$ задаёт на L эрмитову структуру

Связи между этими данными те же, что и в предл. 21.2.

Доказательство. Из условия $I_{\mathbb{C}} \in \mathrm{Sp}_{\omega_{\mathbb{C}}}(V_{\mathbb{C}})$, как и в евклидовом случае, вытекает, что L изотропно для $\omega_{\mathbb{C}}$: для любых $w_1, w_2 \in L$ имеем

$$\omega_{\mathbb{C}}(w_1, w_2) = \omega_{\mathbb{C}}(I_{\mathbb{C}}w_1, I_{\mathbb{C}}w_2) = \omega_{\mathbb{C}}(iw_1, iw_2) = -\omega_{\mathbb{C}}(w_1, w_2)\,,$$

откуда $\omega_{\mathbb{C}}(w_1, w_2) = 0$. Поскольку $\forall\, u, v \in V$, таких что $(u+iv) \in L$, выполняется равенство $Iu = -v$, ограничение полуторалинейной формы $i\,\omega_{\mathrm{H}}$ на L имеет вид[1]

$$\begin{aligned} i\,\omega_{\mathrm{H}}(u_1 + iv_1, u_2 + iv_2) &= \omega(u_1, v_2) - \omega(v_1, u_2) + i\left(\omega(u_1, u_2) + \omega(v_1, v_2)\right) = \\ &= -\omega(u_1, Iu_2) + \omega(Iu_1, u_2) + i\left(\omega(u_1, u_2) + \omega(Iu_1, Iu_2)\right) = \\ &= 2\left(-\omega(u_1, Iu_2) + i\,\omega(u_1, u_2)\right). \end{aligned}$$

Полагая $w_\nu = u_\nu + iv_\nu \in L$ и $g(u_1, u_2) = -\omega(u_1, Iu_2)$, это равенство можно переписать в виде

$$\begin{aligned} i\,\omega_{\mathrm{H}}(w_1, w_2) &= 2\Big(g\big(\mathrm{Re}\,(w_1), \mathrm{Re}\,(w_2)\big) + i\,\omega\big(\mathrm{Re}\,(w_1), \mathrm{Re}\,(w_2)\big)\Big) = \\ &= 2\left(\mathrm{Re}\,(w_1), \mathrm{Re}\,(w_2)\right), \end{aligned} \tag{21-13}$$

где в конце стоит форма (21-12). Итак, положительность формы (21-12) на V равносильна положительности ограничения $i\,\omega_{\mathrm{H}}|_L$.

[1] в нижней строке мы пользуемся условиями $I \in \mathrm{Sp}_{\omega}(V)$ и $I^2 = -1$

Наоборот, для любого n-мерного подпространства $L \subset V_\mathbb{C}$, на которое $\omega_\mathbb{C}$ ограничивается в тождественно нулевую, а $i\,\omega_\mathbb{C}(L,\overline{L})$ в положительно определённую форму, пересечение $L\cap\overline{L} = 0$ (ибо для $u_1, u_2 \in L$ с $u_1 = \overline{u}_2$ получаем противоречивые условия $0 = i\,\omega_\mathbb{C}(u_2, u_1) = i\,\omega_\mathbb{C}(u_2, \overline{u}_2) = \omega_\mathrm{H}(u_2, u_2) > 0$). Поэтому $V = L\oplus\overline{L}$, причём $\overline{L}$ тоже лагранжево для $\omega_\mathbb{C}$, т. к. для любых $w_\nu = u_\nu + iv_\nu \in L$ с $u_\nu, v_\nu \in V$

$$\begin{aligned}\omega_\mathbb{C}(\overline{w}_1, \overline{w}_2) &= \omega_\mathbb{C}(u_1 - iv_1, u_2 - iv_2) = \\ &= \omega(u_1,u_2) - \omega(v_1,v_2) - i\,\omega(u_1,v_2) - i\,\omega(v_1,u_2) = \\ &= \overline{\omega(u_1,u_2) - \omega(v_1,v_2) + i\,\omega(u_1,v_2) + i\,\omega(v_1,u_2)} = \\ &= \overline{\omega_\mathbb{C}(u_1 + iv_1, u_2 + iv_2)} = \overline{\omega_\mathbb{C}(w_1,w_2)} = 0\,.\end{aligned}$$

Это означает, что оператор $I_\mathbb{C} : V_\mathbb{C} \longrightarrow V_\mathbb{C}$, для которого U и $\overline{U}$ служат собственными $\pm i$ подпространствами, является изометрией формы $\omega_\mathbb{C}$:

$$\begin{aligned}\omega_\mathbb{C}(u_1 + \overline{v}_1, u_2 + \overline{v}_2) &= \omega_\mathbb{C}(u_1, \overline{v}_2) + \omega_\mathbb{C}(\overline{v}_1, u_2) = \\ &= \omega_\mathbb{C}(iu_1, -i\overline{v}_2) + \omega_\mathbb{C}(-i\overline{v}_1, iu_2) = \omega_\mathbb{C}(I_\mathbb{C}(u_1 + \overline{v}_1), I_\mathbb{C}(u_2 + \overline{v}_2))\,,\end{aligned}$$

а индуцированная на V полуторалинейная форма $(\,*\,,\,*\,)$ из правой части (21-13) является эрмитовым скалярным произведением. $\square$

21.5.4. Зигелево полупространство $\mathfrak{H}_n \subset \mathrm{Mat}_n(\mathbb{C})$. Зафиксируем в V симплектический базис

$$e'_1, e'_2, \dots, e'_n,\; e''_1, e''_2, \dots, e''_n \tag{21-14}$$

в котором матрица Грама невырожденной кососимметричной формы ω равна

$$J = \begin{pmatrix} 0 & E \\ -E & 0 \end{pmatrix}\,, \tag{21-15}$$

и обозначим через $V', V'' \subset V$ лагранжевы подпространства, натянутые на первые n и на последние n базисных векторов соответственно. Тогда

$$V = V' \oplus V'' \quad \text{и} \quad V_\mathbb{C} = V'_\mathbb{C} \oplus V''_\mathbb{C}\,,$$

где оба подпространства $V'_\mathbb{C}$, $V''_\mathbb{C}$ лагранжевы для $\omega_\mathbb{C}$.

Заметим, что в любом разложении $V_\mathbb{C} = L\oplus\overline{L}$ в прямую сумму лагранжевых подпространств формы $\omega_\mathbb{C}$, таких что полуторалинейная форма $i\,\omega_\mathrm{H}$ положительно определена на L, пространство L должно быть трансверсально любому лагранжеву подпространству $U_\mathbb{C} \subset V_\mathbb{C}$, получающемуся комплексификацией вещественного лагранжева подпространства $U \subset V$, поскольку для любых $u_1, u_2 \in U$ выполняется равенство $i\,\omega_\mathrm{H}(u_1 + iu_2, u_1 + iu_2) = 0$.

В частности, $L \cap V''_{\mathbb{C}} = 0$ и проекция L на $V'_{\mathbb{C}}$ вдоль $V''_{\mathbb{C}}$ является изоморфизмом комплексных векторных пространств. Поэтому в L существует единственный базис

$$w_1, w_2, \dots, w_n \subset L \subset V_{\mathbb{C}}$$

проектирующийся вдоль $V''_{\mathbb{C}}$ в первые n базисных векторов e' симплектического базиса (21-14). Иначе говоря,

$$(w_1, w_2, \dots, w_n) = (e'_1, \, \dots \, , e'_n, \, e''_1, \, \dots \, , e''_n) \cdot \begin{pmatrix} E \\ S \end{pmatrix} \tag{21-16}$$

для некоторой матрицы $S \in \mathrm{Mat}_n(\mathbb{C})$, и подпространство L однозначно определяется матрицей S. Из (21-15) вытекает, что матрицы Грама форм $\omega_{\mathbb{C}}$ и $i\,\omega_{\mathrm{H}}$ в базисе $w = e' + e''S$ имеют вид

$$\begin{aligned} \omega_{\mathbb{C}}|_L &= \begin{pmatrix} E & S^t \end{pmatrix} \cdot \begin{pmatrix} 0 & E \\ -E & 0 \end{pmatrix} \cdot \begin{pmatrix} E \\ S \end{pmatrix} = S - S^t \,, \\ i\omega_{\mathrm{H}}|_L &= i \cdot \begin{pmatrix} E & S^t \end{pmatrix} \cdot \begin{pmatrix} 0 & E \\ -E & 0 \end{pmatrix} \cdot \begin{pmatrix} E \\ \overline{S} \end{pmatrix} = i\,(\overline{S} - S^t) \,. \end{aligned}$$

Таким образом, лагранжевость L равносильна симметричности матрицы S. В этом случае $i\,(\overline{S} - S^t) = \mathrm{Im}\,(S)$, и положительность ограничения $i\omega_{\mathrm{H}}|_L$ означает, что вещественная симметрическая матрица $\mathrm{Im}\,(S)$ положительно определена.

Определение 21.2

Множество симметричных комплексных $n \times n$ матриц $S \in \mathrm{Mat}_n(\mathbb{C})$ с положительно определённой мнимой частью, т. е. удовлетворяющих *соотношениям Римана*[1]

$$S^t = S \;, \quad x \cdot \mathrm{Im}\,(S) \cdot x^t > 0 \quad \forall \text{ ненулевого } x = (x_1, x_2, \dots, x_n) \in \mathbb{R}^n \,, \tag{21-17}$$

называется *верхним полупространством Зигеля*[2] и обозначается $\mathfrak{H}_n$.

Теорема 21.1

Комплексные структуры, продолжающие стандартную кососимметрическую форму на симплектическом пространстве Ω_{2n} до келеровой тройки, взаимно

[1] соотношения Римана возникают в самых разных разделах геометрии; например, они необходимы и достаточны для того, чтобы n-мерный комплексный тор $\mathbb{C}^n/\Lambda$, где $\Lambda \simeq \mathbb{Z}^{2n}$ — целочисленная решётка, натянутая на n стандартных базисных векторов $\mathbb{C}^n$ и n столбцов матрицы S, можно было комплексно аналитически вложить в комплексное проективное пространство как алгебраическое подмногообразие (подробности см. в книгах *Д. Мамфорд. Лекции о тэта-функциях.* (М., «Мир», 1988) и *В. В. Шокуров. Римановы поверхности и алгебраические кривые.* (М., «ВИНИТИ», 1988, сер. «Современные проблемы математики. Фундаментальные направления.», т. 23 «Алгебраическая Геометрия 1»)

[2] по аналогии со случаем $n = 1$, когда условия (21-17) задают верхнюю полуплоскость $\mathrm{Im}\, z > 0$ в $\mathbb{C} = \mathrm{Mat}_1(\mathbb{C})$

однозначно соответствуют точкам зигелева полупространства $\mathfrak{H}_n$. При этом комплексная структура $I_S : \Omega_{2n} \longrightarrow \Omega_{2n}$, отвечающая матрице $S = X + iY \in \mathfrak{H}_n$ с $X, Y \in \mathrm{Mat}_n(\mathbb{R})$ имеет в симплектическом базисе (21-14) блочную матрицу

$$I_S = \begin{pmatrix} -Y^{-1}X & Y^{-1} \\ -Y - XY^{-1}X & XY^{-1} \end{pmatrix} \tag{21-18}$$

Доказательство. Нам осталось проверить только правило (21-18). Согласно предложению предл. 21.2, комплексная структура $I : V \longrightarrow V$, отвечающая разложению $V_{\mathbb{C}} = W \oplus \overline{W}$, переводит $v = \mathrm{Re}\, w \in V$ с $w \in W$ в $I(v) = \mathrm{Re}\,(iw)$. Если $w = e' + e'' \cdot (X + iY)$ то $\mathrm{Re}\,(w) = e' + e'' \cdot X$ и $\mathrm{Re}\,(iw) = -e'' \cdot Y$. Поэтому

$$\begin{aligned} I(e'') &= I\big(\mathrm{Re}\,(-iw \cdot Y^{-1})\big) = \mathrm{Re}\,(w) \cdot Y^{-1} = e' \cdot Y^{-1} + e'' \cdot XY^{-1} \\ I(e') &= I(\mathrm{Re}\,(w) - e'' \cdot X) = \mathrm{Re}\,(iw) - I(e'') \cdot X = \\ &= -e' \cdot Y^{-1}X + e'' \cdot (-Y + XY^{-1}X)\,. \end{aligned}$$

□

Задачи для самостоятельного решения к §21

Задача 21.1. Пусть V — конечномерное вещественное векторное пространство с евклидовым скалярным произведением (u, w). Покажите, что
а) сопоставление линейному оператору $F : V \longrightarrow V$ билинейной формы

$$\beta_F(u, w) = (u, Fw)$$

является линейным изоморфизмом между пространством линейных операторов и пространством билинейных форм
б) (анти) самосопряжённые операторы переводятся этим изоморфизмом соответственно в (косо) симметричные билинейные формы
в) любая квадратичная форма на V приводится к виду $\sum a_i x_i^2$ в некотором *ортонормальном* базисе[1], причём набор чисел a_i не зависит, с точностью до перестановки, от выбора такого ортонормального базиса. г) для построения базиса из предыдущего пункта достаточно найти все собственные подпространства линейного оператора, задаваемого матрицей Грама формы в произвольном ортонормальном базисе, и выбрать в каждом из собственных подпространств любой ортонормальный базис; объединение этих базисов и будет искомым.

[1]отыскание такого базиса называется *приведением квадрики к нормальным осям*

Задача 21.2. Два оператора в евклидовом пространстве $\mathbb{R}^3$ имеют в стандартном базисе матрицы

а) $\begin{pmatrix} 1/2 & -\sqrt{3}/2 & 0 \\ \sqrt{3}/4 & 1/4 & -\sqrt{3}/2 \\ 3/4 & \sqrt{3}/4 & 1/2 \end{pmatrix}$ б) $\begin{pmatrix} \sqrt{2}/2 & -\sqrt{2}/2 & 0 \\ 1/2 & 1/2 & -\sqrt{2}/2 \\ 1/2 & 1/2 & \sqrt{2}/2 \end{pmatrix}$

Выясните про каждый из них, является ли он поворотом или композицией поворота с отражением в плоскости, перпендикулярной оси поворота, а также найдите ось и угол этого поворота.

Задача 21.3. В евклидовом пространстве $\mathbb{R}^3$ найдите минимум и максимум длин больших диагоналей прямоугольных параллелепипедов, описанных вокруг эллипсоида $x_1^2 + \frac{x_2^2}{4} + \frac{x_3^2}{9} = 1$.

Задача 21.4. Для n-мерного векторного пространства W над полем $\mathbb{C}$ с овеществлением $W_{\mathbb{R}}$ найдите коразмерность подпространства $\operatorname{End}_{\mathbb{C}}(W)$ в пространстве $\operatorname{End}_{\mathbb{R}}(W_{\mathbb{R}})$ (оба пространства операторов рассматриваются как вещественные и коразмерность имеется в виду над $\mathbb{R}$).

Задача 21.5 (сопряжённые комплексные структуры). Для комплексного векторного пространства W обозначим через $\overline{W}$ векторное пространство, совпадающее с W как аддитивная абелева группа[1], но с умножением векторов на комплексные числа, заданным по формуле

$$z \bar{\cdot} w \overset{\text{def}}{=} \overline{z} \cdot w$$

(слева написано произведение в $\overline{W}$, которое мы определяем, а справа — известное произведение в W). Покажите, что

а) $\overline{W}$ является векторным пространством над полем $\mathbb{C}$, той же размерности, что и W

б) комплексифицированное овеществление $(W_{\mathbb{R}})_{\mathbb{C}}$ и прямая сумма $W \oplus \overline{W}$ канонически изоморфны (как комплексные векторные пространства)

Задача 21.6. Для комплексно линейного оператора $F : W \longrightarrow W$ на комплексном векторном пространстве W обозначим через $F_{\mathbb{C}}\, (W_{\mathbb{R}})_{\mathbb{C}} \longrightarrow (W_{\mathbb{R}})_{\mathbb{C}}$ комплексификацию вещественно линейного оператора $F : W_{\mathbb{R}} \longrightarrow W_{\mathbb{R}}$ на овеществлённом пространстве $W_{\mathbb{R}}$. Выясните, как связаны друг с другом характеристические многочлены, собственные числа[2] и собственные векторы операторов F и $F_{\mathbb{C}}$

а) в случае, когда $W = \mathbb{C}$ (так что $W_{\mathbb{R}} = \mathbb{R}^2$), а $F : \mathbb{C} \longrightarrow \mathbb{C}$ является оператором умножения на i

б) в общем случае.

Задача 21.7. Проверьте прямым вычислением, что матрица I_S из (21-18) имеет $I_S^2 = -E$ и сохраняет форму ω.

[1] т. е. «состоящее из тех же векторов»

[2] обратите внимание, что характеристический многочлен оператора $F_{\mathbb{C}}$ имеет вдвое большую степень, чем характеристический многочлен оператора F, и собственных чисел у него, соответственно, тоже вдвое больше

Задача 21.8. Постройте изоморфизм групп $U_n \simeq \mathrm{O}_{2n}(\mathbb{R}) \cap \mathrm{Sp}_{2n}(\mathbb{R})$.

Задача 21.9. Покажите, что зигелево полупространство $\mathfrak{H}_n \subset \mathrm{Mat}_n(\mathbb{C})$ непрерывно стягивается по себе в точку.

§22. Кватернионы

22.1. Три инволюции на пространстве $\mathrm{Mat}_2(\mathbb{C})$. На 4-мерном пространстве $W = \mathrm{Mat}_2(\mathbb{C})$ комплексных матриц размера 2×2 имеется $\mathbb{C}$-линейная инволюция, переводящая матрицу в присоединённую транспонированную матрицу

$$\eta = \begin{pmatrix} \eta_{11} & \eta_{12} \\ \eta_{21} & \eta_{22} \end{pmatrix} \longmapsto \eta^{\times} \stackrel{\text{def}}{=} \eta^{\vee t} = \begin{pmatrix} \eta_{22} & -\eta_{12} \\ -\eta_{21} & \eta_{11} \end{pmatrix} \tag{22-1}$$

Упражнение 22.1. Проверьте, что $(\eta\zeta)^{\times} = \zeta^{\times}\eta^{\times}$, т. е. $\eta \mapsto \eta^{\times}$ антигомоморфизм.

Поскольку $\eta \cdot \eta^{\times} = \det(\eta) \cdot E$ комплексная билинейная форма

$$\widetilde{\det}(\eta, \zeta) \stackrel{\text{def}}{=} \frac{1}{2}\,\mathrm{tr}\,(\eta\,\zeta^{\times}) \tag{22-2}$$

является поляризацией комплексной квадратичной формы $\det(\eta)$ на W.

Упражнение 22.2. Убедитесь, что $\mathbb{C}$-билинейная форма (22-2) симметрична и невырождена, и напишите её матрицу Грама в стандартном базисе из матричных единиц.

Кроме того, на W имеется $\mathbb{C}$-антилинейная инволюция эрмитова сопряжения матриц

$$\eta = \begin{pmatrix} \eta_{11} & \eta_{12} \\ \eta_{21} & \eta_{22} \end{pmatrix} \longmapsto \eta^{*} \stackrel{\text{def}}{=} \overline{\eta}^{t} = \begin{pmatrix} \overline{\eta}_{11} & \overline{\eta}_{21} \\ \overline{\eta}_{12} & \overline{\eta}_{22} \end{pmatrix}\ , \tag{22-3}$$

которая также является антигомоморфизмом[1] алгебры матриц, и формула, аналогичная (22-2), задаёт на пространстве W эрмитово скалярное произведение

$$(\eta, \zeta) \stackrel{\text{def}}{=} \frac{1}{2}\,\mathrm{tr}\,(\eta\,\zeta^{*})\ . \tag{22-4}$$

Ассоциированная с этим произведением норма представляет собой полусумму квадратов модулей матричных элементов

$$||\eta||^2 \stackrel{\text{def}}{=} (\eta, \eta) = \frac{1}{2}\sum |\eta_{ij}|^2\ ,$$

и матричные единицы составляют его ортогональный базис со скалярными квадратами $1/2$.

Композиция инволюций $\eta \leftrightarrow \eta^{*}$ и $\eta \leftrightarrow \eta^{\times}$ обозначается через

$$\sigma\ :\ \eta = \begin{pmatrix} \eta_{11} & \eta_{12} \\ \eta_{21} & \eta_{22} \end{pmatrix} \longmapsto \eta^{\sigma} \stackrel{\text{def}}{=} \overline{\eta}^{\vee} = \begin{pmatrix} \overline{\eta}_{22} & -\overline{\eta}_{21} \\ -\overline{\eta}_{12} & \overline{\eta}_{11} \end{pmatrix}\ . \tag{22-5}$$

Видно, что σ является $\mathbb{C}$-антилинейной инволюцией на пространстве W и

$$(\eta, \zeta) = \widetilde{\det}(\eta, \zeta^{\sigma})\,.$$

[1] т. е. $(\eta\zeta)^* = \zeta^*\eta^*$

Упражнение 22.3. Убедитесь, что и три инволюции σ, $\times$, $*$ вместе с тождественным преобразованием образуют группу Клейна $\mathfrak{V}_4 \simeq \mathbb{Z}/(2) \times \mathbb{Z}/(2)$.

Отметим, что будучи композицией двух антигомоморфизмов, σ является автоморфизмом матричной алгебры: $(\eta\zeta)^\sigma = \eta^\sigma\zeta^\sigma$.

Мы используем антилинейную инволюцию $\eta \leftrightarrow \eta^\sigma$ в качестве *вещественной структуры* на W. Подпространство $V = \operatorname{Re}_\sigma(W)$ вещественных векторов этой структуры состоит из матриц вида

$$x = \begin{pmatrix} x_1 + i\,x_2 & x_2 + i\,x_3 \\ -x_2 + i\,x_3 & x_1 - i\,x_2 \end{pmatrix} \quad \text{с} \quad x_\nu \in \mathbb{R}\,, \tag{22-6}$$

и обе формы (22-2), (22-4) ограничиваются на это вещественное подпространство в стандартную евклидову структуру $(x, x) = \sum x_\nu^2$, ортонормальным базисом для которой служат, например, матрицы

$$\boldsymbol{e} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\,, \quad \boldsymbol{i} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}\,, \quad \boldsymbol{j} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\,, \quad \boldsymbol{k} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}\,. \tag{22-7}$$

Итак, комплексное 4-мерное пространство W представляет собой комплексификацию 4-мерного вещественного евклидова пространства $V \simeq \mathbb{R}^4$ матриц (22-6), а формы $\widetilde{\det}$ и $(*, *)$ суть комплексно билинейное и эрмитово продолжения евклидовой структуры с V на W.

22.2. Тело кватернионов $\mathbb{H}$. Поскольку σ является гомоморфизмом относительно матричного умножения, вещественное подпространство $V \subset \operatorname{Mat}_2(\mathbb{C})$ является подалгеброй в алгебре матриц. Эта подалгебра называется *алгеброй кватернионов* и обозначается $\mathbb{H}$. Вектор $\boldsymbol{e}$ является единичным элементом алгебры $\mathbb{H}$, и обычно обозначается просто 1, а в произведениях опускается вовсе. Таблица умножения остальных базисных кватернионов (22-7) имеет вид:

$$\begin{gathered} \boldsymbol{i}^2 = \boldsymbol{j}^2 = \boldsymbol{k}^2 = -1\,, \\ \boldsymbol{i}\boldsymbol{j} = -\boldsymbol{j}\boldsymbol{i} = \boldsymbol{k}\,, \quad \boldsymbol{j}\boldsymbol{k} = -\boldsymbol{k}\boldsymbol{j} = \boldsymbol{i}\,, \quad \boldsymbol{k}\boldsymbol{i} = -\boldsymbol{i}\boldsymbol{k} = \boldsymbol{j}\,. \end{gathered} \tag{22-8}$$

Тем самым, произвольная пара кватернионов перемножается по правилу

$$\begin{aligned} (x_0 + x_1\boldsymbol{i} + x_2\boldsymbol{j} + x_3\boldsymbol{k}) \cdot (y_0 + y_1\boldsymbol{i} + y_2\boldsymbol{j} + y_3\boldsymbol{k}) = \\ = (x_0y_0 - x_1y_1 - x_2y_2 - x_3y_3) + \\ + (x_0y_1 + x_1y_0 + x_2y_3 - x_3y_2)\,\boldsymbol{i} + \\ + (x_0y_2 + x_2y_0 + x_3y_1 - x_1y_3)\,\boldsymbol{j} + \\ + (x_0y_3 + x_3y_0 + x_1y_2 - x_2y_1)\,\boldsymbol{k} \end{aligned} \tag{22-9}$$

Упражнение 22.4. Попробуйте убедиться прямым вычислением, что таблица умножения (22-8) и формула (22-9) задают на абстрактном вещественном векторном пространстве с базисом $\{1, \boldsymbol{i}, \boldsymbol{j}, \boldsymbol{k}\}$ структуру ассоциативной $\mathbb{R}$-алгебры.

22.2.1. Мнимые и вещественные кватернионы. По аналогии с комплексными числами, 1-мерное подпространство $\mathbb{R}\cdot\boldsymbol{e}\subset\mathbb{H}$ называется пространством *чисто вещественных* кватернионов, а 3-мерное подпространство

$$I=\{x\cdot\boldsymbol{i}+y\cdot\boldsymbol{j}+z\cdot\boldsymbol{k}\mid x,y,z\in\mathbb{R}\}$$

называется пространством *чисто мнимых* кватернионов. На языке матриц,

$$I=\{\eta\in\subset\mathrm{Mat}_2(\mathbb{C})\mid\eta^*=-\eta\,,\ \mathrm{tr}\,\eta=0\}$$

это пространство бесследных косоэрмитовых матриц, а $\mathbb{R}\cdot\boldsymbol{e}$ состоит из вещественных скалярных матриц.

Упражнение 22.5. Убедитесь, что I и $\boldsymbol{e}$ ортогональны относительно евклидовой структуры на $\mathbb{H}$.

Инволюция эрмитова сопряжения $\eta\leftrightarrow\eta^*$ переводит $\mathbb{H}$ в себя, тождественно действуя на $\boldsymbol{e}$ и меняя знак у мнимых кватернионов. Она называется *кватернионным сопряжением*. Это *антиавтоморфизм* алгебры кватернионов:

$$(pq)^*=q^*p^*\,.$$

22.2.2. Норма. Так как квадрат евклидовой длины кватерниона

$$\eta=x_0+x_1\boldsymbol{i}+x_2\boldsymbol{j}+x_3\boldsymbol{k}$$

равен $||\eta||^2=\sum x_\nu^2=(\eta,\eta)=\det(\eta)$, из мультипликативности определителя вытекает мультипликативность нормы кватернионов относительно кватернионного умножения:

$$||\eta\zeta||=||\eta||\cdot||\zeta||\quad\forall\,\eta,\zeta\in\mathbb{H}\,.$$

Мультипликативность нормы нетрудно усмотреть и без матричной интерпретации — исходя из одного только абстрактного определения алгебры $\mathbb{H}$ при помощи соотношений (22-8), как в упр. 22.4.

В самом деле, из первой строчки формулы (22-9) очевидно, что скалярное произведение выражается через кватернионное умножение как

$$(p,q)=\mathrm{Re}\,(p\cdot q^*)=\mathrm{Re}\,(p^*\cdot q)\,. \tag{22-10}$$

Поскольку $\forall\,q\in\mathbb{H}$ кватернион $q\cdot q^*$ самосопряжён, он чисто вещественен: $q\cdot q^*=\mathrm{Re}\,(q\cdot q^*)$. Следовательно, беря в (22-10) $p=q$, получаем соотношение

$$||q||^2=\sum x_\nu^2=q\cdot q^*\,, \tag{22-11}$$

из которого вытекает $||pq||^2=pq(pq)^*=pqq^*p^*=p||q||^2p^*=||p||^2||q||^2$.

Упражнение 22.6. Выведите из мультипликативности кватернионной нормы *тождество Эйлера*[1]

$$\begin{aligned}(x_0^2+x_1^2+x_2^2+x_3^2)\cdot(y_0^2+y_1^2+y_2^2+y_3^2) &= (x_0y_0-x_1y_1-x_2y_2-x_3y_3)^2\\ &+(x_0y_1+x_1y_0+x_2y_3-x_3y_2)^2\\ &+(x_0y_2+x_2y_0+x_3y_1-x_1y_3)^2\\ &+(x_0y_3+x_3y_0+x_1y_2-x_2y_1)^2\end{aligned} \tag{22-12}$$

22.2.3. Деление. Важным следствием соотношения (22-11) является наличие в $\mathbb{H}$ *деления*: для любого ненулевого $q\in\mathbb{H}$ кватернион $q^{-1}=q^*/||q||^2$ служит для q двусторонним обратным: $q\cdot q^{-1}=q^{-1}\cdot q=1$. Ассоциативное некоммутативное кольцо, в котором каждый ненулевой элемент обратим, называется *телом*[2]. Итак, кватернионы образуют тело.

Лемма 22.1

Мнимая часть произведения двух чисто мнимых кватернионов совпадает с из векторным произведением:

$$\operatorname{Im}(q_1q_2)=q_1\times q_2\quad\forall\, q_1,\, q_2\in I\,, \tag{22-13}$$

т. е. равна нулю, если $q_1=\lambda q_2$ для некоторого $\lambda\in\mathbb{R}$, а в остальных случаях представляет собою вектор длины, равной евклидовой площади параллелограмма, натянутого на q_1 и q_2, направленный перпендикулярно плоскости этого параллелограмма так, чтобы базис $q_1,q_2,q_1\times q_2$ был положительно ориентирован по отношению к базису $\boldsymbol{i}$, $\boldsymbol{j}$, $\boldsymbol{k}$ из (22-7).

Доказательство. Оба отображения $q_1,q_2\mapsto q_1\times q_2$ и $q_1,q_2\mapsto\operatorname{Im}(q_1q_2)$ представляют собою билинейные отображения $I\times I\longrightarrow I$ (т. е. линейны по каждому из аргументов при фиксированном втором[3]). Поэтому равенство (22-13) достаточно проверить для девяти пар базисных векторов $q_1,q_2=\boldsymbol{i},\,\boldsymbol{j},\boldsymbol{k}$, и в этом случае они превращаются в соотношения (22-8). □

Упражнение 22.7. Убедитесь, что соотношения (22-8) на *произвольные* три кватерниона $(\boldsymbol{i},\boldsymbol{j},\boldsymbol{k})$ равносильны тому, что эти кватернионы образуют ортонормальный базис пространства чисто мнимых кватернионов, ориентированный точно также, как базис (22-7).

[1] оно играет важную роль в доказательстве теоремы о представимости натурального числа в виде суммы четырёх квадратов, поскольку редуцирует её к задаче о представимости простых чисел

[2] таким образом поля — это в точности коммутативные тела

[3] из приведённого в лем. 22.1 геометрического определения векторного произведения вытекает, что в координатах относительно любого ортонормального базиса, ориентированного также, как базис (22-7), векторное произведение векторов $q_1=(x_1,x_2,x_3)$ и $q_2=(y_1,y_2,y_3)$ имеет вид

$$q_1\times q_2=\left(\det\begin{pmatrix}x_2&x_3\\y_2&y_3\end{pmatrix}\,,\ -\det\begin{pmatrix}x_1&x_3\\y_1&y_3\end{pmatrix}\,,\ \det\begin{pmatrix}x_1&x_2\\y_1&y_2\end{pmatrix}\right)$$

из которого билинейность векторного произведения очевидна

Следствие 22.1
Кватернионы p и q ортогональны тогда и только тогда, когда кватернион pq^* чисто мним. Ортогональность чисто мнимых кватернионов $p, q \in I$ равносильна равенству $pq = -qp$, и в этом случае $pq = -qp \in I$ ортогонален плоскости, натянутой на p и q.

Доказательство. Первое утверждение вытекает непосредственно из формулы (22-10), а остальные — из лем. 22.1. □

22.3. Универсальное накрытие $S^3 = \mathrm{SU}_2 \twoheadrightarrow \mathrm{SO}_3(\mathbb{R})$. Трёхмерная сфера кватернионов единичной нормы

$$S^3 = \{\eta \in \mathbb{H} \mid ||\eta|| = 1\} \subset \mathbb{R}^4$$

в матричной интерпретации является специальной унитарной группой

$$\mathrm{SU}_2 \subset \mathrm{Mat}_2(\mathbb{C}) .$$

Действительно, для матриц единичного определителя $\eta^\times = \eta^{-1}$, так что условие σ-вещественности $\eta^\times = \eta^*$ превращается для таких матриц в условие унитарности $\eta^{-1} = \eta^*$:

$$S^3 = \{q \in \mathbb{H} \mid q \cdot q^* = 1\} = \{\eta \in \mathrm{Mat}_2(\mathbb{C}) \mid \det \eta = 1 \;\&\; \eta^{-1} = \eta^*\} = \mathrm{SU}_2 .$$

Группа $S^3 = \mathrm{SU}_2$ действует на алгебре кватернионов сопряжениями[1]

$$S^3 \ni \psi \longmapsto F_\psi : \mathbb{H} \xrightarrow{q \mapsto \psi q \psi^{-1}} \mathbb{H} . \tag{22-14}$$

Упражнение 22.8. Проверьте, что $F_{\varphi\psi} = F_\varphi \circ F_\psi$ и что все F_ψ являются автоморфизмами тела кватернионов, т. е. обратимы и переводят произведения в произведения: $F_\psi(pq) = F_\psi(p)F_\psi(q)$.

Поскольку $\det(\psi q \psi^{-1}) = \det q$, оператор F_ψ является евклидовой изометрией пространства $\mathbb{H}$, а так как он сохраняет $\boldsymbol{e}$, ограничение F_ψ на $I = \boldsymbol{e}^\perp$ является ортогональным преобразованием 3-мерного евклидова пространства I чисто мнимых кватернионов. Это преобразование собственное, ибо может быть непрерывно продеформировано по сфере S^3 в тождественное преобразование $F_{\boldsymbol{e}}$.

Таким образом, мы имеем гомоморфизм групп

$$S^3 = \mathrm{SU}_2 \xrightarrow{\psi \mapsto F_\psi|_I} \mathrm{SO}_{\det}(I) \simeq \mathrm{SO}_3(\mathbb{R}) \tag{22-15}$$

Поскольку $F_\psi(\psi) = \psi$ и $F_\psi(\boldsymbol{e}) = \boldsymbol{e}$, оператор F_ψ при $\psi \neq \boldsymbol{e}$ оставляет на месте двумерную плоскость

$$\Pi_\psi = \mathbb{R} \cdot \boldsymbol{e} \oplus \mathbb{R} \cdot \psi .$$

[1]поскольку $\psi^{-1} = \psi^*$ это действие можно было бы описать и как $q \mapsto \psi q \psi^*$ (именно в таком виде оно переносится на общие *алгебры Клиффорда*, обобщающие кватернионную алгебру в старшие размерности $n > 2$)

Поэтому $F_\psi|_I$ является вращением вокруг прямой $\ell_\psi = \Pi_\psi \cap I$. Зафиксируем на этой прямой один из двух (различающихся знаком) чисто мнимых кватернионов $\boldsymbol{l}$ единичной нормы, и отождествим плоскость Π_ψ с полем комплексных чисел $\mathbb{C}$ по правилу

$$\mathbb{C} \ni (x + iy) \longleftrightarrow (x\boldsymbol{e} + y\boldsymbol{l}) \in \Pi_\psi \,. \tag{22-16}$$

В результате такого отождествления кватернион $\psi \in \Pi_\psi \simeq \mathbb{C}$ приобретает *аргумент* $\alpha = \operatorname{Arg}\psi$, определяемый из равенства $\psi = \cos\alpha + \boldsymbol{l}\cdot\sin\alpha$, так что

$$\psi^{-1} = \cos\alpha - \boldsymbol{l}\cdot\sin\alpha \,.$$

Лемма 22.2
Оператор $F_\psi|_I \in \mathrm{SO}_{\det}(I) = \mathrm{SO}_3(\mathbb{R})$ является поворотом вокруг прямой ℓ_ψ на угол $2\operatorname{Arg}(\psi)$, если смотреть вдоль орта $\boldsymbol{l} \in \ell_\psi$.

Доказательство. Дополним орт $\boldsymbol{l}$ до положительно ориентированного базиса $\{\boldsymbol{l},\, \boldsymbol{m},\, \boldsymbol{n}\}$ пространства I. По упр. 22.7 таблица умножения кватернионов $\{\boldsymbol{l},\, \boldsymbol{m},\, \boldsymbol{n}\}$ такая же, как у $\{\boldsymbol{i},\, \boldsymbol{j},\, \boldsymbol{k}\}$ из (22-8). Поэтому

$$\begin{aligned}
\psi\boldsymbol{m}\psi^{-1} &= (\cos\alpha + \boldsymbol{l}\cdot\sin\alpha)\boldsymbol{m}(\cos\alpha - \boldsymbol{l}\cdot\sin\alpha) = \\
&= (\boldsymbol{m}\cos\alpha + \boldsymbol{n}\cdot\sin\alpha)(\cos\alpha - \boldsymbol{l}\cdot\sin\alpha) = \\
&= \boldsymbol{m}(\cos^2\alpha - \sin^2\alpha) + 2\boldsymbol{n}\cos\alpha\sin\alpha = \boldsymbol{m}\cos(2\alpha) + \boldsymbol{n}\sin(2\alpha) \\
\psi\boldsymbol{n}\psi^{-1} &= (\cos\alpha + \boldsymbol{l}\cdot\sin\alpha)\boldsymbol{n}(\cos\alpha - \boldsymbol{l}\cdot\sin\alpha) = \\
&= (\boldsymbol{n}\cos\alpha - \boldsymbol{m}\cdot\sin\alpha)(\cos\alpha - \boldsymbol{l}\cdot\sin\alpha) = \\
&= \boldsymbol{n}(\cos^2\alpha - \sin^2\alpha) - 2\boldsymbol{m}\cos\alpha\sin\alpha = \boldsymbol{n}\cos(2\alpha) - \boldsymbol{m}\sin(2\alpha)
\end{aligned}$$

т. е. действие F_ψ на векторы $(\boldsymbol{m}, \boldsymbol{n})$ задаётся матрицей

$$\begin{pmatrix} \cos(2\alpha) & -\sin(2\alpha) \\ \sin(2\alpha) & \cos(2\alpha) \end{pmatrix} \,.$$

□

Следствие 22.2
Гомоморфизм (22-15) сюрьективен и имеет ядро $\{\pm 1\} \simeq \mathbb{Z}/(2)$. □

22.3.1. Топологический комментарий. С топологической точки зрения, гомоморфизм (22-15)

$$S^3 \xrightarrow{\psi\mapsto F_\psi|_I} \mathrm{SO}_3(\mathbb{R}) \tag{22-17}$$

является двулистным накрытием, склеивающим между собою диаметрально противоположные точки трёхмерной единичной сферы. По определению, результатом такой склейки является трёхмерное вещественное проективное пространство $\mathbb{P}_3 = \mathbb{P}(\mathbb{H})$. Таким образом, накрытие (22-17) можно воспринимать как гомеоморфизм между вещественным проективным пространством $\mathbb{P}(\mathbb{R}^4)$ и группой $\mathrm{SO}_3(\mathbb{R})$ (ср. с упр. 18.1).

Поскольку сфера S^3 *односвязна* (фундаментальная группа $\pi_1(S^3) = 1$) а группа $\mathrm{SO}_3(\mathbb{R})$, линейно связна, накрытие (22-17) является *универсальным накрытием*. В частности,

$$\pi_1(\mathrm{SO}_3) = \pi_1(\mathbb{RP}_3) = \mathbb{Z}/(2)\,.$$

Это равенство означает, что в группе вращений SO_3 имеется нестягиваемая петля, квадрат которой стягиваем.

В этом можно убедиться на опыте: держа на ладони книгу, непрерывным движением руки поворачиваем её на 360^0 так, чтобы книга в течение всей этой манипуляции оставалась горизонтальной. В этот момент изогнутая рука как раз и представляет нестягиваемую петлю в SO_3, красноречивым свидетельством чего является неприятное напряжение локтевого сустава. Если превозмочь неприятное ощущение и продолжить вращение книгу дальше в том же направлении, то после ещё одного полного оборота скрученный локоть полностью распрямится, как на рис. 22◇1[1].

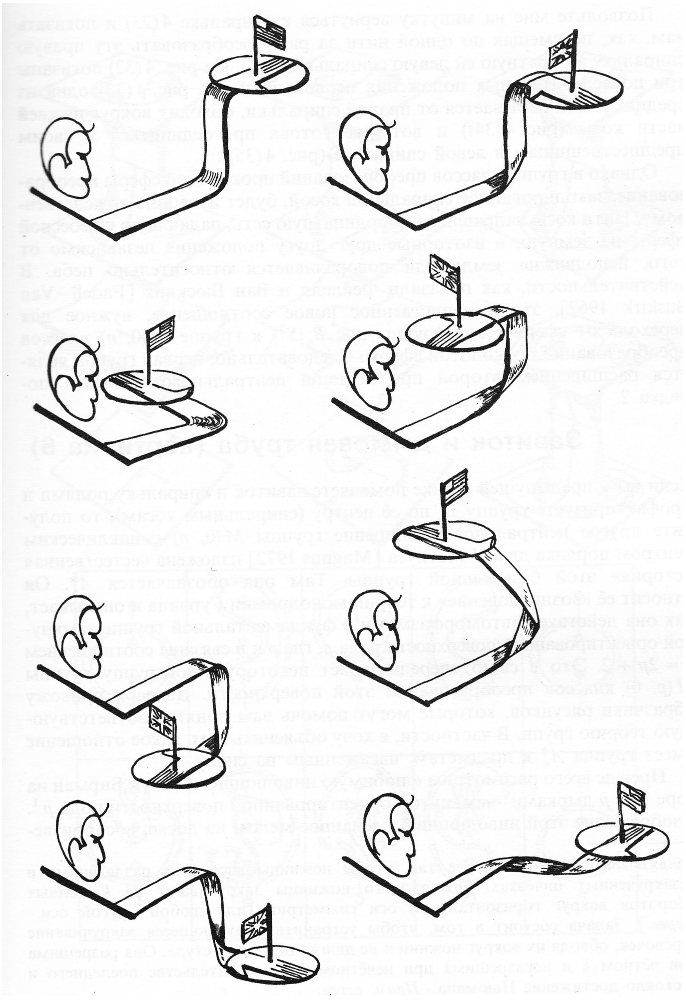


Рис. 22◇1.

Неформально говоря, взятие прообраза относительно (22-17) означает «извлечение корня» из вращения трёхмерного пространства, и два различающихся знаком значения этого корня являются диаметрально противоположными точками трёхмерной сферы.

22.4. Два семейства комплексных структур на $\mathbb{H}$. Поскольку для любого чисто мнимого кватерниона $\boldsymbol{n}$ единичной нормы выполняется равенство

$$\boldsymbol{n}^2 = -\boldsymbol{n}^*\boldsymbol{n} = -(\boldsymbol{n}^*/||\boldsymbol{n}||)\cdot\boldsymbol{n} = -\boldsymbol{n}^{-1}\cdot\boldsymbol{n} = -1\,,$$

[1]рис. 22◇1 позаимствован нами из книги *Франсис Дж. Книжка с картинками по топологии*. М. «Мир» 1991

операторы левого и правого умножения на такой кватернион

$$\begin{aligned} I'_{\boldsymbol{n}} &: \mathbb{H} \xrightarrow{\eta\mapsto \boldsymbol{n}\eta} \mathbb{H} \\ I''_{\boldsymbol{n}} &: \mathbb{H} \xrightarrow{\eta\mapsto \eta\boldsymbol{n}} \mathbb{H} \end{aligned} \tag{22-18}$$

задают на $\mathbb{H} \simeq \mathbb{R}^4$ два семейства комплексных структур, биективно соответствующих точкам единичной сферы

$$S^2 \subset I = \mathbb{R}^3$$

чисто мнимых кватернионов длины 1.

Упражнение 22.9. Докажите, что все кватернионы с квадратом -1 имеют длину 1 и чисто мнимы.

Убедимся, что все эти структуры и в самом деле различны. Операторы (22-18) переводят в себя двумерное вещественное пространство

$$\Pi_{\boldsymbol{n}} = \mathbb{R} \cdot \boldsymbol{e} \oplus \mathbb{R} \cdot \boldsymbol{n}\,,$$

которое, таким образом, является для обеих структур комплексным одномерным подпространством и, более того, может быть канонически отождествлено с полем $\mathbb{C}$ по формуле (22-16):

$$(x + iy) \leftrightarrow (x\boldsymbol{e} + y\boldsymbol{n})\,.$$

С другой стороны, из сл. 22.1 вытекает, что плоскость $\Pi_{\boldsymbol{n}}$ не инвариантна ни для одного из операторов $I'_{\boldsymbol{m}}$, $I''_{\boldsymbol{m}}$ с $\boldsymbol{m} \neq -\boldsymbol{n}$, и значит, не является комплексным подпространством в этих структурах. Таким образом, структуры $I'_{\boldsymbol{n}}$, $I''_{\boldsymbol{n}}$ не совпадают ни с одной из структур $I'_{\boldsymbol{m}}$, $I''_{\boldsymbol{m}}$ при $\boldsymbol{m} \neq \pm\boldsymbol{n}$.

Комплексные структуры $I'_{\boldsymbol{n}}$ и $I'_{-\boldsymbol{n}} = -I'_{\boldsymbol{n}}$, очевидно, различны — они *сопряжены* друг другу в смысле зад. 21.5. Структуры $I''_{\boldsymbol{n}}$ и $I''_{-\boldsymbol{n}} = -I''_{\boldsymbol{n}}$ также сопряжены. По аналогичной причине $I'_{\boldsymbol{n}} \neq I''_{-\boldsymbol{n}}$ — операторы $I'_{\boldsymbol{n}}$ и $I''_{-\boldsymbol{n}}$ задают сопряжённые комплексные структуры на плоскости $\Pi_{\boldsymbol{n}} = \Pi_{-\boldsymbol{n}}$ (их ограничения на эту плоскость отличаются друг от друга знаком).

Наконец, сравним между собою структуры $I'_{\boldsymbol{n}}$ и $I''_{\boldsymbol{n}}$, совпадающие на $\Pi_{\boldsymbol{n}} \simeq \mathbb{C}$. Поскольку обе они переводят в себя ортогонал $\Pi_{\boldsymbol{n}}^{\perp}$, он является в обеих структурах одномерным комплексным подпространством. Зафиксируем какой-нибудь чисто мнимый кватернион единичной нормы $\boldsymbol{m} \in \Pi_{\boldsymbol{n}}^{\perp}$ в качестве базисного вектора этого подпространства. Тогда $\mathbb{H}$ как двумерное векторное пространство над $\mathbb{C}$ разложится в структурах $I'_{\boldsymbol{n}}$ и $I''_{\boldsymbol{n}}$ в прямую сумму двух одномерных комплексных пространств:

$$(\text{в структуре } I'_{\boldsymbol{n}}) \quad \mathbb{C} \oplus \mathbb{C} \cdot \boldsymbol{m} = \mathbb{H} = \mathbb{C} \oplus \boldsymbol{m} \cdot \mathbb{C} \quad (\text{в структуре } I''_{\boldsymbol{n}})\,, \tag{22-19}$$

где умножение базисного орта $\boldsymbol{m}$ на $i \in \mathbb{C}$ задаётся в структурах $I'_{\boldsymbol{n}}$ и $I''_{\boldsymbol{n}}$, соответственно, левым и правым умножением его на $\boldsymbol{n}$. Поскольку по лемме (сл. 22.1) $I'_{\boldsymbol{n}}(\boldsymbol{m}) = \boldsymbol{nm} = -\boldsymbol{mn} = -I''_{\boldsymbol{n}}(\boldsymbol{m})$, комплексные структуры $I'_{\boldsymbol{n}}$ и $I''_{\boldsymbol{n}}$ на пространстве $\Pi^{\perp}_{\boldsymbol{n}}$ будут сопряжены друг другу:

$$\overline{z} \cdot \boldsymbol{m} = \boldsymbol{m} \cdot z \qquad \forall\, z = x + iy = x \cdot \boldsymbol{e} + y \cdot \boldsymbol{n} \in \mathbb{C}\,. \tag{22-20}$$

Итак, $I'_{\boldsymbol{n}} \neq I''_{\boldsymbol{n}}$, и все комплексные структуры (22-18) действительно различны.

Упражнение 22.10. Проверьте, что представление (22-19) аналогично представлению $\mathbb{C} = \mathbb{R} \oplus i\mathbb{R}$ поля $\mathbb{C}$ в виде «удвоенного» поля $\mathbb{R}$ в том смысле, что элементы $\mathbb{H}$ можно было бы *определить* как формальные записи вида $z + w \cdot \boldsymbol{m}$, в которых $z, w \in \mathbb{C}$ суть комплексные числа, формальный символ $\boldsymbol{m}$ имеет $\boldsymbol{m}^2 = -1$ и удовлетворяет соотношениям (22-20), а *кватернионное умножение*

$$(z_1 + w_1 \cdot \boldsymbol{m}) \cdot (z_2 + w_2 \cdot \boldsymbol{m}) \overset{\text{def}}{=} (z_1 z_2 - w_1 \overline{w}_2) + (z_1 w_2 + w_1 \overline{z}_2) \cdot \boldsymbol{m}$$

происходит по обычным правилам раскрытия скобок с учётом всех этих соотношений.

22.5. Спиноры. Согласно предл. 21.3, комплексные структуры на $\mathbb{H}$, продолжающие евклидово скалярное произведение до келеровой тройки, взаимно однозначно соответствуют двумерным изотропным подпространствам $\mathbb{C}$-билинейной формы $\widetilde{\det}$ на $\mathbb{H}_{\mathbb{C}} = \mathrm{Mat}_2(\mathbb{C})$.

Пространство, точки которого параметризуют максимальные изотропные подпространства $U \subset W$ квадратичной формы g, называется *изотропным грассманианом* $\mathrm{Gr}_g(W)$ формы g (см. n° 21.5.2) или — на другом языке — *многообразием спиноров* ортогональной группы $\mathrm{SO}_g(W)$. Геометрически, проективизации максимальных изотропных подпространств образуют семейство проективных подпространств максимальной размерности, лежащих на проективной квадрике $V(g) \subset \mathbb{P}(W)$.

В нашем случае квадрика, задаваемая формой $\det$ в $\mathrm{Mat}_2(\mathbb{C})$, — это *квадрика Сегре* из n° 19.2.1

$$Q = \{\eta \in \mathbb{P}(\mathrm{Mat}_2(\mathbb{C})) \mid \det(\eta) = 0\}\,.. \tag{22-21}$$

Она изоморфна прямому произведению проективных прямых

$$\mathbb{P}_1^- = \mathbb{P}(U^*)\,, \quad \mathbb{P}_1^+ = \mathbb{P}(U)\,, \qquad \text{где} \quad U \simeq \mathbb{C}^2\,, \tag{22-22}$$

посредством отображения Сегре $\mathbb{P}_1^- \times \mathbb{P}_1^+ \xrightarrow{\sim} Q$ сопоставляющего ковектору $\xi = (\zeta_0, \zeta_1) \in U^*$ и вектору $v = (z_0, z_1)^t \in U$ матрицу

$$v \cdot \xi = \begin{pmatrix} z_0 \\ z_1 \end{pmatrix} \cdot (\zeta_0, \zeta_1) = \begin{pmatrix} z_0\zeta_0 & z_0\zeta_1 \\ z_1\zeta_0 & z_1\zeta_1 \end{pmatrix}$$

линейного оператора $v \otimes \xi \in \mathrm{End}(U)$ ранга 1, переводящего $u \in U$ в

$$v \otimes \xi(u) = \xi(u) \cdot v \in U$$

Прямолинейные образующие квадрики Сегре суть образы координатных прямых $\xi \times \mathbb{P}_1^+$ и $\mathbb{P}_1^- \times v$ при этом отображении.

Таким образом, многообразие спиноров в этой ситуации представляет собою дизъюнктное объединение проективной прямой[1] $\mathbb{P}_1^-$, точки ξ которой параметризуют одно семейство[2] прямых на квадрике, и проективной прямой $\mathbb{P}_1^+$, точки v которой параметризуют второе семейство. Отметим, что это хорошо согласуется с описанными выше двумя семействами комплексных структур (22-18), каждое из которых тоже параметризовалось точками двумерной единичной сферой $S^2 \simeq \mathbb{P}_1(\mathbb{C})$.

Остаток этого параграфа будет посвящён написанию различных явных формул, сопоставляющих данному спинору $u \in \mathbb{P}_1^{\pm}$ чисто мнимый кватернион нормы 1 и задаваемую им келерову тройку на $\mathbb{H}$.

22.5.1. Проективная геометрия пространства $\mathbf{Mat_2}(\mathbb{C})$. На бескоординатном языке пространство $\mathrm{Mat}_2(\mathbb{C})$ — это пространство комплексно линейных эндоморфизмов $\mathrm{End}_{\mathbb{C}}(U)$ некоторого двумерного комплексного векторного пространства U. Инволюции $*$ и $\times$ на пространстве $\mathrm{End}_{\mathbb{C}}(U)$ возникают в результате фиксации на U двух дополнительных структур — эрмитова скалярного произведения $h(*,*)$ и $\mathbb{C}$-билинейной кососимметричной *формы площади* $\delta(*,*)$, согласованных друг с другом в том смысле, что абсолютная величина площади любого ортонормального базиса в U равна единице.

Эти две невырожденных формы стандартным образом определяют две биективных корреляции $U \longrightarrow U^*$, действующие по правилам

$$u \longmapsto \widehat{\delta}(u) = \delta(*,u)\ , \qquad u \longmapsto \widehat{h}(u) = h(*,u) \tag{22-23}$$

(первая $\mathbb{C}$-линейна, а вторая $\mathbb{C}$-антилинейна), и две инволюции на $\mathrm{End}_{\mathbb{C}}(U)$, задающие *сопряжение операторов* относительно этих форм:

$$\begin{gathered} F \longleftrightarrow F^{\times} = \widehat{\delta}\ ^{-1} F^t \widehat{\delta} \quad \text{и} \quad F \longleftrightarrow F^* = \widehat{h}\ ^{-1} F^t \widehat{h}\ : \\ \delta(Fu,v) = \delta(u,F^{\times}v)\ , \quad (Fu,v) = (u,F^*v)\ , \end{gathered}$$

где через $U^* \xleftarrow{F^t} U^*$ обозначен оператор, двойственный к $U \xrightarrow{F} U$ в абсолютном смысле, т. е. такой что $F^t\xi(u) = \xi(Fu) \quad \forall\, \xi \in U^* \quad \forall\, u \in U$.

Упражнение 22.11. Проверьте, что в ортонормальном базисе единичной площади[3] действие этих двух инволюций на матрицу оператора описывается формулами (22-1), (22-3), а также что

$$\widehat{\delta}\begin{pmatrix} z_0 \\ z_1 \end{pmatrix} = (z_1, -z_0)\ , \qquad \widehat{h}\begin{pmatrix} z_0 \\ z_1 \end{pmatrix} = (\overline{z}_0, \overline{z}_1)\ .$$

[1] физики обычно называют точки на $\mathbb{P}_1^+ = \mathbb{P}(U)$ «спинорами», а точки на $\mathbb{P}_1^- = \mathbb{P}(U^*)$ «спинорами противоположной киральности»; этимология этих названий отчасти объясняется в §§ 9, 11 второй части книги *А. И. Кострикин, Ю. И. Манин . Линейная алгебра и геометрия.* (М., изд. МГУ, 1980, стр. 176)

[2] а именно, то, что состоит из образов координатных прямых, «параллельных» $\mathbb{P}_1^+$

[3] т. е. таком, где $\delta(e_1, e_2) = 1$

Кроме того, убедитесь, что $\widehat{h}^{-1}\widehat{\delta} = -\widehat{\delta}^{-1}\widehat{h}$ и при каноническом отождествлении U с U^{**} сопряжённые[1] к $\widehat{\delta}$ и $\widehat{h}$ операторы имеют вид $\widehat{\delta}^{\,t} = -\widehat{\delta}$ и $\widehat{h}^{\,t} = \widehat{h}$.

Вещественная структура σ из (22-5) очевидно переводит детерминантную квадрику (22-21) в себя. Поскольку на Q нет вещественных точек[2], а непустое пересечение $\ell \cap \sigma(\ell)$ пары различных лежащих на Q σ-сопряжённых прямых было бы именно такой точкой, мы заключаем, что σ переводит каждую лежащую на Q прямую в прямую из того же семейства, т. е. индуцирует не имеющую неподвижных точек инволюцию $\mathbb{P}_1^{\pm} \xrightarrow{\sigma_{\pm}} \mathbb{P}_1^{\pm}$ на каждой из прямых $\mathbb{P}_1^{\pm}$.

Упражнение 22.12. Проверьте, что $\sigma(F) = \sigma_+^{-1} F \sigma_+$, где $U \xrightarrow{\sigma_+} U$ определяется формулами

$$\sigma_+ = \left(\widehat{h}^{\,-1}\right)^t \delta = \widehat{h}^{\,-1}\widehat{\delta} = -\widehat{\delta}^{\,-1}\widehat{h} = \left(\widehat{\delta}^{\,-1}\right)^t \widehat{h}\,,$$

и что в ортонормальном базисе единичной площади действие σ_+ и $\sigma_- = \sigma_+^t$ описывается формулами

$$\sigma_+ \begin{pmatrix} z_0 \\ z_1 \end{pmatrix} = \begin{pmatrix} \overline{z}_1 \\ -\overline{z}_0 \end{pmatrix} \;, \quad \sigma_-(w_0, w_1) = (-\overline{w}_1, \overline{w}_0)\;.$$

22.5.2. От спиноров к комплексным структурам. Для каждой пары σ_+-сопряжённых спиноров $u, u' \in \mathbb{P}(U)$ прямые $\mathbb{P}_1^- \times u$ и $\mathbb{P}_1^- \times u'$ суть проективизации двумерных пространств L_u, L_u', состоящих из операторов ранга 1, образ которых порождается векторами u и u' соответственно:

$$\begin{aligned} \mathbb{P}_1^- \times u &= \mathbb{P}\left(L_u\right) = \{F \in \operatorname{End}_{\mathbb{C}}(U) \mid \operatorname{im}(F) = \mathbb{C} \cdot u\} \\ \mathbb{P}_1^- \times u' &= \mathbb{P}\left(L_u'\right) = \{F \in \operatorname{End}_{\mathbb{C}}(U) \mid \operatorname{im}(F) = \mathbb{C} \cdot u'\}\;. \end{aligned}$$

Для оператора левого умножения на косоэрмитов оператор $\psi_u \in \operatorname{End}_{\mathbb{C}}(U)$

$$\operatorname{End}_{\mathbb{C}}(U) \xrightarrow{X \mapsto \psi_u X} \operatorname{End}_{\mathbb{C}}(U)\,, \tag{22-24}$$

такой что $\psi_u(u) = iu$ и $\psi_u(u') = -iu'$, подпространства L_u и $L_u' = \sigma(L_u)$ являются собственными с собственными числами $+i$ и $-i$ соответственно. Тем самым, (22-24) задаёт на $\operatorname{End}_{\mathbb{C}}(U) = \operatorname{Mat}_2(\mathbb{C})$ комплексную структуру, соответствующую изотропному подпространству $\mathbb{P}(L_u) \subset Q$.

Матрицу оператора ψ_u в ортонормальном базисе единичной площади легко выписать явно. Если

$$u = \begin{pmatrix} z_0 \\ z_1 \end{pmatrix} \;, \quad u' = \sigma_+(u) = \begin{pmatrix} \overline{z}_1 \\ -\overline{z}_0 \end{pmatrix} \;,$$

[1] отметим, что оператор $U^* \xleftarrow{f^t} V^*$ между комплексными двойственными пространствами, двойственный к *анти*линейному оператору $U \xrightarrow{f} V$ тоже является *анти*линейным

[2] напомню, что ограничение формы det на $\operatorname{Re}_{\sigma} = \mathbb{H}$ положительно определено

то умножая, если надо, представляющий наш спинор вектор $u \in U$ на положительную вещественную константу, мы можем считать, что

$$\det\begin{pmatrix} z_0 & \overline{z}_1 \\ z_1 & -\overline{z}_0 \end{pmatrix} = -||u||_h = -1\ , \quad \text{а значит}\ , \quad \begin{pmatrix} z_0 & \overline{z}_1 \\ z_1 & -\overline{z}_0 \end{pmatrix}^{-1} = \begin{pmatrix} \overline{z}_0 & \overline{z}_1 \\ z_1 & -z_0 \end{pmatrix}\ ,$$

и тогда

$$\begin{aligned} \psi_u = \begin{pmatrix} z_0 & \overline{z}_1 \\ z_1 & -\overline{z}_0 \end{pmatrix} \cdot \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \cdot \begin{pmatrix} z_0 & \overline{z}_1 \\ z_1 & -\overline{z}_0 \end{pmatrix}^{-1} = \\ = \begin{pmatrix} i\,(|z_0|^2 - |z_1|^2) & 2i\,z_0\overline{z}_1 \\ 2i\,\overline{z}_0 z_1 & i\,(|z_1|^2 - |z_0|^2) \end{pmatrix} \end{aligned} \tag{22-25}$$

Таким образом, мы явно сопоставили каждому спинору $u \in \mathbb{P}(U)$ чисто мнимый кватернион с квадратом -1, левое умножение на который задаёт на $\mathbb{H}$ комплексную структуру, отвечающую изотропной прямой $\mathbb{P}_1^- \times u \subset Q$.

Упражнение 22.13. Покажите, что правое умножение на ψ_u задаёт на $\mathbb{H}$ комплексную структуру, отвечающую прямой $\widehat{\delta}(u) \times \mathbb{P}_1^+$ из второго семейства.

Предложение 22.1
Все комплексные структуры на $\mathbb{H}$, продолжающие кватернионную норму до келеровой тройки, исчерпываются левыми и правыми умножениями на чисто мнимые кватернионы нормы 1, а формула (22-25) задаёт взаимно однозначное соответствие между такими кватернионами и спинорами[1] $u \in \mathbb{P}(U)$. □

22.5.3. Расслоение Хопфа. Легко видеть, что правая часть (22-25) не меняется при *изменении фазы* спинора u, т. е. при замене $u \mapsto \vartheta u$ с $|\vartheta| = 1$. Поэтому формула (22-25) задаёт гладкое сюрьективное отображение трёхмерной сферы на двумерную:

$$\{u \in U \simeq \mathbb{C}^2 \mid ||u||_h = 1\} = S^3 \xrightarrow{\psi} S^2 = \{\boldsymbol{n} \in I \simeq \mathbb{R}^3 \mid ||\boldsymbol{n}||_{\mathbb{H}} = 1\}\ ,$$

слоями которого являются непересекающиеся единичные окружности. Это отображение называется *расслоением Хопфа*.

Иначе его можно описать следующим образом. Комплексная проективная прямая $\mathbb{P}_1 = \mathbb{P}(\mathbb{C}^2)$ является фактором множества ненулевых векторов пространства $\mathbb{C}^2$ по действию мультипликативной группы $\mathbb{C}^*$ скалярными гомотетиями. Поскольку $\mathbb{C}^* = \mathbb{R}^*_{>0} \times \mathrm{U}(1)$, эту факторизацию можно осуществить в два приёма: сначала рассмотреть фактор по действию вещественных растяжений, а потом дофакторизовать его по действию умножений на комплексные числа, лежащие на единичной окружности.

Орбиты группы вещественных растяжений $\mathbb{R}^*_{>0}$ биективно соответствуют точкам единичной сферы $S^3 \subset \mathbb{C}^2$, состоящей из векторов эрмитовой длины 1.

[1] напомним, что в (22-25) вектор $u \in U$, представляющий точку из $\mathbb{P}(U)$, предполагается нормированным так, что $||u||_h = 1$ в эрмитовой структуре на U

Эта сфера расслоена на непересекающиеся орбиты группы $\mathrm{U}_1 \simeq S^1$ (каждая такая орбита представляет собою множество векторов единичной длины в данном одномерном комплексном подпространстве $L \subset \mathbb{C}^2$, ср. с n° 20.1.8). Множество этих орбит — это комплексная проективная прямая $\mathbb{P}(\mathbb{C}^2)$, т. е. риманова сфера S^2 (см. рис. 18◇4 на стр. 317). Расслоение Хопфа — это расслоение $S^3 = \mathbb{C}^2/\mathbb{R}^*_{>0}$ над $S^2 = \mathbb{P}(\mathbb{C}^2) = \mathbb{C}^2/\mathbb{C}^*$ со слоями — орбитами группы U_1.

Задачи для самостоятельного решения к §22

Задача 22.1. Укажите в $\mathrm{Mat}_2(\mathbb{C})$ какой-нибудь базис, в котором форма det имеет диагональную матрицу Грама с диагональными элементами $(+1, -1, -1, -1)$.

Задача 22.2. Покажите, что центр тела кватернионов совпадает с пространством чисто вещественных кватернионов[1]: $Z(\mathbb{H}) \overset{\text{def}}{=} \{\zeta \in \mathbb{H} \mid q\zeta = \zeta q \ \ \forall\, q \in \mathbb{H}\} = \mathbb{R} \cdot \boldsymbol{e}$.

Задача 22.3. Покажите, что для любого $q \in \mathbb{H}$ с $q^2 = -1$ множество кватернионов вида $\alpha + q\beta$ с $\alpha, \beta \in \mathbb{R}$ образуют в $\mathbb{H}$ подполе, изоморфное $\mathbb{C}$.

Задача 22.4. Покажите, что любой невещественный кватернион является корнем квадратного уравнения с вещественными коэффициентами и отрицательным дискриминантом.

Задача 22.5 (чисто мнимые кватернионы). Покажите, что

а) $I = \{q \in \mathbb{H} \mid q^* = -q\} = \{q \in \mathbb{H} \mid q^2 \in \mathbb{R}_{\leqslant 0}\}$

б) билинейная форма $(p, q) \overset{\text{def}}{=} (pq^* + qp^*)/2$ является евклидовым скалярным произведением на I

в) множество решений уравнения $q^2 = -1$ в теле $\mathbb{H}$ это единичная сфера в I

г) все ортонормальные базисы в I, ориентированные так же, как $(\boldsymbol{i}, \boldsymbol{j}, \boldsymbol{k})$, имеют одинаковые таблицы умножения

д) I замкнуто относительно коммутаторной скобки $[x, y] \overset{\text{def}}{=} xy - yx$

е) $[x, y]$ ортогонален к x и y, а длина $[x, y]$ равна абсолютной величине площади параллелограмма, натянутого на x и y

Задача 22.6. Покажите, что $\forall\, \alpha \in \mathbb{H}$ отображение сопряжения кватенионом a

$$\varphi_\alpha : \mathbb{H} \xrightarrow{q \mapsto \alpha q \alpha^{-1}} \mathbb{H}$$

является $\mathbb{R}$-линейным автоморфизмом тела $\mathbb{H}$ и собственной евклидовой изометрией пространства I.

Задача 22.7. Явно вычислите вещественную 3×3 матрицу $\varphi_\alpha \in \mathrm{SO}_3(\mathbb{R})$, которой записывается в базисе $\boldsymbol{i}$, $\boldsymbol{j}$, $\boldsymbol{k}$ из (22-7) образ φ_α данной комплексной 2×2 матрицы $a \in \mathrm{SU}_2$ при гомоморфизме $\mathrm{SU}_2 \xrightarrow{a \mapsto \varphi_\alpha|_I} \mathrm{SO}_{\det}(I) \simeq \mathrm{SO}_3(\mathbb{R})$.

[1] в матричной интерпретации — вещественных скалярных матриц

Задача 22.8. Проверьте, что отображение $\mathrm{SL}_2(\mathbb{C}) \times \mathrm{SL}_2(\mathbb{C}) \longrightarrow \mathrm{SO}_{\det}(\mathbb{C})$, переводящее пару матриц $g_1, g_2 \in \mathrm{SL}_2(\mathbb{C})$ в линейное преобразование $A \mapsto g_1 A g_2^{-1}$, является гомоморфизмом групп, найдите его ядро и образ и явно вычислите комплексную ортогональную 4×4-матрицу, которую будет иметь оператор, отвечающий произвольно заданной паре матриц $g_1, g_2 \in \mathrm{SL}_2(\mathbb{C})$, в базисе, который Вы построили в зад. 22.1.

Задача 22.9. Покажите, что следующие наборы кватернионов являются мультипликативными подгруппами в $\mathbb{H}$ а) 8 кватернионов $\pm\boldsymbol{e}$, $\pm\boldsymbol{i}$, $\pm\boldsymbol{j}$, $\pm\boldsymbol{k}$

б) 16 кватернионов $(\pm\boldsymbol{e} \pm \boldsymbol{i} \pm \boldsymbol{j} \pm \boldsymbol{k})/2$

в) 24 кватерниона, получающиеся из $(\pm\boldsymbol{e} \pm \boldsymbol{i})/\sqrt{2}$ перестановками букв $\boldsymbol{e}, \boldsymbol{i}, \boldsymbol{j}, \boldsymbol{k}$

г) 24 кватерниона, получающиеся объединением групп (а) и (б) (ср. с зад. 14.16)

д) 120 кватернионов, получающихся добавлением к группе (г) ещё 96 кватернионов, которые можно изготовить всевозможными чётными перестановками букв $\boldsymbol{e}, \boldsymbol{i}, \boldsymbol{j}, \boldsymbol{k}$ из кватернионов $(\pm\boldsymbol{e} \pm \alpha\boldsymbol{i} \pm \alpha^{-1}\boldsymbol{j})/2$, где $\alpha = (1+\sqrt{5})/2$.

е) Докажите, то группа из (д) изоморфна $\mathrm{SL}_2(\mathbb{F}_5)$ и гомоморфно накрывает группу икосаэдра A_5 (поэтому её называют *бинарной группой икосаэдра*).

Раздел VI
Полилинейная алгебра

§23. Тензорные произведения модулей

23.1. Полилинейные отображения. Рассмотрим произвольные модули

$$V_1, V_2, \ldots, V_n \quad \text{и} \quad W$$

над произвольным коммутативным кольцом K. Отображение φ из декартова произведения множеств V_i в множество W :

$$\varphi : V_1 \times V_2 \times \cdots \times V_n \longrightarrow W \tag{23-1}$$

называется *полилинейным*[1], если оно линейно отдельно по каждому из своих аргументов при произвольным образом зафиксированных остальных:

$$\varphi(\ldots, \lambda v' + \mu v'', \ldots) = \lambda\, \varphi(\ldots, v', \ldots) + \mu\, \varphi(\ldots, v'', \ldots)\,.$$

Так, 1-линейные отображения $V \longrightarrow W$ — это линейные операторы, а 2-линейные отображения $V \times V \longrightarrow K$ — это билинейные формы на модуле V; n-линейные отображения (23-1) непосредственно обобщают эти два примера.

Полилинейные отображения (23-1) можно обычным образом складывать и умножать на числа из K, так что они тоже образуют K-модуль. Он называется *модулем полилинейных отображений* и обозначается $\mathrm{Hom}(V_1, V_2, \ldots, V_n; W)$.

23.1.1. Пример: полилинейные отображения векторных пространств. Если $K = \Bbbk$ — это поле, и $V_1, V_2, \ldots, V_n$ и W — векторные пространства размерностей $d_1, d_2, \ldots, d_n$ и d соответственно, то пространство полилинейных отображений $\mathrm{Hom}(V_1, V_2, \ldots, V_n; W)$ имеет размерность

$$\dim \mathrm{Hom}(V_1, V_2, \ldots, V_n; W) = d_1 \cdot d_2 \cdot \cdots \cdot d_n \cdot d\,.$$

В самом деле, зафиксируем в каждом пространстве V_i некоторый базис

$$e_1^{(i)}, e_2^{(i)}, \ldots, e_{d_i}^{(i)}\,,$$

и базис $e_1, e_2, \ldots, e_d$ в пространстве W. Отображение (23-1) однозначно определяется своими значениями

$$\varphi\big(\, e_{\alpha_1}^{(1)}\,,\, e_{\alpha_2}^{(2)}\,,\, \ldots\,,\, e_{\alpha_n}^{(n)}\,\big) \in W \tag{23-2}$$

[1] или *n-линейным*, когда желательно точно указать количество аргументов

на всевозможных сочетаниях базисных векторов из пространств V_i, поскольку для произвольного набора векторов $v_1, v_2, \dots, v_n$, разложения которых по базисам имеют вид

$$v_i = \sum_{\alpha_i=1}^{d_i} x^{(i)}_{\alpha_i}\, e^{(i)}_{\alpha_i}\,, \tag{23-3}$$

мы в силу полилинейности отображения φ получим

$$\varphi(v_1, v_2, \dots, v_n) = \sum_{\alpha_1,\alpha_2,\dots,\alpha_n} x^{(1)}_{\alpha_1} \cdot x^{(2)}_{\alpha_2} \cdot\ \cdots\ \cdot x^{(n)}_{\alpha_n} \cdot \varphi\big(\, e^{(1)}_{\alpha_1}\,,\, e^{(2)}_{\alpha_2}\,,\, \dots\,,\, e^{(n)}_{\alpha_n}\,\big)\,. \tag{23-4}$$

Раскладывая векторы (23-2) по базису пространства W:

$$\varphi\big(\, e^{(1)}_{\alpha_1}\,,\, e^{(2)}_{\alpha_2}\,,\, \dots\,,\, e^{(n)}_{\alpha_n}\,\big) = \sum_{\nu=1}^{d} a_\nu^{(\alpha_1,\alpha_2,\dots,\alpha_n)} \cdot e^\nu\,,$$

мы можем однозначно закодировать полилинейное отображение φ набором из $d_1 \cdot d_2 \cdot\ \cdots\ \cdot d_n \cdot d$ чисел $a_\nu^{(\alpha_1,\alpha_2,\dots,\alpha_n)} \in \Bbbk$, которые естественно организуются в $(n+1)$-мерную матрицу[1] размера $d_1 \times d_2 \times\ \cdots\ \times d_n \times d$. Формула (23-4) переписывается через эти матричные элементы как

$$\varphi(v_1, v_2, \dots, v_n) = \sum_{\nu,\alpha_1,\dots,\alpha_n} a_\nu^{(\alpha_1,\alpha_2,\dots,\alpha_n)} \cdot x^{(1)}_{\alpha_1} \cdot x^{(2)}_{\alpha_2} \cdot\ \cdots\ \cdot x^{(n)}_{\alpha_n} \cdot e_\nu\,.$$

При сложении полилинейных отображений и умножении их на числа соответствующие этим отображениям матрицы поэлементно складываются и умножаются на числа. Таким образом, пространство полилинейных отображений изоморфно пространству многомерных матриц, и базису пространства матриц, состоящему из матриц с единицей в позиции $(i_1, i_2, \dots, i_n,\, j)$ и нулями в остальных местах отвечает базис пространства полилинейных отображений, состоящий из отображений $\delta^j_{(i_1,i_2,\dots,i_n)}$, действующих на набор векторов (23-3) по правилу

$$\delta^j_{(i_1,i_2,\dots,i_n)} : (v_1, v_2, \dots, v_n) \longmapsto x^{(1)}_{i_1} \cdot x^{(2)}_{i_2} \cdot\ \cdots\ \cdot x^{(n)}_{i_n} \cdot e_j\,, \tag{23-5}$$

а на базисные векторы (23-3) по — правилу

$$\big(\, e^{(1)}_{\alpha_1}\,,\, e^{(2)}_{\alpha_2}\,,\, \dots\,,\, e^{(n)}_{\alpha_n}\,\big) \xmapsto{\ \delta^j_{(i_1,i_2,\dots,i_n)}\ } \begin{cases} e_j\,, & \text{если } \alpha_k = i_k\ \forall\, k \\ 0 & \text{в остальных случаях.} \end{cases} \tag{23-6}$$

Если в предыдущих рассуждениях всюду заменить слова «размерность» и «векторное пространство» словами «ранг» и «свободный модуль», то всё сказанное останется в силе для любых *свободных* модулей конечного ранга над произвольным коммутативным кольцом K.

[1] при $n = 1$ получается обычная 2-мерная матрица (1-) линейного отображения $V \longrightarrow W$ размера $k \times m$, где $k = \dim V$, $m = \dim W$

23.2. Универсальное полилинейное отображение. Рассмотрим какое-нибудь полилинейное отображение модулей

$$V_1 \times V_2 \times \cdots \times V_n \xrightarrow{\tau} U\,. \tag{23-7}$$

Взятие композиции этого отображения со всевозможными линейными операторами $U \xrightarrow{F} W$ в какой-нибудь модуль W задаёт *линейное* отображение модулей

$$\mathrm{Hom}(U, W) \xrightarrow{F \mapsto F \circ \tau} \mathrm{Hom}(V_1, V_2, \ldots, V_n; W) \tag{23-8}$$

из пространства $\mathrm{Hom}(U, W)$ линейных операторов $U \xrightarrow{F} W$ в пространство полилинейных отображений $V_1 \times V_2 \times \cdots \times V_n \xrightarrow{\varphi} W$.

Определение 23.1
Полилинейное отображение (23-7) называется *универсальным*, если *для каждого* модуля W линейный оператор (23-8) является изоморфизмом.

Иначе говоря, полилинейное отображение τ универсально, если для любого модуля W и любого полилинейного отображения $V_1 \times V_2 \times \cdots \times V_n \xrightarrow{\varphi} W$ существует единственный линейный оператор $U \xrightarrow{F} W$ такой, что $\varphi = F \circ \tau$, т. е. пара *полилинейных* сплошных стрелок в диаграмме

$$\begin{tikzcd} & U \arrow[dd, dashed, "F"] \\ V_1 \times V_2 \times \cdots \times V_n \arrow[ur, "\tau"] \arrow[dr, "\varphi"'] & \\ & W \end{tikzcd}$$

всегда замыкается в коммутативный треугольник *единственным* пунктирным *линейным* отображением.

Лемма 23.1
Для любых двух универсальных полилинейных отображений

$$V_1 \times V_2 \times \cdots \times V_n \xrightarrow{\tau_1} U_1 \quad \text{и} \quad V_1 \times V_2 \times \cdots \times V_n \xrightarrow{\tau_2} U_2$$

существует единственный линейный изоморфизм $U_1 \xrightarrow{\iota} U_2$ такой, что $\tau_2 = \iota\tau_1$.

Доказательство. Поскольку и U_1, и U_2 оба универсальны, существуют единственные линейные операторы $U_1 \xrightarrow{F_{21}} U_2$ и $U_2 \xrightarrow{F_{12}} U_1$, которые встраиваются в коммутативные диаграммы

$$\begin{tikzcd}
U_1 \arrow[rr, equal, "\mathrm{Id}_{U_1}"] & & U_1 \arrow[dd, dashed, "F_{21}"] \\
& V_1 \times V_2 \times \cdots \times V_n \arrow[ul, "\tau_1"'] \arrow[ur, "\tau_1"] \arrow[dl, "\tau_2"] \arrow[dr, "\tau_2"'] & \\
U_2 \arrow[uu, dashed, "F_{12}"] \arrow[rr, equal, "\mathrm{Id}_{U_2}"'] & & U_2
\end{tikzcd}$$

$$\begin{tikzcd}
U_1 \arrow[dr, dotted, "F_{21}"] \arrow[dd, equal, "\mathrm{Id}_{U_1}"'] & & & & U_2 \arrow[dl, dotted, "F_{12}"'] \arrow[dd, equal, "\mathrm{Id}_{U_2}"] \\
& U_2 \arrow[dl, dotted, "F_{12}"] & V_1 \times V_2 \times \cdots \times V_n \arrow[l, "\tau_2"'] \arrow[r, "\tau_1"] \arrow[ull, "\tau_1"'] \arrow[dll, "\tau_1"] \arrow[urr, "\tau_2"] \arrow[drr, "\tau_2"'] & U_1 \arrow[dr, dotted, "F_{21}"] & \\
U_1 & & & & U_2
\end{tikzcd}$$

Обе композиции $F_{21}F_{12} = \mathrm{Id}_{U_2}$, $F_{12}F_{21} = \mathrm{Id}_{U_1}$, поскольку представления самих универсальных полилинейных отображений в виде $\tau_1 = \varphi \circ \tau_1$ и $\tau_2 = \psi \circ \tau_2$ в силу единственности таковых представлений возможны только с $\varphi = \mathrm{Id}_{U_1}$, $\psi = \mathrm{Id}_{U_2}$. □

23.3. Тензорное произведение модулей. Универсальное полилинейное отображение обозначается через

$$V_1 \times V_2 \times \cdots \times V_n \xrightarrow{\tau} V_1 \otimes V_2 \otimes \cdots \otimes V_n \tag{23-9}$$

и называется *тензорным произведением векторов*. Значение универсального полилинейного отображения на заданном наборе векторов обозначается через

$$\tau(v_1, v_2, \ldots, v_n) = v_1 \otimes v_2 \otimes \cdots \otimes v_n\,. \tag{23-10}$$

Единственный с точностью до единственного изоморфизма, перестановочного с тензорным произведением векторов, модуль $V_1 \otimes V_2 \otimes \cdots \otimes V_n$ называется *тензорным произведением* модулей $V_1, V_2, \ldots, V_n$. Элементы пространства $V_1 \otimes V_2 \otimes \cdots \otimes V_n$ называются *тензорами*. Тензоры, лежащие в образе универсального полилинейного отображения (23-9) называются *разложимыми*.

Упражнение 23.1. Выведите из универсального свойства тензорного произведения, что разложимые тензоры линейно порождают модуль $V_1 \otimes V_2 \otimes \cdots \otimes V_n$.

Отметим, что наугад взятый тензор обычно неразложим и является линейной комбинацией мономов (23-10), а разложимость означает возможность преобразовать эту линейную комбинацию к одному моному (разложить её на множители). Кроме того, поскольку отображение (23-9) не линейно, а полилинейно, его образ обычно не является подмодулем. Мы ещё обсудим это в n° 23.3.2 и n° 23.4, а сейчас устраним один существенный логический пробел в наших построениях.

Чтобы сделать понятие тензорного произведения содержательным, было бы неплохо показать, что универсальное полилинейное отображение (23-9) *существует* — само по себе определение универсального полилинейного отображения обеспечивает лишь единственность определяемого объекта (при условии что он есть), но не даёт *никаких* гарантий его существования.

Мы построим модуль $V_1 \otimes V_2 \otimes \cdots \otimes V_n$ при помощи образующих и соотношений. А именно, рассмотрим свободный K-модуль $\mathscr{V}$, базисом в котором по определению являются всевозможные слова $[v_1 v_2 \,\ldots\, v_n]$ с произвольными $v_i \in V_i$. В этом большом модуле рассмотрим подмодуль $\mathscr{R} \subset \mathscr{V}$, порождённый всевозможными трёхчленными линейными комбинациями вида

$$\begin{gathered}[v_1 \ldots v_{i-1} (\lambda u + \mu w) v_{i+1} \ldots v_n] - \\ - \lambda\, [v_1 \ldots v_{i-1} u v_{i+1} \ldots v_n] - \mu\, [v_1 \ldots v_{i-1} w v_{i+1} \ldots v_n]\,,\end{gathered} \tag{23-11}$$

где обозначенные многоточиями фрагменты не меняются. Положим, по определению

$$\begin{gathered}V_1 \otimes V_2 \otimes \,\cdots\, \otimes V_n = \mathscr{V}/\mathscr{R} \\ v_1 \otimes v_2 \otimes \,\cdots\, \otimes v_n = [w_1 w_2 \,\ldots\, w_n] \,(\operatorname{mod} \mathscr{R})\,.\end{gathered} \tag{23-12}$$

Иными словами, $V_1 \otimes V_2 \otimes \cdots \otimes V_n$ есть модуль, образованный конечными K-линейными комбинациями формальных тензорных мономов $v_1 \otimes v_2 \otimes \cdots \otimes v_n$ (где $v_i \in V_i$), которые подчиняются соотношениям дистрибутивности: если любой из сомножителей (при фиксированных остальных) записать в виде линейной комбинации векторов, то полученное произведение можно преобразовать по стандартному правилу для раскрытия скобок:

$$\cdots \otimes (\lambda u + \mu w) \otimes \,\cdots\, = \lambda \cdot (\,\cdots \otimes u \otimes \cdots\,) - \mu(\,\cdots \otimes w \otimes \cdots\,)\,. \tag{23-13}$$

Лемма 23.2
Отображение $\tau : V_1 \times V_2 \times \,\cdots\, \times V_n \xrightarrow{(v_1, v_2, \ldots, v_n) \mapsto v_1 v_2 \ldots v_n \,(\operatorname{mod} \mathscr{R})} \mathscr{V}/\mathscr{R}$ является универсальным полилинейным отображением.

Доказательство. Полилинейность отображения τ тавтологически следует из наложенных нами соотношений и выражается в точности формулой (23-13). Проверим его универсальность. Для любого отображения множеств

$$V_1 \times V_2 \times \,\cdots\, \times V_n \xrightarrow{\varphi} W$$

существует единственное линейное отображение $F : \mathscr{V} \longrightarrow W$, переводящее базисный вектор $[v_1 v_2 \,\ldots\, v_n] \in \mathscr{V}$ в $\varphi(v_1, v_2, \ldots, v_n)$. Для того, чтобы это отображение было корректно определено на фактор модуле $\mathscr{V}/\mathscr{R}$, достаточно проверить, что $\mathscr{R} \subset \ker F$. Это следует из полилинейности φ и линейности F: для каждого соотношения (23-11) имеем

$$F\big([\dots(\lambda u+\mu w)\dots]-\lambda\,[\dots u\dots]-\mu\,[\dots w\dots]\big)=$$
$$=F\big([\dots(\lambda u+\mu w)\dots]\big)-\lambda\,F\big([\dots u\dots]\big)-\mu\,F\big([\dots w\dots]\big)=$$
$$=\varphi(\dots,(\lambda u+\mu w),\dots)-\lambda\,\varphi(\dots,u,\dots)-\mu\,\varphi(\dots,w,\dots)=0\,,$$

что и требовалось. □

Лемма 23.3

Если каждый из модулей V_i свободен с базисом $e_1^{(i)},e_2^{(i)},\dots,e_{d_i}^{(i)}$, то модуль $V_1\otimes V_2\otimes\,\cdots\,\otimes V_n$ также свободен с базисом

$$e^{(1)}_{\alpha_1}\otimes e^{(2)}_{\alpha_2}\otimes\,\dots\,\otimes e^{(n)}_{\alpha_n}\,,\quad 1\leqslant\alpha_i\leqslant d_i\,,\tag{23-14}$$

(в частности, $\operatorname{rk}V_1\otimes V_2\otimes\,\cdots\,\otimes V_n=\prod\operatorname{rk}V_i$).

Доказательство. Обозначим через $\mathscr{W}$ свободный модуль, базисом которого, по определению, являются всевозможные выражения (23-14), которые мы временно будем воспринимать просто как формальные символы. Полилинейное отображение $V_1\times V_2\times\,\cdots\,\times V_n\xrightarrow{\tau}\mathscr{W}$, переводящее каждый набор базисных векторов $\big(e^{(1)}_{\alpha_1},\,e^{(2)}_{\alpha_2},\,\dots,\,e^{(n)}_{\alpha_n}\big)\in V_1\times V_2\times\cdots\times V_n$ в соответствующий базисный символ (23-14), является универсальным, поскольку для любого полилинейного отображения

$$V_1\times V_2\times\,\cdots\,\times V_n\xrightarrow{\varphi}W$$

и линейного отображения $\mathscr{W}\xrightarrow{F}W$ равенство $\varphi=F\circ\tau$ однозначно задаёт действие F на каждый базисный вектор:

$$F(\,e^{(1)}_{\alpha_1}\otimes e^{(2)}_{\alpha_2}\otimes\,\dots\,\otimes e^{(n)}_{\alpha_n}\,)=\varphi(e^{(1)}_{\alpha_1},e^{(2)}_{\alpha_2},\,\dots\,,e^{(n)}_{\alpha_n})$$

и тем самым однозначно задаёт F. По лем. 23.1 имеется единственный изоморфизм $\mathscr{W}\xrightarrow{\sim}V_1\otimes V_2\otimes\,\cdots\,\otimes V_n$, переводящий формальные базисные векторы (23-14) пространства $\mathscr{W}$ в соответствующие тензорные произведения базисных векторов, лежащие в $V_1\otimes V_2\otimes\,\cdots\,\otimes V_n$. Тем самым, последние тоже образуют базис. □

23.3.1. Замечание о бесконечномерных пространствах. Последняя лемма сохраняет силу для произведений свободных модулей бесконечного ранга: дословно то же рассуждение показывает, что векторное пространство, состоящее из всевозможных конечных линейных комбинаций базисных мономов (23-14) (которых в бесконечномерном случае будет бесконечно много) обладает требуемым универсальным свойством.

В качестве примера рассмотрим пространства многочленов $V_i=\Bbbk[x_i]$. В этом случае имеется изоморфизм векторных пространств

$$\Bbbk[x_1]\otimes\Bbbk[x_2]\otimes\,\cdots\,\otimes\Bbbk[x_n]\simeq\Bbbk[x_1,x_2,\dots,x_n]\,,$$

сопоставляющий каждому базисному произведению $x_1^{m_1}\otimes x_2^{m_2}\otimes\cdots\otimes x_n^{m_n}$ обычный моном $x_1^{m_1}x_2^{m_2}\,\cdots\,x_n^{m_n}$.

23.3.2. Пример: многообразия Сегре. Пусть $K = \Bbbk$ — поле, и

$$V_1, V_2, \dots, V_n$$

векторные пространства над ним. Из лем. 23.3 вытекает, что пространство $V_1 \otimes V_2 \otimes \cdots \otimes V_n$ линейно порождается разложимыми тензорами. При этом само множество разложимых тензоров, как уже говорилось, векторным пространством как правило не является и образует внутри $V_1 \otimes V_2 \otimes \cdots \otimes V_n$ нелинейное подмногообразие, проективизация которого называется *многообразием Сегре*.

Говоря точнее, многообразие Сегре определяется как образ *отображения Сегре* из прямого произведения проективных пространств $\mathbb{P}_{m_i} = \mathbb{P}(V_i)$ в пространство $\mathbb{P}_m = \mathbb{P}\left(V_1 \otimes V_2 \otimes \cdots \otimes V_n\right)$:

$$s : \mathbb{P}_{m_1} \times \cdots \times \mathbb{P}_{m_n} \longrightarrow \mathbb{P}_m ,$$

которое переводит набор одномерных подпространств, натянутых на ненулевые векторы $v_i \in V_i$, в одномерное подпространство, порождённое разложимым тензором $v_1 \otimes v_2 \otimes \cdots \otimes v_n$.

Упражнение 23.2. Проверьте, что это отображение корректно определено[1] и является вложением.

По построению, многообразие Сегре оно заметается n семействами проективных подпространств размерностей $m_1, m_2, \dots, m_n$. Квадрика Сегре из n° 19.2.1 является простейшим примером такого многообразия.

23.4. Изоморфизм $U^* \otimes V \simeq \mathrm{Hom}(U, V)$ и разложимые операторы. Для любых двух векторных пространств U и W имеется билинейное отображение

$$U^* \times W \longrightarrow \mathrm{Hom}(U, V) ,$$

сопоставляющее паре $(\xi, w) \in U^* \times W$ линейное отображение $U \longrightarrow W$, действующее по правилу

$$U \ni u \longmapsto \xi(u)\, w \in W . \tag{23-15}$$

Это оператор ранга 1, образом которого является 1-мерное подпространство в W, натянутое на вектор w, а ядром — подпространство $\mathrm{Ann}\,(\xi) \subset U$ коразмерности 1.

Упражнение 23.3. Покажите, что всякий оператор $F : U \longrightarrow W$ ранга 1 представляется в виде (23-15) с подходящими $\xi \in U^*$ и $w \in W$.

В силу универсальности тензорного произведения, существует единственное линейное отображение

$$U^* \otimes V \longrightarrow \mathrm{Hom}(U, V) \tag{23-16}$$

[1] т. е. тензор $v_1 \otimes v_2 \otimes \cdots \otimes v_n$ отличен от нуля и заменяется на пропорциональный при замене векторов v_i на пропорциональные

переводящее каждый разложимый тензор $\xi \otimes w$ в оператор (23-15). Если оба пространства U и V конечномерны, то это отображение является изоморфизмом. Чтобы убедиться в этом, зафиксируем в пространствах U и W базисы $u_1, u_2, \dots, u_n$ и $w_1, w_2, \dots, w_m$. Тогда mn разложимых тензоров $u_i^* \otimes w_j$ (где $u_1^*, u_2^*, \dots, u_n^* \in U^*$ составляют двойственный к $u_1, u_2, \dots, u_n$ базис пространства U^*) образуют, согласно лем. 23.2, базис тензорного произведения $U^* \otimes V$, а соответствующие им операторы будут действовать на базисные векторы пространства U по правилу

$$u_i^* \otimes w_j : u_k \longmapsto \begin{cases} w_j & \text{при } k = i \\ 0 & \text{в остальных случаях} \end{cases}$$

Иначе говоря, матрица оператора $u_i^* \otimes w_j$ в выбранных нами базисах — это стандартная базисная матрица с единицей в пересечении j-той строки и i-того столбца и с нулями в остальных местах. Таким образом, стандартный базис тензорного произведения $U^* \otimes V$ переводится в стандартный базис пространства операторов.

На геометрическом языке операторы ранга 1, рассматриваемые с точностью до пропорциональности, составляют многообразие Сегре

$$S \subset \mathbb{P}_{mn-1} = \mathbb{P}(\mathrm{Hom}(U, W))\,.$$

Оно линейно порождает всё пространство $\mathbb{P}(\mathrm{Hom}(U, W))$. Если использовать в качестве однородных координат на $\mathbb{P}(\mathrm{Hom}(V, W))$ матричные элементы (a_{ij}) операторов в каких-нибудь фиксированных базисах, то многообразие Сегре можно задать в этих координатах системой квадратичных уравнений — обращением в нуль всех миноров второго порядка:

$$\det \begin{pmatrix} a_{ij} & a_{ik} \\ a_{\ell j} & a_{\ell k} \end{pmatrix} = a_{ij}a_{\ell k} - a_{ik}a_{\ell j} = 0\,.$$

Отображение Сегре

$$\mathbb{P}_{n-1} \times \mathbb{P}_{m-1} = \mathbb{P}(U^*) \times \mathbb{P}(V) \longrightarrow \mathbb{P}_{mn-1} = \mathbb{P}(\mathrm{Hom}(U, W))\,,$$

переводящее пару точек (ξ, w) в точку $\xi \otimes w$, устанавливает биекцию между произведением проективных пространств и многообразием Сегре. Оно переводит пару точек с однородными координатами $(x_1 : x_2 : \cdots : x_n)$ и $(y_1 : y_2 : \cdots : y_n)$ в точку, однородными координатами которой являются mn всевозможных произведений $x_j y_i$, т. е. матрица $y^t \cdot x$ ранга 1 (произведение столбца y на строку x). Два семейства «координатных плоскостей» $\xi \times \mathbb{P}_{m-1}$ и $\mathbb{P}_{n-1} \times w$ при этом перейдут в два семейства проективных пространств, заметающих многообразие Сегре. При $\dim U = \dim W = 2$ мы получаем в точности обсуждавшуюся в n° 19.2.1 биекцию между $\mathbb{P}_1 \times \mathbb{P}_1$ и детерминантной квадрикой Сегре в $\mathbb{P}_3$.

23.5. Тензорные произведения абелевых групп. Для произвольных модулей V_i над произвольным кольцом K из данного в n° 23.3 описания модуля

$$V_1 \otimes V_2 \otimes \cdots \otimes V_n$$

в терминах образующих и соотношений не очевидно ни его строение, ни даже отличен он от нуля или нет.

Проиллюстрируем это на примере вычисления тензорных произведений конечно порождённых $\mathbb{Z}$-модулей. Обозначим для краткости через $\mathbb{Z}_n$ аддитивную абелеву группу вычетов $\mathbb{Z}/(n)$, рассматриваемую как модуль над кольцом $\mathbb{Z}$. Покажем, что при взаимно простых m и n произведение $\mathbb{Z}_m \otimes \mathbb{Z}_n = 0$, где мы обозначаем через 0 тривиальный модуль, состоящий из одного только нулевого вектора.

В самом деле, при $\text{нод}(m,n) = 1$ класс $[n]_m \in \mathbb{Z}_m$ обратим в кольце $\mathbb{Z}/(m)$, и каждое число $a \in \mathbb{Z}_m$ представляется в виде $a = n \cdot a'$, где $a' = [n]^{-1}a$. С другой стороны, для любого $b \in \mathbb{Z}_n$ произведение $nb = 0$ в $\mathbb{Z}_n$. Поэтому в силу полилинейности тензорного произведения мы для любого разложимого тензора $a \otimes b \in \mathbb{Z}_m \otimes \mathbb{Z}_n$ имеем равенство

$$\begin{aligned} a \otimes b = (n \cdot a') \otimes b = n \cdot (a' \otimes b) = a' \otimes (n \cdot b) = \\ = \alpha' \otimes 0 = \alpha' \otimes (0 \cdot 0) = 0 \cdot (\alpha' \otimes 0) = 0\,, \end{aligned}$$

а поскольку разложимые тензоры линейно порождают тензорное произведение, оно нулевое.

Вычислим теперь тензорное произведение $\mathbb{Z}_{p^n} \otimes \mathbb{Z}_{p^m}$ при $n \leqslant m$. Отображение

$$\mathbb{Z}_{p^n} \times \mathbb{Z}_{p^m} \xrightarrow{\mu} \mathbb{Z}_{p^n}\,,$$

переводящее пару вычетов $([a]_{p^n}, [b]_{p^m})$ в вычет $[ab]_{p^n} = ab \cdot [1]_{p^n}$ билинейно. Покажем, что оно универсально. Для любого билинейного отображения

$$\mathbb{Z}_{p^n} \times \mathbb{Z}_{p^m} \xrightarrow{\varphi} W$$

выполняется равенство $\varphi([a]_{p^n}, [b]_{p^m}) = ab \cdot \varphi\left([1]_{p^n}, [1]_{p^m}\right)$, из которого вытекает, что линейное отображение $F : \mathbb{Z}_{p^n} \longrightarrow W$, такое что $\varphi = F \circ \mu$, обязано переводить образующий элемент $[1]_{p^n} \in \mathbb{Z}_{p^n}$ в $\varphi\left([1]_{p^n}, [1]_{p^m}\right)$. Таким образом, отображение F единственно, если существует. Так как единственным соотношением на элемент $e = [1]_{p^n} \in \mathbb{Z}_{p^n}$ является равенство $p^n \cdot e = 0$, которому элемент $\varphi\left([1]_{p^n}, [1]_{p^m}\right)$ удовлетворяет, поскольку

$$p^n \cdot \varphi\left([1]_{p^n}, [1]_{p^m}\right) = \varphi\left(p^n \cdot [1]_{p^n}, [1]_{p^m}\right) = \varphi\left(0, [1]_{p^m}\right) = 0\,,$$

мы заключаем, что правило $[1]_{p^n} \longmapsto \varphi\left([1]_{p^n}, [1]_{p^m}\right)$ корректно определяет отображение

$$F : \mathbb{Z}_{p^n} \longrightarrow W\,,$$

что и доказывает универсальность. Таким образом,

$$\mathbb{Z}_{p^n} \otimes \mathbb{Z}_{p^m} \simeq \mathbb{Z}_{p^{\min(n,m)}}\,.$$

Упражнение 23.4. Покажите, что $\mathbb{Z} \otimes A \simeq A$ для любой абелевой группы A.

Вычисление тензорных произведений произвольных конечно порождённых абелевых групп сводится к только что рассмотренным случаям при помощи канонических изоморфизмов коммутативности, ассоциативности и дистрибутивности, обсуждаемых ниже.

23.6. Канонические изоморфизмы. Всюду далее речь идёт о произвольных модулях над любым коммутативным кольцом K. Линейные отображения

$$f : V_1 \otimes V_2 \otimes \cdots \otimes V_n \longrightarrow W \tag{23-17}$$

часто бывает удобно задавать указанием значений f на множестве разложимых векторов

$$v_1 \otimes v_2 \otimes \cdots \otimes v_n \longmapsto f(v_1, v_2, \dots, v_n)\,, \tag{23-18}$$

а затем по линейности продолжать это правило на произвольные тензоры. Поскольку разложимые тензоры линейно порождают $V_1 \otimes V_2 \otimes \cdots \otimes V_n$, такое описание однозначно определяет f при условии, что оно корректно: множество разложимых тензоров, как правило, линейно зависимо[1], и все имеющиеся между ними линейные соотношения должны выполняться и между векторами (23-18) в модуле W. Эти соотношения линейно порождаются соотношениями полилинейности (или дистрибутивности) (23-13). Таким образом, мы получаем следующий критерий:

Лемма 23.4
Если векторы $f(v_1, v_2, \dots, v_n)$ в (23-18) полилинейно зависят от векторов v_i (т. е. линейны по каждому v_i при фиксированных остальных), то существует единственное линейное отображение (23-17), действующее на разложимые тензоры по правилу

$$v_1 \otimes v_2 \otimes \cdots \otimes v_n \longmapsto f(v_1, v_2, \dots, v_n)\,.$$

Предложение 23.1
Имеется канонический изоморфизм $U \otimes W \simeq W \otimes U$, переводящий разложимый тензор $u \otimes w$ в $w \otimes u$.

Доказательство. Правило $u \otimes w \longmapsto w \otimes u$ билинейно по u, w и по лем. 23.4 корректно определяет линейное отображение $U \otimes W \longrightarrow W \otimes U$. По тем же причинам существует линейное отображение $W \otimes U \longrightarrow U \otimes W$, переводящее $w \otimes u$ в $u \otimes w$. Эти два отображения обратны друг другу (поскольку обе их композиции тождественно действуют на разложимых тензорах, линейно порождающих тензорное произведение), и значит, являются изоморфизмами. □

[1] например, если K — бесконечное поле, а V_i — конечномерные пространства, пространство $V_1 \otimes V_2 \otimes \cdots \otimes V_n$ тоже конечномерно, а разложимых тензоров в нём бесконечно много

Предложение 23.2
Имеются канонические изоморфизмы $V \otimes (U \otimes W) \simeq V \otimes U \otimes W \simeq (V \otimes U) \otimes W$, переводящие друг в друга разложимые тензоры $v \otimes (u \otimes w)$, $v \otimes u \otimes w$ и $(v \otimes u) \otimes w$.

Доказательство. Тензор $v \otimes (u \otimes w) \in V \otimes (U \otimes W)$ трилинейно зависит от (v, u, w). Следовательно, по лем. 23.4 имеется линейное отображение

$$V \otimes U \otimes W \longrightarrow V \otimes (U \otimes W),$$

переводящее $v \otimes u \otimes w$ в $v \otimes (u \otimes w)$. Обратное отображение строится в два шага. При каждом $v \in V$ тензор $v \otimes u \otimes w$ билинейно зависит от u и w, и значит, по лем. 23.4 мы имеем линейное отображение

$$\tau_v : U \otimes W \xrightarrow{u \otimes w \mapsto v \otimes u \otimes w} V \otimes U \otimes W,$$

которое само по себе линейно зависит от v, т. е. тензор $\tau_v(t) = v \otimes t$ билинеен по $v \in V$ и $t \in U \otimes W$. По лем. 23.4 существует линейное отображение

$$V \otimes (U \otimes W) \longrightarrow V \otimes U \otimes W,$$

переводящее $v \otimes (u \otimes w)$ в $v \otimes u \otimes w$, что и требовалось. Изоморфизм между $V \otimes U \otimes W$ и $(V \otimes U) \otimes W$ устанавливается аналогично. □

Предложение 23.3
Имеются канонические изоморфизмы

$$V \otimes (U \oplus W) \simeq (V \otimes U) \oplus (V \otimes W) \quad \text{и} \quad (U \oplus W) \otimes V \simeq (U \otimes V) \oplus (W \otimes V),$$

действующие на разложимые тензоры по правилам:

$$v \otimes (u \dotplus w) \leftrightarrows (v \otimes u) \dotplus (v \otimes w) \quad \text{и} \quad (u \dotplus w) \otimes v \leftrightarrows (u \otimes v) \dotplus (w \otimes v)$$

где через $a \dotplus b$ для $a \in A$ и $b \in B$ обозначено сложение элементов $(a, 0)$ и $(0, b)$ в прямой сумме модулей $A \oplus B$.

Доказательство. Достаточно построить первый изоморфизм — второй получится из него применением предл. 23.1. Отображение

$$V \otimes (U \oplus W) \xrightarrow{v \otimes (u \dotplus w) \mapsto (v \otimes u) \dotplus (v \otimes w)} (V \otimes U) \oplus (V \otimes W)$$

существует, поскольку $(v \otimes u) \dotplus (v \otimes w)$ билинеен по v и $u \dotplus w$. Обратное отображение снова строится в два шага: сначала убеждаемся в наличии линейных отображений

$$\varphi_1 : V \otimes U \longrightarrow V \otimes (U \oplus W) \quad \text{и} \quad \varphi_2 : V \otimes W \longrightarrow V \otimes (U \oplus W),$$

действующих на разложимые тензоры по правилам

$$v \otimes u \mapsto v \otimes (u \dotplus 0) \quad \text{и} \quad v \otimes w \mapsto v \otimes (0 \dotplus w)\,,$$

затем комбинируем их в отображение

$$\psi : (V \otimes U) \oplus (V \otimes W) \xrightarrow{\;a \dotplus b \mapsto \varphi_1(a) + \varphi_2(b)\;} V \otimes (U \oplus W)\,,$$

очевидно, линейное и обратное к построенному в начале доказательства. □

Задачи для самостоятельного решения к §23

Задача 23.1. Покажите, что набор векторов $v_1, v_2, \dots, v_n$, $v_i \in V_i$, тогда и только тогда содержит нулевой вектор, когда любое полилинейное отображение $V_1 \times V_2 \times \cdots \times V_n \xrightarrow{\varphi} W$ зануляется на этом наборе векторов?

Задача 23.2. В соответствии с изоморфизмом (23-16) запишем операторы

$$U \xrightarrow{A} V \quad \text{и} \quad V \xrightarrow{B} W$$

в виде $A = \sum \alpha_\nu \otimes a_\nu$, $B = \sum \beta_\mu \otimes b_\mu$ с $\alpha_\nu \in U^*$, $a_\nu \in V$, $\beta_\mu \in V^*$, $b_\mu \in W$. Запишите аналогичным образом произведение $BA \in \mathrm{Hom}(U, W) \simeq U^* \otimes W$.

Задача 23.3. Пусть $e_i \in V$ и $x_i \in V^*$ — двойственные базисы. В какой эндоморфизм пространства V переходит при изоморфизме $\mathrm{End} V \simeq V^* \otimes V$ *тензор Казимира*

$$\sum x_i \otimes e_i = x_1 \otimes e_1 + x_2 \otimes e_2 + \cdots + x_n \otimes e_n \in V^* \otimes V$$

Задача 23.4. Рассмотрим корреляцию $\tau : \mathrm{End}(V) \longrightarrow \mathrm{End}(V)^*$, которая переводит вектор $\xi \otimes v \in V^* \otimes V \simeq \mathrm{End}(V)$ в линейную форму $\mathrm{End}(V) \longrightarrow \Bbbk$, значение которой на разложимом операторе $v' \otimes \xi' \in V^* \otimes V \simeq \mathrm{End}(V)$ равно $\xi(v') \cdot \xi'(v)$. Какой билинейной форме на $\mathrm{Hom}(V, V)$ отвечает эта корреляция? Вырождена ли эта форма? Симметрична ли она? Какая квадратичная форма ей соответствует? Напишите формулу, вычисляющую значение этой формы на операторах A и B, используя только буквы A и B и операции над матрицами (не прибегая к выбору базисов и рассмотрению матричных элементов).

Задача 23.5. Постройте для конечномерных пространств U, V, W канонические изоморфизмы а) $U^* \otimes V^* \simeq (U \otimes V)^*$ б) $\mathrm{Hom}(\mathrm{Hom}(U, V), W) \simeq \mathrm{Hom}(V, U \otimes W)$

Задача 23.6. Пусть U, V — конечномерные векторные пространства над произвольным полем. а) Покажите, что пространства

$$\mathrm{Hom}\big(U \otimes \mathrm{Hom}(U, W)\,,\, W\big)\,,\ \mathrm{End}\big(\mathrm{Hom}(U, W)\big)\,,\ \mathrm{Hom}\big(U\,,\, W \otimes \mathrm{Hom}(U, W)^*\big)$$

канонически изоморфны друг другу. б) Выясните, какому эндоморфизму пространства $\mathrm{Hom}(U,W)$ отвечает при этом изоморфизме отображение

$$U \otimes \mathrm{Hom}(U,W) \xrightarrow{c} W\,,$$

действующее на разложимые тензоры по правилу $c(u\otimes\varphi)=\varphi(u)$. в) Верно ли, что оператор $U \xrightarrow{\widetilde{c}} \mathrm{Hom}(U,W)^*\otimes W$, который соответствует оператору c, всегда инъективен?

Задача 23.7. Пусть U, V, W — конечномерные векторные пространства над произвольным полем. Покажите, что пространства

$$\mathrm{End}(U\otimes V\otimes W) \quad \text{и} \quad \mathrm{Hom}\big(\mathrm{Hom}(U,V)\otimes\mathrm{Hom}(V,W)\,,\,\mathrm{Hom}(U,W)\big)$$

канонически изоморфны, и выясните, какому линейному отображению

$$\mathrm{Hom}(U,V)\otimes\mathrm{Hom}(V,W)\longrightarrow\mathrm{Hom}(U,W)$$

отвечает тождественный эндоморфизм пространства $U\otimes V\otimes W$.

Задача 23.8. Для любых модулей над любым коммутативным кольцом с единицей постройте канонические изоморфизмы а) $(M\oplus N)\otimes L=(M\otimes L)\oplus(N\otimes L)$
б) $\mathrm{Hom}(M\oplus N,L)=\mathrm{Hom}(M,L)\oplus\mathrm{Hom}(N,L)$
в) $\mathrm{Hom}(L,M\oplus N)=\mathrm{Hom}(L,M)\oplus\mathrm{Hom}(L,N)$
г) $\mathrm{Hom}(L\otimes M,N)=\mathrm{Hom}(L,\mathrm{Hom}(M\otimes N))$

Задача 23.9. Опишите абелеву группу[1]: а) $\mathbb{Z}/(3)\otimes\mathbb{Z}/(4)$ б) $\mathbb{Z}/(6)\otimes\mathbb{Z}/(4)$
в) $\mathbb{Z}/(m)\otimes\mathbb{Z}/(n)$, где $(m,n)=(1)$ г) $\mathbb{Z}/(p^m)\otimes\mathbb{Z}/(p^n)$, где p — простое.

Задача 23.10. Опишите (аддитивную[2]) абелеву группу: а) $\mathrm{Hom}(\mathbb{Z}/(6),\mathbb{Z}/(5))$
б) $\mathrm{Hom}(\mathbb{Z}/(6),\mathbb{Z}/(10)$ в) $\mathrm{Hom}(\mathbb{Z}/(m),\mathbb{Z}/(n)$, где $(m,n)=(1)$
г) $\mathrm{Hom}(\mathbb{Z}/(p^m),\mathbb{Z}/(p^n)$, где p — простое

Задача 23.11. Опишите мультипликативную[3] абелеву группу:
а) $\mathrm{Aut}\,(\mathbb{Z}/(30))$ б) $\mathrm{Aut}\,(\mathbb{Z}/(2)\oplus\mathbb{Z})$ в) $\mathrm{Aut}\,(\mathbb{Z}/(p^n))$, где p — простое

Задача 23.12. Постройте изоморфизм пространства n-линейных форм

$$V^*\times\cdots\times V^*\longrightarrow\Bbbk$$

а) с пространством $V^{\otimes n}$ б) с пространством, двойственным к $V^{*\otimes n}$.

Задача 23.13. Найдите размерность пространства трилинейных форм

$$\varphi: V\times V\times V\longrightarrow\Bbbk$$

[1]укажите каноническое представление в виде прямой суммы циклических групп $\mathbb{Z}$ и $\mathbb{Z}/(p^m)$

[2]групповая операция здесь — сложение гомоморфизмов

[3]групповая операция здесь — композиция автоморфизмов

удовлетворяющих $\forall\, u, v, w \in V$ условиям: а) $\varphi(u,v,w) = \varphi(v,u,w) = \varphi(u,w,v)$ б) $\varphi(u,v,w) = \varphi(v,u,w)$ в) $\varphi(u,v,v) = \varphi(u,u,v) = 0$ г) $\varphi(u,u,u) = 0$ д) $\varphi(u,v,w) = \varphi(v,u,w) = \varphi(u,w,w)$ е) $\varphi(u,v,w) + \varphi(v,w,u) + \varphi(w,u,v) = 0$ ж) $\varphi(u,v,w) = \varphi(v,w,u)$

Задача 23.14. Зафиксируем ненулевой $\xi \in V^*$. Назовём *внутренним умножением* на ξ оператор $i_\xi : V^{\otimes(n+1)} \longrightarrow V^{\otimes n}$, двойственный оператору левого тензорного умножения $\mu_\xi : V^{*\otimes n} \xrightarrow{\tau \mapsto \xi\otimes\tau} V^{*\otimes(n+1)}$ при каноническом отождествлении $V^{\otimes n}$ с $\left(V^{*\otimes n}\right)^*$ из зад. 23.12. Выясните, эпиморфен ли оператор внутреннего умножения, и явно опишите его действие на заданную n-линейную форму

$$w : V^* \times \cdots \times V^* \longrightarrow \Bbbk\,.$$

§24. Тензорная алгебра векторного пространства

24.1. Свободная ассоциативная алгебра $\mathsf{T}(V)$. Всюду в этом параграфе мы обозначаем через V конечномерное векторное пространство над произвольным полем $\Bbbk$. Тензорное произведение

$$V^{\otimes n} = \underbrace{V \otimes V \otimes \cdots \otimes V}_{n}$$

называется n-той *тензорной степенью* пространства V. Мы также полагаем, по определению,

$$V^{\otimes 0} = \Bbbk \quad \text{и} \quad V^{\otimes 1} = V \,.$$

Все тензорные степени объединяются в (бесконечномерную) прямую сумму

$$\mathsf{T}V \stackrel{\text{def}}{=} \bigoplus_{n \geqslant 0} V^{\otimes n} \,.$$

Согласно предл. 23.2 тензорное умножение векторов задаёт на пространстве $\mathsf{T}V$ структуру ассоциативной некоммутативной градуированной алгебры. Если выбрать в пространстве V какой-нибудь базис $\{e_\nu\}$, то эту алгебру можно воспринимать как алгебру многочленов от *некоммутирующих* переменных e_ν, поскольку всевозможные некоммутативные мономы вида

$$e_{\nu_1} \otimes e_{\nu_2} \otimes \cdots \otimes e_{\nu_m} \tag{24-1}$$

составят, согласно лем. 23.3, базис пространства $\mathsf{T}V$ над $\Bbbk$. Перемножение мономов (24-1) состоит в приписывании их друг к другу через значок $\otimes$. Компонента $V^{\otimes n} \subset \mathsf{T}V$ при такой интерпретации становится пространством всех однородных некоммутативных многочленов степени n.

Алгебра $\mathsf{T}V$ называется *тензорной алгеброй* пространства V, а также *свободной ассоциативной $\Bbbk$-алгеброй*, порожденной пространством V.

Второе название обусловлено универсальным свойством вложения

$$\iota : V \hookrightarrow \mathsf{T}V \tag{24-2}$$

в качестве подпространства $V^{\otimes 1} \subset \mathsf{T}V$, аналогичным универсальному свойству базиса свободного модуля. А именно, для любой ассоциативной $\Bbbk$-алгебры A и любого $\Bbbk$-линейного отображения векторных пространств $V \xrightarrow{f} A$ существует единственный гомоморфизм алгебр $\mathsf{T}V \xrightarrow{\alpha} A$ такой, что $f = \alpha \circ \iota$. Иными словами, гомоморфизмы алгебр $\mathsf{T}V \longrightarrow A$ биективно соответствуют линейным отображениям $V \longrightarrow A$.

Упражнение 24.1. Следуя доказательству лем. 23.1 убедитесь, что алгебра $\mathsf{T}V$ вместе с вложением (24-2) определяются этим свойством однозначно с точностью до единственного изоморфизма алгебр, перестановочного с (24-2), и проверьте, что для описанного выше вложения (24-2) это универсальное свойство действительно выполнено.

24.2. Двойственность и свёртки. Для конечномерного V векторные пространства $V^{\otimes n}$ и $(V^*)^{\otimes n}$ канонически двойственны друг другу:

$$\left(V^{\otimes n}\right)^* \simeq (V^*)^{\otimes n} \tag{24-3}$$

Спаривание между ними называется *полной сверткой* и сопоставляет разложимым тензорам

$$v = v_1 \otimes v_2 \otimes \cdots \otimes v_n \in V^{\otimes n} \quad \text{и} \quad \xi = \xi_1 \otimes \xi_2 \otimes \cdots \otimes \xi_n \in V^{*\otimes n}$$

произведение

$$\langle v, \xi \rangle \overset{\text{def}}{=} \prod_{i=1}^{n} \xi_i(v_i)\,. \tag{24-4}$$

Поскольку правая часть полилинейна по каждому v_i и ξ_i, правило $v \mapsto \langle v, \xi \rangle$ корректно продолжается до линейного функционала $V^{\otimes n} \longrightarrow \Bbbk$, который, в свою очередь, полилинейно зависит от каждого ξ_i, и значит сопоставление разложимому $\xi \in V^{*\otimes n}$ такого функционала корректно продолжается до линейного отображения $V^{*\otimes n} \longrightarrow (V^{\otimes n})^*$, при котором действие разложимых «ковекторных» тензоров на разложимые «векторные» тензоры задаётся правилом (24-4).

Конечномерность существенна для проверки того, что это отображение изоморфизм. Выберем двойственные базисы

$$e_1, e_2, \dots, e_n \subset V\,, \quad x_1, x_2, \dots, x_n \subset V^* \quad : \quad x_i(e_j) = \delta_{ij}$$

и рассмотрим соответствующие базисы в $V^{\otimes n}$ и $(V^*)^{\otimes n}$ из тензорных мономов

$$e_{i_1} \otimes e_{i_2} \otimes \cdots \otimes e_{i_r} \quad \text{и} \quad x_{j_1} \otimes x_{j_2} \otimes \cdots \otimes x_{j_s}\,.$$

Из (24-4) немедленно вытекает, что они двойственны друг другу.

Из универсального свойства тензорного произведения $V^{\otimes n}$ тавтологиччески получается ещё одна двойственность — пространство $(V^{\otimes n})^*$ линейных отображений $V^{\otimes n} \longrightarrow \Bbbk$ канонически изоморфно пространству n-линейных форм $\underbrace{V \times V \times \cdots \times V}_{n} \longrightarrow \Bbbk$:

$$\left(V^{\otimes n}\right)^* \simeq \operatorname{Hom}(V, \dots, V\,;\, \Bbbk)\,. \tag{24-5}$$

Комбинируя изоморфизмы (24-3) и (24-5) получаем канонический изоморфизм

$$(V^*)^{\otimes n} \simeq \operatorname{Hom}(V, \dots, V\,;\, \Bbbk)\,, \tag{24-6}$$

который сопоставляет разложимому тензору $\xi = \xi_1 \otimes \xi_2 \otimes \cdots \otimes \xi_n \in V^{*\otimes n}$ n-линейную форму

$$(v_1, v_2, \dots, v_n) \longmapsto \prod_{i=1}^{n} \xi_i(v_i)$$

на $V \times V \times \cdots \times V$ со значениями в поле $\Bbbk$.

24.2.1. Частичные свертки. Зафиксируем какие-нибудь два инъективных (но не обязательно монотонных) отображения

$$\{1,2,\,\dots\,,p\} \xleftarrow{\ I\ } \{1,2,\,\dots\,,m\} \xhookrightarrow{\ J\ } \{1,2,\,\dots\,,q\}$$

и будем, как обычно, писать i_ν и j_ν вместо $I(\nu)$ и $J(\nu)$. Образы этих отображений суть упорядоченные (но не обязательно монотонные) наборы неповторяющихся индексов $I = (i_1, i_2, \dots, i_m)$, $J = (j_1, j_2, \dots, j_m)$, состоящие из одинакового числа элементов. Линейный оператор

$$c^I_J : V^{*\otimes p} \otimes V^{\otimes q} \longrightarrow V^{*\otimes(p-m)} \otimes V^{\otimes(q-m)}$$

сворачивающий для каждого $\nu = 1,\, 2,\, \dots\,,\, m$ ковектор i_ν-тый сомножитель в $V^{*\otimes p}$ с j_ν-тым сомножителем в $V^{\otimes q}$ и оставляющий все остальные сомножители стоящими в том же порядке, в каком они стояли

$$\xi_1 \otimes \xi_2 \otimes \,\cdots\, \otimes \xi_p \otimes v_1 \otimes v_2 \otimes \,\cdots\, \otimes v_q \longmapsto \prod_{\nu=1}^{m} \xi_{i_\nu}(v_{j_\nu}) \cdot \big(\bigotimes_{i\notin I} \xi_i\big) \otimes \big(\bigotimes_{j\notin J} v_j\big) \tag{24-7}$$

называется *частичной сверткой* по индексам I и J. Подчеркнём, что при разных выборах отображений I и J будут, как правило, получаться *различные* отображения свёртки.

24.2.2. Пример: свертка вектора с полилинейной формой. Если при помощи изоморфизма (24-6) проинтерпретировать n-линейную форму

$$\varphi(v_1, v_2, \dots, v_n)$$

как тензор из $V^{*\otimes n}$ и свернуть его по первому тензорному сомножителю с вектором $v \in V$, мы получим тензор из $V^{*\otimes(n-1)}$, который можно обратно проинтерпретировать как $(n-1)$-линейную форму на V. Полученная форма называется *внутренним произведением* v и φ и обозначается $i_v\varphi$ или $v\llcorner\varphi$.

Упражнение 24.2. Проверьте, что внутреннее умножение на v есть не что иное, как фиксация v в качестве первого аргумента формы φ:

$$i_v\varphi(w_1, w_2, \dots, w_{n-1}) = \varphi(v, w_1, w_2, \dots, w_{n-1})\,.$$

24.3. Линейный носитель тензора. Для заданного тензора $t \in V^{\otimes n}$ обозначим через $\mathrm{Supp}(t) \subset V$ пересечение всех векторных подпространств $U \subset V$, таких что $t \in U^{\otimes n}$. Иначе $\mathrm{Supp}(t)$ можно охарактеризовать как наименьшее по включению подпространство $U \subset V$, такое что $t \in U^{\otimes n}$, или как наименьшее по размерности подпространство с таким свойством.

Правомочность всех этих переформулировок вытекает из того, что если $t \in U^{\otimes n}$ и $t \in W^{\otimes n}$ для некоторых подпространств $U, W \subset V$, то $t \in (U \cap W)^{\otimes n}$.

В самом деле, выбирем в V базис

$$e_1,\, \dots\,,\, e_p,\, u_1,\, \dots\,,\, u_q,\, w_1,\, \dots\,,\, w_r,\, v_1,\, \dots\,,\, v_s\,,$$

такой что e_i образуют базис в $U \cap W$, u_j и w_k дополняют его до базисов в U и W соответственно, а v_m дополняют всё предыдущее до базиса в V, и разложим t по базисным тензорным мономам. Условие $t \in U^{\otimes n} \cap W^{\otimes n}$ означает, что в t входят только мономы, не содержащие никаких иных векторов, кроме e_i, что мы и утверждали.

Определение 24.1
Подпространство $\mathrm{Supp}(t)$, описанное выше, называется *линейным носителем* тензора t, а его размерность $\dim \mathrm{Supp}(t)$ *рангом* тензора t.

24.3.1. Вырожденные тензоры. Тензоры, ранг которых меньше размерности пространства V, на котором они определены, называются *вырожденными*. Условие $\mathrm{Supp}(t) \neq V$ означает, что тензор t эффективно зависит от меньшего числа «координат», чем имеется в V, т. е. существует линейная замена базиса, уничтожающая часть переменных в многочлене t. Например, если $\dim \mathrm{Supp}(t) = 1$, то $t = c \cdot v^{\otimes n}$ для некоторого $c \in \Bbbk$ и $v \in V$, порождающего $\mathrm{Supp}(t)$.

24.3.2. Линейные порождающие носителя. Для нахождения ранга данного тензора t желательно иметь более явное описание $\mathrm{Supp}(t)$ — например, в виде линейной оболочки конкретного конечного набора векторов, эффективно вычислимого по t. Одно из таких описаний можно получить при помощи свёрток.

А именно, для каждого инъективного (не обязательно монотонного) отображения

$$I = (i_1, i_2, \dots, i_{n-1}) : \{1, 2, \dots, (n-1)\} \hookrightarrow \{1, 2, \dots, n\} \tag{24-8}$$

рассмотрим отображение полной свёртки с тензором t, спаривающее ν-й сомножитель $V^{*\otimes(n-1)}$ с j_ν-тым сомножителем t для всех $1 \leqslant \nu \leqslant (n-1)$:

$$\begin{gathered} c_t^I : V^{*\otimes(n-1)} \longrightarrow V \\ \xi \longmapsto c^{(1,2,\dots,(n-1))}_{(j_1,j_2,\dots,j_{n-1})}(\xi \otimes t) \end{gathered} \tag{24-9}$$

в результате чего тензор t превращается в линейную комбинацию векторов, стоявших в том тензорном сомножителе, номер которого не попал в образ отображения I. Очевидно, что эта линейная комбинация лежит в $\mathrm{Supp}(t)$.

Теорема 24.1
Пространство $\mathrm{Supp}(t)$ линейно порождается образами всех отображений свёртки (24-9) со всевозможными выборами сворачиваемых индексов (24-8).

Доказательство. Пусть $\mathrm{Supp}(t) = W$. Чтобы убедиться в том, что образы свёрток (24-9) линейно порождают W, достаточно доказать, что каждая линейная форма $\xi \in V^*$, которая аннулирует все подпространства $\mathrm{im}\left(c_t^I\right)$, аннулирует и подпространство W.

Предположим противное: пусть $\xi \in V^*$ имеет ненулевое ограничение на W, но аннулирует все $c_t^I\left(V^{*\otimes(n-1)}\right)$. Выберем в V^* такой базис $\xi_1, \xi_2, \ldots, \xi_d$, чтобы $\xi_1 = \xi$, а ограничения $\xi_1, \xi_2, \ldots, \xi_k$ на W составляли базис в W^*. Обозначим через $w_1, w_2, \ldots, w_k$ двойственный к нему базис в W и разложим t по этому базису. Значение $\xi\left(c_t^I\left(\xi_{\nu_1} \otimes \xi_{\nu_2} \otimes \cdots \otimes \xi_{\nu_{n-1}}\right)\right)$ равно полной свёртке t с базисным мономом $\xi_1 \otimes \xi_{\nu_1} \otimes \xi_{\nu_2} \otimes \cdots \otimes \xi_{\nu_{n-1}}$ (по индексам, переставленным согласно отображению I), которая, в свою очередь, равна коэффициенту при соответствующем двойственном мономе из разложения t. Выбирая подходящие I, мы можем таким образом получить коэффициент при любом содержащем w_1 мономе из разложения t. Следовательно, все эти коэффициенты нулевые, т. е. t не зависит от w_1 и, тем самым, w_1 не входит в $\mathrm{Supp}(t)$ — противоречие. $\square$

24.4. Соотношения (косо) симметричности. Пусть V и U — произвольные модули над любым коммутативным кольцом K. Полилинейное отображение

$$\underbrace{V \times V \times \cdots \times V}_{n} \xrightarrow{\varphi} U \tag{24-10}$$

называется *симметричным*, если при перестановках аргументов оно не изменяет своего значения, и *кососимметричным*, если оно принимает нулевое значение, когда какие-то два из аргументов совпадают.

Упражнение 24.3. Покажите, что значение кососимметричного полилинейного отображения изменяет знак при перестановке любых двух аргументов, а над полем характеристики $\neq 2$ этого условия также и достаточно для кососимметричности.

Симметричные и кососимметричные полилинейные отображения (24-10) составляют в модуле всех полилинейных отображений $\mathrm{Hom}(V, \ldots, V; U)$ подмодули, которые мы будем обозначать $\mathrm{Sym}^n(V, U)$ и $\mathrm{Skew}^n(V, U)$ соответственно.

Взятие композиции фиксированного (косо) симметричного отображения

$$\underbrace{V \times V \times \cdots \times V}_{n} \xrightarrow{\varphi} U$$

со линейными операторами $F : U \longrightarrow W$ задаёт линейное отображения $F \mapsto F \circ \varphi$ из $\mathrm{Hom}(U, W)$ в $\mathrm{Sym}^n(V, W)$ (соотв. в $\mathrm{Skew}^n(V, W)$). (Косо)симметричное полилинейное отображение φ называется *универсальным*, если для всех модулей W это отображение — изоморфизм.

Универсальное симметричное полилинейное отображение обозначается через

$$\underbrace{V \times V \times \cdots \times V}_{n} \xrightarrow{\sigma} S^n V \tag{24-11}$$

и называется *коммутативным произведением* векторов, а модуль $S^n V$, в который оно действует, называется n-той *симметрической степенью* модуля V.

Произведение $\sigma(v_1, v_2, \dots, v_n)$ обычно обозначается через $v_1 \cdot v_2 \cdot \dots \cdot v_n$ или просто $v_1 v_2 \dots v_n$.

Универсальное кососимметричное полилинейное отображение обозначается через

$$\underbrace{V \times V \times \dots \times V}_{n} \xrightarrow{\alpha} \Lambda^n V \tag{24-12}$$

и называется *внешним произведением* векторов, а модуль $\Lambda^n V$, в который оно действует, называется n-той *внешней степенью* модуля V. Произведение $\alpha(v_1, v_2, \dots, v_n)$ принято обозначать через $v_1 \wedge v_2 \wedge \dots \wedge v_n$.

Упражнение 24.4. Покажите, что $S^n V$ и $\Lambda^n V$ (если они существуют) единственны с точностью до единственного изоморфизма, коммутирующего с универсальным отображением.

Существование универсального (косо)симметричного полилинейного отображения вытекает из существования тензорного произведения: симметрическая и внешняя степени модуля V получаются из тензорной степени наложением дополнительных соотношений (анти)коммутирования. Это можно сделать одновременно для всех n беря факторы свободной ассоциативной алгебры по (двусторонним) идеалам, порождённым соотношениями (анти)коммутирования.

24.4.1. Симметрическая алгебра пространства V. Рассмотрим в тензорной алгебре $\mathsf{T}V$ пространства V двусторонний идеал $\mathscr{I}_{\mathrm{sym}} \subset \mathsf{T}V$, порождённый линейным подпространством в $V \otimes V$, натянутым на всевозможные разности

$$u \otimes w - w \otimes u\,. \tag{24-13}$$

По определению, он состоит из конечных линейных комбинаций всевозможных тензоров, которые можно получить из тензоров (24-13), умножая их слева и справа (или одновременно и слева и справа) на любые элементы тензорной алгебры. Пересечение $\mathscr{I}_{\mathrm{sym}} \cap V^{\otimes n}$ этого идеала с однородной компонентой $V^{\otimes n} \subset \mathsf{T}V$ степени n представляет собою линейную оболочку всевозможных разностей разложимых тензоров вида

$$(\cdots \otimes v \otimes w \otimes \cdots) - (\cdots \otimes w \otimes v \otimes \cdots) \tag{24-14}$$

(обозначенные многоточиями фрагменты не меняются), а весь идеал является прямой сумой таких однородных компонент:

$$\mathscr{I}_{\mathrm{sym}} = \bigoplus_{n \geqslant 0} \left(\mathscr{I}_{\mathrm{sym}} \cap V^{\otimes n}\right)\,.$$

Фактор алгебра $SV \overset{\mathrm{def}}{=} \mathsf{T}V / \mathscr{I}_{\mathrm{sym}}$ называется *симметрической алгеброй* векторного пространства V, а индуцированное в ней умножение называется *симметрическим умножением* и обозначается точкой (которую принято опускать).

Симметрическая алгебра является прямой суммой своих однородных компонент:

$$SV = \bigoplus_{n\geqslant 0} S^nV\ , \quad \text{где} \quad S^nV \overset{\text{def}}{=} V^{\otimes n}/(\mathscr{I}_{\text{sym}} \cap V^{\otimes n})\ .$$

Если зафиксировать базис $e_1, e_2, \dots, e_d \subset V$, то алгебру SV можно отождествить с алгеброй $\Bbbk[e_1, e_2, \dots, e_d]$ обычных коммутативных многочленов от базисных векторов e_i, а подпространство $S^nV \subset \Bbbk[e_1, e_2, \dots, e_d]$ — с пространством однородных полиномов степени n.

Упражнение 24.5. Найдите $\dim S^nV$.

Предложение 24.1
Композиция тензорного умножения с факторизацией по $\mathscr{I}_{\text{sym}}$:

$$\underbrace{V \times V \times \cdots \times V}_{n} \overset{\tau}{\dashrightarrow} V^{\otimes n} \xrightarrow{\pi} S^n(V) \tag{24-15}$$

является универсальной симметрической полилинейной формой.

Доказательство. Любое полилинейное отображение

$$V \times V \times \cdots \times V \xrightarrow{\varphi} W$$

единственным образом разлагается в композицию $\varphi = F{\circ}\tau$, где

$$F : V^{\otimes n} \longrightarrow W$$

линейно. При этом F пропускается через π тогда и только тогда, когда

$$F(\cdots \otimes v \otimes w \otimes \cdots) = F(\cdots \otimes w \otimes v \otimes \cdots)\,,$$

что равносильно тому что $\varphi(\dots, v, w, \dots) = \varphi(\dots, w, v, \dots)$. □

Упражнение 24.6. Убедитесь, что SV является *свободной коммутативной алгеброй*, порождённой модулем V, в том смысле, что для любых коммутативной K-алгебры A и линейного отображения K-модулей $V \xrightarrow{f} A$ существует единственный гомоморфизм K-алгебр $SV \xrightarrow{\alpha} A$ такой, что $f = \alpha{\circ}\iota$, где $\iota : V \hookrightarrow SV$ вкладывает V в SV в качестве многочленов первой степени. Проверьте также, что SV и ι определяются этим универсальным свойством однозначно с точностью до единственного изоморфизма алгебр, перестановочного с ι.

24.4.2. Внешняя алгебра пространства V определяется как фактор алгебра

$$\Lambda V \overset{\text{def}}{=} \mathsf{T}V/\mathscr{I}_{\text{skew}}$$

свободной ассоциативной алгебры $\mathsf{T}V$ по двустороннему идеалу $\mathscr{I}_{\text{skew}} \subset \mathsf{T}V$, порожденному всеми тензорами вида

$$v \otimes v \in V \otimes V\,. \tag{24-16}$$

Упражнение 24.7. Покажите, что подпространство $\mathscr{I}_{\text{skew}} \cap V^{\otimes 2}$ содержит все суммы $v \otimes w + w \otimes v$ (с любыми $v, w \in V$), и если $1+1$ обратимо в K, то и линейно порождается такими суммами.

Как и в симметричном случае, идеал $\mathscr{I}_{\text{skew}}$ является прямой суммой своих однородных компонент

$$\mathscr{I}_{\text{skew}} = \bigoplus_{n \geqslant 0} \left(\mathscr{I}_{\text{skew}} \cap V^{\otimes n}\right)$$

и его компонента n-той степени $\mathscr{I}_{\text{skew}} \cap V^{\otimes n}$ является линейной оболочкой разложимых тензоров вида $(\cdots \otimes v \otimes v \otimes \cdots)$ и по упр. 24.7 содержит все суммы вида

$$(\cdots \otimes v \otimes w \otimes \cdots) + (\cdots \otimes w \otimes v \otimes \cdots)\,. \tag{24-17}$$

Фактор алгебра ΛV называется *внешней* (или *грассмановой*) алгеброй пространства V. Как и симметрическая алгебра, она является прямой суммой подпространств

$$\Lambda^n V = V^{\otimes n}/(\mathscr{I}_{\text{skew}} \cap V^{\otimes n})\,.$$

Упражнение 24.8. Докажите, что композиция тензорного умножения с факторизацией по $\mathscr{I}_{\text{skew}}$

$$\underbrace{V \times V \times \cdots \times V}_{n} \xrightarrow{\tau} V^{\otimes n} \xrightarrow{\pi} \Lambda^n(V) \tag{24-18}$$

является универсальным кососимметричным полилинейным отображением.

Индуцированное умножение в алгебре ΛV называется *внешним* (а также *суперкоммутативным* или *грассмановым*) и обозначается $v_1 \wedge v_2 \wedge \cdots \wedge v_n$. Согласно упр. 24.7 оно меняет знак при перестановке любых двух последовательных сомножителей, и стало быть, при произвольной перестановке сомножителей внешнее произведение умножается на знак перестановки.

Как и в симметрическом случае, фиксация базиса $e_1, e_2, \ldots, e_d \subset V$ отождествляет внешнюю алгебру с алгеброй *грассмановых многочленов* от базисных векторов e_i

$$\Lambda V \xrightarrow{\sim} \Bbbk\left\langle e_1, e_2, \ldots, e_d\right\rangle\ ,$$

которую мы уже рассматривали, когда занимались определителями. По построению, грассмановы переменные e_i *анти*коммутируют $e_i \wedge e_j = -e_j \wedge e_i$, и всякий грассманов моном *линеен* по каждой входящей в него переменной. Таким образом, любой грассманов моном степени n с точностью до знака можно записать в виде $e_{i_1} \wedge e_{i_2} \wedge \cdots \wedge e_{i_n}$ с $1 \leqslant i_1 < i_2 < \cdots < i_n \leqslant d$.

Лемма 24.1
Мономы $e_I = e_{i_1} \wedge e_{i_2} \wedge \cdots \wedge e_{i_n}$, где $I = (i_1, i_2, \dots, i_n)$ пробегает все строго возрастающие n-элементные подмножества в $\{1, 2, \dots, d\}$, образуют базис пространства $\Lambda^n V$ однородных грассмановых мономов степени n. В частности, $\Lambda^n V = 0$ для $n > \dim V$, $\dim \Lambda^n V = \binom{d}{n}$, и $\dim \Bbbk \langle e_1, e_2, \dots, e_d \rangle = 2^d$.

Доказательство. Рассмотрим $\binom{d}{n}$-мерное векторное пространство U, базис которого состоит из символов ξ_I, где $I = (i_1, i_2, \dots, i_n)$ пробегает все возрастающие n-элементные подмножества в $\{1, 2, \dots, d\}$. Определим кососимметрическое полилинейное отображение

$$\underbrace{V \times V \times \cdots \times V}_{n} \xrightarrow{\alpha} U \ : \ (e_{j_1}, e_{j_2}, \dots, e_{j_n}) \longmapsto \operatorname{sgn}(\sigma) \cdot \xi_I \ ,$$

где $I = (j_{\sigma(1)}, j_{\sigma(2)}, \dots, j_{\sigma(n)})$ — это единственная *возрастающая* перестановка индексов

$$(j_1, j_2, \dots, j_n) \, .$$

Проверим, что построенное отображение универсально. Для любого кососимметрического полилинейного отображения

$$\underbrace{V \times V \times \cdots \times V}_{n} \xrightarrow{\varphi} W$$

правило $F(\alpha(e_{j_1}, e_{j_2}, \dots, e_{j_n})) \overset{\text{def}}{=} \varphi(e_{j_1}, e_{j_2}, \dots, e_{j_n})$ корректно определяет единственно возможный линейный оператор $U \xrightarrow{F} W$ такой, что $\varphi = F \circ \alpha$. Поэтому имеется канонический изоморфизм между U и $\Lambda^n V$, переводящий ξ_I в $e_{i_1} \wedge e_{i_2} \wedge \cdots \wedge e_{i_n} = e_I$. □

Задачи для самостоятельного решения к §24

Задача 24.1. Для любых $U, W \subset V$ проверьте, что $S^n U \cap S^n W = S^n(U \cap W)$ в $S^n V$ и $\Lambda^n U \cap \Lambda^n W = \Lambda^n(U \cap W)$ в $\Lambda^n V$.

Задача 24.2. Покажите, что подпространство $\mathscr{I}_{\text{sym}} \cap V \otimes V$ из (24-13), порождающее идеал соотношений коммутирования в $\mathsf{T}V$, и подпространство $\mathscr{I}_{\text{skew}} \cap V^* \otimes V^*$ вида (24-16), порождающее идеал соотношений антикоммутирования в тензорной алгебре $\mathsf{T}V^*$ двойственного к V пространства V^*, являются аннуляторами друг друга при каноническом спаривании между $V \otimes V$ и $V^* \otimes V^*$, задаваемом полной свёрткой.

Задача 24.3. Выберем какой-нибудь базисный вектор η в одномерном пространстве $\Lambda^n V$ (где $n = \dim V$) и зададим между пространствами $\Lambda^k V$ и $\Lambda^m V$, такими что $k+m=n$, спаривание $\langle *,* \rangle : \Lambda^k V \times \Lambda^m V \longrightarrow \Bbbk$ правилом

$$\omega_1 \wedge \omega_2 = \langle \omega_1, \omega_2 \rangle \cdot \eta\,, \quad \text{где } \omega_1 \in \Lambda^k V,\ \omega_2 \in \Lambda^m V\,.$$

а) покажите, что это спаривание невырождено для всех m и k с $k+m=n$
б) выясните, как устроен оператор $v^* : \Lambda^k V \longrightarrow \Lambda^{k-1} V$, двойственный относительно этого спаривания к оператору левого внешнего умножения на заданный вектор $v \in V$: $\Lambda^m V \xrightarrow{\xi \mapsto v \wedge \xi} \Lambda^{m+1} V$.

Задача 24.4. Для любого векторного пространства V над полем $\Bbbk$ характеристики $\mathrm{char}(\Bbbk) \neq 2$ постройте канонический изоморфизм $V \otimes V \simeq S^2 V \oplus \Lambda^2 V$ и покажите, что $V \otimes V \otimes V \not\simeq S^3 V \oplus \Lambda^3 V$.

Задача 24.5 (спинорное разложение). Пусть $\mathrm{char}\,\Bbbk \neq 2$ и $V = \mathrm{Hom}(U_-, U_+)$, где $\dim U_\pm = 2$. Покажите, что $V^{\otimes 2} \simeq S^2 V \oplus \Lambda^2 V$ где

$$S^2 V \simeq \left(S^2 U_-^* \otimes S^2 U_+\right) \oplus \left(\Lambda^2 U_-^* \otimes \Lambda^2 U_+\right)$$
$$\Lambda^2 V \simeq \left(S^2 U_-^* \otimes \Lambda^2 U_+\right) \oplus \left(\Lambda^2 U_-^* \otimes S^2 U_+\right)$$

Задача 24.6. Рассмотрим на пространстве $V = \mathbb{C}^4$ невырожденную квадратичную форму g с поляризацией $\widetilde{g}$ и обозначим через $G \subset \mathbb{P}_3 = \mathbb{P}(V)$ квадрику, задаваемую уравнением $g(x) = 0$. Определим на $\Lambda^2 V$ билинейную форму $\Lambda^2 \widetilde{g}$ так, чтобы её значение на разложимых тензорах вычислялось по формуле

$$\Lambda^2 \widetilde{g}(\, v_1 \wedge v_2\,,\, w_1 \wedge w_2\,) \overset{\text{def}}{=} \det \begin{pmatrix} \widetilde{g}(v_1, w_1) & \widetilde{g}(v_1, w_2) \\ \widetilde{g}(v_2, w_1) & \widetilde{g}(v_2, w_2) \end{pmatrix}\,.$$

а) Покажите, что эта форма симметрична и невырождена, и напишите её матрицу Грама в базисе $e_i \wedge e_j$, где e_i образуют ортонормальный базис в V
б) Напомним, грассманиан $\mathrm{Gr}(2, V)$, точки которого биективно соответствуют прямым в $\mathbb{P}_3 = \mathbb{P}(V)$, можно вложить в $\mathbb{P}_5 = \mathbb{P}(\Lambda^2 V)$ как *квадрику Плюккера* $P = \{\omega \in \Lambda^2 V \mid \omega \wedge \omega = 0\}$. Покажите, что множество всех касательных прямых к квадрике $G \subset \mathbb{P}_3$ изображается на квадрике P точками её пересечения с квадрикой $\Lambda^2 G \subset \mathbb{P}_5 = \mathbb{P}(\Lambda^2 V)$, задаваемой формой $\Lambda^2 \widetilde{g}$.

Задача 24.7. Возьмём в предыдущей задаче в качестве 4-мерного пространства $V = \mathrm{Hom}(U_-, U_+)$ из зад. 24.5 над $\Bbbk = \mathbb{C}$, а в качестве g форму $\det$, задающую в $\mathbb{P}_3 = \mathbb{P}(V)$ квадрику Сегре. Следуя зад. 24.6 (б), мы продолжаем изображать прямые в $\mathbb{P}_3 = \mathbb{P}(V)$ точками квадрики Плюккера $P \simeq \mathrm{Gr}(2, V) \subset \mathbb{P}_5 = \mathbb{P}(\Lambda^2 V)$. Покажите, что два семейства прямых, живущих на квадрике Сегре

$$G \subset \mathbb{P}(V) = \mathbb{P}(\mathrm{Hom}(U_-, U_+))$$

изображаются на P двумя гладкими кониками, которые вырезаются из P двумя дополнительными 2-мерными плоскостями

$$\Lambda_- = \mathbb{P}\left(S^2 U_-^* \otimes \Lambda^2 U_+\right) \quad \text{и} \quad \Lambda_+ = \mathbb{P}\left(\Lambda^2 U_-^* \otimes S^2 U_+\right)\,,$$

канонически вложенными в $\mathbb{P}(\Lambda^2\mathrm{Hom}(U_-,U_+))$ по зад. 24.5 , и обе эти коники являются образами прямых $\mathbb{P}_1^{\pm}=\mathbb{P}(U_{\pm})$ при квадратичных вложениях Веронезе $\mathbb{P}(U_{\pm})\hookrightarrow\mathbb{P}(S^2U_{\pm})=\mathbb{P}(S^2U_{\pm}\otimes\Lambda^2U_{\mp})$, так что возникает коммутативная диаграмма[1]:

$$\begin{tikzcd}
\mathbb{P}(U_+) \arrow[rr, hook, "\text{Веронезе}"] & & \mathbb{P}(S^2U_+)\simeq\Lambda_+ \arrow[d, hook] \\
\mathbb{P}_1^+\times\mathbb{P}_1^- \arrow[u, "\pi_+"] \arrow[d, "\pi_-"'] \arrow[r, "\text{Сегре}", "\sim"'] & G\subset\mathbb{P}\mathrm{Hom}(U_-,U_+) \arrow[r, dashed, "\text{Плюккер}"] & P\subset\mathbb{P}\begin{pmatrix}\Lambda^2U_-^*\otimes S^2U_+\\ \oplus\\ S^2U_-^*\otimes\Lambda^2U_+\end{pmatrix} \\
\mathbb{P}(U_-^*) \arrow[rr, hook, "\text{Веронезе}"'] & & \mathbb{P}(S^2U_-^*)\simeq\Lambda_- \arrow[u, hook]
\end{tikzcd}$$

Задача 24.8 (звёздочка Ходжа). В условиях предыдущих трёх задач, оператор Ходжа $*:\Lambda^2V\xrightarrow{\omega\mapsto\omega^*}\Lambda^2V$, ассоциированный с невырожденной квадратичной формой g на V, определяется соотношением

$$\omega_1\wedge\omega_2^*=\Lambda^2\widetilde{g}(\omega_1,\omega_2)\cdot e_1\wedge e_2\wedge e_3\wedge e_4$$

в котором $\omega_{1,2}\in\Lambda^2$ произвольны, а $e_i\in V$ составляют фиксированный ортонормальный базис формы g. Покажите что это определение корректно (не зависит от выбора базиса), найдите собственные значения и собственные подпространства оператора Ходжа и укажите их место в предыдущей картинке.

Задача 24.9 (тензорное произведение операторов). Пусть имеется набор линейных операторов $f_i:V_i\longrightarrow W_i$ действующих между векторными пространствами $V_1,V_2,\dots,V_n$ и $W_1,W_2,\dots,W_n$

а) Покажите, что существует единственный линейный оператор

$$f_1\otimes f_2\otimes\cdots\otimes f_n:V_1\otimes V_2\otimes\cdots\otimes V_n\longrightarrow W_1\otimes W_2\otimes\cdots\otimes W_n$$

действующий на разложимые тензоры по правилу

$$v_1\otimes v_2\otimes\cdots\otimes v_n\longmapsto f_1(v_1)\otimes f_2(v_2)\otimes\cdots\otimes f_n(v_n)$$

б) Пусть оператор $f:U\longrightarrow U$ имеет матрицу F в базисе $u_1,u_2,\dots,u_n\in U$, а оператор $g:W\longrightarrow W$ имеет матрицу G в базисе $w_1,w_2,\dots,w_m\in W$. Опишите матрицу оператора $F\otimes G:U\otimes W\longrightarrow U\otimes W$ в базисе из векторов $u_\nu\otimes w_\mu$ и её матричные элементы в терминах матриц F и G и их матричных элементов.

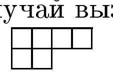
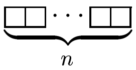
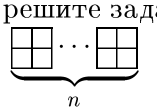
в) Пусть $F:U\hookrightarrow W$ вложение, $U\neq 0$, и $E:V\xrightarrow{\sim}V$ тождественный оператор. Покажите, что $F\otimes E:U\otimes V\longrightarrow W\otimes V$ тоже вложение.

Задача 24.10. Опишите цикловой тип тензорного квадрата

$$N^{\otimes 2}=N\otimes N:V^{\otimes 2}\longrightarrow V^{\otimes 2}$$

[1] отображение Плюккера показано пунктиром, поскольку переводит прямые в точки

нильпотентного оператора $N : V \longrightarrow V$ через цикловой тип N. Если общий случай вызывает затруднения, решите задачу для операторов циклового типа

а)  б)  в) 

Задача 24.11. Пусть операторы F и G диагонализуемы с собственными значениями $\{\lambda_1, \lambda_2, \dots, \lambda_d\}$ и $\{\mu_1, \mu_2, \dots, \mu_d\}$. Найдите все собственные значения $F \otimes G$ и проанализируйте, каковы могут быть их кратности.

Задача 24.12. Пусть оператор $F : V \longrightarrow V$ диагонализуем с собственными значениями $\lambda_1, \lambda_2, \dots, \lambda_n$. Вычислите собственные значения всех тензорных его тензорных степеней $F^{\otimes n}$.

Задача 24.13. Покажите, что ни для какого конечного множества ненулевых линейных операторов $F_1, F_2, \dots, F_m$ на произвольно заданном векторном пространстве V над произвольным полем $\Bbbk$ не существует ненулевого набора констант $\lambda_1, \lambda_2, \dots, \lambda_m \in \Bbbk$, таких что $\lambda_1 F_1^{\otimes n} + \lambda_2 F_2^{\otimes n} + \dots + \lambda_m F_m^{\otimes n} = 0 \quad \forall n \in \mathbb{N}$.

Задача 24.14. Пусть в условиях зад. 24.12 известны все коэффициенты характеристического многочлена оператора F. Выразите через них

а) $\operatorname{tr} F^{\otimes 2}$ б) $\operatorname{tr} F^{\otimes 3}$ в) $\det F^{\otimes 2}$ г) $\det F^{\otimes 3}$

д) след и определитель действия F на пространстве $\operatorname{Hom}(V, V)$ сопряжением: $G \mapsto FGF^{-1}$

е) след и определитель действия F на пространстве квадратичных форм на V по правилу $F\varphi(x) = \varphi\left(F^{-1}x\right)$.

Задача 24.15 (принцип расщепления). Покажите, что ответы, полученные Вами в зад. 24.14, верны *для любых* (в том числе недиагонализуемых) операторов F. Примените такое рассуждение. Все ответы имеют вид полиномиальных соотношений с коэффициентами из поля $\mathbb{Q}$ на матричные элементы f_{ij} оператора F в каком-то базисе и могут восприниматься как равенства в кольце многочленов $\mathbb{Q}[f_{ij}]$ от независимых переменных f_{ij}. Именно эти равенства в $\mathbb{Q}[f_{ij}]$ мы и будем доказывать. Покажите, что

а) если многочлен $f \in \mathbb{Q}[x_1, x_2, \dots, x_n]$ тождественно обращается в нуль как функция на $\mathbb{C}^n$, то это нулевой многочлен (таким образом, достаточно проверить равенства для *всех комплексных* матриц F).

б) диагонализуемые матрицы[1] $F \in \operatorname{Mat}_n(\mathbb{C})$ всюду плотны в $\operatorname{Mat}_n(\mathbb{C})$ (жорданова клетка малым шевелением диагональных элементов сдвигается в диагонализуемую матрицу)

в) в силу непрерывности многочленов, равенства достаточно проверять только для *диагонализуемых* матриц F

г) доказываемые равенства на матрицу F не меняют своего вида при замене F на CAC^{-1} с любым $C \in \operatorname{GL}_n(\mathbb{C})$ (тем самым, их достаточно проверить только для всех *диагональных* матриц, что уже было сделано в зад. 24.14).

[1]для которых существует матрица $C \in \operatorname{GL}_n(\mathbb{C})$, такая что матрица CFC^{-1} диагональна

Задача 24.16. Следуя принципу расщепления, докажите тождество Гамильтона–Кэли $\chi_F(F) = 0$, сведя его к случаю диагональных комплексных F.

Задача 24.17. Убедитесь, что всякий линейный оператор $F : V \longrightarrow V$ корректно индуцирует операторы $S^kF : S^kV \longrightarrow S^kV$ и $\Lambda^kF : \Lambda^kV \longrightarrow \Lambda^kV$, действующие на разложимые тензоры по правилам

$$F(v_1 \cdot v_2 \cdot \cdots \cdot v_k) = F(v_1) \cdot F(v_2) \cdot \cdots \cdot F(v_k)$$
$$F(v_1 \wedge v_2 \wedge \cdots \wedge v_k) = F(v_1) \wedge F(v_2) \wedge \cdots \wedge F(v_k)$$

Для диагонализуемого оператора F выразите все собственные значения всех степеней S^nF и Λ^nF через собственные значения F и покажите, что над произвольным полем $\Bbbk$ характеристики нуль в кольце $\Bbbk[[t]]$ справедливы формулы

а) $\dfrac{1}{\det(E - tF)} = \sum\limits_{k\geqslant 0} \operatorname{tr}\Big(S^kF\Big) \cdot t^k$ б) $\det(E + tF) = \sum\limits_{k=0}^{\dim V} \operatorname{tr}\Big(\Lambda^kF\Big) \cdot t^k$.

Задача 24.18. Докажите, что $e^{F\otimes E + E\otimes F} = e^F \otimes e^F$ в $\operatorname{Mat}_{n^2}(\mathbb{C})$, где F — любая, а E — единичная матрица.

Задача 24.19. Покажите, что в кольце формальных степенных рядов (с рациональными коэффициентами) от матричных элементов $n\times n$ матрицы A выполняется равенство $\ln\det(E-A) = \operatorname{tr}\,\ln(E-A)$, а над полем $\mathbb{C}$ для всех достаточно малых комплексных A оно выполняется также и численно.

§25. Поляризация полиномов

Всюду в этом параграфе речь идёт о векторных пространствах над полем характеристики нуль.

25.1. Симметрические и кососимметрические тензоры. Симметрическая группа S_n действует на $V^{\otimes n}$ перестановками сомножителей в разложимых тензорах. А именно, для каждого $g \in S_n$ положим

$$g(v_1 \otimes v_2 \otimes \cdots \otimes v_n) = v_{g(1)} \otimes v_{g(2)} \otimes \cdots \otimes v_{g(n)} . \tag{25-1}$$

Поскольку правая часть полилинейно зависит от $v_1, v_2, \ldots, v_n$, эта формула по лем. 23.4 корректно определяет линейный оператор $g : V^{\otimes n} \longrightarrow V^{\otimes n}$.

Определение 25.1
Тензор $t \in V^{\otimes n}$ называется *симметрическим*, если $g(t) = t$ для всех перестановок $g \in S^n$. Тензор $t \in V^{\otimes n}$ называется *кососимметрическим*, если $g(t) = \operatorname{sgn}(g) \cdot t$ для всех перестановок $g \in S^n$. Подпространства симметрических и кососимметрических тензоров в $V^{\otimes n}$ обозначаются через

$$\begin{aligned}\operatorname{Sym}^n V &= \{\, t \in V^{\otimes n} \mid \sigma(t) = t \quad \forall\, g \in S_n \,\}\\ \operatorname{Skew}^n V &= \{\, t \in V^{\otimes n} \mid g(t) = \operatorname{sgn}(g) \cdot t \quad \forall\, g \in S_n \,\}\end{aligned}$$

25.1.1. Стандартные базисы. Зафиксируем в пространстве V базис

$$e_1, e_2, \ldots, e_d .$$

Поскольку вместе с каждым тензорным мономом в любой симметрический тензор входит (с одним и тем же коэффициентом) вся S_n-орбита этого монома, *полные симметрические тензоры* $e_{[m_1, m_2, \ldots, m_d]}$, определённые для каждого набора целых неотрицательных чисел $(m_1, m_2, \ldots, m_n)$ с $\sum\limits_{\nu} m_\nu = n$ равенством

$$e_{[m_1,m_2,\ldots,m_d]} = \left(\begin{array}{c} \text{сумма всех различных тензорных мономов,} \\ \text{содержащих } m_1 \text{ множителей } e_1,\ m_2 \text{ множителей } e_2, \ldots \\ \ldots\ m_d \text{ множителей } e_d \end{array} \right) \tag{25-2}$$

образуют базис пространства симметрических тензоров $\operatorname{Sym}^n V$.

Упражнение 25.1. Убедитесь, что сумма в правой части (25-2) состоит из

$$\frac{n!}{m_1!\, m_2! \cdots m_d!}$$

слагаемых.

Аналогичным образом, *полные кососимметрические тензоры*

$$e_{\langle i_1, i_2, \ldots, i_n \rangle} = \sum_{g \in S_n} \operatorname{sgn}(g) \cdot e_{i_{g(1)}} \otimes e_{i_{g(2)}} \otimes \cdots \otimes e_{i_{g(n)}} \tag{25-3}$$

составляют базис в пространстве $\operatorname{Skew}^n V$ (сумма в правой части состоит из $n!$ слагаемых).

25.1.2. Симметризация и альтернирование. Над полем характеристики нуль легко написать явные формулы для проекторов n-той тензорной степени $V^{\otimes n}$ на подпространства симметрических и кососимметрических тензоров. Это операторы *симметризации* и *альтернирования*, действующие по правилам

$$\mathrm{sym}_n(t) = \frac{1}{n!}\sum_{g\in S_n} g(t) \ : \quad V^{\otimes n} \longrightarrow \mathrm{Sym}^{\,n}(V) \tag{25-4}$$

$$\mathrm{alt}_n(t) = \frac{1}{n!}\sum_{g\in S_n} \mathrm{sgn}(g)\cdot g(t) \ : \quad V^{\otimes n} \longrightarrow \mathrm{Skew}^{\,n}(V) \tag{25-5}$$

Упражнение 25.2. Покажите, что для любых тензоров

$$t \in V^{\otimes n}\ , \quad s \in \mathrm{Sym}^{\,n}(V)\ , \quad a \in \mathrm{Skew}^{\,n}(V)$$

выполняются равенства а) $\mathrm{sym}_n(t) \in \mathrm{Sym}^{\,n}(V)$ б) $\mathrm{alt}_n(t) \in \mathrm{Skew}^{\,n}(V)$
в) $\mathrm{sym}_n(s) = s$ г) $\mathrm{alt}_n(a) = a$ д) $\mathrm{sym}_n(a) = \mathrm{alt}_n(s) = 0$

При $n = 2$ симметризация и альтернирование доставляют прямое разложение

$$V^{\otimes 2} = \mathrm{Sym}^{\,2}(V) \oplus \mathrm{Skew}^{\,2}(V)\,. \tag{25-6}$$

В самом деле, поскольку каждый разложимый тензор представляется в виде суммы

$$u\otimes w = \frac{u\otimes w + w\otimes u}{2} + \frac{u\otimes w - w\otimes u}{2} = \mathrm{sym}_2(u\otimes w) + \mathrm{alt}_2(u\otimes w)\,,$$

образы проекторов sym_2 и alt_2 порождают $V^{\otimes 2}$, а т. к. каждый из них по упр. 25.2 аннулирует образ другого, эти образы имеют нулевое пересечение. Если интерпретировать $V^{\otimes 2}$ как пространство билинейных форм на V^*, разложение (25-6) будет ни чем иным, как каноническим разложением билинейной формы в сумму симметрической и кососимметрической.

Сравнение размерностей показывает, что при $n = 3$ уже не любой тензор является суммой своей симметризации и альтернирования. Чтобы найти дополнение к $\mathrm{Sym}^{\,3}(V) \oplus \mathrm{Skew}^{\,3}(V)$ в $V^{\otimes 2}$, рассмотрим разность

$$p = E - \mathrm{sym}_3 - \mathrm{alt}_3 = \left(2\,E - T - T^2\right)/\,3\,, \tag{25-7}$$

где через $V^{\otimes 3} \xrightarrow{T} V^{\otimes 3}$ обозначен оператор, отвечающий циклической перестановке $|123\rangle \in S_3$, а через $E = T^3$ — тождественный оператор. Поскольку

$$p^2 = \left(4E + T^2 + T - 4\,T - 4\,T^2 + 2\,E\right)/\,9 = \left(2E - T - T^2\right)/\,3 = p\,,$$

оператор p также является проектором.

Упражнение 25.3. Покажите, что $p\circ\mathrm{alt}_3 = \mathrm{alt}_3\circ p = p\circ\mathrm{sym}_3 = \mathrm{sym}_3\circ p = 0$ и выведите отсюда, что $V^{\otimes 3}$ является прямой суммой $\mathrm{Sym}^{\,3}(V)$, $\mathrm{Skew}^{\,3}(V)$ и $\mathrm{Im}\,(p)$.

Образ проектора p изящно описывается в терминах трилиненйых форм на V^*.

Упражнение 25.4. Покажите, что $\mathrm{im}\,(p)$ состоит из трилинейных форм

$$V^* \times V^* \times V^* \xrightarrow{\varphi} \Bbbk\,,$$

удовлетворяющих $\forall\, \xi,\eta,\zeta \in V^*$ *тождеству Якоби*

$$\varphi(\xi,\eta,\zeta) + \varphi(\eta,\zeta,\xi) + \varphi(\zeta,\xi,\eta) = 0\,,$$

и приведите явный пример такой формы на двумерном пространстве V^*.

При бóльших n разложение $V^{\otimes n}$ в прямую сумму подпространств тензоров с «различными типами симметрии» становится более сложным. Мы обсудим его во второй части этого курса (в разделе, посвящённом линейным представлениям симметрической группы).

Предложение 25.1
Если $\mathrm{char}(\Bbbk) = 0$, то ограничение симметрического умножения[1]

$$V^{\otimes n} \longrightarrow S^n V$$

на подпространство $\mathrm{Sym}^{\,n} \subset V^{\otimes n}$ и ограничение внешнего умножения[2]

$$V^{\otimes n} \longrightarrow \Lambda^n V$$

на подпространство кососимметрических тензоров $\mathrm{Skew}^{\,n} \subset V^{\otimes n}$ являются изоморфизмами векторных пространств. Действие этих изоморфизмов на стандартные базисные мономы (25-2) и (25-3) задаётся формулами

$$e_{[m_1,m_2,\dots,m_d]} \longmapsto \frac{(m_1+m_2+\dots+m_d)!}{m_1!\cdot m_2!\,\cdots\, m_d!}\cdot e_1^{m_1} e_2^{m_2}\dots e_d^{m_d} \in S^n V \tag{25-8}$$

$$e_{\langle i_1,i_2,\dots,i_n\rangle} \longmapsto n!\cdot e_{i_1}\wedge e_{i_2}\wedge\dots\wedge e_{i_d} \in \Lambda^n V \tag{25-9}$$

Доказательство. Действительно, каждое из $n!/(m_1!m_2!\cdots m_d!)$ слагаемых суммы (25-2) перейдёт при проекции в симметрическую алгебру в коммутативный моном $e_1^{m_1}e_2^{m_2}\dots e_d^{m_d}$, а каждое из $n!$ слагаемых суммы (25-3) перейдёт при проекции во внешнюю алгебру в грассманов моном $n!\, e_{i_1}\wedge e_{i_2}\wedge\,\cdots\,\wedge e_{i_n}$. □

25.1.3. Предостережение. Не смотря на изоморфизмы из предл. 25.1, *подпространства* $\mathrm{Sym}^{\,n}V$ и $\mathrm{Skew}^{\,n}V$, *содержащиеся* в $V^{\otimes n}$, ни в коем случае не следует путать с *фактор* пространствами S^nV и Λ^nV, которые получаются из $V^{\otimes n}$ *склейкой* некоторых тензоров между собою.

Над полем положительной характеристики $\mathrm{char}(\Bbbk) = p$ все симметрические тензоры, степень которых является степенью p, и все кососимметрические тензоры, степень которых больше p, спроектируются при проекциях $V^{\otimes n} \twoheadrightarrow S^nV$ и $V^{\otimes n} \twoheadrightarrow \Lambda^nV$ в *нулевые* элементы симметрической и внешней алгебры.

[1] т.е. отображения факторизации по соотношениям коммутирования (24-14)
[2] т.е. отображения факторизации по соотношениям антикоммутирования (24-17)

Даже в характеристике нуль стандартные базисные векторы тензорных и полиномиальных пространств *не отождествляются* друг с другом изоморфизмами из предл. 25.1, а переходят лишь в некоторые кратности друг друга. Эти поправочные множители приходится учитывать как при попытке поднять на (косо) симметрические тензоры (косо) коммутативное умножение, которое имеется в симметрической и грассмановой алгебрах, так и при попытке спустить в симметрическую и внешнюю алгебры отображения свёртки, которые имеются между тензорами.

25.2. Поляризация коммутативных многочленов. Рассмотрим векторное пространство V с базисом $e_1, e_2, \dots, e_d$ и двойственное пространство V^* с двойственным базисом $x_1, x_2, \dots, x_d$. Выбор базисов устанавливает изоморфизм симметрической алгебры SV^* с алгеброй многочленов от базисных векторов пространства V^*, т. е. с алгеброй многочленов от координат

$$SV^* \simeq \Bbbk[x_1, x_2, \dots, x_d]\,.$$

Пользуясь этим изоморфизмом, каждому элементу $f \in S^nV^*$ можно сопоставить однородную полиномиальную функцию степени n

$$\underline{f} : V \longrightarrow \Bbbk$$

значение которой на векторе $v = \sum \alpha_i e_i \in V$ равно числу

$$\underline{f}(v) = f(\alpha_1, \alpha_2, \dots, \alpha_d) \in \Bbbk\,.$$

Покажем, что над полем характеристики нуль определённый таким образом гомоморфизм $f \mapsto \underline{f}$ из симметрической алгебры S^nV^* в алгебру функций $V \longrightarrow \Bbbk$ не зависит от выбора базиса.

Согласно предл. 25.1, для каждого элемента $f \in S^n(V^*)$ существует единственный симметричный тензор $\widetilde{f} \in \operatorname{Sym}^n V^*$, который проектируется в f при факторизации по соотношениям коммутирования. Этот тензор задаёт симметричную n-линейную форму

$$\widetilde{f} : V \times V \times \dots \times V \longrightarrow \Bbbk$$

значение которой на наборе векторов $(v_1, v_2, \dots, v_n)$ равно полной свёртке $\widetilde{f}$ с $v_1 \otimes v_2 \otimes \dots \otimes v_n$ и определено канонически (без использования базисов). Многочлен $\underline{f}$ есть не что иное как ограничение этой полилинейной формы на главную диагональ $\Delta \subset V_1 \times V_2 \times \dots \times V_n$:

$$\underline{f}(v) = \widetilde{f}(v, v, \dots, v) \qquad \forall\, v \in V\,. \tag{25-10}$$

В самом деле, полная свёртка базисного симметричного тензора $x_{[m_1, m_2, \dots, m_d]}$ с тензором $v^{\otimes n}$ представляет собой сумму $n!/(m_1! \cdot m_2! \cdots m_d!)$ одинаковых произведений $x_1(v)^{m_1}x_2(v)^{m_2}\cdot x_d(v)^{m_d}$ и совпадает со значением на векторе v полиномиальной функции $\underline{f}$, построенной по элементу

$$f = \frac{n!}{m_1!\cdot m_2!\,\cdots\, m_d!}x_1^{m_1}x_2^{m_2}\cdot x_d^{m_d} \in S^nV^*$$

в которую проектируется тензор $x_{[m_1,m_2,\dots,m_d]}$. А так как линейное по f равенство (25-10) выполнено на базисных элементах, оно выполнено и для любых f.

Коль скоро сопоставление $f \mapsto \underline{f}$ не зависит от выбора базиса, мы будем называть элементы симметрической алгебры SV^* *многочленами*[1] или *полиномиальными функциями* на пространстве V, и не будем делать разницы между f и $\underline{f}$ (в частности, обозначение $\underline{f}$ больше нигде не будет использоваться).

Симметричная n-линейная форма $\widetilde{f}(v_1, v_2, \dots, v_n)$, однозначно связанная с многочленом $f \in S^nV^*$ соотношением (25-10) называется *полной поляризацией* многочлена f.

При $n = 2$ полная поляризация есть не что иное как поляризация квадратичной формы до симметричной билинейной формы, многократно использовавшаяся нами ранее. Для произвольной степени n полная поляризация каждого базисного монома $f = x_1^{m_1}x_2^{m_2}\cdots x_d^{m_d}$ степени $\sum m_i = n$, согласно формуле (25-8) из предл. 25.1, имеет вид

$$\widetilde{f} = \frac{m_1!\,m_2!\,\cdots\, m_d!}{n!}\cdot x_{[m_1,m_2,\dots,m_d]}\,. \tag{25-11}$$

Полная поляризация произвольного многочлена вычисляется по этим формулам в силу линейности отображения $f \mapsto \widetilde{f}$.

25.2.1. Пример: двойственность. Полная свёртка между $V^{\otimes m}$ и $V^{*\otimes m}$ индуцирует (в характеристике нуль) двойственность между пространствами многочленов S^mV и S^mV^*. По определению, результатом спаривания элементов $f \in S^nV$ и $g \in S^nV^*$ является полная свёртка их полных поляризаций $\widetilde{f} \in V^{\otimes m}$ и $\widetilde{g} \in V^{*\otimes m}$.

Упражнение 25.5. Проверьте, что мономы, составленные из элементов двойственных базисов пространств V и V^*, спариваются при этом по правилу

$$\langle e_1^{m_1}e_2^{m_2}\,\cdots\, e_d^{m_d}, x_1^{m_1}x_2^{m_2}\,\cdots\, x_d^{m_d}\rangle = \frac{m_1!\cdot m_2!\cdot\,\cdots\,\cdot m_d!}{n!} \tag{25-12}$$

(спаривания между всеми остальными парами базисных векторов нулевые).

25.3. Производные и поляры. Для любого вектора $v \in V$ имеется отображение свёртки

$$c_v^1 : V^{*\otimes n} \longrightarrow V^{*\otimes(n-1)}$$

[1] как мы, собственно, и делали это до сих пор

первого тензорного сомножителя в $V^{*\otimes n}$ с вектором v. На языке n-линейных форм на пространстве V это отображение фиксирует вектор $v \in V$ в качестве первого аргумента n-линейной формы. Применяя его к полной поляризации $\widetilde{f}$ многочлена $f \in S^n(V^*)$ и затем проектируя результат из $V^{*\otimes(n-1)}$ обратно в симметрическую степень $S^{n-1}(V^*)$, мы получаем линейное отображение $S^nV^* \longrightarrow S^{n-1}V^*$, которое включается в качестве нижней горизонтальной стрелки в коммутативную диаграмму

$$\begin{tikzcd} V^{*\otimes n} \supset \mathrm{Sym}^{\,n}V^* \arrow[r, "c_v^1"] \arrow[d] & \mathrm{Sym}^{\,(n-1)}V^* \subset V^{*\otimes(n-1)} \arrow[d] \\ S^nV^* \arrow[r, "\mathrm{pl}_v"] & S^{n-1}V^* \end{tikzcd}$$

и переводит многочлен $f(x) = \widetilde{f}(x, x, \dots x) \in S^n(V^*)$ в многочлен

$$\mathrm{pl}_v f(x) = \widetilde{f}(v, x, \dots x) \in S^{n-1}(V^*)\,, \tag{25-13}$$

который называется *полярой* вектора v относительно f и линейно зависит как от многочлена f, так и от вектора $v \in V$. При $n = 2$ эта конструкция задаёт полярное преобразование относительно квадрики $f = 0$ в $\mathbb{P}(V)$ и сопоставляет вектору v уравнение его полярной гиперплоскости.

В двойственных базисах $e_1, e_2, \dots, e_d \in V$ и $x_1, x_2, \dots, x_d \in V^*$ отображение свёртки по первому индексу с базисным вектором $e_i \in V$ переводит базисный симметрический моном (25-2) в точно такой же базисный моном, но содержащий $(m_i - 1)$ множителей e_i, или в нуль, если $m_i = 0$. Поэтому, по формуле (25-8) из предл. 25.1

$$\mathrm{pl}_{e_i} x_1^{m_1} x_2^{m_2} \,\cdots\, x_d^{m_d} = \frac{m_i}{n}\, x_1^{m_1} \cdots x_{i-1}^{m_{i-1}} x_i^{m_i - 1} x_{i+1}^{m_{i+1}} \cdots x_d^{m_d} = \\ = \frac{1}{n}\,\frac{\partial}{\partial x_i}\, x_1^{m_1} x_2^{m_2} \,\cdots\, x_d^{m_d}\,.$$

Из линейности $\mathrm{pl}_v f$ по v и f мы получаем, что поляра вектора $v = \sum \alpha_i e_i$ относительно многочлена f есть делённая на $\deg f$ *производная* от f в направлении вектора v:

$$\mathrm{pl}_v f = \frac{1}{\deg(f)}\,\partial_v f = \frac{1}{\deg(f)} \sum \alpha_i \,\frac{\partial f}{\partial x_i}\,.$$

Отметим, что из сказанного немедленно вытекает независимость правой части этой формулы от выбора двойственных координат в V и V^*, а также коммутирование частных производных между собой: $\partial_u \partial_w = \partial_w \partial_u$ и замечательное равенство между кратными производными

$$m!\,\frac{\partial^m f}{\partial u^m}(w) = n!\,\widetilde{f}(\underbrace{u, u, \dots, u}_{m}, \underbrace{w, w, \dots, w}_{n}) = (n-m)!\,\frac{\partial^{n-m} f}{\partial w^{n-m}}(u)\,, \tag{25-14}$$

для любых $u, w \in V$, любого $f \in S^n V^*$ и любого m в пределах $0 \leqslant m \leqslant n$.

Упражнение 25.6. Докажите правило Лейбница: $\partial_v(f \cdot g) = \partial_v(f) \cdot g + f \cdot \partial_v(g)$.

Поскольку форма $\widetilde{f}$ симметрична, аргументы в среднем члене формулы (25-14) можно писать в любом порядке. Условимся для упрощения обозначений писать

$$\widetilde{f}(u^m, w^{n-m}),$$

когда какие-то m аргументов формы $\widetilde{f}$ равны u, а остальные $(n-m)$ равны w (не важно в каком порядке).

Из полилинейности и симметричности $\widetilde{f}$ дословно тем же рассуждением, что и формула Ньютона для раскрытия скобок в биноме $(u+w)^n$, выводится равенство

$$\widetilde{f}(u+w,\, u+w,\, \dots,\, u+w) = \sum_{m=0}^{n} \binom{n}{m} \widetilde{f}(u^m, w^{n-m}),$$

где $n = \deg f$. С учётом (25-14) его можно переписать как *разложение Тейлора*: для любого многочлена f и векторов u, w имеется *точное* равенство

$$f(u+w) = \sum_{m=0}^{\deg f} \frac{1}{m!}\, \partial_w^m f(u), \tag{25-15}$$

правая часть которого симметрична по u и w в силу соотношения (25-14).

Упражнение 25.7. Покажите, что значение полной поляризации многочлена $f \in S^n V^*$ на заданном наборе векторов описывается в терминах частных производных формулой $\widetilde{f}(v_1, v_2, \dots, v_n) = \dfrac{1}{n!}\, \partial_{v_1}\partial_{v_2} \,\dots\, \partial_{v_n} f \qquad \forall v_1, v_2, \dots, v_n \in V$.

25.3.1. Пример: линейный носитель многочлена $f \in S^n V^*$ определятся как минимальное подпространство $W \subset V^*$ такое, что $f \in S^n W^*$, и обозначается $\mathrm{Supp}(f)$. Очевидно, что это подпространство совпадает с линейным носителем полной поляризации $\widetilde{f} \in \mathrm{Sym}^n V^*$ многочлена f. Таким образом, по теор. 24.1 $\mathrm{Supp}(f)$ является образом отображения $V^{\otimes(n-1)} \longrightarrow V^*$ задаваемого полной свёрткой[1] с $\widetilde{f}$. Этот образ порождается всеми линейными формами, которые можно получить из f всевозможными $(n-1)$-кратными дифференцированиями вида

$$\frac{\partial^{m_1}}{\partial x_1^{m_1}} \frac{\partial^{m_2}}{\partial x_2^{m_2}} \cdots \frac{\partial^{m_d}}{\partial x_d^{m_d}}\, f(x), \tag{25-16}$$

с $\sum m_\nu = n-1$. Вклад в коэффициент при x_i у линейной формы (25-16) даёт ровно один коэффициент многочлена f — тот, что стоит при мономе $x_1^{m_1} \dots x_{i-1}^{m_{i-1}} x_i^{m_i+1} x_{i+1}^{m_{i+1}} \dots x_d^{m_d}$. Поэтому, если записать многочлен f в виде

$$f = \sum_{\nu_1+\dots+\nu_d=n} \frac{n!}{\nu_1!\nu_2! \,\cdots\, \nu_d!}\, a_{\nu_1\nu_2\dots\nu_d}\, x_1^{\nu_1} x_2^{\nu_2} \,\cdots\, x_d^{\nu_d}, \tag{25-17}$$

[1] из-за симметричности тензора $\widetilde{f}$ отображения свёртки из теор. 24.1 не зависят от выбора последовательности индексов J, по которым производится свёртка

то линейная форма (25-16) будет иметь вид

$$n! \cdot \sum_{i=1}^{d} a_{m_1 \dots m_{i-1}(m_i+1)m_{i+1}\dots m_d} x_i \tag{25-18}$$

и всего таких форм будет $\binom{n+d-2}{d-1}$ (количество способов разложить $n-1$ в сумму d занумерованных целых неотрицательных слагаемых $m_1, m_2, \dots, m_d$). Отсюда мы получаем, например, критерий представимости многочлена в виде n-той степени линейной формы.

Предложение 25.2
Над алгебраически замкнутым полем характеристики нуль однородный многочлен (25-17) тогда и только тогда является n-той степенью линейной формы, когда ранг $d \times \binom{n+d-2}{d-1}$ матрицы, составленной из коэффициентов линейных форм (25-18), равен единице. В этом случае форма φ, такая что $\varphi^n = f$, также пропорциональна формам (25-18).

Доказательство. В самом деле, из равенства $f = \varphi^n$ вытекает, что $\operatorname{Supp}(f)$ — одномерное пространство, порождённое формой φ, и тогда все формы (25-18) пропорциональны форме φ. Наоборот, если все формы (25-18) пропорциональны друг другу, то $\operatorname{Supp}(f)$ — одномерное пространство $U = \Bbbk \cdot \psi$, порождённое какой-то формой $\psi \in V^*$. Поскольку $S^nU = \Bbbk \cdot \psi^n$ тоже одномерно, условие $f \in S^nU$ означает, что $f = \lambda\psi^n$ для некоторого $\lambda \in \Bbbk$. Если $\Bbbk$ алгебраически замкнуто, последнее равенство переписывается как $f = \varphi^n$ с $\varphi = \sqrt[n]{\lambda} \cdot \psi$. □

Следствие 25.1
Образ *вложения Веронезе* $\mathbb{P}(V^*) \xhookrightarrow{\varphi \mapsto \varphi^n} \mathbb{P}(S^nV^*)$ является проективным алгебраическим многообразием, задаваемым системой квадратных уравнений — равенством нулю всех 2×2 миноров $d \times \binom{n+d-2}{d-1}$ матрицы, составленной из коэффициентов линейных форм (25-18). □

Например, однородный многочлен от двух переменных

$$f(x_0, x_1) = \sum_{k=0}^{n} a_k \cdot \binom{n}{k} \cdot x_0^{n-k} x_1^k$$

тогда и только тогда имеет вид $(\alpha_0 x_0 + \alpha_1 x_1)^n$, когда

$$\operatorname{rk} \begin{pmatrix} a_0 & a_1 & \dots & a_{n_1} \\ a_1 & a_2 & \dots & a_n \end{pmatrix} = 1\,,$$

что выражается системой квадратных уравнений

$$\det \begin{pmatrix} a_i & a_j \\ a_{i+1} & a_{j+1} \end{pmatrix} = 0$$

на коэффициенты a_i многочлена f, и в этом случае $(\alpha_0 : \alpha_1) = (a_i : a_{i+1})$ для любого i, Такого что $a_i a_{i+1} \neq 0$.

25.3.2. Поляры проективной гиперповерхности. Рассмотрим проективную гиперповерхность $S \subset \mathbb{P}(V)$, заданную однородным уравнением $F(x) = 0$ степени n. Пересечение S произвольной прямой $\ell = (pq)$ состоит из таких точек $\lambda p + \mu q \in \ell$, что отношение $(\lambda : \mu)$ удовлетворяет уравнению $f(\lambda, \mu) = 0$, которое получается подстановкой $x = \lambda p + \mu q$ в уравнение гиперповерхности $F(x) = 0$. Если основное поле алгебраически замкнуто, и прямая ℓ не лежит на S целиком (что означало бы тождественное обращение $f(\lambda, \mu)$ в нуль), то ℓ пересекает S в конечном наборе точек $a_1, a_2, \dots, a_k$, причём если учитывать каждую из них с надлежащей кратностью, то сумма этих кратностей будет равна n. Для этого кратность пересечения поверхности S с прямой ℓ в точке $a_i = (\alpha_i' : \alpha_i'')$ надо определить как показатель, с которым линейный множитель

$$\det \begin{pmatrix} \lambda & \mu \\ \alpha_i' & \alpha_i'' \end{pmatrix} = (\alpha_i''\lambda - \alpha_i'\mu)$$

входит в разложение $f(\lambda, \mu) = \prod(\alpha_i''\mu - \alpha_i'\lambda)^{s_i}$ однородного многочлена $f(\lambda, \mu)$ на линейные множители.

Показатель s_i называется *локальным индексом пересечения* поверхности S с прямой ℓ в точке a_i и обозначается $(S, \ell)_{a_i}$. Прямая ℓ называется *касательной* к S в точке $a \in \ell \cap S$, если $(S, \ell)_a \geqslant 2$ или $\ell \subset S$.

По формуле Тэйлора (25-15) коэффициент при $\lambda^{n-m}\mu^m$ в уравнении $f(\lambda, \mu) = 0$ равен

$$\binom{n}{m}\widetilde{f}(p^{n-m}, q^m) = \frac{1}{m!}\,\frac{\partial^m F}{\partial q^i}(p) = \frac{1}{(n-m)!}\,\frac{\partial^{n-m} F}{\partial p^{n-m}}(q)\,. \qquad (25\text{-}19)$$

и если $p \in S$, то разложение Тейлора в окрестности p начинается как

$$F(p + tq) = t\binom{d}{1}\widetilde{F}(p^{n-1}, q) + t^2\binom{d}{2}\widetilde{F}(p^{n-2}, q^2) + \cdots\,.$$

Таким образом, прямая pq, проходящая через точку $p \in S$, касается S в этой точке тогда и только тогда, когда $\widetilde{F}(p^{n-1}, q) = 0$.

Если $F(p^{n-1}, x) \not\equiv 0$ как линейная форма от x, то точки q, для которых прямая (pq) касается S в точке p, заметут в $\mathbb{P}(V)$ гиперплоскость, задаваемую линейным уравнением $F(p^{n-1}, x) = 0$. Она называется *касательным пространством* к S в p и обозначается T_pS. Точка p называется в этом случае *гладкой* точкой поверхности S.

Если $F(p^{n-1}, x) \equiv 0$, то поверхность S называется *особой* в точке p, а p называется *особой точкой* поверхности S. Согласно (25-19), коэффициентами линейной формы

$$F(p^{n-1}, x) = \partial_x F(p)$$

являются частные производные от F, вычисленные в точке p, так что особость p равносильна занулению в p всех частных производных от уравнения гиперповерхности. В этом случае любая проходящая через p прямая имеет с S как минимум двукратное пересечение, и касательное пространство T_pS, понимаемое как объединение всех прямых, касающихся S в точке p, совпадает со всем пространством $\mathbb{P}(V)$.

Если q — гладкая точка на S или любая точка вне S, то замыкание множества точек касания с S всевозможных касательных, опущенных на S из точки q образует на поверхности S фигуру, называемую *контуром* поверхности S, видимым из точки q. Видимый контур высекается из S полярной к q относительно S гиперповерхностью $(n-1)$-й степени

$$\mathrm{pl}_q S = \{y \in \mathbb{P}(V) \mid \widetilde{F}(q, y^{n-1}) = 0\}\,, \tag{25-20}$$

автоматически отличной от всего пространства. Действительно, условие касания прямой (qy) поверхности S в точке y — это $\widetilde{F}(y^{n-1}, q) = 0$. Если многочлен $G(y) = \widetilde{F}(y^{n-1}, q)$ тождественно нулевой (как многочлен от y), то, взяв $y = q$, мы получим $F(q) = 0$, откуда $q \in S$. С другой стороны, т. к. все производные от G в этом случае тоже нулевые, мы получаем равенство

$$\widetilde{F}(q^{n-1}, y) = \widetilde{G}(q^{n-2}, y) = \frac{\partial^{n-2}}{\partial q^{n-2}} G(y) \equiv 0\,,$$

означающее, что q — особая точка поверхности S.

Гиперповерхность $\mathrm{pl}_q^{n-r} = \left\{ y \in \mathbb{P}(V) \mid \widetilde{F}(q^{n-r}, y^r) = 0 \right\}$ называется *полярой r-й степени* поверхности S относительно точки q. Если $q \in S$ — гладкая точка, то поляра первой степени — эта касательная гиперплоскость T_qS к S в точке q, а каждая поляра степени $r \geqslant 2$ — это поверхность степени r, которая проходит через q и имеет те же поляры степеней $< r$ относительно точки q, что и исходная поверхность S. Так, квадратичная поляра — это проходящая через q квадрика, имеющая в точке q ту же касательную гиперплоскость, что и S, кубическая поляра — это проходящая через q кубическая поверхность с той же касательной плоскостью и квадратичной полярой, что и S, и т. д.

25.4. Поляризация грассмановых многочленов. Хотя грассманов многочлен $\omega \in \Lambda V^*$ и не задаёт никакой функции на векторах двойственного пространства V, большая часть сказанного в предыдущем разделе имеет смысл и для грассмановых многочленов. А именно, по предл. 25.1 над полем характеристики нуль для любого однородного грассманова многочлена n-той степени $\omega \in \Lambda^n V^*$ существует единственная n-линейная кососимметричная форма $\widetilde{\omega} \in \mathrm{Skew}^n V^* \subset V^{*\otimes n}$, которая проектируется в этот многочлен при факторизации тензорной алгебры по соотношениям антикоммутирования. Эта форма (равно как и соответствующий ей кососимметрический тензор) называется *полной поляризацией* грассманова многочлена ω.

Согласно формуле (25-9) из предл. 25.1 полная поляризация базисного грассманова монома $\omega = e_{i_1} \wedge e_{i_2} \wedge \cdots \wedge e_{i_n}$ равна

$$\widetilde{\omega} = \frac{1}{n!}\, e_{\langle i_1, i_2, \ldots, i_n \rangle} = \mathrm{alt}_n \left(e_{i_1} \otimes e_{i_2} \otimes \cdots \otimes e_{i_n} \right)\,. \tag{25-21}$$

Как и в симметрическом случае, полная поляризация индуцирует двойственность между пространствами грассмановых многочленов на двойственных пространствах, при которой результатом спаривания между многочленами

$$\omega \in \Lambda^n V^* \quad \text{и} \quad \tau \in \Lambda^n V$$

по определению считается полная свёртка их полных поляризаций $\langle\widetilde{\omega},\widetilde{\tau}\rangle$.

Упражнение 25.8. Покажите, что результатом спаривания двух базисных грассмановых мономов $e_I = e_{i_1}\wedge e_{i_2}\wedge\cdots\wedge e_{i_n}$ и $x_J = e_{i_1}\wedge e_{i_2}\wedge\cdots\wedge e_{i_n}$ от двойственных базисных векторов пространств V и V^* (оба набора индексов I и J строго возрастают) является $1/n!$, если $i_\nu = j_\nu \ \forall \nu$, и нуль во всех остальных случаях.

25.4.1. Частные производные в грассмановой алгебре. Рассмотрим отображение

$$\mathrm{pl}_v : \Lambda^n V^* \longrightarrow \Lambda^{n-1} V^*,$$

сопоставляющее грассманову многочлену $\omega \in \Lambda^n V^*$ проекцию во внешнюю алгебру тензора, получающегося свёрткой по первому тензорному сомножителю полной поляризации $\widetilde{\omega} \in V^{*\otimes n}$ с вектором $v \in V$. Оно включается в коммутативную диаграмму

$$\begin{array}{ccc} V^{*\otimes n} \supset \mathrm{Skew}\,^n V^* & \xrightarrow{c_v^1} & \mathrm{Skew}\,^{(n-1)} V^* \subset V^{*\otimes(n-1)} \\ \big\downarrow & & \big\downarrow \\ \Lambda^n V^* & \xrightarrow{\mathrm{pl}_v} & \Lambda^{n-1} V^* \end{array}$$

горизонтальные стрелки которой суть проекции во внешнюю алгебру (отображения факторизации по соотношениям антикоммутирования), а верхняя горизонтальная стрелка — свёртка первого тензорного сомножителя с вектором v . По аналогии с симметрическим случаем, определим *грассманову производную* кососимметричного многочлена $\omega \in \Lambda^n V^*$ в направлении вектора $v \in V$ формулой

$$\partial_v \omega \stackrel{\mathrm{def}}{=} \deg\omega \cdot \mathrm{pl}_v \omega \,.$$

Из билинейности $\mathrm{pl}_v\omega$ по v и ω мы сразу же получаем, что производная в направлении вектора $v = \sum \alpha_i e_i$ является линейной комбинацией частных производных вдоль базисных векторов:

$$\partial_v = \sum \alpha_i \, \partial_{e_i} \,.$$

Если ω не зависит от x_j, из определений очевидно, что $\partial_{e_j}\omega = 0$. Поэтому ненулевой вклад в производную от базисного монома

$$\omega = x_{i_1} \wedge x_{i_2} \wedge \cdots \wedge x_{i_n}$$

дадут только дифференцирования $\partial_{e_{i_1}}, \partial_{e_{i_2}}, \ldots, \partial_{e_{i_n}}$. Из формулы (25-21) вытекает, что

$$\partial_{e_{i_1}} x_{i_1} \wedge x_{i_2} \wedge \cdots \wedge x_{i_n} = x_{i_2} \wedge x_{i_3} \wedge \ldots \wedge x_{i_n}$$

вне зависимости от того, образуют ли неповторяющиеся индексы

$$I = (i_1, i_2, \dots, i_n)$$

строго возрастающую последовательность или нет. Таким образом, частная производная грассманова монома по направлению первого слева сомножителя действует как $\partial/\partial x_{i_1}$ (т. е. просто уничтожает этот сомножитель). При дифференцировании по остальным направлениям будут появляться знаки:

$$\begin{aligned}\partial_{e_{i_k}} x_{i_1} \wedge x_{i_2} \wedge \dots \wedge x_{i_n} = \partial_{e_{i_k}} (-1)^{k-1} x_{i_k} \wedge x_{i_1} \wedge \dots \wedge x_{i_{k-1}} \wedge x_{i_{k+1}} \dots x_{i_n} = \\ = (-1)^{k-1} \partial_{e_{i_k}} x_{i_k} \wedge x_{i_1} \wedge \dots \wedge x_{i_{k-1}} \wedge x_{i_{k+1}} \dots x_{i_n} = \\ = (-1)^{k-1} x_{i_1} \wedge \dots \wedge x_{i_{k-1}} \wedge x_{i_{k+1}} \dots x_{i_n} \,.\end{aligned}$$

Иначе говоря, дифференцирование грассманова монома по направлению k-той слева входящей в него переменной ведёт себя как $(-1)^{k-1}\partial/\partial x_{i_k}$. Удобно воспринимать это явление как *грассманово правило Лейбница*:

Упражнение 25.9. Докажите, что грассмановы частные производные удовлетворяют грассманову правилу Лейбница: $\partial_v(\omega \wedge \tau) = \partial_v(\omega) \wedge \tau + (-1)^{\deg \omega} \omega \wedge \partial_v(\tau)$.

Поскольку $\widetilde{\omega}(u, w, *, \dots, *) = -\widetilde{\omega}(w, u, *, \dots, *)$ операции pl_u и pl_w антикоммутируют относительно композиции: $\mathrm{pl}_u \mathrm{pl}_w \omega = -\mathrm{pl}_w \mathrm{pl}_u \omega$. Поэтому грассмановы частные производные также *антикоммутируют*: $\partial_u \partial_w = -\partial_w \partial_u$. В частности, $\partial_v^2 \omega \equiv 0$ для любых v и ω.

25.4.2. Линейный носитель грассманова многочлена $\boldsymbol{\omega} \in \boldsymbol{\Lambda^n V}$ определяется как минимальное подпространство $W \subset V$, такое что $\omega \in \Lambda^n W$, и обозначается $\mathrm{Supp}(\omega)$. Очевидно, что носитель ω совпадает с носителем поляризации $\widetilde{\omega}$, который по теор. 24.1 является образом отображения

$$V^{*\otimes(n-1)} \longrightarrow V \,,$$

задаваемого полной свёрткой с тензором $\widetilde{\omega}$. В виду кососимметричности тензора $\widetilde{\omega}$ различные отображения свёртки из теор. 24.1 отличаются друг от друга лишь знаком, и поэтому неважно, какую из свёрток взять. Таким образом, линейный носитель грассманова многочлена степени n порождается векторами

$$\partial_J \omega = \partial_{j_1} \partial_{j_2} \dots \partial_{j_{n-1}} \omega \,,$$

где $\partial_j = \partial_{x_j}$ и $J = (j_1, j_2, \dots, j_{n-1})$ пробегает всевозможные наборы из $(n-1)$ попарно различных индексов[1]. Если разложить ω в сумму мономов

$$\omega = \sum_I a_I e_I = \sum_{i_1 i_2 \dots i_n} \alpha_{i_1 i_2 \dots i_n} e_{i_1} \wedge e_{i_2} \wedge \dots \wedge e_{i_n}$$

[1] в силу кососимметричности грассмановых частных производных достаточно ограничиться только строго возрастающими наборами

(коэффициенты $\alpha_{i_1 i_2 \dots i_n}$ кососимметричны по индексам $i_1, i_2, \dots, i_n$), то вклад в $\partial_J \omega$ дадут только мономы $a_I e_I$ с $I \supset J$. В результате, с точностью до общего знака, мы получим

$$\partial_J \omega = \pm \sum_{i \notin J} \alpha_{j_1 j_2 \dots j_{n-1} i} \, e_i \,. \tag{25-22}$$

Отсюда получается, например, следующий критерий разложимости грассманова многочлена.

Предложение 25.3
Следующие условия на грассманов многочлен

$$\omega = \sum_{i_1 i_2 \dots i_n} \alpha_{i_1 i_2 \dots i_n} e_{i_1} \wedge e_{i_2} \wedge \cdots \wedge e_{i_n}$$

где все коэффициенты $\alpha_{i_1 i_2 \dots i_n}$ кососимметричны по индексам $i_1, i_2, \dots, i_n$, эквивалентны друг другу:

1) $\omega = u_1 \wedge u_2 \wedge \cdots \wedge u_n$ для некоторых $u_1, u_2, \dots, u_n \in V$

2) $u \wedge \omega = 0 \;\; \forall \, u \in \operatorname{Supp}(\omega)$

3) для любых двух наборов неповторяющихся индексов

$$i_1, i_2, \dots, i_{m+1} \quad \text{и} \quad j_1, j_2, \dots, j_{m-1}$$

выполнено *соотношение Плюккера*[1] $\displaystyle\sum_{\nu=1}^{m+1} (-1)^{\nu-1} a_{j_1 \dots j_{m-1} i_\nu} a_{i_1 \dots \widehat{i}_\nu \dots i_{m+1}} = 0 \,.$

Доказательство. Условие (1) означает, что многочлен ω лежит в самой старшей внешней степени $\Lambda^{\dim \operatorname{Supp}(\omega)}$ своей линейной оболочки $\operatorname{Supp}(\omega)$. Поэтому равносильность условий (1) и (2) вытекает из следующего общего факта:

Упражнение 25.10. Докажите, что $\omega \in \Lambda U$ тогда и только тогда однороден степени $\dim U$, когда $u \wedge \omega = 0$ для всех $u \in U$.

Формулы (3) представляют собою координатную запись условия (2) и констатирует зануление коэффициента при $e_{i_1} \wedge e_{i_2} \wedge \cdots \wedge e_{i_{n+1}}$ в $u \wedge \omega$, где u — это вектор (25-22). Поскольку (2) достаточно проверить только для какой-нибудь системы векторов u, линейно порождающей пространство $\operatorname{Supp}(\omega)$, написанных в (3) условий достаточно. $\square$

Упражнение 25.11. Выпишите соотношения Плюккера для грассмановой квадратичной формы ω от четырёх переменных и выведите из них, что такая форма тогда и только тогда является произведением двух линейных, когда $\omega \wedge \omega = 0$.

[1] «крышка» в $a_{i_1 \dots \widehat{i}_\nu \dots i_{m+1}}$ означает, что индекс i_ν следует пропустить

Следствие 25.2 (плюккерово вложение)
Отображение Плюккера $\mathrm{Gr}(m,V) \hookrightarrow \mathbb{P}(\Lambda^m V)$, переводящее m-мерное подпространство $U \subset V$ в одномерное подпространство $\Lambda^m U \subset \Lambda^m V$, вкладывает грассманиан в проективное пространство в качестве алгебраического многообразия, задаваемого квадратичными соотношениями (3) из предл. 25.3.

Доказательство. Если подпространство $U \subset V$ имеет базис $u_1, u_2, \dots, u_m$, то отображение Плюккера переведёт его в класс пропорциональности грассманова многочлена $u_1 \wedge u_2 \wedge \dots \wedge u_m$. Поэтому образ отображения Плюккера состоит из всех разложимых однородных грассмановых форм степени m, т. е. является пересечением квадрик из п. (3) предл. 25.3. С другой стороны, отображение Плюккера инъективно, поскольку при $U \neq W$ в V имеется базис

$$v_1, v_2, \dots, v_r,\ u_1, u_2, \dots, u_{m-r},\ w_1, w_2, \dots, w_{m-r},\ v_{2m-r},\ v_{2m-r+1},\ \dots,\ v_n,$$

в котором $v_1, v_2, \dots, v_r$ образуют базис пересечения $U \cap W$, а

$$v_1, v_2, \dots, v_r,\ u_1, u_2, \dots, u_{m-r} \quad \text{и} \quad v_1, v_2, \dots, v_r,\ w_1, w_2, \dots, w_{m-r}$$

составляют базисы в U и W, так что отображение Плюккера сопоставляет им различные *базисные* мономы

$$v_1 \wedge \dots \wedge v_r \wedge u_1 \wedge \dots \wedge u_{m-r} \neq v_1 \wedge \dots \wedge v_r \wedge w_1 \wedge \dots \wedge w_{m-r}$$

алгебры ΛV. □

Задачи для самостоятельного решения к §25

Задача 25.1. Явно предъявите тензор $t \in V^{\otimes 3}$, не являющийся суммой кососимметричного и симметричного.

Задача 25.2. Над полем характеристики нуль постройте канонические изоморфизмы между следующими пространствами:
а) симметричных n-линейных форм $V \times V \times \dots \times V \xrightarrow{\varphi} \Bbbk$
б) функций $V \xrightarrow{f} \Bbbk$, задаваемых однородным многочленом степени n от линейных координат в каком-нибудь (а значит, и в любом) базисе
в) $\mathrm{Sym}^n(V^*)$ г) $\mathrm{Sym}^n(V)^*$ д) $(S^n V)^*$ е) $(S^n V^*)$
Какие из построенных изоморфизмов останутся таковыми и над всеми полями конечной характеристики?

Задача 25.3. Над полем характеристики нуль постройте канонические изоморфизмы между следующими пространствами:
а) кососимметричных n-линейных форм $V \times V \times \dots \times V \xrightarrow{\varphi} \Bbbk$
б) $\mathrm{Skew}^n(V^*)$ в) $\mathrm{Skew}^n(V)^*$ г) $(\Lambda^n V)^*$ д) $(\Lambda^n V^*)$
Какие из построенных изоморфизмов останутся таковыми и над всеми полями конечной характеристики?

Задача 25.4 (принцип Аронгольда). Пусть V — конечномерное векторное пространство над полем характеристики нуль. Покажите, что пространство симметрических тензоров $\operatorname{Sym}^n(V) \subset V^{\otimes n}$ линейно порождается тензорами вида $v^{\otimes n} = v \otimes v \otimes \cdots \otimes v$ со всевозможными $v \in V$ и явно выразите через тензоры вида $v^{\otimes 3}$ симметрический кубический тензор $u \otimes w \otimes w + w \otimes u \otimes w + w \otimes w \otimes u$, где $u, w \in V$ — два произвольных линейно независимых вектора.

Задача 25.5. Можно ли обратимой линейной заменой переменных преобразовать многочлен $9\,x^3 - 15\,yx^2 - 6\,zx^2 + 9\,xy^2 + 18\,z^2x - 2\,y^3 + 3\,zy^2 - 15\,z^2y + 7\,z^3$ в многочлен от $\leqslant 2$ переменных?

Задача 25.6. Покажите, что многочлен $\det(A)$ на пространстве $n \times n$-матриц имеет следующее разложение Тейлора: $\det(\lambda A + \mu B) = \sum\limits_{p+q=n} \lambda^p \mu^q \cdot \operatorname{tr}\left(\Lambda^p A \cdot \Lambda^q B^t\right)$, где $\Lambda^p A$ и $\Lambda^q B$ суть внешние степени[1] матриц A и B.

Задача 25.7. Обозначим через $S \subset \mathbb{P}_N = \mathbb{P}(S^2 V^*)$ множество всех вырожденных квадрик на $\mathbb{P}_n = \mathbb{P}(V)$. Покажите, что

а) S является алгебраической гиперповерхностью, и точка $Q \in S$ является неособой точкой поверхности S тогда и только тогда, когда соответствующая квадрика $Q \subset \mathbb{P}_n$ имеет единственную особую точку $p \in Q$

б) касательная гиперплоскость $T_Q S \subset \mathbb{P}_N$ в такой неособой точке $Q \in S$ состоит из всех квадрик на $\mathbb{P}_n$, проходящих через особую точку p квадрики $Q \subset \mathbb{P}_n$.

Задача 25.8. Найдите все особые точки следующих трёх кривых на $\mathbb{P}_2 = \mathbb{P}(\mathbb{C}^3)$:

а) $(x_0 + x_1 + x_2)^3 = 27\,x_0 x_1 x_2$

б) $x^2 y + x\,y^2 = x^4 + y^4$

в) $(x^2 - y + 1)^2 = y^2(x^2 + 1)$

(последние две кривые заданы аффинным уравнением в стандартной карте U_0 и речь в задаче идёт про их проективные замыкания).

Задача 25.9. Напишите явную рациональную параметризацию проективной плоской квартики $(x_0^2 + x_1^2)^2 + 3\,x_0^2 x_1 x_2 + x_1^3 x_2 = 0$, воспользовавшись проекцией из особой точки на какую-нибудь прямую.

Задача 25.10 (комплексы Кошуля и Де Рама). Заиксируем в пространстве V базис $e_1, e_2, \dots, e_n$ и обозначим через x_i и ξ_i классы вектора e_i в симметрической и внешней алгебре соответственно. Покажите, что а) операторы

$$\begin{gathered}
\Lambda^{k+1} V \otimes S^{m-1} V \xleftarrow{\ d\ } \Lambda^k V \otimes S^m V \xrightarrow{\ \partial\ } \Lambda^{k-1} V \otimes S^{m+1} V \\
d = \sum_\nu \xi_\nu \otimes \frac{\partial}{\partial x_\nu} \;:\; \omega \otimes f \longmapsto \sum_\nu \frac{\partial \omega}{\partial \xi_\nu} \otimes x_\nu \cdot f \\
\partial = \sum_\nu \frac{\partial}{\partial \xi_\nu} \otimes x_\nu \;:\; \omega \otimes f \longmapsto \sum_\nu \xi_\nu \wedge \omega \otimes \frac{\partial f}{\partial x_\nu}
\end{gathered} \tag{25-23}$$

[1] т. е. матрицы операторов, индуцированных операторами A и B на пространствах однородных грассмановых многочленов от базисных векторов степеней p и q соответственно (см. зад. 24.17); матричные элементы этих матриц суть миноры порядков p и q матриц A и B, занумерованные так, чтобы дополнительные миноры имели одинаковые номера

не зависят от выбора базиса и имеют $d^2 = 0$ и $\partial^2 = 0$
б) оператор $d\partial + \partial d$ действует на $\Lambda^k V \otimes S^m V$ как $(k+m)\cdot \mathrm{Id}$.
в) Вычислите $\ker d / \operatorname{im} d$ и $\ker \partial / \operatorname{im} \partial$

Задача 25.11 (грассманова экспонента). Над полем *любой* характеристики положим $e^{\omega} \overset{\text{def}}{=} 1 + \omega$ для *разложимых* $\omega \in \Lambda^{2m}$ и продолжим это определение на всё пространство $\Lambda^{2m} V$ правилом $e^{\sum \omega_i} = \prod e^{\omega_i}$. Покажите, что
а) определение e^f корректно (не зависит ни от способа представления f в виде суммы разложимых мономов, ни от порядка расположения сомножителей в стоящем в правой части *грассмановом* произведении)
б) экспоненциальное отображение $\Lambda^{\text{even}} V \hookrightarrow \Lambda^{\text{even}} V$ является инъективным гомоморфизмом из аддитивной группы всех чётных грассмановых многочленов в мультипликативную группу чётных грассмановых многочленов со свободным членом 1.

Задача 25.12. Выполняется ли в условиях предыдущей задачи над полем характеристики нуль равенства: а) $\partial_v e^f = e^f \wedge \partial_v f$ б) $e^f = \sum\limits_{k \geqslant 0} \frac{1}{k!} f^{\wedge k}$

Задача 25.13. Выясните, разложима ли грассманова кубическая форма от четырёх переменных $-\xi_1 \wedge \xi_2 \wedge \xi_3 + 2\,\xi_1 \wedge \xi_2 \wedge \xi_4 + 4\,\xi_1 \wedge \xi_3 \wedge \xi_4 + 3\,\xi_2 \wedge \xi_3 \wedge \xi_4$ (если да, то напишите какое-нибудь из разложений явно, если нет — объясните, почему).

Раздел VII
Симметрические функции, массивы и таблицы Юнга

§26. Симметрические функции

26.1. Симметрические и кососимметрические многочлены. Симметрическая группа S_n действует на кольце многочленов $\mathbb{Z}[x_1, x_2, \dots, x_n]$ перестановками номеров переменных:

$$gf(x_1, x_2, \dots, x_n) = f(x_{g(1)}, x_{g(2)}, \dots, x_{g(n)}) \qquad \forall\, g \in S_n\,. \tag{26-1}$$

Будем называть многочлен $f \in \mathbb{Z}[x_1, x_2, \dots, x_n]$ *симметрическим*, если $gf = f$ для всех $g \in S^n$, и *кососимметрическим*, если $g(t) = \operatorname{sgn}(g) \cdot t$ для всех $g \in S^n$. Симметрические многочлены образуют в $\mathbb{Z}[x_1, x_2, \dots, x_n]$ подкольцо, а кососимметрические многочлены — модуль над этим кольцом (произведение симметрического многочлена на кососимметрический — это кососимметрический многочлен).

Иногда удобно смотреть на симметрические и кососимметрические многочлены как на симметрические и кососимметрические тензоры в n-той тензорной степени кольца многочленов от одной переменной. Имеется изоморфизм $\mathbb{Z}$-модулей (см. n° 23.3.1)

$$\varkappa : \mathbb{Z}[t]^{\otimes n} \xrightarrow{\sim} \mathbb{Z}[x_1, x_2, \dots, x_n]\,, \tag{26-2}$$

переводящий базисный (некоммутативный) тензорный моном

$$t^{m_1} \otimes t^{m_2} \otimes \cdots \otimes t^{m_n} \in \mathbb{Z}[t]$$

в базисный моном $x_1^{m_1} x_2^{m_2} \cdots x_n^{m_n} \in \mathbb{Z}[x_1, x_2, \dots, x_n]$ (номера тензорных сомножителей слева соответствуют номерам переменных справа). Изоморфизм $\varkappa$ перестановочен с действием симметрической группы и отождествляет симметрические и кососимметрические тензоры слева с симметрическими и кососимметрическими многочленами справа. Умножению многочленов в кольце $\mathbb{Z}[x_1, x_2, \dots, x_n]$ отвечает покомпонентное умножение тензорных сомножителей в $\mathbb{Z}[t]^{\otimes n}$:

$$(f_1 \otimes f_2 \otimes \cdots \otimes f_n) \cdot (g_1 \otimes g_2 \otimes \cdots \otimes g_n) = (f_1 g_1) \otimes (f_2 g_2) \otimes \cdots \otimes (f_n g_n)$$

Упражнение 26.1. Проверьте, что так определённое умножение наделяет $\mathbb{Z}[t]^{\otimes n}$ структурой коммутативного кольца с единицей $1 \otimes 1 \otimes \cdots \otimes 1$.

Изоморфизм $\varkappa$ переводит стандартные базисы $\mathbb{Z}$-модулей

$$\operatorname{Sym}^n(\mathbb{Z}[t]) \quad \text{и} \quad \operatorname{Skew}^n(\mathbb{Z}[t]),$$

описанные в (25-2) и (25-3), в стандартные базисы $\mathbb{Z}$-модулей симметрических и кососимметрических многочленов, которые называются *мономиальным* и *детерминантным*.

26.1.1. Мономиальный базис модуля симметрических многочленов состоит из *мономиальных симметрических многочленов*

$$m_\lambda = (\text{сумма всех мономов из } S_n\text{-орбиты монома } x_1^{\lambda_1} x_2^{\lambda_2} \cdots x_n^{\lambda_n}), \tag{26-3}$$

где $\lambda = (\lambda_1, \lambda_2, \dots, \lambda_n)$ пробегает диаграммы Юнга из $\leqslant n$ строк. Поскольку любой симметрический многочлен вместе с каждым своим мономом содержит (с одинаковыми коэффициентами) все мономы из его S_n-орбиты, и каждая S_n-орбита однозначно определяется своим лексикографически старшим мономом, показатели которого слева направо не убывают, любой симметрический многочлен однозначно представляется в виде целочисленной линейной комбинации многочленов m_λ. Прообразом многочлена m_λ при изоморфизме (26-2) является стандартный базисный симметрический тензор (25-2), равный сумме всех различных тензорных произведений из $m_0(\lambda)$ сомножителей $t^0 = 1$, $m_1(\lambda)$ сомножителей t^1, $m_2(\lambda)$ сомножителей t^2 и т. д., где $m_i(\lambda)$ равно числу строк длины i в диаграмме λ.

26.1.2. Детерминантный базис модуля кососимметрических многочленов состоит из альтернированных S_n-орбит

$$\Delta_\nu = \sum_{g \in S_n} \operatorname{sgn}(g)\, x_{g(1)}^{\nu_1} x_{g(2)}^{\nu_2} \cdots x_{g(n)}^{\nu_n}. \tag{26-4}$$

Прообразом такого многочлена при изоморфизме (26-2) является стандартный базисный кососимметрические тензор (25-3). Поскольку в кососимметрическом многочлене нет мономов, содержащих одинаковые степени разных переменных[1], индекс ν в (26-4) пробегает множество диаграмм Юнга с неповторяющимися длинами строк $\nu_1 > \nu_2 > \dots > \nu_n$. Такая диаграмма ν всегда содержит в себе минимальную треугольную диаграмму из n строк разной длины

$$\delta = ((n-1),\, (n-2),\, \dots,\, 1,\, 0)$$

Разность $\lambda = \nu - \delta = ((\nu_1 - n + 1),\, (\nu_2 - n + 2),\, \dots,\, (\nu_{n-1} - 1),\, \nu_n)$ имеет $\lambda_i = \nu_i - n + i$ и представляет собою произвольную диаграмму Юнга из $\leqslant n$ строк (без ограничений на длины этих строк). Иногда бывает удобно нумеровать

[1] при транспозиции любых двух переменных многочлен должен менять знак

базис (26-4) именно такими диаграммами λ, и в этих случаях мы будем писать $\Delta_{\lambda+\delta}$ вместо Δ_ν.

Легко видеть, что многочлен (26-4) представляет собою определитель[1]

$$\Delta_\nu = \det(x_j^{\nu_i}) = \det\begin{pmatrix} x_1^{\nu_1} & x_2^{\nu_1} & \cdots & x_n^{\nu_1} \\ x_1^{\nu_2} & x_2^{\nu_2} & \cdots & x_n^{\nu_2} \\ \vdots & \vdots & \cdots & \vdots \\ x_1^{\nu_n} & x_2^{\nu_n} & \cdots & x_n^{\nu_n} \end{pmatrix} \tag{26-5}$$

Упражнение 26.2. Убедитесь в этом прямым раскрытием правой части (26-5).

В частности, при $\nu = \delta$ получаем *определитель Вандермонда*

$$\Delta_\delta = \det(x_j^{n-i}) = \det\begin{pmatrix} x_1^{n-1} & x_2^{n-1} & \cdots & x_n^{n-1} \\ x_1^{n-2} & x_2^{n-2} & \cdots & x_n^{n-2} \\ \vdots & \vdots & \cdots & \vdots \\ x_1 & x_2 & \cdots & x_n \\ 1 & 1 & \cdots & 1 \end{pmatrix} = \prod_{i<j}(x_i - x_j)\,. \tag{26-6}$$

Упражнение 26.3. Убедитесь в справедливости равенства $\Delta_\delta = \prod\limits_{i<j}(x_i - x_j)$.

26.1.3. Базис Шура. Поскольку любой кососимметрический многочлен f обращается в нуль при подстановке $x_i = x_j$, он делится в кольце $\mathbb{Z}[x_1, x_2, \dots, x_n]$ на $(x_i - x_j)$, а так как каждая из разностей $(x_i - x_j)$ неприводима, f делится на их произведение $\Delta_\delta = \prod\limits_{i<j}(x_i - x_j)$, причём частное от этого деления

$$\frac{f}{\Delta_\delta} \in \mathbb{Z}[x_1, x_2, \dots, x_n]$$

является симметрическим многочленом. Мы получаем

Предложение 26.1

Умножение на определитель Вандермонда Δ_δ задаёт $\mathbb{Z}$-линейный изоморфизм $\mathbb{Z}$-модуля симметрических многочленов с $\mathbb{Z}$-модулем кососимметрических многочленов. Этот изоморфизм также является изоморфизмом модулей над кольцом симметрических многочленов. □

Следствие 26.1

Многочлены[2] $s_\lambda = \Delta_{\delta+\lambda}/\Delta_\delta$, где λ пробегает все диаграммы Юнга из не более n строк, образуют базис $\mathbb{Z}$-модуля симметрических многочленов.

---

[1] здесь и далее запись $(f(i,j))$, где $f(i,j)$ некоторая функция от i, j, будет означать матрицу, в i-той строке и j-том столбце которой стоит результат применения функции f к данным значениям i и j

[2] многочлены $s_\lambda = \Delta_{\delta+\lambda}/\Delta_\delta$ называются *многочленами Шура*

26.2. Элементарные симметрические многочлены. Многочлен $E(t)$ с коэффициентами в кольце $\mathbb{Z}[x_1, x_2, \dots, x_n]$, задаваемый формулой

$$E(t) = \prod_i (1 + x_i t) = \sum_{k=0}^{n} e_k(x) \cdot t^k \tag{26-7}$$

имеет в качестве коэффициентов *элементарные симметрические многочлены* $e_0 = 1$ и

$$e_k(x) = \sum_{i_1 < i_2 < \dots < i_k} x_{i_1} x_{i_2} \dots x_{i_k} \tag{26-8}$$

(сумма всех произведений из k различных переменных, где $k \geqslant 1$). Эти же многочлены возникают в *формулах Виета*: если $\alpha_1, \alpha_2, \dots, \alpha_n$ являются корнями приведённого многочлена

$$t^n + a_1 t^{n-1} + \dots + a_{n-1} t + a_n = \prod_{i=1}^{n} (x - \alpha_i)\,, \tag{26-9}$$

то $a_i = (-1)^i e_i(\alpha_1, \alpha_2, \dots, \alpha_n)$.

Для любого набора неотрицательных целых чисел $\lambda_1, \lambda_2, \dots, \lambda_m$ положим по определению

$$e_\lambda = e_{\lambda_1} e_{\lambda_2} \cdots e_{\lambda_m} = \prod_{k=1}^{m} e_{\lambda_k}\,.$$

Если λ — диаграмма Юнга, то лексикографически старшим мономом многочлена e_λ будет $x_1^{\lambda_1^t} x_2^{\lambda_2^t} \dots x_n^{\lambda_n^t}$, возникающий при перемножении монома $x_1 \dots x_{\lambda_1}$ из e_{λ_1}, монома $x_1 \dots x_{\lambda_2}$ из e_{λ_2} и т. д. вплоть до $x_1 \dots x_{\lambda_m}$ из e_{λ_m} — это можно представлять себе как результат перемножения букв $x_1, x_2, \dots, x_n$, расставленных в клетки диаграммы λ так, что x_1 стоит во всех клетках первого столбца, x_2 — во всех клетках второго и т. д. В результате показатель у переменной x_i будет равен длине i-того столбца диаграммы λ, т. е. длине i-той строки *транспонированной*[1] диаграммы λ^t. Таким образом, разложение многочлена e_λ по базису m_λ из мономиальных симметрических многочленов (26-3) имеет вид:

$$e_\lambda = m_{\lambda^t} + (\text{лексикографически младшие члены}) \tag{26-10}$$

Предложение 26.2

Многочлены $e_\lambda = e_{\lambda_1} e_{\lambda_2} \cdots e_{\lambda_m}$, где λ пробегает диаграммы Юнга, содержащие не более n столбцов, образуют базис $\mathbb{Z}$-модуля симметрических функций.

Доказательство. Многочлены e_λ нумеруются диаграммами λ из не более n столбцов, элементы мономиального базиса m_μ модуля симметрических функций — диаграммами из не более n строк. Выпишем векторы m_μ в строку

[1] диаграммы Юнга, получающиеся друг из друга отражением относительно главной диагонали (как при транспонировании матрицы) называются *сопряжёнными* или *транспонированными*

в порядке лексикографического возрастания диаграмм μ, а векторы e_λ — в порядке лексикографического возрастания транспонированных диаграмм λ^t. Формула (26-10) утверждает теперь, что матрица координат векторов e_λ в мономиальном базисе m_λ верхнетреугольная с единицами по главной диагонали. Поскольку такая целочисленная матрица обратима над $\mathbb{Z}$, многочлены e_λ также образуют базис. □

Следствие 26.2

Многочлены $e_1, e_2, \dots, e_n$ алгебраически независимы в $\mathbb{Z}[x_1, x_2, \dots, x_n]$ и любой симметрический многочлен однозначно записывается в виде многочлена от $e_1, e_2, \dots, e_n$. Иначе говоря, кольцо симметрических функций есть кольцо многочленов $\mathbb{Z}[e_1, e_2, \dots, e_n]$.

Доказательство. Переписывая многочлен e_λ как $e_1^{m_1} e_2^{m_2} \cdots e_n^{m_n}$, где m_i — это число строк длины i в диаграмме λ, видим, что множество многочленов e_λ — это в точности множество всех различных мономов от $e_1, e_2, \dots, e_n$. □

Следствие 26.3

Всякий симметрический многочлен от корней $\alpha_1, \alpha_2, \dots, \alpha_n$ приведённого многочлена (26-9) является многочленом от его коэффициентов $a_1, a_2, \dots, a_n$, а всякая симметрическая рациональная функция от корней произвольного (не обязательно приведённого) многочлена является рациональной функцией от его коэффициентов. □

26.3. Полные симметрические многочлены. Обозначим через $h_k(x)$ сумму всех мономов степени k. Многочлен h_k называется *полным симметрическим многочленом* степени k. Он равен коэффициенту при t^k у формального степенного ряда $H(t) \in \mathbb{Z}[x_1, x_2, \dots, x_n]\,[[t]]$, возникающего при перемножении n бесконечных геометрических прогрессий

$$H(t) = \prod_i \frac{1}{1 - x_i t} = \prod_i \left(1 + x_i t + x_i^2 t^2 + x_i^3 t^3 + \cdots\right) = \sum_{k \geqslant 0} h_k(x) \cdot t^k \qquad (26\text{-}11)$$

(выбор в i-той скобке m_i-того слагаемого добавляет в произведение моном $x_1^{m_1} x_2^{m_2} \cdots x_n^{m_n}$). Таким образом, $H(t)E(-t) = 1$. Вычисляя в этом равенстве коэффициент при t^k получаем рекурсивные формулы, выражающие e_i и h_i друг через друга:

$$(-1)^k h_k = e_k - e_{k-1} h_1 + e_{k-2} h_2 - \cdots + (-1)^{k-1} e_1 h_{k-1} \qquad (26\text{-}12)$$

$$(-1)^k e_k = h_k - h_{k-1} e_1 + h_{k-2} e_2 - \cdots + (-1)^{k-1} h_1 e_{k-1}. \qquad (26\text{-}13)$$

Предложение 26.3

Отображение ω, переводящее многочлен e_k в многочлен h_k (при $k = 1, \dots, n$) является инволютивным автоморфизмом кольца симметрических многочленов.

Доказательство. Так как кольцо симметрических функций изоморфно кольцу многочленов от $e_1, e_2, \dots, e_n$, отображение $e_k \mapsto h_k$ однозначно продолжается до гомоморфизма ω из кольца симметрических функций в себя. Из рекурсивных формул (26-12) и (26-13) вытекает, что этот гомоморфизм переводит h_k обратно в e_k, т. е. является инволюцией и, как следствие, автоморфизмом. $\square$

Следствие 26.4
Многочлены $h_1, h_2, \dots, h_n$ алгебраически независимы в $\mathbb{Z}[x_1, x_2, \dots, x_n]$ и любой симметрический многочлен (в том числе h_m с $m > n$) однозначно записывается в виде многочлена от $h_1, h_2, \dots, h_n$.

26.4. Степенные суммы Ньютона. Сумма k-тых степеней всех переменных

$$p_k(x) = \sum_i x_i^k \tag{26-14}$$

называется k-тым *симметрическим многочленом Ньютона*. Многочлены $p_k(x)$ с $k \geqslant 1$ удобно воспринимать как коэффициенты ряда

$$\begin{aligned} P(t) = \sum_{k\geqslant 1} p_k(x)\cdot t^{k-1} = \sum_i \sum_{k\geqslant 1} x_i^k \cdot t^{k-1} = \sum_i \frac{d}{dt} \sum_{k\geqslant 1} x_i^k \cdot \frac{t^k}{k} = \\ = -\frac{d}{dt}\sum_i \ln(1 - x_i\cdot t) = \frac{d}{dt}\ln\prod_i \frac{1}{1 - x_i\cdot t} = \frac{d}{dt}\ln H(t) \end{aligned} \tag{26-15}$$

который является логарифмической производной от ряда $H(t) = 1/E(-t)$. Таким образом,

$$P(t) = H'(t)/H(t) = E'(-t)/E(-t)\,.$$

Сравнивая коэффициенты при t^{k-1} в равенствах

$$H(t)P(t) = H'(t) \quad \text{и} \quad E(-t)P(t) = E'(-t)\,,$$

получаем рекурсивные *формулы Ньютона* для выражения p_k через h_k и e_k соответственно:

$$p_k = kh_k - h_{k-1}p_1 - h_{k-2}p_2 - \dots - h_1 p_{k-1} \tag{26-16}$$

$$(-1)^{k-1}p_k = ke_k - e_{k-1}p_1 + e_{k-2}p_2 - \dots + (-1)^{k-1}e_1 p_{k-1}\,. \tag{26-17}$$

Индукция по k показывает, что многочлен p_k является собственным вектором инволюции ω из предл. 26.3 с собственным значением $(-1)^{k-1}$:

$$\omega(p_k) = (-1)^{k-1}p_k\,. \tag{26-18}$$

Следствие 26.5
Многочлены $p_1, p_2, \dots, p_n$ алгебраически независимы в $\mathbb{Q}[x_1, x_2, \dots, x_n]$ и любой симметрический многочлен с рациональными коэффициентами (в том числе p_m с $m > n$) однозначно записывается в виде многочлена с рациональными коэффициентами от $p_1, p_2, \dots, p_n$.

Доказательство. Из формулы (26-17) вытекает, что в пространстве многочленов $\mathbb{Q}[x_1, x_2, \dots, x_n]_{\leqslant N}$ (степень которых ограничена произвольным $N \in \mathbb{N}$) $\mathbb{Q}$-линейные оболочки всевозможных мономов $p_1^{m_1} p_2^{m_2} \cdots p_n^{m_n}$ от $p_1, p_2, \dots, p_n$ и всевозможных мономов $e_1^{m_1} e_2^{m_2} \cdots e_n^{m_n}$ от $e_1, e_2, \dots, e_n$ совпадают. Поскольку количества этих мономов при фиксированном N одинаковы, и по сл. 26.4 мономы $e_1^{m_1} e_2^{m_2} \cdots e_n^{m_n}$ линейно независимы, мономы $p_1^{m_1} p_2^{m_2} \cdots p_n^{m_n}$ также линейно независимы. □

26.4.1. Явное выражение e_k и h_k через p_k. Для любого конечного набора $\lambda = (\lambda_1, \lambda_2, \dots)$ невозрастающих неотрицательных целых чисел, состоящего из m_1 единиц, m_2 двоек, m_3 троек и т. д. (так что $\sum\limits_k k \cdot m_k = |\lambda|$), положим

$$\begin{aligned} p_\lambda &= p_{\lambda_1} p_{\lambda_2} p_{\lambda_3} \cdots = p_1^{m_1} p_2^{m_2} p_3^{m_3} \cdots \\ \varepsilon_\lambda &= (-1)^{\sum (k-1) m_k} = (-1)^{|\lambda|} (-1)^{\sum m_k} = (-1)^{\sum (\lambda_i - 1)} \\ z_\lambda &= \prod_k (m_k! \cdot k^{m_k}) \end{aligned} \tag{26-19}$$

и условимся в дальнейшем не различать между собою наборы λ, получающиеся друг из друга приписыванием справа любого количества нулей. Множество многочленов p_λ — это в точности множество всевозможных мономов от p_i. Переход от нумерации мономов диаграммами Юнга к их обычному представлению при помощи набора показателей степеней — это переход от невозрастающей последовательности $\lambda = (\lambda_1, \lambda_2, \dots)$ длин строк диаграммы к вектору $m(\lambda) = (m_1, m_2, \dots)$ i-тая компонента которого равна количеству строк длины i в λ. Отметим, что все мономы p_λ являются собственными векторами инволюции ω:

$$\omega(p_\lambda) = \varepsilon_\lambda \cdot p_\lambda \,. \tag{26-20}$$

Упражнение 26.4. Покажите, что для любой диаграммы Юнга λ число z_λ равно количеству перестановок в симметрической группе $S_{|\lambda|}$, коммутирующих с произвольным образом фиксированной перестановкой циклового типа λ, и что всего в $S_{|\lambda|}$ имеется $|\lambda|!/z_\lambda$ перестановок циклового типа λ.

Предложение 26.4

Многочлены e_k и h_k выражаются через $\mathbb{Q}$-базис p_λ по формулам:

$$h_k = \sum_{|\lambda|=k} z_\lambda^{-1} p_\lambda \tag{26-21}$$

$$e_k = \sum_{|\lambda|=k} \varepsilon_\lambda z_\lambda^{-1} p_\lambda \tag{26-22}$$

(суммирование по всем k-клеточным диаграммам Юнга).

Доказательство. Достаточно доказать формулу (26-21), формула (26-22) получается из неё применением инволюции ω из предл. 26.3. Согласно (26-15)

$$H(t) = e^{\int P(t)\,dt} = e^{\sum p_i t^i/i} = \prod e^{p_i t^i/i} = \prod_{i \geqslant 1} \sum_{m \geqslant 0} \frac{p_i^m}{i^m m!}\, t^{im}\,.$$

Коэффициент при t^k в правой части возникает при выборе в i-той перемножаемой скобке m_i-того слагаемого так, чтобы $\sum\limits_i i \cdot m_i = k$. Такие выборы биективно соответствуют диаграммам Юнга λ веса k, имеющих m_1 строк длины 1, m_2 строк длины 2 и т. д., а произведение слагаемых, отвечающих такому выбору, равно p_λ/z_λ. □

26.5. Детерминантные тождества. В этом разделе мы установим связь между многочленами Шура s_λ и полными симметрическим функциями h_k в кольце $\mathbb{Z}[x_1, x_2, \dots, x_n]$. Обозначим через $e_k^{(p)}(x)$ результат подстановки в $e_k(x)$ значения $x_p = 0$. Таким образом, $e_k^{(p)}$ — это элементарная симметрическая функция от $(n-1)$ переменных $(x_1, \dots, \widehat{x}_p, \dots, x_n)$, где «крышка» означает пропуск переменной x_p. Производящая функция для многочленов $e_k^{(p)}$ с фиксированным p имеет вид

$$E^{(p)}(t) = \sum_k e_k^{(p)}(x) \cdot t^k = \prod_{i \neq p}(1 + x_i t)\,.$$

Поэтому $H(t)E^{(p)}(-t) = (1 - x_p t)^{-1}$. Сравнивая коэффициенты при t^k в обеих частях, получаем соотношение

$$h_0 \cdot (-1)^k e_k^{(p)} + h_1 \cdot (-1)^{k-1} e_{k-1}^{(p)} + \dots + h_k \cdot e_0^{(p)} = x_p^k\,,$$

справедливое для всех целых неотрицательных k, если положить $e_j^{(p)} = 0$ при $j > n-1$. С учётом этого замечания, удобно записать предыдущую формулу как

$$\begin{aligned} x_p^k = h_{k-n+1} \cdot (-1)^{n-1} e_{n-1}^{(p)} + h_{k-n+2} \cdot (-1)^{n-2} e_{n-2}^{(p)} + \dots + h_k \cdot e_0^{(p)} = \\ = \sum_{j=1}^{n} h_{k-n+j} \cdot (-1)^{n-j} e_j^{(p)}\,. \end{aligned} \tag{26-23}$$

и воспринимать её как произведение строки $(h_{k-n+1}, h_{k-n+2}, \dots, h_k)$ длины n на столбец

$$\begin{pmatrix} (-1)^{n-1} e_{n-1}^{(p)} \\ \vdots \\ e_2^{(p)} \\ -e_1^{(p)} \\ 1 \end{pmatrix}$$

высоты n. Если организовать h-строки, отвечающие каким-нибудь n фиксированным строго убывающим значениям $k = \nu_1, \nu_2, \dots, \nu_n$ (где $\nu_1 > \nu_2 > \dots > \nu_n$) в матрицу

$$H_\nu = (h_{\nu_i - n + j}) = \begin{pmatrix} h_{\nu_1-n+1} & h_{\nu_1-n+2} & \cdots & h_{\nu_1} \\ h_{\nu_2-n+1} & h_{\nu_2-n+2} & \cdots & h_{\nu_2} \\ \vdots & \vdots & \cdots & \vdots \\ h_{\nu_n-n+1} & h_{\nu_n-n+2} & \cdots & h_{\nu_n} \end{pmatrix}$$

(где мы полагаем $h_0 = 1$ и $h_j = 0$ при $j < 0$), а все e-столбцы, отвечающие n различным значениям $p = 1,\ 2,\ \dots,\ n$, — в матрицу

$$M = \left((-1)^{n-i} e^{(j)}_{n-i}\right) = \begin{pmatrix} (-1)^{n-1} e^{(1)}_{n-1} & (-1)^{n-1} e^{(2)}_{n-i} & \cdots & (-1)^{n-1} e^{(n)}_{n-1} \\ (-1)^{n-2} e^{(1)}_{n-2} & (-1)^{n-2} e^{(2)}_{n-i} & \cdots & (-1)^{n-2} e^{(n)}_{n-2} \\ \vdots & \vdots & \cdots & \vdots \\ 1 & 1 & \cdots & 1 \end{pmatrix}$$

то формула (26-23) превратится в матричное равенство $D_\nu = H_\nu \cdot M$, где

$$D_\nu = (x_j^{\nu_i}) = \begin{pmatrix} x_1^{\nu_1} & x_2^{\nu_1} & \cdots & x_n^{\nu_1} \\ x_1^{\nu_2} & x_2^{\nu_2} & \cdots & x_n^{\nu_2} \\ \vdots & \vdots & \cdots & \vdots \\ x_1^{\nu_n} & x_2^{\nu_n} & \cdots & x_n^{\nu_n} \end{pmatrix}$$

Таким образом, для любой диаграммы Юнга ν со строго убывающими длинами строк

$$\Delta_\nu = \det D_\nu = \det H_\nu \cdot \det M\,.$$

При $\nu = \delta$ матрица H_δ верхняя унитреугольная. Поэтому $\det H_\delta = 1$ и $\det M = \det D_\delta = \Delta_\delta$. Мы получаем искомое выражение полиномов Шура через полные симметрические функции:

$$s_\lambda = \Delta_{\delta+\lambda}/\Delta_\delta = \det D_{\delta+\lambda}/\det M = \det H_{\delta+\lambda} = \det\left(h_{\lambda_i+j-i}\right) \tag{26-24}$$

Предложение 26.5 (первая формула Джамбелли)

$$s_\lambda = \det \begin{pmatrix} h_{\lambda_1} & h_{\lambda_1+1} & \ddots & h_{\lambda_1+n-1} \\ h_{\lambda_2-1} & h_{\lambda_2} & \ddots & \ddots \\ \ddots & \ddots & \ddots & h_{\lambda_{n-1}+1} \\ h_{\lambda_n-n+1} & \ddots & h_{\lambda_n-1} & h_{\lambda_n} \end{pmatrix} \tag{26-25}$$

(по главной диагонали стоят $h_{\lambda_1}, h_{\lambda_2}, \dots, h_{\lambda_n}$, и при движении вдоль строк слева направо индексы у h с каждым шагом увеличиваются на единицу). □

26.5.1. Примеры. В $\mathbb{Z}[x_1, x_2]$ получаем соотношение

$$s_{(2,1)} = \det \begin{pmatrix} h_2 & h_3 \\ 1 & h_1 \end{pmatrix} = h_1h_2 - h_3 = e_1e_2 - e_3\,.$$

При $n = 3$, т. е. в $\mathbb{Z}[x_1, x_2, x_3]$, получаем в точности то же самое разложение

$$s_{(2,1)} = s_{(2,1,0)} = \det \begin{pmatrix} h_2 & h_3 & h_4 \\ 1 & h_1 & h_2 \\ 0 & 0 & 1 \end{pmatrix} = \det \begin{pmatrix} h_2 & h_3 \\ 1 & h_1 \end{pmatrix}$$

Упражнение 26.5. Убедитесь, что выражение s_λ через h_k, полученное при числе переменных n, равном высоте диаграммы λ, сохраняется и при любом большем числе переменных.

Беря в качестве λ диаграмму из одной строки длины k, мы получаем равенство $s_{(k)} = h_k$, очевидное при $n = 1$ и по упр. 26.5 справедливое для всех n. Отметим, что при непосредственном вычислении определителей $\Delta_{\delta+(n)}$ и Δ_δ произвольного размера $n \times n$ равенство $\Delta_{\delta+(n)} = h_k \cdot \Delta_\delta$ отнюдь не очевидно.

Упражнение 26.6. Покажите, что $s_{(1^k)} = e_k$ при любом $n \geqslant k$, где $\lambda = (1^k)$ означает k строк длины 1, т. е. столбец высоты k.

26.5.2. Формула Пьери выражает произведение $s_\lambda \cdot h_k = s_\lambda \cdot s_{(k)}$ через многочлены s_μ. Для её вывода нам придётся слегка обобщить сказанное в n° 26.1. А именно, рассмотрим вместо кольца многочленов кольцо формальных степенных рядов $\mathbb{Z}[[x_1, x_2, \dots, x_n]]$, а в нём — симметрические и кососимметрические ряды (первые образуют подкольцо, вторые — модуль над этим подкольцом). То же рассуждение, что и в n° 26.1.2 показывает, что всякий кососимметричный ряд A однозначно записывается в виде бесконечной целочисленной линейной комбинации альтернированных S_n-орбит мономов

$$A = \sum_{\nu_1 > \nu_2 > \dots > \nu_n} c_\nu \cdot \Delta_\nu \tag{26-26}$$

где суммирование происходит по всем диаграммам Юнга $\nu = (\nu_1, \nu_2, \dots, \nu_n)$ из n строк строго убывающей длины, коэффициенты $c_\nu \in \mathbb{Z}$, и

$$\Delta_\nu = \sum_{g \in S_n} \operatorname{sgn}(g)\, x_{g(1)}^{\nu_1} x_{g(2)}^{\nu_2} \,\cdots\, x_{g(n)}^{\nu_n}\,.$$

Лемма 26.1

Разложение (26-26) для произведения базисного кососимметрического многочлена Δ_ν на симметрический ряд

$$H(x) = \prod_{i=1}^{n} (1 - x_i)^{-1} = \prod_{i=1}^{n} \left(1 + x_i + x_i^2 + x_i^3 + \,\cdots\right) = \sum_{k \geqslant 0} h_k(x)$$

имеет вид $\Delta_\nu \cdot H = \sum\limits_\eta \Delta_\eta$, где суммирование идёт по всем $\eta = (\eta_1, \eta_2, \dots, \eta_n)$ с

$$\eta_1 \geqslant \nu_1 > \eta_2 \geqslant \nu_2 > \cdots \eta_n \geqslant \nu_n .$$

Доказательство. Для любых n рядов $f_1(t)$, $f_2(t)$, … , $f_n(t) \in \mathbb{Z}[[t]]$ положим

$$f_1 \wedge f_2 \wedge \cdots \wedge f_n = \sum_{g \in S_n} \operatorname{sgn}(g) f_1\left(x_{g(1)}\right) f_2\left(x_{g(2)}\right) \cdots f_n\left(x_{g(n)}\right) \in \mathbb{Z}[x_1, x_2, \dots, x_n] .$$

Например, $t^{\nu_1} \wedge t^{\nu_2} \wedge \ldots \wedge t^{\nu_n} = \Delta_\nu$. Произведение $f_1 \wedge f_2 \wedge \cdots \wedge f_n$ является кососимметрическим рядом, полилинейно и кососимметрично зависящим от $f_1, f_2, \dots, f_n$. В частности, $f_1 \wedge f_2 \wedge \cdots \wedge f_n$ не изменяется при добавлении к любому из рядов любой линейной комбинации остальных. В этих обозначениях

$$\Delta_\nu \cdot H = \sum_{g \in S_n} \operatorname{sgn}(g) \prod_{i=1}^{n} x_{g(i)}^{\nu_i} \left(1 - x_{g(i)}\right)^{-1} = f_1 \wedge f_2 \wedge \cdots \wedge f_n ,$$

где $f_i(t) = x^{\nu_i}(1 - x_i t)^{-1} = t^{\nu_i} + t^{\nu_i + 1} + t^{\nu_i + 2} + \cdots$. Вычитая f_1 из всех остальных рядов, мы обрезаем их до многочленов степени $< \nu_1$. Вычитая второй из них из всех последующих, обрезаем их до многочленов степени $< \nu_2$. Действуя в таком духе, получим равенство $f_1 \wedge f_2 \wedge \cdots \wedge f_n = \widehat{f_1} \wedge \widehat{f_2} \wedge \cdots \wedge \widehat{f_n}$, в котором $\widehat{f_1} = f_1 = \sum\limits_{j \geqslant \nu_1} t^j$, а каждый следующий $\widehat{f_i} = t^{\nu_i} + t^{\nu_i + 1} + \cdots + t^{\nu_{i-1} - 1}$. В силу полилинейности $\wedge$-произведения

$$\widehat{f_1} \wedge \widehat{f_2} \wedge \cdots \wedge \widehat{f_n} = \sum_\eta t^{\eta_1} \wedge t^{\eta_2} \wedge \ldots \wedge t^{\eta_n} = \sum_\eta \Delta_\eta ,$$

где суммирование идёт по всем $\eta_1 \geqslant \nu_1 > \eta_2 \geqslant \nu_2 > \eta_3 \geqslant \nu_3 > \cdots \eta_n \geqslant \nu_n$. □

Следствие 26.6 (формула Пьери)

$$s_\lambda \cdot h_k = \sum_\mu s_\mu ,$$

где суммирование происходит по всем диаграммам μ из $\leqslant n$ строк, которые можно получить, добавляя к диаграмме λ ровно k клеток так, чтобы никакие две из них не попали в один столбец.

Доказательство. По лем. 26.1 имеем равенство $\Delta_{\delta+\lambda} \sum\limits_{k \geqslant 0} h_k = \sum\limits_\tau \Delta_{\delta+\mu}$, где суммирование происходит по всем диаграммам μ, Таким что[1]

$$\mu_1 \geqslant \lambda_1 \geqslant \mu_2 \geqslant \lambda_2 \geqslant \ldots .$$

Деля обе части на Δ_δ и беря в полученном равенстве однородную компоненту степени $|\lambda| + k$ по x, получаем требуемую формулу. □

[1]напомним (см. n° 26.1.2), что $\lambda_i = \nu_i - n + i$, $\mu_i = \eta_i - n + i$, поэтому неравенства $\eta_i \geqslant \nu_i > \eta_{i+1}$ равносильны неравенствам $\mu_i \geqslant \lambda_i \geqslant \mu_{i+1}$

Замечание 26.1. Если диаграмма λ состоит из $k < n$ строк, что отвечает значениям $\lambda_{k+1} = \lambda_{k+2} = \cdots = \lambda_n = 0$, диаграммы μ в формуле Пьери могут содержать на одну строку больше, чем в диаграмме λ. Например, при $n = 2$ получаем $s_{(2)} \cdot h_1 = s_{(2,1)} + s_{(3)}$ (откуда, между прочим, снова получается равенство $s_{(2,1)} = h_2 h_1 - h_3$ из n° 26.5.1).

26.6. Кольцо симметрических функций. Удобно думать про симметрические многочлены, не привязываясь к конкретному числу переменных, а считая, что переменных достаточно много для того, чтобы все участвующие в рассуждении функции были определены. Формализуется это следующим образом.

Условимся не различать между собою две диаграммы λ', λ'', а также два набора показателей m', m'', если они получаются друг из друга дописыванием справа любого числа нулей. Для любого набора занумерованных натуральными числами букв q_i, $i \in \mathbb{N}$, положим

$$q_\lambda = q_{\lambda_1} q_{\lambda_2} q_{\lambda_3} \cdots \quad \text{и} \quad q^m = q_1^{m_1} q_2^{m_2} q_1^{m_3} \cdots .$$

Запись $\lambda = (\lambda_1, \lambda_2, \lambda_3, \dots) = (1^{m_1}, 2^{m_2}, 3^{m_3}, \dots)$ всегда будет означать, что λ содержит m_i строк длины i для всех $i \in \mathbb{N}$. Это происходит тогда и только тогда, когда $q_\lambda = q^m$. Наконец, положим $m_\lambda = s_\lambda = 0$ всякий раз, когда число переменных меньше количества строк в диаграмме λ, и $e_\lambda = 0$, когда число переменных меньше количества столбцов в диаграмме λ.

При так соглашениях каждый из симметрических многочленов $m_\lambda(x)$, $s_\lambda(x)$, $e_\lambda(x)$, $h_\lambda(x)$ и $p_\lambda(x)$ определён для переменной $x = (x_1, x_2, \dots, x_r)$ любой размерности r, причём при $r > s$ при подстановке

$$x_{s+1} = x_{s+2} = \cdots = x_r = 0 \tag{26-27}$$

каждый из этих многочленов превращается в одноимённый многочлен от меньшего набора переменных $x = (x_1, x_2, \dots, x_s)$. Подстановка (26-27) задаёт сюрьективный гомоморфизм колец

$$\zeta_{sr} : \mathbb{Z}[x_1, x_2, \dots, x_r] \twoheadrightarrow \mathbb{Z}[x_1, x_2, \dots, x_s] . \tag{26-28}$$

Будем называть последовательность симметрических многочленов

$$f^{(n)} \in \mathbb{Z}[x_1, x_2, \dots, x_n]$$

(по одному многочлену для каждого числа переменных $n \in \mathbb{N}$) *симметрической функцией степени* d и обозначать такую функцию просто через f, если выполняются два условия:

- при всех n многочлен $f^{(n)}$ однороден степени d
- $\zeta_{rs}\left(f^{(r)}\right) = f^{(s)}$ при любых $r > s$

При этом запись $f(x_1, x_2, \dots, x_n)$ по определению означает $f^{(n)}(x_1, x_2, \dots, x_n)$, но поскольку верхний индекс у f равен числу подставляемых переменных, писать его нет смысла.

Так, последовательность мономиальных многочленов

$$(m_\lambda(x_1, x_2, \dots, x_n))_{n\in\mathbb{N}}$$

с фиксированной диаграммой λ веса $|\lambda| = d$ образует симметрическую функцию степени d, которая обозначается m_λ. Например, на наборах из одной, двух и трёх переменных кубическая симметрическая функция $m_{(2,1)}$ имеет вид

$$\begin{aligned} m_{(2,1)}(x_1) &= 0 \\ m_{(2,1)}(x_1, x_2) &= x_1^2x_2 + x_1x_2^2 \\ m_{(2,1)}(x_1, x_2, x_3) &= x_1^2x_2 + x_1x_2^2 + x_1^2x_3 + x_1x_3^2 + x_2^2x_3 + x_2x_3^2\,. \end{aligned}$$

Аналогичным образом определяются и симметрические функции s_λ, e_λ, h_λ и p_λ степени $|\lambda|$.

Симметрические функции степени d образуют $\mathbb{Z}$-модуль. Его принято обозначать Λ_d. Из сказанного в предыдущих разделах вытекает, что симметрические функции m_λ, s_λ, e_λ и h_λ, занумерованные всевозможными диаграммами Юнга веса $|\lambda| = d$, являются базисами в Λ_d, а симметрические функции p_λ составляют базис векторного пространства $\mathbb{Q} \otimes \Lambda_d$ симметрических функций с рациональными коэффициентами. Таким образом, Λ_d является свободным модулем *конечного* ранга, равного количеству диаграмм Юнга веса d. Это количество принято обозначать $p(d)$ и называть *числом разбиений* натурального числа d.

Поскольку произведение симметрических функций степеней d_1 и d_2 является симметрической функцией степени d_1d_2, прямая сумма

$$\Lambda = \bigoplus_{d\geqslant 0} \Lambda_d$$

представляет собою градуированное кольцо. Оно называется *кольцом симметрических функций*. Все доказанные выше соотношения между функциями m_λ, s_λ, e_λ, h_λ и рекурсивные выражения p_i через e_j и h_j являются тождествами в кольце Λ, а выражения h_i и e_i через p_λ — тождествами в кольце $\mathbb{Q} \otimes \Lambda$ симметрических функций с рациональными коэффициентами.

Задачи для самостоятельного решения к §26

Задача 26.1. Сумма двух из трёх комплексных корней многочлена $2x^3 - x^2 - 7x + \lambda$ равна 1. Чему равно λ?

Задача 26.2. Найдите все комплексные решения системы уравнений

$$\begin{cases} x_1 + x_2 + x_3 = 0 \\ x_1^2 + x_2^2 + x_3^2 = 0 \\ x_1^3 + x_2^3 + x_3^3 = 24\,. \end{cases}$$

Задача 26.3. Выразите через элементарные симметрические многочлены e_i следующие функции: а) $(x_1 + x_2 - x_3 - x_4)(x_1 - x_2 + x_3 - x_4)(x_1 - x_2 - x_3 + x_4)$ б) $(x_1 + x_2)(x_2 + x_3)(x_3 + x_4)(x_1 + x_3)(x_2 + x_4)(x_1 + x_4)$ в) $\sum\limits_{i \neq j \neq k \neq i} x_i(x_j + x_k)/2$ г) $\sum\limits_{i \neq j} x_i^2 x_j$

Задача 26.4. Выразите дискриминант[1] D_f кубического трёхчлена

$$f = x^3 + px + q$$

через p и q.

Задача 26.5. Пусть в зад. 26.4 $p, q \in \mathbb{R}$. Покажите, что при $D_f < 0$ у f есть ровно один вещественный корень, а при $D_f > 0$ — ровно три, и в этом случае уравнение $f = 0$ перескалированием переменной приводится к виду $4t^3 - 3t = a$ и решается в тригонометрических функциях.

Задача 26.6. Найдите все (комплексные) значения λ, при которых многочлен

$$x^4 - 4\,x + \lambda$$

имеет кратный корень.

Задача 26.7 (циркулянт). Выразите определитель матрицы, строки которой являются последовательными циклическими перестановками строки

$$(\alpha_0, \alpha_1, \ldots, \alpha_n) \in \mathbb{C}^n\,,$$

через значения полинома $f(x) = \alpha_0 x^n + \alpha_1 x^{n-1} + \cdots + \alpha_{n-1} x + \alpha_n$ на комплексных корнях n-той степени из единицы.

Задача 26.8. Вычислите дискриминант[2] n-того кругового многочлена[3] $\Phi_n(x)$. Если общий случай вызывает затруднения, решите задачу для всех $3 \leqslant n \leqslant 7$.

---

[1] *дискриминантом* приведённого многочлена $f(x) = \prod\limits_i (x - x_i)$ называется произведение квадратов разностей всех его корней $D_f = \Delta_0^2 = \prod\limits_{i<j} (x_i - x_j)^2$, выраженное через коэффициенты многочлена, ср. с зад. 10.17

[2] см. зад. 26.4

[3] напомним, что n-тый круговой многочлен — это приведённый многочлен, корнями которого являются все примитивные комплексные корни степени n из единицы, см. n° 2.3.4 и зад. 4.22

Задача 26.9. Многочлен $x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n$ имеет корни $x_1, x_2, \dots, x_n$. Верно ли, что любой симметрический многочлен от x_2, … , x_n переписывается в виде многочлена от x_1 ?

Задача 26.10. Обозначим через $\zeta \in \mathbb{C}$ какой-нибудь первообразный корень m-той степени из единицы. Для каждого $a \in \mathbb{C}$ раскройте скобки и приведите подобные в $\prod\limits_{\nu=1}^{m}(a - \zeta^{\nu-1}x)$, покажите, что $\forall\, f \in \mathbb{C}[x]\ \exists\, h \in \mathbb{C}[x]$: $\prod\limits_{\nu=1}^{m} f(\zeta^{\nu-1}x) = h(x^m)$ и выразите корни многочлена h через корни многочлена f.

Задача 26.11. Найдите в $\mathbb{C}[x]$ многочлен 4-й степени, корнями которого являются
а) квадраты всех комплексных корней многочлена $x^4 + 2\,x^3 - x + 3$
б) кубы всех комплексных корней многочлена $x^4 - x - 1$.

Задача 26.12. Выразите а) $s_{(1^n)}$ через e_ν б) $s_{(n)}$ через h_ν .

Задача 26.13. Представьте а) $s_{(1)}^2$ б) $s_{(1,1)} \cdot s_{(2)}$ в виде целочисленных линейных комбинаций многочленов s_λ.

Задача 26.14. Пусть $h_0 = e_0 = 1$ и $h_k = e_k = 0$ при $k < 0$. Покажите, что матрицы (h_{i-j}) и $\left((-1)^{i-j}e_{i-j}\right)$ обратны друг другу и получите отсюда соотношение $\det\left(h_{\lambda_i+j-i}\right) = \det\left(e_{\lambda_i^t+j-i}\right)$ на дополнительные миноры этих матриц.

§27. Исчисление массивов, таблиц и диаграмм

27.1. Массивы и элементарные операции над ними. Зафиксируем два конечных упорядоченных множества из n и m элементов:

$$I = \{1, 2, \dots, n\}, \quad J = \{1, 2, \dots, m\} \tag{27-1}$$

и будем рассматривать прямоугольные таблицы из n столбцов и m строк, занумерованных элементами I и J соответственно. Такую таблицу a мы будем называть *массивом* и размещать в *первом* квадранте декартовой системы координат так, чтобы элементы из I росли слева направо по горизонтальной оси, а элементы из J росли снизу вверх по вертикальной оси. Содержимое $a(i,j)$ клетки с координатами (i,j) у нас всегда будет целым неотрицательным числом, которое стоит воспринимать как «количество» или «массу». Весь массив удобно представлять себе как набор шариков одинаковой массы, наделенных двумя группами признаков и в соответствии с этим разложенных по ячейкам массива. Мы никогда не будем вычислять с числами $a(i,j)$, но будем перекладывать шарики из ячейки в ячейку, меняя тем самым их принадлежность к тому или иному признаку каждой из двух групп.

С массивом a связан *столбцовый вес* (или *I-вес*)

$$w^I = \Big(\sum_j a(1,j), \sum_j a(2,j), \dots, \sum_j a(n,j) \Big) \in \mathbb{Z}^n_{\geqslant 0}, \tag{27-2}$$

представляющий собой n-мерный целочисленный вектор, i-тая координата которого равна общему количеству шариков в i-том столбце. Аналогично определяется *строчный вес* (или *J-вес*)

$$w^J = \Big(\sum_i a(i,1), \sum_i a(i,2), \dots, \sum_i a(i,m) \Big) \in \mathbb{Z}^m_{\geqslant 0}. \tag{27-3}$$

Массивы можно транспонировать относительно диагонали $i = j$:

$$a \longmapsto a^t \,:\, a^t(i,j) = a(j,i). \tag{27-4}$$

На множестве $\mathscr{M}$ всех массивов действуют четыре набора *элементарных операций*

$$D_j, \quad U_j, \quad L_i, \quad R_i, \quad \text{где } 1 \leqslant i \leqslant n-1,\ 1 \leqslant j \leqslant m-1.$$

При применении любой из этих операций к данному массиву $a \in \mathscr{M}$ массив a либо никак не меняется, либо ровно один его шарик перемещается ровно на одну клетку вниз (Down), вверх (Up), влево (Left) или вправо (Right) в соответствии с обозначением для операции.

27.1.1. Вертикальные операции D_j и U_j перемещают шар по вертикали в пределах соседних j-той и $(j+1)$-ой строки. Чтобы узнать, какой именно шар следует передвинуть (или убедиться в том, что такого шара нет), следует вначале установить между j-той и $(j+1)$-ой строкой *устойчивое паросочетание*[1]. Делается это следующим образом.

Будем последовательно перебирать шарики в $(j+1)$-ой строке двигаясь слева направо и либо назначать им партнёров в j-той строке, либо объявлять *свободными*. Пусть очередной шарик $ш$ лежит в клетке $(i, j+1)$. Его партнёром называем *самый правый* шар из тех, что лежат в строке j *строго левее* i-того столбца и ещё не назначены никому партнёрами. Если таких шаров нет, шар $ш$ объявляется свободным. После того, как все шары $(j+1)$-ой строки будут разделены на свободные и имеющие партнёров, все шары j-той строки, не являющиеся ни чьими партнёрами, также объявляются свободными. Вот пример такого паросочетания (в скобках указано число свободных шаров):

$$\begin{array}{ccccc} 2\,(2) & 2\,(0) & 4\,(1) & 3\,(0) & 3\,(0) \\ \\ 3\,(0) & 2\,(0) & 6\,(1) & 1\,(0) & 3\,(3) \end{array} \tag{27-5}$$

По определению, операция D_j опускает на одну клетку вниз самый правый свободный шар $(j+1)$-ой строки или ничего не делает, если свободных шаров в $(j+1)$-ой строчке нет. Операция U_j поднимает на одну клетку вверх самый левый свободный шар j-той строки или ничего не делает, если в j-ой строке нет свободных шаров. Так, в примере (27-5) операция D_j (соотв. U_j) опускает вниз (соотв. поднимает вверх) верхний (соотв. нижний) свободный шар в третьей колонке.

Если операция изменяет массив, мы будем говорить, что она действует на этот массив *эффективно*. Из конструкции устойчивого паросочетания ясно, что все свободные шары j-той строки лежат нестрого правее свободных шаров $(j+1)$-ой строки. Поэтому, когда операция D_j действует на массив a эффективно, опущенный ею шар становится самым левым свободным шаром j-той строки в устойчивом паросочетании между преобразованными строками. Стало быть, операция U_j, применённая к массиву $D_j a$ поднимет этот опущенный шар назад, т. е. $U_j D_j a = a$ всякий раз, когда D_j действует на a эффективно. Аналогично, если U_j действует эффективно, то $D_j U_j a = a$.

Говоря неформально, набор вертикальных операций D, U образует структуру, близкую к групповой — исходный массив a однозначно восстанавливается из результата применения к нему слова $D = D_{j_1} \cdots D_{j_k}$ по формуле

$$a = U_{j_k} \cdots U_{j_1} \left(D_{j_1} \cdots D_{j_k}(a) \right)$$

[1]по-английски: *stable matching*

при условии, что каждая буква D_j действует эффективно. Мы будем называть такие D-слова *a-эффективными* (или просто *эффективными*, если понятно, о каком a речь).

27.1.2. Горизонтальные операции L_{i+1} и R_i определяются симметричным образом: они действуют в i-м и $(i+1)$-м столбцах и превращаются в операции D и U при транспонировании массива, т. е.

$$L_i(a) = \big(D_i(a^t)\big)^t \quad \text{и} \quad R_i(a) = \big(U_i(a^t)\big)^t \ .$$

Упражнение 27.1. Переговорите это определение явно: скажите, как установить устойчивое паросочетание между i-тым и $(i+1)$-м столбцом, и какой шар будут перемещать R_i и L_i .

Отметим, что операции D, L сохраняют столбцовый вес, а операции R, L — строчный.

Лемма 27.1 (лемма о коммутировании)
Каждый горизонтальный оператор U_i, R_i перестановочен с каждым вертикальным D_j, L_j.

Доказательство. Мы покажем, что D_j и U_j перестановочны с L_i — остальные случаи разбираются аналогично. Пусть действие операции L_i заключается в перемещении шара $ш$ на одну клетку влево. Достаточно убедиться, что эта процедура не изменяет устойчивого паросочетания между $(j+1)$-ой и j-той строкой в том смысле, что после применения L_i связанными в пары будут в точности те же самые шары, что и до применения. Это очевидно, когда $ш$ лежит вне $(j+1)$-ой и j-той строк. Остаются два случая, представленные на рис. 27◇1.

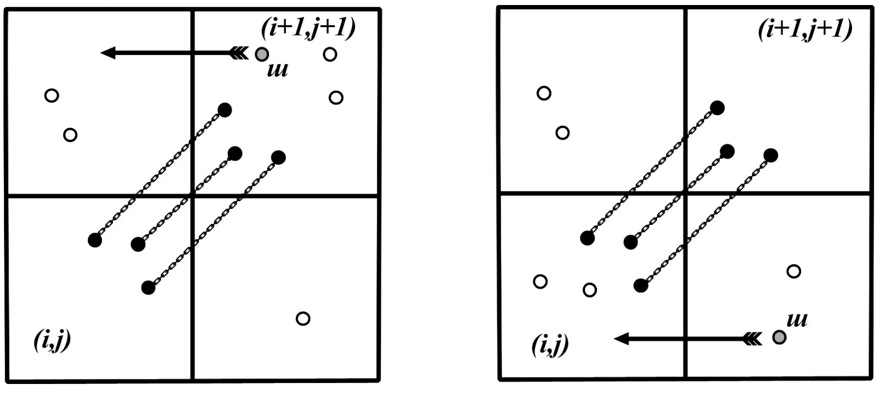


Рис. 27◇1. Горизонтальная операция L_i не меняет устойчивого вертикального паросочетания.

Пусть $ш$ лежит в $(j+1)$-ой строчке, т. е. в клетке $(i+1, j+1)$ (левая картинка на рис. 27◇1). Тогда все шары из клетки (i, j) имеют партнёров в клетке

$(i+1, j+1)$, иначе шар $ш$ получил бы себе партнёра в клетке (i, j) в паросочетании между i-тым и $(i+1)$-м столбцом. Поэтому, если в строчном паросочетании у шара $ш$ был партнёр, то он был строго левее клетки (i, j), а значит и останется партнёром после перемещения $ш$ на клетку влево. А если партнёра у $ш$ не было, то он и не появится. Таким образом, при перемещении $ш$ строчное паросочетание не изменяется.

Пусть $ш$ лежит в j-той строчке (правая картинка на рис. 27◇1). Поскольку он является самым верхним свободным шаром в столбцовом паросочетании, все шары из клетки $(i+1, j+1)$ имеют партнёров в клетке (i, j). Но тогда и в строчном паросочетании все шары из $(i+1, j+1)$-той клетки получат партнёров в клетке (i, j). Поэтому перемещение шара $ш$ на клетку влево и в этом случае не изменит ни его статуса, ни партнёра (если таковой был). □

Следствие 27.1

Слово H, составленное из горизонтальных операций, тогда и только тогда эффективно действует на a, когда оно эффективно действует на любой массив, получающийся из a вертикальными операциями. Аналогично, слово V, составленное из вертикальных операций, тогда и только тогда эффективно действует на a, когда оно эффективно действует на любой массив, получающийся из a горизонтальными операциями.

Доказательство. Мы докажем первое утверждение, оставив второе читателю. Достаточно проверить, что для любых i, j операция L_i эффективно действует на a тогда и только тогда, когда она эффективно действует на $D_j a$, и только тогда, когда она эффективно действует на $U_j a$.

Если $L_i a = a$, то $L_i D_j a = D_j L_i a = D_j a$, и $L_i U_j a = U_j L_i a = U_j a$. Наоборот, если $L_i a \neq a$, то i-тая компонента столбцового веса $w^I(L_i a)$ будет строго больше i-той компоненты $w^I(a)$, а так как D_j и U_j не меняют столбцовый вес, то $L_i D_j a = D_j L_i a \neq D_j a$, и $L_i U_j a = U_j L_i a \neq U_j a$. □

27.2. Уплотнение массивов. Будем называть массив D-, L-, R- или U- плотным (т. е. плотным вниз, влево, вправо или вверх), если все элементарные операции соответствующего типа действуют на него тождественно.

Очевидно, что применение к данному массиву достаточно большого числа операций одного из типов в конце концов приведёт к плотному в соответствующую сторону массиву. Такое уплотнение, как правило, можно производить многими разными способами.

В качестве примера, на рис. 27◇2 ниже показаны два пути уплотнения достаточно случайно взятого массива 3×2. Обратите внимание, что результат уплотнения оказался не зависящим от способа уплотнения. Мы докажем это фундаментальное свойство уплотнений в предл. 27.1, сделав в начале одно важное замечание о связи массивов с диаграммами Юнга.

27.2.1. Биплотные массивы и диаграммы Юнга. Из сл. 27.1 вытекает, что при действии вертикальных операций на плотный влево или вправо массив этот массив будет оставаться плотным в ту же сторону. То же самое справедливо для действия горизонтальных операций на массив, который плотен вниз или вверх. Поэтому любой массив можно сделать плотным одновременно в каком-нибудь вертикальном и в каком-нибудь горизонтальном направлении. Мы будем называть такие массивы DL-плотными, DR-плотными, и т. п.

В дальнейшем мы будем заниматься в основном DL-уплотнениями, поэтому условимся называть *биплотными* массивы, которые плотны одновременно *вниз* и *влево*. Очевидно, что все шары в биплотном массиве лежат лишь в клетках главной диагонали $i = j$, причём их количества нестрого убывают с ростом i. Тем самым, столбцовый вес биплотного массива равен строчному и представляет собой диаграмму Юнга $\lambda = w^I(b) = w^J(b)$, т. е. биплотные массивы b взаимно однозначно соответствуют диаграммам Юнга[1]. Диаграмма Юнга, отвечающая биплотному массиву, который получается DU-уплотнением данного массива a, называется *формой* массива a и обозначается $\varPhi(a)$. Докажем теперь, что это понятие корректно.

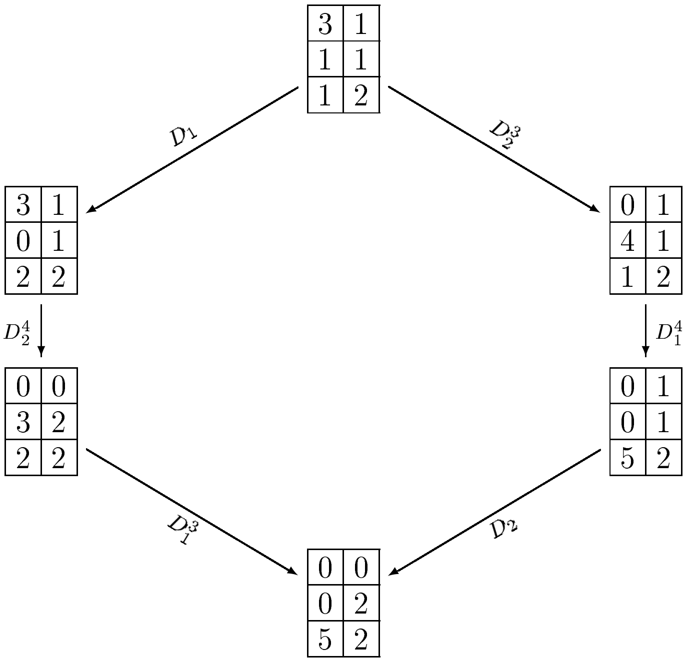


Рис. 27◇2. Два пути уплотнения вниз

Предложение 27.1

Результат D-, L-, R- или U- уплотнения не зависит от выбора последовательности уплотняющих операций.

[1]здесь и далее в этом параграфе мы отождествляем между собою две конечных последовательности неотрицательных целых чисел, получающиеся одна из другой приписыванием справа любого числа нулей; например, мы считаем равными диаграммы $(2,1,1)$ и $(2,1,1,0,0,0)$

Доказательство. Мы рассмотрим только случай D-уплотнения. Если массив a плотен влево, то результат его D-уплотнения — это биплотный массив, отвечающий диаграмме Юнга $w^I(a)$. Поскольку $w^I(a)$ не меняется при вертикальных уплотняющих операциях, результат D-уплотнения L-плотного массива не зависит от способа уплотнения. Пусть теперь a произволен. Зафиксируем какое-нибудь слово $L = L_{i_1}L_{i_2}\,\dots\,L_{i_k}$, эффективно уплотняющее a влево до массива $a' = La$. Тогда для любого слова $D = D_{j_1}D_{j_2}\,\dots\,D_{j_k}$, такого что Da плотен вниз, действие L на Da тоже будет эффективным, а массив $LDa = DLa$ будет биплотен (поскольку применение L сохраняет свойство массива Da быть плотным вниз, а применение D сохраняет свойство массива La быть плотным влево). Таким образом, мы можем записать Da как $L^{-1}DLa$. Так как массив DLa, по уже доказанному, не зависит от выбора уплотняющего слова D (ибо DLa есть D-уплотнение L-плотного массива La), массив $Da = L^{-1}DLa$ тоже не зависит от выбора D. □

27.2.2. Плотные массивы и таблицы Юнга. Из любого массива высоты m и ширины n можно изготовить m слов (по одному слову из каждой строки массива), записанных алфавитом $\{1, 2, \dots, n\}$. Делается это при помощи процедуры, которая называется *строчной развёрткой* массива и состоит в следующем.

Интерпретируем все шарики массива как буквы, равные номеру того столбца, где стоит шарик. После этого пройдём по каждой строке слева направо, выписывая подряд все встречающиеся нам буквы. В результате j-тая строка массива развернётся в слово

$$\underbrace{11\dots1}_{a(1,j)}\underbrace{22\dots2}_{a(2,j)}\,\cdots\cdots\cdots\,\underbrace{nn\dots n}_{a(n,j)}\,.$$

Получающиеся m слов запишем друг под другом в столбик, *сверху вниз*[1], выровняв их по левому краю. Например:

$$\begin{array}{|c|c|c|c|c|}\hline 0&0&0&0&1\\\hline 0&0&1&1&0\\\hline 0&4&0&0&0\\\hline 3&1&0&0&1\\\hline\end{array}\;\rightsquigarrow\;\begin{array}{ccccc} 1&1&1&2&5\\ 2&2&2&2&\\ 3&4&&&\\ 5&&&&\end{array}\;,\qquad \begin{array}{|c|c|c|c|c|}\hline 2&0&3&0&1\\\hline 0&2&1&1&0\\\hline 0&1&0&2&3\\\hline 1&1&2&0&1\\\hline\end{array}\;\rightsquigarrow\;\begin{array}{cccccc} 1&1&3&3&3&5\\ 2&2&3&4&&\\ 2&4&4&5&5&5\\ 1&2&3&3&5&\end{array}\,.$$

Очевидно, что буквы в каждом слове строчной развёртки нестрого возрастают.

Условие плотности массива вниз (как в левом примере выше) означает, что под каждой буквой «i» в j-том слове (т. е. под шариком, пришедшим из клетки $a(i,j)$) стоит строго большая, чем «i», буква $(j+1)$-го слова (партнёр этого шарика при устойчивом паросочетании между j-той и $(j+1)$-ой строками массива). Следовательно, длины слов строчной развёртки плотного вниз массива нестрого убывают сверху вниз, т. е. образуют диаграмму Юнга, а буквы

[1] таким образом из нижней строки массива получается верхнее слово и т. д.

$\{1, 2, \ldots, n\}$ заполняют эту диаграмму нестрого возрастая по строкам и *строго* возрастая по столбцам. Такие заполнения данной диаграммы λ называются *таблицами Юнга* формы λ на алфавите $I = \{1, 2, \ldots, n\}$. Мы доказали следующий комбинаторный факт:

Лемма 27.2
Строчная развёртка устанавливает биекцию между плотными вниз массивами размера $m \times n$ и таблицами Юнга на алфавите $\{1, 2, \ldots, n\}$, состоящими из $\leqslant m$ строк. □

Упражнение 27.2. Покажите, что массив $a = \big(a(i,j)\big)$ плотен вниз тогда и только тогда, когда для всех $i \in I$ и $j \in J$ выполняются неравенства:

$$a(1,j+1) + a(2,j+1) + \cdots + a(i,j+1) \leqslant a(1,j) + a(2,j) + \cdots + a(i-1,j)\,,$$

и напишите аналогичные неравенства, эквивалентные L-, R- и U- плотности массива a.

27.2.3. Плотные массивы и тексты Ямануч. L-плотность массива a можно воспринимать как D-плотность транспонированного массива a^t и формулировать в терминах столбцовой развёртки: плотные влево массивы биективно соответствуют таблицам Юнга из $\leqslant n$ строк в алфавите J.

Однако часто оказывается полезным характеризация L-плотности в терминах строчной развёртки. Для этого будем читать слова *строчной* развёртки L-плотного массива *a справа налево* одно за другим, сверху вниз. Условие плотности влево означает тогда, что в любом начальном куске получающейся последовательности букв единиц будет не меньше, чем двоек, двоек — не меньше, чем троек, и т. д. для всех пар последовательных букв «i» и «$(i+1)$» из I. В комбинаторике текст с таким свойством называется *текстом Ямануч*. Например, левая из двух строчных развёрток

$$\begin{array}{|c|c|c|}\hline 1 \\ \cline{1-1} 1 & 2 \\ \cline{1-2} 1 & 1 & 2 \\ \hline 3 & 3 \\ \cline{1-2}\end{array}\quad,\qquad \begin{array}{|c|c|c|c|}\hline 1 & 1 & 1 & 1 \\ \hline 2 & 2 & 2 \\ \cline{1-3} 2 & 3 & 3 \\ \cline{1-3} 1 & 2 \\ \cline{1-2}\end{array}$$

является текстом Ямануч, а правая — нет. Итак, нами установлена

Лемма 27.3
Строчная развёртка устанавливает биекцию между плотными влево массивами размера $m \times n$ и текстами Ямануч из $\leqslant m$ слов на алфавите $\{1, 2, \ldots, n\}$. □

27.2.4. Послойное произведение. Напомним одну конструкцию из теории множеств. Если заданы два отображения множеств: $X \xrightarrow{\varphi} Z$ и $Y \xrightarrow{\psi} Z$, то дизъюнктное объединение прямых произведений слоёв этих отображений над точками $z \in Z$ обозначается

$$X \underset{Z}{\times} Y \overset{\text{def}}{=} \bigsqcup_{z \in Z} \varphi^{-1}(z) \times \psi^{-1}(z)$$

и называется *послойным* (или *расслоенным*) произведением множеств X и Y над Z.

Упражнение 27.3. Покажите, что коммутативная диаграмма отображений множеств

$$\begin{tikzcd}
& X \underset{Z}{\times} Y \arrow[dl, "\pi_X"'] \arrow[dr, "\pi_Y"] & \\
X \arrow[dr, "\varphi"'] & & Y \arrow[dl, "\psi"] \\
& Z &
\end{tikzcd} \tag{27-6}$$

(в которой $\pi_X : (x,y) \mapsto x$ и $\pi_Y : (x,y) \mapsto y$) универсальна в том смысле, что для любого другого коммутативного квадрата

$$\begin{tikzcd}
& M \arrow[dl, "\xi"'] \arrow[dr, "\eta"] & \\
X \arrow[dr, "\varphi"'] & & Y \arrow[dl, "\psi"] \\
& Z &
\end{tikzcd}$$

имеется единственное отображение $M \xrightarrow{\alpha} X \underset{Z}{\times} Y$, такое что $\xi = \pi_X \circ \alpha$, $\eta = \pi_Y \circ \alpha$, и убедитесь, что это свойство определяет множество M и квадрат[1] (27-6) однозначно с точностью до единственного изоморфизма, перестановочного со всеми стрелками квадрата (27-6) .

Теорема 27.1

Множество всех массивов $\mathscr{M}$ представляет собою расслоенное произведение $\mathscr{M} = \mathscr{L} \underset{\mathscr{B}}{\times} \mathscr{D}$ множества плотных влево массивов $\mathscr{L}$ на множество плотных вниз массивов $\mathscr{D}$ над множеством биплотных массивов $\mathscr{B}$, причём диаграмма

$$\begin{tikzcd}
& \mathscr{M} \arrow[dl, "L"'] \arrow[dr, "D"] & \\
\mathscr{L} \arrow[dr, "D"'] & & \mathscr{D} \arrow[dl, "L"] \\
& \mathscr{B} &
\end{tikzcd}$$

(в которой стрелки L и D переводят массив в его уплотнения влево и вниз соответственно) коммутативна и представляет собою универсальный декартов квадрат (27-6).

[1] он называется *декартовым квадратом*

Доказательство. По предл. 27.1 стрелки L и D корректно определены и перестановочны друг с другом. Мы должны показать, что отображение

$$\mathscr{M} \longrightarrow \mathscr{L} \underset{\mathscr{B}}{\times} \mathscr{D}\,,$$

сопоставляющее массиву a пару (La, Da) со свойством $DLa = LDa \in \mathscr{B}$ взаимно однозначно.

Инъективность. Пусть массивы a и a' таковы, что $La = La'$ и $Da = Da'$. Выберем для $Da = Da'$ эффективное уплотняющее влево слово Λ. Тогда оно эффективно действует и на a, и на a'. Получаем: $a = \Lambda^{-1}La = \Lambda^{-1}La' = a'$.

Сюрьективность. Для любой пары массивов (a_ℓ, a_d), в которой a_ℓ плотен влево, a_d плотен вниз, и $Da_\ell = La_d$, рассмотрим слово Λ, эффективно уплотняющее a_d влево до La_d. Обратное слово Λ^{-1} эффективно действует на La_d, а значит, и на a_ℓ. Массив $a = \Lambda^{-1}a_\ell$ таков, что $La = a_\ell$, и $Da = D\Lambda^{-1}a_\ell = \Lambda^{-1}Da_\ell = \Lambda^{-1}La_d = a_d$. □

27.2.5. Пример: графики отображений и стандартные таблицы. График отображения множеств $I \xrightarrow{a} J$ — это массив, в каждом столбце которого имеется ровно один шарик. По теор. 27.1 такие массивы взаимно однозначно параметризуются парами (a_ℓ, a_d) в которой a_ℓ плотен влево, a_d плотен вниз, причём оба этих массива имеют одинаковую форму $Da_\ell = La_d$, и $w^I(a_d) = (1, 1, \ldots, 1)$. Каждая такая пара, согласно n° 27.2.2, является собою следующий набор данных: диаграмма Юнга $\lambda = DLa = LDa$ веса $|\lambda| = n$ (форма массива a), таблица Юнга формы λ на алфавите J (строчная развёртка транспонированного L-уплотнения a_ℓ^t) и таблица Юнга формы λ на алфавите I, в которой каждая буква используется ровно один раз (строчная развёртка D-уплотнения a_d).

Таблицы формы λ заполненные без повторений числами от 1 до $|\lambda|$ называются *стандартными таблицами* формы λ. Число стандартных таблиц формы λ принято обозначать через d_λ, а число всех таблиц формы λ на m-буквенном алфавите — через $d_\lambda(m)$.

Поскольку всего имеется m^n отображений $I \longrightarrow J$, мы получаем соотношение

$$\sum_\lambda d_\lambda \cdot d_\lambda(m) = m^n\,, \tag{27-7}$$

где суммирование идёт по всем n-клеточным диаграммам Юнга и числа $d_\lambda(m)$ отличны от нуля только для диаграмм из $\leqslant m$ строк.

Если положить $\#J = \#I = n$, и ограничиться только биективными отображениями $I \xrightarrow{\sim} J$, то эта же конструкция даст биекцию между $n!$ элементами симметрической группы S_n и парами стандартных таблиц одинаковой формы веса n, т. е. равенство

$$\sum_\lambda d_\lambda^2 = n!\,, \tag{27-8}$$

где сумма идёт о всем n-клеточным диаграммам. Эта последняя биекция взаимно однозначно переводит инволютивные перестановки[1] $\sigma \in S_n$ в самосопряжённые массивы $a = a^t$, которым в теореме о биекции отвечают пары одинаковых стандартных таблиц. Поэтому

$$\sum_{\lambda} d_\lambda = \#\{\sigma \in S_n \mid \sigma^2 = 1\}\,. \tag{27-9}$$

27.3. Действие симметрической группы на DU-множествах. Будем называть *DU-множеством* всякое множество массивов, которое переводится в себя вертикальными операциями D и U. Гомоморфизмы DU-множеств — это отображения, перестановочные с действием операций D и U.

DU-множество, на котором операции D и U действуют транзитивно, будем называть *DU-орбитой*. DU-орбиты взаимно однозначно соответствуют плотным вниз массивам. Орбита O такого массива a_d состоит из всевозможных массивов, которые можно получить из a_d эффективными U-словами. Мы будем называть a_d *нижним концом* орбиты O.

Лемма 27.4
Объединения, пересечения и разности DU-множеств также являются DU-множествами. В частности, всякое DU-множество распадается в дизъюнктное объединение DU-орбит.

Доказательство. Не очевидно, разве что, утверждение про разности. Пусть A' и A'' DU-инвариантны и $a' \in A' \smallsetminus A''$. Если $D_j a' \in A''$, то D_j действует эффективно, и тогда $a' = U_j D_j a'$ тоже лежит в A''. □

27.3.1. Стандартные орбиты. DU-орбиты O_λ биплотных массивов λ называются *стандартными*. Например, при $m = 3$ стандартная орбита $O_{(2,1)}$, отвечающая диаграмме – таблице – массиву

$$\begin{array}{|c|c|}\hline & \\ \hline & \multicolumn{1}{c}{} \\ \cline{1-1} \end{array} \quad - \quad \begin{array}{|c|c|}\hline 1 & 1 \\ \hline 2 & \multicolumn{1}{c}{} \\ \cline{1-1} \end{array} \quad - \quad \begin{array}{|c|c|}\hline 0 & 0 \\ \hline 0 & 1 \\ \hline 2 & 0 \\ \hline \end{array}$$

состоит из восьми массивов, представленных на рис. 27◇3.

Из теоремы о биекции вытекает, что уплотнение влево задаёт изоморфизм любой DU-орбиты O со стандартной орбитой O_λ, нижний конец которой является биуплотнением нижнего конца орбиты O. Мы будем называть λ *типом* орбиты O. Количество орбит типа λ в данном DU-множестве M равно количеству плотных вниз массивов строчного веса λ, имеющихся в M.

[1] т.е. такие, что $\sigma^2 = 1$

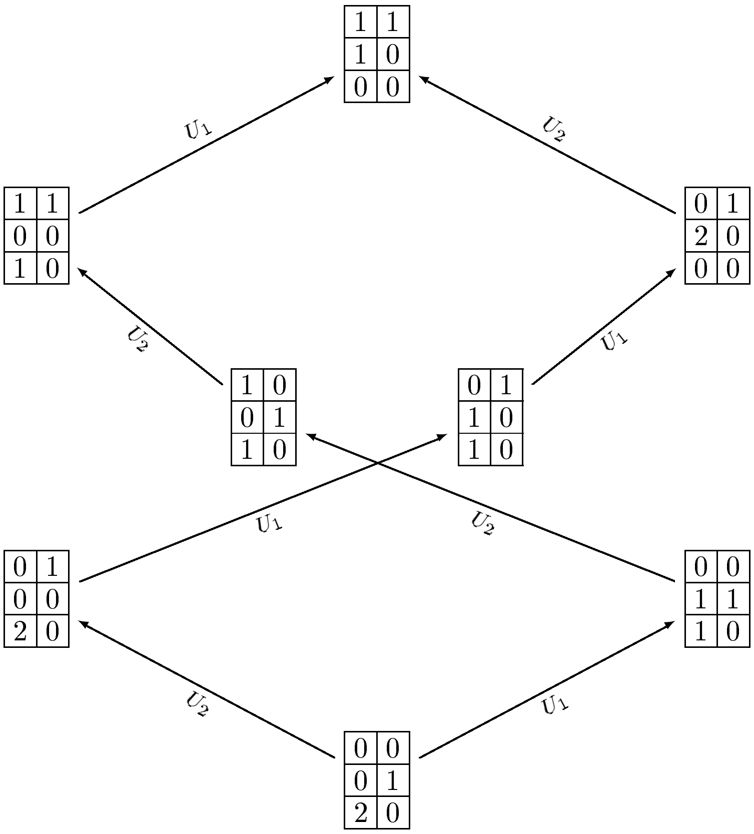


Рис. 27◇3. Стандартная DU-орбита $O_{(2,1)}$.

27.3.2. Действие симметрической группы $S_m = \mathrm{Aut}\,(J)$. На любом DU-множестве массивов M имеется действие элементарных транспозиций $\sigma_j = (j, j+1)$, порождающих симметрическую группу S_m, переставляющую строки массива. Оно определяется следующим образом.

Пусть в j-той и $(j+1)$-ой строках после установления между ними устойчивого паросочетания образовалось, соответственно, s_j и s_{j+1} свободных шаров. Положим

$$\sigma_j = D_j^{s_{j+1}-s_j} = U_j^{s_j-s_{j+1}} \,. \tag{27-10}$$

Подробнее эту процедуру можно описать так. Свернём массив в вертикальный цилиндр, приклеив правую границу n-того столбца к левой границе первого, и продолжим устойчивое паросочетание по кругу, т. е. назначим в пару самому правому нижнему свободному шару самый левый свободный верхний и т. д. В результате останется ровно $|s_{j+1} - s_j|$ свободных шаров и все они будут располагаться или только в верхней или только в нижней строке — там где их вначале было больше. Операция σ_j просто передвигает их по вертикали в другую строку (или ничего не делает, если $s_j = s_{j+1}$). В частности, действие σ_j на строчный вес w^J состоит в перестановке j-той и $(j+1)$-ой координаты.

Из предыдущего описания видно, что $\sigma_j^2 = \mathrm{Id}$, а также, что σ_j *коммутирует с циклическими перестановками столбцов*. Очевидно также, что σ_j перестановочна с горизонтальными операциями R, L и со всеми σ_k с $|k-j| \geqslant 2$.

Таким образом, для того чтобы действие σ_j непротиворечиво продолжалось на всю симметрическую группу S_m остаётся проверить выполнение *уравнения треугольника*

$$\sigma_j \sigma_{j+1} \sigma_j = \sigma_{j+1} \sigma_j \sigma_{j+1} \,.$$

Это достаточно сделать для трёхстрочного массива. Пользуясь уплотнениями влево L и циклическими перестановками столбцов C мы редуцируем любой трёхстрочный массив в одностолбцовому:

$$\begin{array}{|c|}\hline * \; * \; * \\ \hline * \; * \; * \\ \hline * \; * \; * \\ \hline\end{array} \overset{L}{\longmapsto} \begin{array}{|c|c|c|}\hline a & b & c \\ \hline d & e & 0 \\ \hline f & 0 & 0 \\ \hline\end{array} \overset{C}{\longmapsto} \begin{array}{|c|c|c|}\hline b & c & a \\ \hline e & 0 & d \\ \hline 0 & 0 & f \\ \hline\end{array} \overset{L}{\longmapsto} \begin{array}{|c|c|c|}\hline g & h & 0 \\ \hline k & 0 & 0 \\ \hline f & 0 & 0 \\ \hline\end{array} \overset{C}{\longmapsto} \begin{array}{|c|c|}\hline h & g \\ \hline 0 & k \\ \hline 0 & f \\ \hline\end{array} \overset{L}{\longmapsto} \begin{array}{|c|c|}\hline \ell & 0 \\ \hline k & 0 \\ \hline f & 0 \\ \hline\end{array}$$

для которого действие σ_j просто переставляет строки, и потому удовлетворяет соотношению треугольника.

27.4. Полиномы Шура. Будем интерпретировать все шарики j-той строки как переменные x_j и сопоставим каждому массиву a моном, получающийся перемножением всех шариков массива:

$$x^a = x_1^{w_1^J(a)} x_2^{w_2^J(a)} \cdots x_m^{w_m^J(a)}$$

(показатель у x_j равен j-той координате строчного веса $w^J(A)$). Суммируя мономы x^a по всем массивам из произвольного DU-множества M, мы получаем многочлен

$$s_M(x) = \sum_{a \in M} x^a \in \Bbbk[x_1, x_2, \dots, x_m] \,,$$

который называется *многочленом Шура* DU-множества M. Поскольку симметрическая группа S_m переставляет координаты весового вектора, она действует на мономы x^a перестановками переменных. Таким образом, все многочлены Шура являются симметрическими.

Поскольку каждое DU-множество M является объединением непересекающихся орбит, а всякая орбита изоморфна стандартной орбите O_λ, произвольный полином Шура является линейной комбинацией (с неотрицательными целыми коэффициентами) *стандартных* многочленов Шура $s_\lambda(x)$, отвечающих биплотным массивам (диаграммам Юнга) λ:

$$s_M(x) = \sum_{\lambda \in \Phi(M)} c_M^\lambda \cdot s_\lambda(x) \,. \tag{27-11}$$

Суммирование в этой формуле происходит по всем формам λ массивов из M, и коэффициент c_M^λ равен числу DU-орбит, изоморфных O_λ, т. е. количеству всех плотных вниз массивов J-веса λ в M.

Согласно n° 27.2.2, элементы стандартной орбиты O_λ суть всевозможные L-плотные массивы формы λ, и столбцовая развёртка устанавливает биекцию между такими массивами и таблицами Юнга формы λ в алфавите

$$\{x_1, x_2, \dots, x_m\}\,.$$

Таким образом, стандартный полином Шура имеет вид

$$s_\lambda(x) = \sum_\eta K_{\lambda,\eta} \cdot x^\eta = \sum_\eta K_{\lambda,\eta} \cdot x_1^{\eta_1} x_2^{\eta_2} \,\cdots\, x_m^{\eta_m}\;, \tag{27-12}$$

где $\eta \in \mathbb{Z}^m_{\geqslant 0}$ пробегает m-мерные целочисленные векторы с неотрицательными координатами, а коэффициент $K_{\lambda,\eta}$ равен числу таблиц формы λ, заполненных η_1 единицами, η_2 двойками и т. д. Мы будем говорить, что такая таблица имеет *состав* η.

Например, при $m = 3$ из представленной на рис. 27◇3 схемы получаем

$$s_{(2,1)}(x_1, x_2, x_3) = x_1^2 x_2 + x_1^2 x_3 + x_1 x_2^2 + 2\, x_1 x_2 x_3 + x_1 x_3^2 + x_2^2 x_3 + x_2 x_3^2\,.$$

Число $K_{\lambda,\eta}$ таблиц формы λ и состава μ называется *числом Костки*. Отметим, что $K_{\lambda,(1^{|\lambda|})} = d_\lambda$ равно числу стандартных таблиц формы λ, все $K_{\lambda,\lambda} = 1$, и $K_{\lambda,\eta} \neq 0$ только когда при каждом $j = 1,\, 2,\, 3,\, \dots$ выполняются неравенства

$$\lambda_1 + \lambda_2 + \;\cdots\; + \lambda_j \geqslant \eta_1 + \eta_2 + \;\cdots\; + \eta_j \quad \forall\, j\,. \tag{27-13}$$

В этой ситуации говорят, что диаграмма λ *доминирует* диаграмму μ и пишут $\lambda \trianglerighteq \mu$.

Упражнение 27.4. Покажите, что отношение доминирования задаёт на множестве диаграмм Юнга заданного веса n частичный порядок, полный при $n \leqslant 5$, и приведите пример двух несравнимых между собою диаграмм Юнга веса 6.

Таким образом, стандартные многочлены Шура $s_\lambda(x_1, x_2, \dots, x_m)$, где λ пробегает все диаграммы Юнга из не более, чем m строк, выражаются через базисные мономиальные симметрические многочлены m_λ при помощи обратимой над $\mathbb{Z}$ нижней унитреугольной матрицы:

$$s_\lambda = \sum_{\mu \trianglelefteq \lambda} K_{\lambda,\mu} \cdot m_\mu\,. \tag{27-14}$$

Тем самым, многочлены s_λ образуют базис $\mathbb{Z}$-модуля симметрических функций.

27.4.1. Пример: полные и элементарные симметрические многочлены. Многочлен Шура $s_{(k)}(x)$, отвечающий DU-орбите одностолбцового массива, т. е. диаграммы-строки

$$\lambda = (k,\, 0,\, \cdots,\, 0) = \underbrace{\square\square\cdots\square\square}_{k}\,,$$

представляет собой *полный симметрический многочлен* $h_k(x)$ — сумму всех мономов общей степени k от $x_1, x_2, \dots, x_m$, поскольку для любого содержания η веса $|\eta| = k$ имеется ровно одна однострочная таблица, в которой все координаты выстроены монотонно[1]. Симметричным образом, $s_{(1^k)}$, отвечающий DU-орбите диаграммы-столбца

$$1^k = (1,\,1,\,\cdots,\,1) = \left.\begin{array}{c}\square\\ \vdots\\ \square\end{array}\right\}k$$

это *элементарный симметрический многочлен* $e_k(x)$, т. е. сумма всех линейных по каждой переменной мономов общей степени k от $x_1, x_2, \dots, x_m$. Причина та же, только теперь номера переменных в таблице-столбце должны строго возрастать.

27.4.2. Пример: тождества Коши и Шура. Проинтерпретируем каждый шарик в клетке (i,j) массива a как билинейный моном $x_i y_j$ от двух наборов переменных $x = x^I = (x_1, x_2, \dots, x_n)$ и $y = y^J = (y_1, y_2, \dots, y_m)$. Перемножая вместе все шарики массива a, мы получим (в обозначениях n° 27.4) моном $x^{a^t} y^a$. По теореме о биекции из теор. 27.1 сумма таких мономов по всем массивам a фиксированной формы $\lambda = \Phi(a)$ равна произведению многочленов Шура $s_\lambda(x) \cdot s_\lambda(y)$, и значит сумма мономов $x^{a^t} y^a$ по вообще всем массивам a формата $I \times J$ равна сумме таких произведений по всем диаграммам Юнга λ.

С другой стороны, сумма всех мономов $x^{a^t} y^a$ по всем массивам a получается при раскрытии скобок в произведении бесконечных геометрических прогрессий

$$\prod_{\substack{i\in I\\ j\in J}} \bigl(1 + x_i y_j + (x_i y_j)^2 + (x_i y_j)^3 + \ \cdots\bigr)$$

(выбирая из (i,j)-того сомножителя слагаемое $(x_i y_j)^{a(i,j)}$ мы получаем в точности моном $x^{a^t} y^a$, отвечающий массиву a). Таким образом, мы приходим к *тождеству Коши*:

$$\sum_\lambda s_\lambda(x) \cdot s_\lambda(y) = \prod_{i,j} \frac{1}{1 - x_i y_j} \tag{27-15}$$

Если взять $I = J$, ограничиться только симметричными массивами $a = a^t$, положить $x = y = \xi$ и извлечь из каждого a-монома корень

$$\xi^a = \sqrt{\xi^{a^t} \xi^a} = \sqrt{x^{a^t} y^a}\big|_{x=y=\xi}\,,$$

то, суммируя по всем симметричным массивам a заданной формы λ, мы получим $s_\lambda(\xi)$, а суммируя по вообще всем симметричным массивам a — сумму

[1] эквивалентно: DU-орбита одностолбцового массива веса k образована всеми возможными расположениями k шариков по m ящикам

$\sum\limits_{\lambda} s_\lambda(\xi)$. Тот же результат получится при раскрытии скобок в произведении прогрессий

$$\prod_k \left(1+\xi_k+(\xi_k)^2+(\xi_k)^3+\ \cdots\right)\cdot\prod_{i<j}\left(1+\xi_i\xi_j+(\xi_i\xi_j)^2+(\xi_i\xi_j)^3+\ \cdots\right).$$

Мы получаем *тождество Шура*:

$$\sum_\lambda s_\lambda(\xi)=\prod_i\frac{1}{1-\xi_i}\cdot\prod_{i<j}\frac{1}{1-\xi_i\xi_j}\,. \tag{27-16}$$

27.5. Правило Литтлвуда – Ричардсона. Произведение полиномов Шура

$$s_M(x)\cdot s_N(x)$$

DU-множеств M и N является полиномом Шура для DU-множества, состоящего из всевозможных массивов вида ab размера $(2n)\times m$, получающихся приписыванием какого-нибудь массива $b\in N$ справа к какому-нибудь массиву[1] $a\in M$. Множество таких массивов естественно обозначить через $M\otimes N$ и называть *тензорным произведением* DU-множеств M и N. Итак,

$$s_M(x)\cdot s_N(x)=\Big(\sum_{a\in M}x^a\Big)\cdot\Big(\sum_{b\in N}x^b\Big)=\sum_{\substack{a\in M\\ b\in N}}x^{ab}=\sum_{c\in M\otimes N}x^c\,.$$

Разложение произведения $s_\lambda s_\mu$ стандартных полиномов Шура по базису s_ν даёт

Теорема 27.2 (правило литтлвуда – ричардсона)
$s_\lambda\cdot s_\mu=\sum\limits_\nu c^\nu_{\lambda\mu}\cdot s_\nu$, где суммирование происходит по всем диаграммам ν, получающимся добавлением $|\mu|$ клеток к диаграмме λ, а коэффициент $c^\nu_{\lambda\mu}$ равен количеству заполнений этих дописанных клеток μ_1 единицами, μ_2 двойками, μ_3 тройками и т. д., так что вдоль строк «косой диаграммы» $\nu\smallsetminus\lambda$ числа возрастают нестрого, а вдоль столбцов — строго (как в таблице Юнга), и одновременно слово, получающееся при прочтении этой «косой диаграммы» строку за строкой справа налево сверху вниз, содержит в каждом своём начальном куске единиц не меньше, чем двоек, двоек не меньше, чем троек и т. д. (как в n° 27.2.3).

Доказательство. Мы должны подсчитать в DU-множестве $O_\lambda\otimes O_\mu$ количество DU-орбит, которые уплотняются влево до стандартной орбиты O_ν. Пусть массив ab лежит в такой орбите. Поскольку массивы a, b получены из биплотных массивов λ, μ вертикальными операторами, оба они плотны влево и имеют I-веса λ и μ соответственно. Заметим, что действие вертикальной уплотняющей

[1] при этом вертикальный J-алфавит не меняется, а горизонтальный I-алфавит заменяется дизъюнктным объединением I-алфавитов массивов a и b

операции D_j на «толстый» массив ab состоит либо в её действии отдельно на[1] b , либо в её действии отдельно на[2] a. Поэтому при уплотнении вниз «толстого» массива ab мы получим массив вида $a'b'$, в котором a' плотен вниз, и оба массива a', b' по прежнему плотны влево и имеют I-веса λ, μ. Таким образом, a' биплотен формы λ. Если форма массива $a'b' = \lambda b'$ равна ν, то строки горизонтальной развёртки массива b' — это выровненные по левому краю строки «косой таблицы» $\nu \setminus \lambda$, заполненные именно так, как требует правило Литтлвуда – Ричардсона: первое, «табличное», ограничение выражает плотность вниз «толстого» массива ab, а второе, «словестное», ограничение выражает, согласно n° 27.2.3, плотность влево массива b'. □

Упражнение 27.5. Пользуясь правилом Литтлвуда – Ричардсона вычислите в Λ_3 произведения $s_{(1)} \cdot s_{(1,1)}$ и $s_{2,1}^2$. В частности, убедитесь непосредственно, что в первом случае «честное» и «халявное[3]» вычисления приводят к одному и тому же результату.

Упражнение 27.6 (формулы Пьери). Выведите из правила Литтлвуда-Ричардсона *формулы Пьери* для умножения полиномов Шура на элементарные и полные симметрические многочлены:

$$s_\lambda \cdot e_k = s_\lambda \cdot s_{(1^k)} = \sum_\mu s_\mu \tag{27-17}$$

$$s_\lambda \cdot h_k = s_\lambda \cdot s_{(k)} = \sum_\nu s_\nu \tag{27-18}$$

где μ и ν пробегают все диаграммы, которые можно получить приписыванием k новых клеток к диаграмме λ так, чтобы никакие две новые клетки не попали в одну строку μ и в один столбец ν.

27.5.1. Тождество Якоби – Труди. Из формулы Пьери (27-18) и формулы Пьери из сл. 26.6 на стр. 456 вытекает, что детерминантные полиномы Шура $\Delta_{\delta+\lambda}$ из предыдущего параграфа и комбинаторные полиномы Шура s_λ стандартных DU-орбит — это одни и те же полиномы.

В самом деле, формулы Пьери позволяют однозначно выразить все многочлены Шура через многочлены h_k. Например, согласно (27-18)

$$\begin{aligned}
s_{(2,2,1)} &= s_{(2,2)}h_1 - s_{(3,2)}\\
s_{(3,2)} &= s_{(3)}h_2 - s_{(5)} - s_{(4,1)} = h_3h_2 - h_5 - s_{(4,1)}\\
s_{(2,2)} &= s_{(2)}h_2 - s_{(3,1)} - s_{(4)} = h_2^2 - h_4 - s_{(3,1)}\\
s_{(4,1)} &= s_{(4)}h_1 - s_{(5)} = h_4h_1 - h_5\\
s_{(3,1)} &= s_{(3)}h_1 - s_{(4)} = h_3h_1 - h_4
\end{aligned}$$

[1] если самый правый свободный шар при паросочетании внутри «толстого» массива ab лежит в b, то он подавно будет самым правым свободным шаром и для паросочетания, установленного отдельно внутри b

[2] если в b нет свободных шаров при паросочетании внутри «толстого» массива ab

[3] т. е. применяющее правило теор. 27.2 не к $s_{(1)} \cdot s_{(1,1)}$, а к $s_{(1,1)} \cdot s_{(1)}$, что не всё равно

откуда[1] $s_{(2,2,1)} = -h_3h_2+h_4h_1+h_1(h_2^2-h_1h_3)$. В общем случае, оставляя в правой части формулы (27-18) диаграмму с самой длинной нижней строкой среди всех диаграмм с наибольшим количеством строк, мы выражаем её через h_k (где k равно длине этой нижней строки) и диаграммы, имеющие то же число строк, но более короткую нижнюю строчку, или строго меньшее число строк. Далее используем убывающую индукцию по количеству строк диаграммы Юнга и длине её нижней строки.

Совпадение детерминантного и комбинаторного описания полиномов Шура называется *тождеством Якоби – Труди*.

27.5.2. Выражение e_λ и h_λ через s_λ. Напомним, что для диаграммы Юнга μ мы обозначаем через m_i количество строк длины i в этой диаграмме и полагаем

$$e_\mu = e_{\mu_1}e_{\mu_2}\,\cdots\,e_{\mu_r} = e_1^{m_1}e_2^{m_2}\cdots e_n^{m_n} \tag{27-19}$$
$$h_\mu = h_{\mu_1}h_{\mu_2}\,\cdots\,h_{\mu_r} = h_1^{m_1}h_2^{m_2}\cdots h_n^{m_n}\,. \tag{27-20}$$

Многочлены (27-19) и (27-20) называются, соответственно, *элементарными* и *полными* симметрическими многочленами. Отметим, что при $k \in \mathbb{N}$

$$e_k(x) = s_{(1^k)}(x_1,x_2,\dots,x_m) \quad \text{и} \quad h_k(x) = s_{(k)}(x_1,x_2,\dots,x_m)\,.$$

Произвольный многочлен $h_\eta = s_{(\eta_1)}s_{(\eta_2)}\,\cdots\,s_{(\eta_r)}$ представляет собою полином Шура DU-множества $O_{(\eta_1)}\otimes O_{(\eta_2)}\otimes\cdots\otimes O_{(\eta_r)}$. Орбиты формы ν в этом множестве биективно соответствуют своим нижним концам, которые в свою очередь, взаимно однозначно описываются таблицами формы ν и содержания η. Тем самым,

$$h_\eta = \sum_\nu K_{\nu,\eta}\cdot s_\nu\,. \tag{27-21}$$

Произвольный многочлен $e_\eta = s_{(1^{\eta_1})}s_{(1^{\eta_2})}\,\cdots\,s_{(1^{\eta_r})}$ представляет собою многочлен Шура DU-множества $O_{(1^{\eta_1})}\otimes O_{(1^{\eta_2})}\otimes\cdots\otimes O_{(1^{\eta_r})}$, каждый массив в котором имеет $|\eta|$ столбцов, разбитых на вертикальные подмассивы $a_1a_2\,\dots\,a_r$ ширины $\eta_1,\eta_2,\dots,\eta_r$, причём в каждом столбце находится ровно один шар, и j-номера этих шаров строго возрастают внутри каждого вертикального подмассива a_i. При уплотнении вниз последнее свойство сохранится, и в результате такого уплотнения мы получим массив $a_1'a_2'\,\dots\,a_r'$ в котором шары каждого подмассива a_i' располагаются в разных строках, номера которых строго возрастают слева направо. Тем самым, каждый подмассив a_i' внесёт не более одного шара в каждую компоненту J-веса. Если суммарный J-вес при этом получится ν, то записывая в каждую строку диаграммы ν последовательно номера i тех подмассивов a_i', которые дают вклад в эту компоненту J-веса, мы получим таблицу содержания η и формы ν^t, *сопряжённой*[2] к форме ν: в силу вышесказанного

[1] читателю рекомендуется проверить этот результат по формуле Джамбелли (26-25)

[2] или *транспонированной*, т. е. симметрично отражённой относительно главной диагонали

номера будут строго возрастать по строкам диаграммы ν, а поскольку массив плотен вниз, они также должны не строго возрастать по столбцам; кроме того, по построению, каждый номер i будет представлен ровно в η_i различных строчках. Таким образом,

$$e_\eta = \sum_\nu K_{\nu^t,\eta} \cdot s_\nu \,. \tag{27-22}$$

Следствие 27.2
Инволюция ω из предл. 26.3, переводящая e_k и h_k друг в друга, действует на полиномы Шура по правилу $\omega(s_\lambda) = s_{\lambda^t}$, т. е. переводит друг в друга многочлены, отвечающие транспонированным диаграмм Юнга.

Доказательство. Так как многочлены s_λ образуют базис $\mathbb{Z}$-модуля симметрических функций, отображение $s_\lambda \mapsto s_{\lambda^t}$ однозначно задаёт на модуле симметрических функций $\mathbb{Z}$-линейную инволюцию. Из формул (27-21) и (27-22) следует, что эта инволюция переводит e_k в h_k и наоборот, т. е. совпадает с ω. □

Следствие 27.3 (вторая формула Джамбелли)

$$s_{\lambda^t} = \det \begin{pmatrix} e_{\lambda_1} & e_{\lambda_1+1} & \ddots & e_{\lambda_1+n-1} \\ e_{\lambda_2-1} & e_{\lambda_2} & \ddots & \ddots \\ \ddots & \ddots & \ddots & e_{\lambda_{n-1}+1} \\ e_{\lambda_n-n+1} & \ddots & e_{\lambda_n-1} & e_{\lambda_n} \end{pmatrix} \tag{27-23}$$

(по главной диагонали стоят $e_{\lambda_1}, e_{\lambda_2}, \dots, e_{\lambda_n}$, и при движении вдоль строк слева направо индексы у e с каждым шагом увеличиваются на единицу). □

Доказательство. Применяем инволюцию ω к формуле Джамбелли (26-25). □

27.6. Скалярное произведение Введём на $\mathbb{Z}$-модуле симметрических функций Λ скалярное произведение $\langle *, * \rangle$, для которого базис из полиномов Шура s_λ является ортонормальным. Из формул (27-21) и (27-14)

$$h_\lambda = \sum_{\mu \trianglerighteq \lambda} K_{\mu,\lambda} \cdot s_\mu \,, \quad s_\mu = \sum_{\lambda \trianglerighteq \mu} K_{\mu,\lambda} \cdot m_\lambda$$

вытекает, что $\langle h_\lambda, s_\mu \rangle = K_{\mu,\lambda} = \langle m^*_\lambda, s_\mu \rangle$, где m^*_λ — базис, двойственный к m_λ. Таким образом, $m^*_\lambda = h_\lambda$, т. е. базисы h_λ и m_λ двойственны друг другу:

$$\langle h_\lambda, m_\mu \rangle = \delta_{\lambda\mu} \,. \tag{27-24}$$

Из сл. 27.2 вытекает, что инволюция ω является ортогональным оператором.

Предложение 27.2

Многочлены Ньютона p_λ составляют ортогональный базис пространства $\mathbb{Q}\otimes\Lambda$ симметрических функций с рациональными коэффициентами и имеют скалярные квадраты $\langle p_\lambda, p_\lambda\rangle = z_\lambda$, где[1] $z_\lambda = \prod\limits_k (m_k! \cdot k^{m_k})$.

Доказательство. Выразим произведение геометрических прогрессий в правой части тождества Коши (27-15) через функции Ньютона от наборов переменных x и y:

$$\sum_\lambda s_\lambda(x)s_\lambda(y) = \prod_{i,j}\frac{1}{1-x_iy_j} = \prod_j H(y_j) = \prod_j \exp\left(\int\limits_0^{y_j} P(t)\,dt\right) =$$
$$= \exp\left(\sum_j\sum_k \frac{1}{k}\,p_k(x)y_j^k\right) = \exp\left(\sum_k \frac{p_k(x)p_k(y)}{k}\right) = \prod_k \exp\left(\frac{p_k(x)p_k(y)}{k}\right) =$$
$$= \prod_k\sum_{\ell\geqslant 0}\frac{1}{\ell!\cdot k^\ell}\,\left(p_k(x)p_k(y)\right)^\ell = \sum_\lambda \frac{1}{z_\lambda}\,p_\lambda(x)p_\lambda(y)$$

(переход в последнем равенстве тот же, что и в доказательстве равенства 26-21 на стр. 452). Если обозначить через $C_{\lambda\mu} = \langle s_\lambda, p_\mu\rangle$ коэффициенты разложений Ньютоновских полиномов по базису из полиномов Шура, так что $p_\mu = \sum\limits_\lambda C_{\lambda\mu}s_\lambda$, то подставляя эти разложения в правую часть полученного выше равенства и приравнивая коэффициенты при $s_\lambda(x)s_\eta(y)$ в левой и правой части, получаем соотношения

$$\sum_\nu C_{\nu\lambda}C_{\nu\eta} = \begin{cases} z_\lambda & \text{при } \eta=\lambda\\ 0 & \text{при } \eta\neq\lambda\end{cases}$$

т. е. матрица Грама $(\langle p_\lambda, p_\mu\rangle) = C^t\cdot C$ диагональна с диагональными элементами z_λ. □

Задачи для самостоятельного решения к §27

Задача 27.1. Нарисуйте плотный вниз массив со строчной развёрткой

1	4	6
2	5	7
3	8	9

[1]ср. с формулами (26-19) на стр. 452

и плотный влево массив со столбцовой развёрткой[1]

$$\begin{array}{|c|c|c|}\hline 1&2&3\\ \hline 4&5&8\\ \hline 6&7&9\\ \hline\end{array}\,.$$

Какой перестановке из симметрической группы S_9 отвечает по теореме о биекции эта пара массивов?

Задача 27.2. Каким перестановкам $g \in S_9$ соответствует по теореме о биекции пара таблиц[2]

$$\text{а) }\begin{array}{|c|c|c|c|c|c|c|}\hline 1&2&3&6&7&8&9\\ \hline 4\\ \cline{1-1} 5\\ \cline{1-1}\end{array}\ \text{ и }\ \begin{array}{|c|c|c|c|c|c|c|}\hline 1&4&5&6&7&8&9\\ \hline 2\\ \cline{1-1} 3\\ \cline{1-1}\end{array}\qquad \text{б) }\begin{array}{|c|c|c|c|}\hline 1&3&5&6\\ \hline 2&4&9\\ \cline{1-3} 7&8\\ \cline{1-2}\end{array}\ \text{ и }\ \begin{array}{|c|c|c|c|}\hline 1&3&5&7\\ \hline 2&4&8\\ \cline{1-3} 6&9\\ \cline{1-2}\end{array}$$

Задача 27.3. Выпишите явно многочлены Шура

а) $s_{2,1}(x_1, x_2, x_3)$ б) $s_{3,1}(x_1, x_2, x_3)$ в) $s_{2,1,1}(x_1, x_2, x_3)$

Задача 27.4. Из скольких мономов состоит $s_{(2,1,1)}(x_1, x_2, x_3, x_4)$?

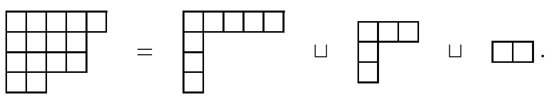
Задача 27.5. Выразите $\det\begin{pmatrix} x_1^6 & x_2^6 & x_3^6 & x_4^6\\ x_1^3 & x_2^3 & x_3^3 & x_4^3\\ x_1 & x_2 & x_3 & x_4\\ 1&1&1&1\end{pmatrix}$ через элементарные симметрические многочлены и произведение $\prod\limits_{i<j}(x_i - x_j)$.

Задача 27.6 (доминирование). Для двух диаграмм Юнга λ и μ одинакового веса $|\lambda| = |\mu| = n$ мы пишем $\lambda \trianglerighteq \mu$, если $\lambda_1 + \lambda_2 + \dots + \lambda_j \geqslant \mu_1 + \mu_2 + \dots + \mu_j$ $\forall j$. Покажите, что если $\lambda \vartriangleright \mu$ наименьший из элементов, больших μ, то μ получается из λ переносом ровно одной клетки в юго-западном направлении на ближайшее возможное расстояние, и в этом случае $\mu^t \vartriangleright \lambda^t$. Выведите отсюда, что для любых диаграмм $\lambda \trianglerighteq \mu \iff \lambda^t \trianglelefteq \mu^t$.

Задача 27.7. Разрежем диаграмму λ в объединение Г-образных диаграмм

$$\gamma_1, \gamma_2, \dots, \gamma_k$$

с углами на главной диагонали, как, например



[1]напомним, что столбцовая развёртка массива a — это строчная развёртка транспонированного массива a^t

[2]первая таблица есть строчная развёртка уплотнения вниз, вторая — столбцовая развёртка уплотнения влево, а перестановка задаёт отображение из горизонтальных номеров в вертикальные

В общем случае k — это число клеток на главной диагонали λ и

$$\gamma_i = (\lambda_i - i + 1, \underbrace{1, \ldots, 1}_{\lambda_i^t - i}).$$

Покажите, что s_λ входит в разложение произведения $s_{\gamma_1} s_{\gamma_2} \cdots s_{\gamma_k}$ по базису Шура с коэффициентом 1.

Задача 27.8* (инволюция Шютценберже). Покажите, что центральная симметрия

$$a \mapsto a^* \; : \; a^*(i,j) = a(n+1-i, m+1-j)$$

массива размера $n \times m$ не меняет его форму: $\Phi(a) = \Phi(a^*)$.

Ответы и указания к некоторым упражнениям

<u>упр. 1.1</u>. Ответ: 2^n.

<u>упр. 1.2</u>. Ответ на второй вопрос: нет. Решение: пусть $X = \{1,2\}$, $Y = \{2\}$; тогда все возможные значения пересечений и объединений между ними суть

$$X \cap Y = Y \cap X = Y \cap Y = Y \cup X = Y$$
$$X \cup Y = Y \cup X = X \cap X = X \cup X = X$$

и любая формула, составленная из X, Y, $\cap$ и $\cup$, даст на выходе либо $X = \{1,2\}$, либо $Y = \{2\}$, тогда как $X \smallsetminus Y = \{1\}$.

<u>упр. 1.3</u>. В первом случае имеется 6 наложений и ни одного вложения, во втором — 6 вложений и ни одного наложения.

<u>упр. 1.5</u>. Если множество X конечно, всякое отображение $X \longrightarrow X$, которое инъективно или сюрьективно, автоматически биективно. Если множество X бесконечно, то оно содержит подмножество, изоморфное $\mathbb{N}$, а у $\mathbb{N}$ есть инъективные небиективные эндоморфизмы (например, $n \mapsto (n+1)$) и сюрьективные небиективные эндоморфизмы (например, $1 \mapsto 1$ и $n \mapsto (n-1)$ при $n \geqslant 2$), и их можно продолжить до эндоморфизмов $X \longrightarrow X$ тождественным действием на $X \smallsetminus \mathbb{N}$.

<u>упр. 1.6</u>. Ответ: нет. Воспользуйтесь рассуждением Кантора: предположите, что все биекции $\mathbb{N} \longrightarrow \mathbb{N}$ можно занумеровать натуральными числами, и, пользуясь этим списком, постройте биекцию, которая при каждом $k = 1, 2, 3, \dots$ отображает число $k \in \mathbb{N}$ не туда, куда его отображает k-тая биекция из списка.

<u>упр. 1.7</u>. Ответ: $\binom{n+k-1}{k-1} = \binom{n+k-1}{n} = \frac{(n+k-1)!}{n!(k-1)!}$. Указание: слагаемых столько же, сколько имеется упорядоченных наборов неотрицательных целых чисел $(m_1, m_2, \dots, m_k)$ с суммой $\sum m_i = n$. Такой набор можно закодировать словом, составленным из $(k-1)$ букв 0 и n букв 1: сначала пишем m_1 единиц, потом нуль, потом m_2 единиц, потом нуль, и т. д. (слово кончится m_k единицами, стоящими следом за последним, $(k-1)$-м нулём).

<u>упр. 1.8</u>. Пусть $[x']_n = [x]_n$ и $[y']_n = [y]_n$, т. е. $x' = x + nk$, $y' = y + n\ell$ с некоторыми $k, \varepsilon ll \in \mathbb{Z}$. Тогда $x' + y' = x + y + n(k + \ell)$ и $x'y' = xy + n(\ell x + ky + k\ell n)$ сравнимы по модулю n с $x + y$ и xy соответственно, т. е. $[x' + y']_n = [x + y]_n$ и $[x'y']_n = [xy]_n$.

<u>упр. 1.9</u>. Рефлексивность и симметричность очевидны. Транзитивность: если $(p,q) \sim (r,s)$ и $(r,s) \sim (u,w)$, т. е. $ps - rq = 0 = us - rw$, то $psw - rqw = 0 = usq - rwq$, откуда $s(pw - uq) = 0$, и $pw = uq$, т. е. $(p,q) \sim (u,w)$.

<u>упр. 1.11</u>. Если прямые ℓ_1 и ℓ_2 пересекаются в точке O под углом $0 < \alpha \leqslant \pi/2$, то отражение относительно ℓ_1, а потом отражение относительно ℓ_2 — это поворот вокруг точки O на угол 2α в направлении от первой прямой ко второй. Таким образом, отражения относительно ℓ_1 и ℓ_2 коммутируют тогда и только тогда, когда прямые перпендикулярны.

<u>упр. 1.12</u>. а) $\Rightarrow$ б). Левое обратное к вложению $X \overset{f}{\hookrightarrow} Y$ должно переводить $y = f(x) \in \operatorname{im} f$ в x, а на элементах $Y \smallsetminus \operatorname{im} f$ может действовать как угодно. В частности, ответ на последний вопрос задачи — $(m-n)^n$.

б) $\Rightarrow$ в). Равенство $g_1 = g_2$ получается из равенства $fg_1 = fg_2$ умножением обеих частей слева на любое левое обратное к f отображение.

в) $\Rightarrow$ а). Если $f(x_1) = f(x_2)$ для каких-то $x_1 \neq x_2$, положим $g_1 = \mathrm{Id}_X$, а в качестве g_2 возьмём автоморфизм $X \longrightarrow X$, который меняет между собой точки x_1 и x_2, а все остальные точки оставляет на месте. Тогда $g_1 \neq g_2$, но $fg_1 = fg_2$.

<u>УПР. 1.13</u>. Аналогично предыдущему упр. 1.12.

<u>УПР. 1.14</u>. Таблица композиций gf в симметрической группе S_3:

$g \diagdown f$	$(1,2,3)$	$(1,3,2)$	$(3,2,1)$	$(2,1,3)$	$(2,3,1)$	$(3,1,2)$
$(1,2,3)$	$(1,2,3)$	$(1,3,2)$	$(3,2,1)$	$(2,1,3)$	$(2,3,1)$	$(3,1,2)$
$(1,3,2)$	$(1,3,2)$	$(1,2,3)$	$(3,1,2)$	$(2,3,1)$	$(2,1,3)$	$(3,2,1)$
$(3,2,1)$	$(3,2,1)$	$(2,3,1)$	$(1,2,3)$	$(3,1,2)$	$(1,3,2)$	$(2,1,3)$
$(2,1,3)$	$(2,1,3)$	$(3,1,2)$	$(2,3,1)$	$(1,2,3)$	$(3,2,1)$	$(1,3,2)$
$(2,3,1)$	$(2,3,1)$	$(3,2,1)$	$(2,1,3)$	$(1,3,2)$	$(3,1,2)$	$(1,2,3)$
$(3,1,2)$	$(3,1,2)$	$(2,1,3)$	$(1,3,2)$	$(3,2,1)$	$(1,2,3)$	$(2,3,1)$

<u>УПР. 2.2</u>. Ответы: $1 + x$ и $xy + x + y$.

<u>УПР. 2.3</u>. При умножении числителя и знаменателя любой из дробей в левых частях равенств (2-11) на одно и то же число c, числитель и знаменатель дроби в правой части соответствующего равенства также умножатся на c. Отсюда следует корректность. Проверка выполнения аксиом поля производится непосредственно.

<u>УПР. 2.5</u>. Число $\zeta = \cos(2\pi/5) + i \cdot \sin(2\pi/5)$ удовлетворяет соотношению $\zeta^5 = 1$. Поскольку $z^5 - 1 = (z-1)(z^4 + z^3 + z^2 + z + 1)$, число ζ является корнем уравнения

$$z^4 + z^3 + z^2 + z + 1 = 0,$$

которое можно решить в радикалах при помощи стандартной замены переменной z на переменную $t = z + z^{-1}$.

<u>УПР. 2.6</u>. Пусть $\zeta = \zeta_1 = \cos(2\pi/n) + i\sin(2\pi/n)$ — первообразный корень с наименьшим положительным аргументом, и $\xi = \zeta^k$. Докажем более сильное утверждение: среди целых степеней корня ξ встречаются те и только те степени первообразного корня ζ, которые делятся на $\text{нод}(k,n)$. В самом деле, равенство $\zeta^m = \xi^x$ означает, что $m = kx + ny$ для некоторого $y \in \mathbb{Z}$, а согласно n° 2.5.1 число m представимо в виде $m = kx + ny$ с целыми x и y тогда и только тогда, когда оно делится на $\text{нод}(k,n)$.

<u>УПР. 2.7</u>. Решение этого упражнения намечено в зад. 4.22 к §4 (см. стр. 67).

<u>УПР. 2.9</u>. Из равенства $z_1 z_2 = 1$ вытекает равенство $|z_1| \cdot |z_2| = 1$ на длины. Поскольку гауссово число $z \neq 0$ имеет $|z| \in \mathbb{N}$, обратимым может быть только z с $|z| = 1$. Таких чисел в $\mathbb{Z}[i]$ ровно четыре: ± 1 и $\pm i$, и все они обратимы.

<u>УПР. 2.11</u>. Возрастающая индукция по k, начинающаяся с $k = 0$, показывает, что все $E_k \in (a,b)$. С другой стороны, убывающая индукция по k, начинающаяся с $k = r+1$, показывает, что все числа E_k (в том числе $E_0 = a$ и $E_1 = b$) делятся на E_r. Таким образом, $(a,b) = (E_r)$, т. е. $E_r = \text{нод}(a,b)$.

<u>УПР. 2.13</u>. Существование. Если число n простое, то оно само и будет своим разложением; если n составное, представим его в виде произведения строго меньших по

абсолютной величине чисел, которые в свою очередь или неприводимы или являются произведениями строго меньших по абсолютной величине чисел и т. д. Поскольку модуль целого числа нельзя бесконечно долго уменьшать, мы в конце концов получим требуемое разложение.

Единственность. Для любого простого числа p и любого целого числа z выполняется следующая альтернатива: либо $\text{нод}(z,p) = |p|$, и тогда z делится на p, либо $\text{нод}(z,p) = 1$, и тогда z взаимно прост с p. Пусть в равенстве $p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_m$ все сомножители просты. Поскольку $\prod q_i$ делится на p_1, число p_1, в силу лем. 2.1, не может быть взаимно просто с каждым q_i. Согласно упомянутой выше альтернативе, найдётся q_i (можно считать, что q_1) который делится на p_1. Поскольку q_1 прост, $q_1 = \pm p_1$. Сокращаем первый множитель и повторяем рассуждение.

упр. 3.2. Класс $\binom{mp^n}{p^n} \pmod p$ равен коэффициенту при x^{p^n}, возникающему после раскрытия скобок и приведения подобных слагаемых в биноме $(1+x)^{mp^n}$ над полем $\mathbb{F}_p$. Последовательно применяя формулу (3-3), получаем

$$\begin{aligned}(1+x)^{p^n m} &= \left((1+x)^p\right)^{p^{n-1}m} = (1+x^p)^{p^{n-1}m} = \\ &= \left((1+x^p)^p\right)^{p^{n-2}m} = \left(1+x^{p^2}\right)^{p^{n-2}m} = \dots \\ &\cdots = \left(1+x^{p^n}\right)^m = 1 + m x^{p^n} + \text{ старшие степени}\end{aligned}$$

упр. 3.4. Поскольку через любую пару различных точек z, w проходит единственная прямая, общее число прямых на плоскости $\mathbb{F}_p^2$ равно количеству пар различных точек, делённому на количество пар различных точек, лежащих на одной прямой, т. е. $\binom{p^2}{2}/\binom{p}{2}$ (плоскость $\mathbb{F}_p^2$ состоит из p^2 точек, а каждая прямая на ней — из p точек). Если зафиксировать одну из точек и рассматривать только прямые, проходящие через эту точку, то таких прямых будет $(p^2-1)/(p-1)$ — число способов выбрать вторую точку на плоскости, делённому на число способов выбрать эту вторую точку на прямой.

упр. 3.10. Любой автоморфизм $\varphi : \mathbb{F} \longrightarrow \mathbb{F}$ оставляет на месте каждый элемент из $\operatorname{im}\varkappa$, т. к.

$$\varphi(\underbrace{1 + \cdots + 1}_{p}) = \underbrace{1 + \cdots + 1}_{p},$$

а простое подполе либо совпадает с $\operatorname{im}\varkappa$, либо состоит из элементов a/b с $a, b \in \operatorname{im}\varkappa$.

упр. 3.11. Пусть $\operatorname{char}(\mathbb{F}) = p$ и $\operatorname{char}(\Bbbk) = q$. При $q \neq p$ элемент $\underbrace{1 + \cdots + 1}_{p} \in \Bbbk$ отличен от нуля, но переводится в нуль любым гомоморфизмом $\varphi : \Bbbk \longrightarrow \mathbb{F}$. Тем самым, φ не инъективен и по предл. 3.3 должен быть нулевым.

упр. 4.3. Ответ: $(y^n - x^n)/(y-x) = y^{n-1} + y^{n-2}x + y^{n-3}x^2 + \cdots + yx^{n-2} + x^{n-1}$.

упр. 4.4. Годятся дословно те же аргументы, что и в упр. 2.13.

Существование. если f неприводим, то он сам и будет своим разложением, если f приводим, то он является произведением многочленов строго меньшей степени, которые в свою очередь или неприводимы или являются произведениями многочленов строго меньшей степени и т. д. Поскольку степень не может бесконечно уменьшаться, мы в конце концов получим требуемое разложение.

Единственность. Для любого приведённого неприводимого многочлена p и любого многочлена g выполняется следующая альтернатива: либо $\text{НОД}(p, g) = p$, и тогда g делится на p, либо $\text{НОД}(p, g) = 1$, и тогда g взаимно прост с p. Пусть в равенстве $p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_m$ все сомножители неприводимы. Деля p_1 на старший коэффициент, мы можем считать, что он приведён. Поскольку $\prod q_i$ делится на p_1, многочлен p_1, в силу лем. 2.1, не может быть взаимно прост с каждым q_i. Согласно упомянутой выше альтернативе, найдётся q_i (скажем, q_1), который делится на p_1. Так как q_1 неприводим, $q_1 = \lambda p_1$, где λ — ненулевая константа. Сокращаем первый множитель и повторяем рассуждение.

упр. 4.6. Единственность вытекает из сл. 4.2 : разность двух многочленов степени n, принимающих одинаковые значения в $n+1$ точках, обращается в нуль в этих $n+1$ точках, т. е. имеет $n+1$ разных корней, что возможно только если эта разность нулевая. Существование: по формуле Виета, приведённый многочлен, равный нулю во всех точках a_ν кроме i-той, есть $\prod\limits_{\nu \neq i}(x - a_\nu)$. Деля этот многочлен на его значение в точке a_i, получаем многочлен $f_i(x) = \prod\limits_{\nu \neq i}(x - a_\nu) / \prod\limits_{\nu \neq i}(a_i - a_\nu)$, такой что

$$f_i(a_\nu) = \begin{cases} 1, \text{ при } \nu = i \\ 0, \text{ при } \nu \neq i \,. \end{cases}$$

Таким образом, искомый многочлен равен $\sum\limits_{i=0}^{n} b_i \cdot f_i(x) = \sum\limits_{i=0}^{n} b_i \prod\limits_{\nu \neq i}(x - a_\nu)/(a_i - a_\nu)$.

упр. 4.7. Если многочлен степени $\leqslant 3$ приводим, то он имеет делитель степени один, корень которого будет корнем исходного многочлена.

упр. 4.8. См. упр. 1.8 на стр. 13.

упр. 4.9. Вложение $\varphi : \Bbbk \hookrightarrow \Bbbk[x]/(x - \alpha)$ в качестве констант сюрьективно, поскольку число $\alpha \in \Bbbk$ переходит в класс $[x]$, и значит, для любого $g \in \Bbbk[x]$ число $g(\alpha)$ переходит в класс $[g]$.

упр. 4.10. Пусть f неприводим. Если $[g][h] = [0]$ в $\Bbbk[x]/(f)$, то gh делится на f в $\Bbbk[x]$. Если g не делится на f, то $\text{НОД}(g, f) = 1$, т. к. у f нет отличных от констант делителей, не делящихся на f . Следовательно, g взаимно прост с f, а значит h делится на f по лем. 2.1 , т. е. $[h] = [0]$. Наоборот, если $f = gh$, где оба многочлена g, h не константы, то $\deg f \ \ \deg g < \deg f$, и значит, классы $[g]$ и $[h]$ отличны от нуля в $\Bbbk[x]/(f)$, однако $[g] \cdot [h] = [gh] = [0]$.

упр. 4.11. Обратным элементом к произвольному ненулевому $a + b\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$ является $\frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2}$. Кольцо в (а) содержит делители нуля: $[t+1] \cdot [t^2 - t + 1] = [0]$ и, тем самым, не является полем. Кольцо в (б) является полем: многочлен $p = \vartheta^3 + 2$ не имеет корней в $\mathbb{Q}$, и значит, не делится в $\mathbb{Q}[x]$ ни на какой многочлен первой или второй степени; следовательно, p взаимно прост со всеми $g \in \mathbb{Q}[x]$, не делящимися на p , т. е. для любого $[g] \neq [0]$ существуют $h_1, h_2 \in \mathbb{Q}[x]$, такие что $h_1 g + h_2 p = 1$; тем самым, $[h_1] = [g]^{-1}$.

упр. 4.13. Указание: достаточно рассмотреть случай $a_1 = 1$ и найти обратные ко всем элементам $\vartheta - a$; для этого воспользуйтесь алгоритмом Евклида (см. n° 4.2.3) — класс $h(\vartheta)$, обратный к классу $\vartheta - a$, задаётся таким многочленом $h \in \mathbb{Q}[x]$, что

$h(x)(x-a)+g(x)(x^2+x+1)=1$ для некоторого $g\in\mathbb{Q}[x]$; остаток от деления x^2+x+1 на $x-a$ равен a^2+a+1, так что алгоритм Евклида остановится уже на втором шагу.

упр. 4.16. Равенство $(b_1b_2)^k=1$ равносильно равенству $b_1^k=b_2^{m_2-k}$. Тогда $b_2^{m_1(m_2-k)}=b_1^{m_1k}=1$, откуда $m_1(m_2-k)$ делится на m_2, а значит, k делится на m_2. В силу симметрии между b_1 и b_2, показатель k делится также и на m_1. А так как m_1 и m_2 взаимно просты, k делится на m_1m_2. Поскольку $(b_1b_2)^{m_1m_2}=1$, $\operatorname{ord}(b_1b_2)=m_1m_2$.

упр. 4.17. В силу универсальности гомоморфизма ι, гомоморфизм ι' единственным образом представляется в виде $\iota'=\psi\circ\iota$, а в силу универсальности гомоморфизма ι', гомоморфизм ι точно так же единственным образом представляется в виде $\iota=\psi'\circ\iota'$. Композиция $\psi'\circ\psi$ доставляет разложение самого гомоморфизма ι в виде $\iota=\psi'\circ\psi\circ\iota$. Поскольку одновременно $\iota=\mathrm{Id}_{Q_K}\circ\iota$, из единственности такого представления вытекает, что $\psi'\circ\psi=\mathrm{Id}_{Q_K}$. По той же причине $\psi\circ\psi'=\mathrm{Id}_{Q'_K}$. Таким образом, ψ' и ψ являются взаимно обратными изоморфизмами.

упр. 4.18. Равенство несократимых записей $p/q=r/s$ означает равенство $ps=qr$, в котором p взаимно просто с q, а s взаимно просто с r. Из лем. 2.1 следует, что в этом случае $p=rf$, а $q=sg$, откуда $frs=grs$ и $f=g$. Поскольку запись p/q предполагалась несократимой, $\deg f=0$.

упр. 5.1. Указание к (в): разложите дробь над $\mathbb{C}$ в сумму простейших

упр. 5.3. Если $f(x)=\sum a_kx^k$, то $f(x+t)=\sum\limits_{k,\nu}a_k\binom{k}{\nu}\cdot x^{k-\nu}t^\nu=\sum\limits_{\nu}t^\nu\cdot f_\nu(x)$, где

$$f_\nu(x)=\sum_{k\geqslant\nu}a_k\binom{k}{\nu}\cdot x^{k-\nu}=\frac{1}{\nu!}\frac{d^k}{dx^k}\sum_{k\geqslant 0}a_kx^k\,.$$

упр. 5.6. Продифференцируйте обе части.

упр. 6.1. Импликации (а)⇒(б)⇒(в) очевидны. Если $s\in I$ обратим, то среди его кратных есть единица, а среди её кратных — все элементы кольца. Значит, (в)⇒(а).

упр. 6.2. Из того, что I является абелевой подгруппой в K немедленно вытекает, что отношение $a_1\equiv a_2 \pmod I$ рефлексивно, транзитивно и симметрично. Корректность операций проверяется так же, как в упр. 1.8: если $[a']_I=[a]_I$ и $[b']_I=[b]_I$, т. е. $a'=a+x$, $b'=b+y$ с некоторыми $x,y\in I$, то $a'+b'=a+b+(x+y)$ и $a'b'=ab+(ay+bx+xy)$ сравнимы по модулю I с $a+b$ и ab соответственно, поскольку суммы в скобках лежат в I (именно в этот момент мы пользуемся тем, что идел вместе с каждым элементом содержит и все его кратные); таким образом, $[a'+b']I=[a+b]_I$ и $[a'b']_I=[ab]_I$.

упр. 6.4. Если $\exists\, b^{-1}$, то $\nu(ab)\leqslant\nu(abb^{-1})=\nu(a)$; наоборот, если $\nu(ab)=\nu(a)$, то деля a на ab с остатком, получаем $a=abq+r$, где либо $\nu(r)<\nu(ab)=\nu(a)$, либо $r=0$; из равенства $r=a(1-bq)$ вытекает, что либо $\nu(r)\geqslant\nu(a)$, либо $1-bq=0$; с учётом предыдущего, такое возможно только при $1-bq=0$ или $r=0$; во втором случае $a(1-bq)=0$, что тоже влечёт $1-bq=0$; следовательно $bq=1$ и b обратим.

упр. 6.5. Если $b=ax$ и $a=by=axy$, то $a(1-xy)=0$, откуда $xy=1$.

упр. 6.7. Многочлены x и y не имеют в $\mathbb{Q}[x,y]$ никаких общих делителей, кроме констант. Общими делителями элементов 2 и x в $\mathbb{Z}[x]$ являются только ± 1.

упр. 6.8. Рассмотрим эпиморфизм факторизации $\pi : K \twoheadrightarrow K/I$. Полный прообраз $\pi^{-1}(J)$ любого идеала $J \subset K/I$ является идеалом в K. Классы элементов, порождающих этот идеал в K порождают идеал J в K/I.

упр. 6.10. Указание: повторите доказательство теор. 6.1, следя за младшими коэффициентами вместо старших.

упр. 6.12. По аналогии с комплексными числами, назовём *сопряжённым* к числу $\vartheta = a + b\sqrt{5}$ число $\overline{\vartheta} = a - b\sqrt{5}$, и будем называть *нормой* числа $\vartheta = a + b\sqrt{5}$ целое число $||\vartheta|| = a^2 - 5b^2 = \vartheta \cdot \overline{\vartheta}$. Легко видеть, что $\overline{\vartheta_1\vartheta_2} = \overline{\vartheta}_1 \cdot \overline{\vartheta}_2$, так что $||\vartheta_1\vartheta_2|| = \vartheta_1\vartheta_2\overline{\vartheta}_1\overline{\vartheta}_2 = ||\vartheta_1|| \cdot ||\vartheta_2||$. Поэтому $\vartheta \in \mathbb{Z}[\sqrt{5}]$ обратим тогда и только тогда, когда $||\vartheta|| = \pm 1$, и в этом случае $\vartheta^{-1} = \pm\overline{\vartheta}$. Поскольку $||2|| = 4$, а $||1 \pm \sqrt{5}|| = -4$, разложение этих элементов в произведение xy с необратимыми x и y возможно только, если $||x|| = ||y|| = \pm 2$. Однако элементов с нормой ± 2 в $\mathbb{Z}[\sqrt{5}]$ нет, т. к. равенство $a^2 - 5b^2 = \pm 2$ при редукции по модулю 5 превращается в равенство $a^2 = \pm 2$ в поле $\mathbb{F}_5$, где ± 2 не являются квадратами.

упр. 6.13. К разложению $n = q_1 q_2 \dots q_r$, в котором $q_i = p_i^{m_i}$ взаимно просты, применимы дословно те же рассуждения, что были проделаны нами в предл. 4.6 и n° 3.5. Ещё более общую версию китайской теоремы об остатках см. в зад. 6.7.

упр. 6.14. Это следует из равенства $a_0 q^n + a_1 q^{n-1} p + \dots + a_{n-1} q p^{n-1} + a_n p^n = 0$

упр. 6.15. Ответ: $(x^2 - 2x + 2)(x^2 + 2x + 2)$

упр. 6.16. Годится дословно то же рассуждение, что и при доказательстве неприводимости кругового многочлена $\Phi_p(x)$, предшествовавшего условию этой задачи.

упр. 6.17. Из функций, тождественно зануляющихся на образе φ, т. е. из *уравнений*, задающих $\varphi(X)$ в Y.

упр. 6.18. (а) следует из того, что функция (или отображение) непрерывно тогда и только тогда, когда прообраз любого открытого множества открыт; (б): инъективность гомоморфизма подъёма $\varphi^* : C \longrightarrow C$ означает, что не существует ненулевой непрерывной функции на $[0, 1]$, обращающейся в нуль на $\varphi([0, 1])$; из этого следует, что образ φ всюду плотен на $[0, 1]$; поскольку φ непрерывно, это возможно только при $\varphi([0, 1]) = [0, 1]$.

упр. 6.19. Покажем, что всякий ненулевой гомоморфизм $\varphi : C \longrightarrow \mathbb{R}$ является гомоморфизмом вычисления значения функций в некоторой точке $x \in [0, 1]$. Для этого рассмотрим его ядро $\mathfrak{m} = \ker\varphi$. Поскольку $C/\mathfrak{m} = \mathbb{R}$ — поле, идеал $\mathfrak{m}$ максимален, т. е. не содержится ни в каком строго большем идеале, отличном от всего кольца C (см. зад. 6.11). Каждая функция $f \in \mathfrak{m}$ не обратима, и потому обращается в нуль на некотором замкнутом подмножестве $Z_f \subset [0, 1]$. Если существует точка $x \in \bigcap_f Z_f$, то $\mathfrak{m} \subset \mathfrak{m}_x \stackrel{\text{def}}{=} \{g \in C \mid g(x) = 0\}$. Поскольку $\mathfrak{m}$ максимален, $\mathfrak{m} = \mathfrak{m}_x$, т. е. гомоморфизм φ есть гомоморфизм факторизации по модулю идеала $\mathfrak{m}_x$ и, тем самым, представляет собою гомоморфизм вычисления $f \mapsto f(x)$. Остаётся проверить, что $\bigcap_f Z_f \neq \varnothing$. Допустим противное. Тогда открытые множества $U_f = [0, 1] \smallsetminus Z_f$ покрывают $[0, 1]$. Выберем из этого покрытия конечное подпокрытие $[0, 1] = U_{f_1} \cup \dots \cup U_{f_n}$. Функция $f_1^2 + \dots + f_n^2 \in \mathfrak{m}$ нигде не обращается в нуль, т. е. обратима, что невозможно, т. к. $\mathfrak{m} \neq C$.

упр. 7.1. Пусть $0 \cdot v = w$. Тогда $w + v = 0 \cdot v + 1 \cdot v = (0+1) \cdot v = 1 \cdot v = v$. Прибавляя к обеим частям этого равенства $-v$, получаем $w = 0$. Из равенства $0 \cdot v = 0$ вытекает, что $\lambda \cdot 0 = \lambda(0 \cdot v) = (\lambda \cdot 0) \cdot v = 0 \cdot v = 0$. Наконец, равенство

$$(-1) \cdot v + v = (-1) \cdot v + 1 \cdot v = ((-1) + 1) \cdot v = 0 \cdot v = 0$$

означает, что $(-1) \cdot v = -v$.

упр. 7.3. По определению базиса отображение c биективно. Остаётся проверить что оно линейно. Если $w = \sum x_i v_i$ и $u = \sum y_i v_i$, то $\lambda w + \mu u = \sum(\lambda x_i + \mu y_i) e_i$, так что

$$\begin{aligned} c(\lambda w + \mu u) = \big((\lambda x_1 + \mu y_1)\,,\,(\lambda x_2 + \mu y_2)\,,\,\dots\,,\,(\lambda x_n + \mu y_n)\,,\,\big) = \\ = \lambda(x_1, x_2, \dots, x_n) + \mu(y_1, y_2, \dots, y_n) = \lambda c(w) + \mu c(u)\,. \end{aligned}$$

упр. 7.4. По индукции проверяется, что каждый моном x^m (где $m = 0, 1\ \dots\ , n$) линейно выражается через многочлены $f_0, f_1, \dots, f_m$, а значит, и любой многочлен степени $\leqslant m$ линейно выражается через $f_0, f_1, \dots, f_m$. Для доказательства единственности такого выражения заметим, что в равенстве $\sum \lambda_i f_i = \sum \mu_i f_i$ старший моном x^n появляется в обеих частях только из многочлена f_n. Поэтому сравнение коэффициента при x^n в обеих частях приводит к равенству $\lambda_n = \mu_n$. Вычитая из обеих частей $\lambda_n f_n = \mu_n f_n$, получаем равенство между многочленами меньшей степени, к которому применимо то же рассуждение.

упр. 7.6. Пусть $f(x) = \sum \lambda_i \cdot \delta_i(x)$. Подставляя $x = a_i$, получаем $\lambda_i = f(a_i)$, что даёт единственность разложения. С другой стороны $\forall\ f \in \Bbbk[x]$ с $\deg f \leqslant n - 1$ разность

$$f(x) - \sum_{i=1}^{n} f(a_i) \cdot \delta_i(x)$$

равна нулю, т.к. имеет степень $\leqslant (n-1)$ и n различных корней a_i.

упр. 7.7. Пусть какая-то конечная линейная комбинация векторов из объединения всех наборов обратилась в нуль. Каждый вектор из этой комбинации лежит в одном из наборов цепочки, а значит, и все они лежат в одном из наборов цепочки (том, что содержит остальные — такой существует, поскольку про любые два набора цепочки известно, что один из них является подмножеством другого). Так как каждый набор из цепочки предполагался линейно независимым, все коэффициенты этой линейной комбинации нулевые.

упр. 7.8. Рассмотрим множество всех пар (G, E), таких что $G \subset \mathscr{G}$, $E \subset \mathscr{E}$, G равномощно E, и после замены в $\mathscr{G}$ векторов из G на векторы из E набор остаётся порождающим. Первый шаг доказательства лем. 7.2 показывает, что это множество пар непусто. Введём на нём частичный порядок, полагая $(G, E) \leqslant (G', E')$, если $G \subset G'$ и $E \subset E'$. Поскольку любая линейно упорядоченная цепочка пар мажорируется парой, у которой G- и E-множества являются объединениями всех G- и E-множеств рассматриваемой цепочки, по лемме Цорна найдётся пара (G, E), не содержащаяся строго ни в какой большей паре. Если при этом $E \neq \mathscr{E}$, то же рассуждение, что и в доказательстве лем. 7.2 позволит добавить к множествам G и E ещё по одному элементу, что противоречит максимальности пары (G, E).

упр. 7.9. Нет, поскольку количество векторов в конечномерном пространстве над полем из 9 элементов является степенью девятки.

упр. 7.11. Пусть $W \not\subseteq U$ два подпространства в V. Выберем вектор $w \in W \smallsetminus U$. Если $W \cup U$ — подпространство, то $\forall\, u \in U \;\; w + u \in W \cup U$. Поскольку $w + u \notin U$ (т. к. $w \notin U$), $w + u \in W$, откуда $u \in W$, т. е. $U \subset W$.

упр. 7.12. Индукция по числу подпространств с использованием разобранного перед этим случая двух подпространств.

упр. 7.13. Поскольку каждый вектор $v \in V$ имеет единственное представление в виде $v = \sum u_i$ с $u_i \in U_i$, гомоморфизм *сложения* $\oplus U_i \xrightarrow{(u_1, u_2, \dots, u_m) \mapsto \sum u_i} V$ биективен.

упр. 8.1. Равенство $\sum \lambda_i/(1 - a_i t) = 0$ равносильно равенству $\sum \lambda_i p_i(t) = 0$, где $p_i(t) = \prod\limits_{\nu \neq i} (1 - a_\nu t) \in \Bbbk[t]$. Поскольку при $t = 1/a_i$ все $p_\nu(1/a_i)$ с $\nu \neq i$ зануляются, а $p_i(1/a_i) \neq 0$, мы заключаем, что $\lambda_i = 0$ для каждого i.

упр. 8.2. Набор $v_1, v_2, \dots, v_n \in V$ линейно независим, поскольку применяя ξ_i к обеим частям соотношения $\lambda_1 v_1 + \lambda_2 v_2 + \dots + \lambda_n v_n = 0$ получаем $\lambda_i = 0$ (и так для каждого i). Поскольку $\dim V = n$, этот набор является базисом, тогда из условия вытекает, что ξ_i составляют двойственный базис, т. е. являются координатами вдоль v_i.

упр. 8.3. Это пространство является образом гомоморфизма вычисления

$$\mathrm{ev}_D : \Bbbk[[t]] \longrightarrow \mathrm{End}\left(\Bbbk[x]_{\leqslant n}\right),$$

сопоставляющего ряду $g(t)$ оператор $g(D)$. Ядро этого гомоморфизма — главный идеал $\ker \mathrm{ev}_D = \left(t^{n+1}\right)$. В самом деле, всякий ряд вида $t^{n+1}h(t)$ действует на $\Bbbk[x]$ оператором $h(D)D^{n+1}$ аннулирует пространство $\Bbbk[x]_{\leqslant n}$, т. е. все ряды, делящиеся на t^{n+1}, лежат в $\ker \mathrm{ev}_D$. Если ряд $g(t)$ не делится на t^{n+1} и имеет младший член $a_m t^m$ с $m \leqslant n$ и $a_m \neq 0$, то $g(D)x^m = m! a_m \neq 0$, т. е. $g \notin \ker \mathrm{ev}_D$. Таким образом,

$$\mathrm{im}\, \mathrm{ev}_D \simeq \Bbbk[[t]]/\ker \mathrm{ev}_D \simeq \Bbbk[[t]]/\left(t^{n+1}\right) \simeq \Bbbk[D]/\left(D^{n+1}\right).$$

упр. 8.5. Если какие-то две функции обращаются тождественно в нуль на некотором множестве M, то и любая их линейная комбинация обращается в нуль.

упр. 8.6. Если $\langle \varphi, v \rangle = 0$ для всех $\varphi \in M$, то $\langle \psi, v \rangle = 0$ для любого ψ из линейной оболочки $\mathrm{span}(M)$ множества M.

упр. 8.7. Типичный для алгебры перенос из левой части в правую:

$$\langle G^* F^* \xi, v \rangle = \langle F^* \xi, Gv \rangle = \langle \xi, FGv \rangle$$

упр. 8.8. Ответ: операторы умножения на обрезанные по модулю D^{n+1} ряды $1 - e^{-D}$ и $e^D - 1$ соответственно.

упр. 8.9. Все проверки проводятся дословно также, как для классов вычетов по модулю идеала (ср. с упр. 6.2 и упр. 6.2).

упр. 8.10. Эквивалентность свойств (а)–(г) и единственность базиса (г) следуют из лем. 8.2, применённой к подпространству $\mathrm{Ann}\, U \subset \Bbbk^{n*}$. Покажем, что $u_\mu^\perp = e_{j_\mu}^* + \tau_\mu$

с $\tau_\mu = -\sum\limits_{\nu=1}^{r} \langle e^*_{j_\mu}, w_\nu\rangle \cdot e^*_{i_\nu}$ составляют базис в $\operatorname{Ann} U$. Они лежат в $\operatorname{Ann} U$, поскольку

$$\langle u^\perp_\mu, u_\nu\rangle = \langle e^*_{j_\mu} + \tau_\mu\,,\, e_{i_\nu} + w_\nu\rangle = \langle e^*_{j_\mu}, w_\nu\rangle + \langle \tau_\mu, e_{i_\nu}\rangle = \\ = \langle e^*_{j_\mu}, w_\nu\rangle - \sum_{\alpha=1}^{r}\langle e^*_{j_\mu}, w_\alpha\rangle \cdot \langle e^*_\alpha, e_{i_\nu}\rangle = \langle e^*_{j_\mu}, w_\nu\rangle - \langle e^*_{j_\mu}, w_\nu\rangle = 0$$

и линейно независимы, так как $e^*_{j_\mu}$ линейно независимы.

упр. 8.11. При проекции $c_I : \Bbbk^n \longrightarrow E_I$ векторы w_i перейдут в строки этой подматрицы, и для того, чтобы $c_I|_U$ была изоморфизмом, необходимо и достаточно, чтобы размерность их линейной оболочки была r.

упр. 8.12. Векторы $u^\perp_\nu$ линейно независимы, поскольку базисный ковектор $e^*_{j_\nu}$ входит только в u_ν и не может быть сокращён никакой линейной комбинацией остальных u_μ. Они все лежат в $\operatorname{Ann} U$, так как

$$\langle u^\perp_\nu, u_\mu\rangle = \left\langle e^*_{j_\nu} - \sum_k \alpha_{kj_\nu} e^*_{i_k}\,,\, e_{i_\mu} + \sum_\ell \alpha_{\mu j_\ell} e_{j_\ell}\right\rangle = \alpha_{\mu j_\nu}\langle e^*_{j_\nu}, e_{j_\nu}\rangle - \alpha_{\mu j_\nu}\langle e^*_{i_\mu}, e_{i_\mu}\rangle = 0$$

упр. 8.13. Поскольку пространство V^i порождается пространством V^{i+1} и вектором e_i, пространство $U \cap V^i$ содержится в линейной оболочке $U \cap V^{i+1}$ и вектора e_i, размерность которой, отличается от $\dim(U \cap V_{i+1})$ не больше, чем на единицу.

упр. 8.14. Для такого подпространства $d_i = \dim \pi_i(U)$ равна числу ненулевых строк в подматрице, сосредоточенной в первых i столбцах.

упр. 8.15. Если отнять из произвольной матрицы комбинаторного типа I матрицу E_I, в столбцах I которой стоит единичная $r \times r$ подматрица, а в остальных местах нули, получится матрица имеющая нули в столбцах I, а также при всех $\nu = 1, \dots, r$ нули в строке ν в позициях с 1-й по i_ν-тую включительно. Такие матрицы составляют в $\operatorname{Mat}_{r\times n}(\Bbbk)$ векторное подпространство указанной коразмерности $r^2 + \sum\limits_{\nu=1}^{r}(i_\nu - \nu + 1)$.

упр. 9.1. Первое доказывается выкладкой $0 \cdot a = (b + (-1) \cdot b)a = ba + (-1)ba = 0$, второе — выкладкой $e' = e' \cdot e'' = e''$.

упр. 9.2. $E_{ij}E_{k\ell} = \begin{cases} E_{i\ell} & \text{при } j = k \\ 0 & \text{в остальных случаях.}\end{cases}$ в частности, $E_{12}E_{21} \neq E_{21}E_{12}$. Полный список коммутационных соотношений таков:

$$[E_{ij}, E_{k\ell}] \overset{\text{def}}{=} E_{ij}E_{k\ell} - E_{k\ell}E_{ij} = \begin{cases} E_{ii} - E_{jj} & \text{при } j = k \text{ и } i = \ell \\ E_{i\ell} & \text{при } j = k \text{ и } i \neq \ell \\ -E_{kj} & \text{при } j \neq k \text{ и } i = \ell \\ 0 & \text{в остальных случаях.}\end{cases}$$

упр. 9.4. Пусть $AB = C$, $B^tA^t = D$, тогда $c_{ij} = \sum\limits_k a_{ik}b_{kj} = \sum\limits_k a^t_{ki}b^t_{jk} = \sum\limits_k b^t_{jk}a^t_{ki} = d_{ji}$.

упр. 9.7. См. указания к упр. 9.1

упр. 9.9. Легко видеть, что $\det(FG) = \det F \cdot \det G$. Поэтому, если матрица F обратима, то $\det F \cdot \det F^{-1} \det(FF^{-1}) = \det E = 1$, и тем самым $\det F$ обратим. То, что формула (9-6) при обратимом $\det F$ даёт обратную матрицу, устанавливается прямым вычислением.

упр. 9.10. Можно воспользоваться тем, что

$$\begin{pmatrix} a & b \\ c & 0 \end{pmatrix} = \begin{pmatrix} b & a \\ 0 & c \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \text{и} \quad \begin{pmatrix} 0 & b \\ c & d \end{pmatrix} = \begin{pmatrix} b & 0 \\ d & c \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

упр. 10.1. В обозначениях n° 1.6.1 (см. стр. 18), произвольную перестановку $g = (g_1, g_2, \dots, g_n)$ символов $\{1, 2, \dots, n\}$ можно представить в виде композиции $g = \sigma \circ g'$, где σ — транспозиция символов n и g_n, а $g' = \sigma \circ g$ оставляет на месте элемент n. Используя индукцию по n, разложим g' в композицию транспозиций, не затрагивающих элемента n.

упр. 10.3. При условии, что все точки пересечения двойные и трансверсальные, две нити, идущие из i и из j пересекаются между собою нечётное число раз, если пара (i, j) инверсна, и чётное число раз, если пара не инверсна (в действительности, картинку всегда можно нарисовать так, чтобы количества точек пересечения в этих двух ситуациях равнялись 1 и 0 соответственно). Знак тасующей перестановки $(i_1, i_2, \dots, i_k, j_1, j_2, \dots, j_m)$ равен $(-1)^{|I| + \frac{1}{2}k(k+1)}$, где *вес* $|I| \overset{\text{def}}{=} \sum_\nu i_\nu$. Действительно, нити, выходящие из чисел $i_1, i_2, \dots, i_k$ верхней строчки не пересекаются между собою и пересекают, соответственно, $i_1 - 1$, $i_2 - 2$, $\dots$, $i_k - k$ начинающихся левее нитей, выходящих из j-точек и тоже между собою не пересекающихся.

упр. 10.4. Независимость от выбора ненулевой формы объёма вытекает из того, что все такие формы пропорциональны друг другу, независимость от выбора линейно независимой системы векторов $v_1, v_2, \dots, v_n$ — из того, что любые две такие системы получаются друг из друга умножением на обратимую матрицу, и переход к другой системе умножает и числитель и знаменатель дроби в правой части формулы (10-7) на определитель этой матрицы.

упр. 10.5. Указание: j-тый столбец b_j матрицы b решает систему уравнений $Ab_j = e_j$. Его i-тую координату b_{ij} можно вычислить по правилу Крамера:

$$b_{ij} = \det(a_1, \dots, a_{i-1}, e_j, a_{i+1}, \dots, a_n) / \det(A)\,.$$

Поскольку единственный ненулевой элемент i-того столбца матрицы в числителе — это это единица, стоящая в j-той строчке, ненулевой вклад в сумму дадут только те произведения элементов матрицы, которые отвечают перестановкам $g \in S_n$, переводящим элемент i в элемент j. Это ровно те произведения, которые используются для вычисления определителя матрицы, получающейся из A выкидыванием i-того столбца и j-той строки. Остаётся внимательно разобраться со знаками перестановок.

упр. 10.6. При чётном n центр $\Bbbk\langle \xi_1, \xi_2, \dots, \xi_n \rangle$ линейно порождается мономами чётных степеней, при нечётном n — мономами чётных степеней и старшим (имеющим нечётную степень) мономом $\xi_1 \wedge \xi_2 \wedge \dots \wedge \xi_n$.

упр. 10.7. Перенумеровывая, если надо, переменные ξ_i, запишем f как

$$f(\xi) = \xi_1 \wedge (\alpha_2 \xi_2 + \dots + \alpha_n \xi_n) + \xi_2 \wedge (\beta_3 \xi_3 + \dots + \beta_n \xi_n) + (\text{члены без } \xi_1 \text{ и } \xi_2)$$

где $\alpha_2 \neq 0$. Перейдём к новым координатам $\xi_1', \xi_2', \dots, \xi_n'$:

$$\xi_2' = \alpha_2\xi_2 + \dots + \alpha_n\xi_n\,, \quad \xi_i' = \xi_i \text{ при } i \neq 2\,.$$

Подставляя $\xi_2 = \alpha_2^{-1}\left(\xi_2' - \beta_3\xi_3' - \dots - \beta_n\xi_n'\right)$ и $\xi_i = \xi_i'$ при $i \neq 2$, получаем:

$$\begin{aligned} f(\xi') = \xi_1' \wedge \xi_2' + \xi_2' \wedge (\gamma_3\xi_3' + \dots + \gamma_n\xi_n') + (\text{члены без } \xi_1' \text{ и } \xi_2') = \\ = (\xi_1' - \gamma_3\xi_3' - \dots - \gamma_n\xi_n') \wedge \xi_2' + (\text{члены без } \xi_1' \text{ и } \xi_2')\,. \end{aligned}$$

Теперь перейдём к координатам $\xi_1'', \xi_2'', \dots, \xi_n''$:

$$\xi_1'' = \xi_1' - \gamma_3\xi_3' - \dots - \gamma_n\xi_n'\,, \quad \xi_i'' = \xi_i' \text{ при } i \neq 1\,.$$

Подставляя $\xi_1' = \xi_1'' + \gamma_3\xi_3'' + \dots + \gamma_n\xi_n''$, $\xi_i' = \xi_i''$ при $i \neq 1$, получаем:

$$q = \xi_1'' \wedge \xi_2'' + (\text{члены без } \xi_1'' \text{ и } \xi_2'')\,.$$

Переобозначаем ξ_1'' и ξ_2'' через η_1 и η_2 и по индукции повторяем процедуру с оставшимися переменными.

упр. 10.8. Это сразу следует из равенства $\det A = \det A^t$.

упр. 10.10. Равенство $\det A^t = \det A$ и линейность определителя по строкам и столбцам над любым коммутативным кольцом следуют прямо из его определения (см. рассуждение в начале n° 10.3 на стр 175). Из линейности вытекает, что определитель умножается на число, если какая-то строка или столбец умножаются на число. Поэтому определитель матрицы с нулевой строкой или с нулевым столбцом нулевой. Доказательство лем. 10.3 также работает над любым кольцом, поэтому определитель матрицы, имеющей одинаковые строки или одинаковые столбцы нулевой. Из сказанного вытекает, что определитель не меняется при элементарных преобразованиях первого типа (когда к строке (соотв. столбцу) прибавляется другая строка (соотв. столбец), умноженная на любой элемент кольца). Из этого следует, что если столбцы $a_1, a_2, \dots, a_n$ матрицы A линейно зависимы: $\lambda_1a_1 + \lambda_2a_2 + \dots + \lambda_na_n = 0$, то

$$\begin{aligned} 0 = \det(0,\, a_2,\, \dots,\, a_n) = \det\left(\sum_\nu \lambda_\nu a_\nu,\, a_2,\, \dots,\, a_n\right) = \\ = \sum_\nu \lambda_\nu \det(a_\nu,\, a_2,\, \dots,\, a_n) = \det(a_1,\, a_2,\, \dots,\, a_n) \end{aligned}$$

Доказательство равенства $\det(AB) = \det A \cdot \det B$, данное в (10-10)–(10-11), проходит над любым коммутативным кольцом.

упр. 11.1. Все проверки проводятся дословно также, как для классов вычетов по модулю идеала коммутативного кольца (ср. с упр. 6.2 и упр. 6.2).

упр. 11.2. Изоморфизм $M_1/\ker(\varphi) \xrightarrow{\sim} \operatorname{im}(\varphi)$ переводит класс $m \pmod{\ker\varphi}$ в $\varphi(m)$. Проверка корректности и биективности стандартна.

упр. 12.1. Пусть проделанные с матрицей C преобразования строк заключаются в последовательном умножении слева на матрицы $S_kS_{k-1}\dots S_2S_1$, а проделанные преобразования столбцов — в умножении справа на $R_1R_2\,\dots\,R_\ell$. Тогда

$$F = S_kS_{k-1}\cdots S_2S_1E \quad \text{и} \quad G = ER_1R_2\,\dots\,R_\ell\,.$$

упр. 12.3. Равносильность условий (а), (б) и (в) очевидна после перехода к взаимным базисам $\mathbb{Z}^m$ и подрешётки. Равносильность (в) и (г) вытекает прямо из определения ранга.

упр. 12.4. Равенство $\varphi_n = 0$ при $n \geqslant m$ очевидно. Пусть $0 \leqslant n < m$. Если $\varphi_n(x) = 0$, то $p^n x = p^m y$ для некоторого $y \in K$, откуда $x = p^{m-n} y$ (мы воспользовались тем, что в K нет делителей нуля). Наоборот, если $x = p^{m-n} y$, то $p^n x = 0 \pmod{p^m}$. Таким образом $\ker \varphi_n = \operatorname{im} \varphi_{m-n}$. Легко видеть, что

$$K/\,(p^n) \xrightarrow{x \pmod{p^n} \mapsto p^{m-n} x \pmod{p^m}} K/\,((p^m)$$

является корректно определённым инъективным гомоморфизмом K-модулей, изоморфно отображающим $K/\,(p^n)$ на $\operatorname{im} \varphi_{m-n}$. Таким образом,

$$\ker \varphi_n \simeq \operatorname{im} \varphi_{m-n} \simeq \frac{K/\,(p^m)}{\ker \varphi_{m-n}} \simeq K/\,(p^n)\ .$$

упр. 13.1. Пусть $\Bbbk[t]/\,(t^n) = U \oplus W$, где U и W переводятся в себя умножением на t. Оба этих подпространства не могут целиком содержаться в образе оператора умножения на t (иначе их сумма тоже бы в нём содержалась), поэтому в одном из них, скажем, в U, есть класс $a \pmod{t^n}$, где $a \in \Bbbk$ отлично от нуля. Но тогда в U лежат все классы $at^m \pmod{t^n}$ с $0 \leqslant m \leqslant (n-1)$, а они линейно порождают всё пространство $\Bbbk[t]/\,(t^n)$.

упр. 13.2. Если $V = U \oplus W$, где U и W F-инвариантны, то $V^* = \operatorname{Ann} U \oplus \operatorname{Ann} W$ и оба подпространства $\operatorname{Ann} U$ и $\operatorname{Ann} W$ будут F^*-инвариантны: скажем, если $\xi \in \operatorname{Ann} U$, то $\forall\, u \in U \quad \langle F^*\xi, u\rangle = \langle \xi, Fu\rangle = 0$, поскольку $Fu \in U$, и значит, $F^*\xi \in \operatorname{Ann} U$. Обратная импликация получается по двойственности в силу изоморфизма $V^{**} = V$.

упр. 13.3. Для любого другого базиса $w = v\, C_{vw}$ согласно формуле (9-13) со стр. 160 выполняется равенство $F_w = C_{vw}^{-1} F_v C_{vw}$, из которого вытекает, что

$$\begin{aligned} \det(\lambda E - F_w) &= \det\left(\lambda\, C_{vw}^{-1} E C_{vw} - C_{vw}^{-1} F_v C_{vw}\right) = \det\left(C_{vw}^{-1}\,(\lambda E - F_v)\, C_{vw}\right) = \\ &= \det C_{vw}^{-1} \det(\lambda E - F_v) \det C_{vw} = \det(\lambda E - F_v)\ . \end{aligned}$$

упр. 13.4. Если $\lambda \in \operatorname{Spec} F$ и $g(\lambda) \neq 0$, то $g(F)$ действует на (ненулевом!) собственном подпространстве V_λ умножением на ненулевое число $g(\lambda)$. Тем самым, $g(F) \neq 0$.

упр. 13.5. См. например § 9 книги *Кострикин А. И., Манин Ю. И. Линейная алгебра и геометрия*. М. «Наука».

упр. 13.6. Если $a^n = 0$, $b^m = 0$ и $ab = ba$, то $(a+b)^{m+n-1} = 0$ по формуле Ньютона.

упр. 13.8. Отображение (13-13) линейно. Равенство $s(fg) = s(f)s(g)$ достаточно проверять отдельно для каждой струи. По формуле Лейбница $(fg)^k = \sum\limits_{\nu+\mu=k} \binom{k}{\nu} f^{(\nu)} g^{(\mu)}$.

Поэтому

$$\begin{aligned} s_\lambda^m(fg) &\equiv \sum_k \frac{(t-\lambda)^k}{k!} \sum_{\nu+\mu=k} \frac{k!}{\nu!\mu!} f^{(\nu)}(\lambda) g^{(\mu)}(\lambda) \equiv \\ &\equiv \sum_k \sum_{\nu+\mu=k} \frac{f^{(\nu)}(\lambda)}{\nu!}(t-\lambda)^\nu \cdot \frac{g^{(\mu)}(\lambda)}{\mu!}(t-\lambda)^\mu \equiv s_\lambda^m(f) s_\lambda^m(g) \end{aligned}$$

упр. 14.2. Если $(u, v) < 0$, то неравенство в выкладке, предшествовавшей условию задачи, строгое.

упр. 14.3. Значение линейной формы g_{e_j} на базисном векторе e_α равно (e_α, e_j), и значит, столбец координат этой формы в двойственном базисе e^* состоит из произведений (e_α, e_j).

упр. 14.6. Барицентр c объединения всех точек определяется из условия

$$\sum_i \lambda_i \overrightarrow{cp_i} + \sum_j \mu_j \overrightarrow{cq_j} = 0\,.$$

Подставляя в него $\overrightarrow{cp}_i = \overrightarrow{cp} + \overrightarrow{pp}_i$, $\overrightarrow{qq}_j = \overrightarrow{cq} + \overrightarrow{qq}_j$, и пользуясь равенствами $\sum \lambda_i \overrightarrow{pp_i} = 0$, $\sum \mu_j \overrightarrow{qq_j} = 0$, получаем $\left(\sum \lambda_i\right)\overrightarrow{cp} + \left(\sum \mu_j\right)\overrightarrow{cq} = 0$.

упр. 14.11. Первое вытекает из того, что если точки a и b лежат в Φ вместе с некоторыми ε-кубами $B_\varepsilon(a) \subset \Phi$ и $B_\varepsilon(b) \subset \Phi$ (см. рис. 27◇4), то из выпуклости Φ вытекает, что все точки отрезка $[ab]$ тоже содержаться в Φ вместе с некоторыми кубическими окрестностями. Второе вытекает из того, что если $a = \lim a_k$ и $b = \lim b_k$, то при любых фиксированных λ, μ мы имеем $\lim(\lambda a_i + \mu b_i) = \lambda a + \mu b$.

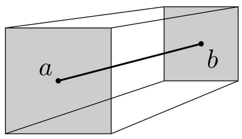


Рис. 27◇4.

упр. 15.2. Если $y = f(x)$ и $g(x) = x$, то $y = fg(x) = fgf^{-1}(y)$, т. е. $f \cdot \mathrm{Stab}_G(x) \cdot f^{-1} \subset \mathrm{Stab}_G(y)$. Поскольку $x = f^{-1}(y)$, меняя в предыдущем рассуждении x на y, f — на f^{-1}, а $g \in \mathrm{Stab}_G(x)$ — на $h \in \mathrm{Stab}_G(y)$, получаем $f^{-1} \cdot \mathrm{Stab}_G(y) \cdot f \subset \mathrm{Stab}_G(x)$. Остаётся заметить, что отображения сопряжения элементами f и f^{-1}

$$\mathrm{Ad}_f : G \xrightarrow{g \mapsto fgf^{-1}} G \quad \text{и} \quad \mathrm{Ad}_{f^{-1}} : G \xrightarrow{g \mapsto f^{-1}gf} G$$

обратны друг другу: $\mathrm{Ad}_f \mathrm{Ad}_{f^{-1}} = \mathrm{Ad}_{f^{-1}} \mathrm{Ad}_f = \mathrm{Id}_G$. Поэтому оба отображения

$$\mathrm{Stab}_G(x) \underset{\mathrm{Ad}_{f^{-1}}}{\overset{\mathrm{Ad}_f}{\rightleftarrows}} \mathrm{Stab}_G(y)$$

взаимно однозначны.

упр. 15.7. Ответ: $|1,2,3,4\rangle = \sigma_{12}\sigma_{23}\sigma_{34}$, $|1,2,4,3\rangle = \sigma_{12}\sigma_{24}\sigma_{34}$, $|1,3,2,4\rangle = \sigma_{13}\sigma_{23}\sigma_{24}$, $|1,3,4,2\rangle = \sigma_{13}\sigma_{34}\sigma_{24}$, $|1,4,2,3\rangle = \sigma_{24}\sigma_{23}\sigma_{13}$, $|1,4,3,2\rangle = \sigma_{34}\sigma_{23}\sigma_{12}$.

упр. 15.9. Обозначим через g^{-1} один из левых обратных к g элементов, а через e — одну из левых единиц. Тогда $g^{-1}gg^{-1} = eg^{-1} = g^{-1}$. Умножая правую и левую части этого равенства слева на левый обратный к g^{-1} элемент, получаем $gg^{-1} = e$. Тем самым, g^{-1} автоматически является и правым обратным к g (и потому единственен, см. n° 15.2.1). Отсюда, в свою очередь, вытекает, что e является также и правой единицей: $ge = g(g^{-1}g) = (gg^{-1})g = eg = g$.

упр. 15.11. Ответ: $[-2]_7$ и $[3]_7$.

упр. 15.12. Пусть $k = dr$, $m = \mathrm{ord}\,(\tau) = ds$, где $\text{нод}(r, s) = 1$. Если $d > 1$, то τ^d является произведением d независимых циклов длины s, и $\tau^k = \left(\tau^d\right)^r$ будет произведением s-тых степеней этих циклов. Остаётся показать, что когда $\mathrm{ord}\,(\tau) = m$ взаимно прост с k, то τ^k тоже цикл длины m. Если для какого-то элемента a цикла τ выполняется равенство $\left(\tau^k\right)^r(a) = a$, то kr делится на m, что при $\text{нод}(k, m) = 1$ возможно только когда r делится на m. Поэтому $r \geqslant m$, т. е. длина содержащего a цикла перестановки τ^k не меньше m.

упр. 15.13. Ответ: $n(n-1)\cdots(n-k+1)/k$ (в числителе дроби k сомножителей).

упр. 15.14. Непересекающиеся циклы очевидно коммутируют. Если коммутирующие циклы τ_1 и τ_2 пересекаются по элементу a, то $\tau_1(a)$ является элементом цикла τ_2, поскольку в противном случае $\tau_2\tau_1(a) = \tau_1(a)$, а $\tau_1\tau_2(a) \neq \tau_1(a)$, так как $\tau_2(a) \neq a$. По той же причине $\tau_2(a)$ является элементом цикла τ_1, и значит, оба цикла состоят из одних и тех же элементов. Пусть $\tau_1(a) = \tau_2^s(a)$. Любой элемент b, на который оба цикла реально действуют имеет вид $b = \tau_2^r(a)$, и цикл τ_1 действует на него как τ_2^s:

$$\tau_1(b) = \tau_1\tau_2^r(a) = \tau_2^r\tau_1(a) = \tau_2^r\tau_2^s(a) = \tau_2^s\tau_2^r(a) = \tau_2^s(b)\,.$$

Второе утверждение следует из упр. 15.12.

упр. 15.15. Ответ: $n!/\prod\limits_{i=1}^{n} i^{m_i}m_i!$ (ср. с формулой (1-12) на стр. 11).

Решение: сопоставим каждому заполнению диаграммы циклов λ неповторяющимися числами от 1 до n произведение независимых циклов, циклически переставляющих элементы каждой строки слева направо; получаем сюрьективное отображение множества заполнений на множество всех перестановок циклового типа λ; прообраз каждой перестановки состоит из $\prod\limits_{i=1}^{n} i^{m_i}m_i!$ заполнений, получающихся друг из друга независимыми циклическими перестановками элементов в каждой строке и произвольными перестановками строк одинаковой длины между собою как единого целого.

упр. 15.16. $|1,6,3,4\rangle^{15} \cdot |2,5,8\rangle^{15} \cdot |7,9\rangle^{15} = |1,6,3,4\rangle^{-1} \cdot |7,9\rangle = (4,\ 2,\ 6,\ 3,\ 5,\ 1,\ 9,\ 8,\ 7)$

упр. 15.19. Проще всего это увидеть на модели додекаэдра: каждая из пяти диагоналей некоторой фиксированной грани додекаэдра однозначно достраивается до такого куба, при этом на каждой из граней ровно одна из диагоналей будет ребром этого куба.

упр. 15.20. Подсказка: центральная симметрия коммутирует со всеми элементами полной группы додекаэдра; покажите, что единственная перестановка в S_5, коммутирующая со всеми перестановками из S_5 — это тождественное преобразование.

упр. 16.1. Рефлексивность: $\forall\, g \in G\ \ g = ge$ и $e \in H$; транзитивность: $g_1 = g_2h_{21}$, $g_2 = g_3h_{32} \Rightarrow g_1 = g_3h_{31}$, где $h_{31} = h_{32}h_{21}$; симметричность: $g_1 = g_2h_{21} \Rightarrow g_2 = g_1h_{12}$, где $h_{12} = h_{21}^{-1}$.

упр. 16.2. То, что орбиты правого умножения на H суть левые смежные классы gH — очевидно, а первое утверждение в предл. 16.1 есть утверждение о том, что орбиты не пересекаются или совпадают. Импликация $xh^{-1} = x \Rightarrow h = e$ доказывается умножением обеих частей первого равенства слева на x^{-1}. Из тривиальности стабилизаторов по формуле для длины орбиты получается, что длины всех орбит равны $|H|$, откуда $|G| = |X_G| = |H| \cdot |G/H|$.

упр. 16.6. Поскольку аффинные отображения F и $G = F\tau_v$ имеют одинаковый дифференциал $DG = DF$, по формуле (14-19) из n° 14.6.4 $G = \tau_w \circ F$, где $w = \overrightarrow{F(p)G(p)} = \overrightarrow{F(p)F(p+v)} = DF(v)$.

упр. 16.8. Правая часть формулы (16-5), приведённая по модулю 3, по модулю 4 и по модулю 5, равна, соответственно, $1-\varepsilon_3$, $1-\varepsilon_4$ и $1+2(\varepsilon_1+\varepsilon_2)$. Она может делиться на 3 или на 4 только если $\varepsilon_3 = 1$ или $\varepsilon_4 = 1$. В обоих случаях $|H| \geqslant 16$, так что $|H|$ не может быть ни 3, ни 4, ни $3 \cdot 4$, ни $3 \cdot 5$. Если $|H|$ делится на 5, то $\varepsilon_1 = \varepsilon_2 = 1$ и $|H| \geqslant 25$, так что $|H|$ не может быть ни 5, ни $4 \cdot 5$. Остаются ровно две возможности: $|H| = 1$ и $|H| = 3 \cdot 4 \cdot 5$.

упр. 16.9. Воспользуйтесь индукцией. Вложите A_{n-1} в A_n как стабилизатор символа n, и докажите, что нетривиальная нормальная подгруппа в A_n обязана иметь нетривиальное пересечение с A_{n-1}. Тогда оно будет автоматически нормально в A_{n-1}, что будет противоречить индуктивному предположению о простоте A_{n-1}.

упр. 16.10. Пусть центр $C(G) = C$. Если $|C| = p$, то $C \simeq G/C \simeq \mathbb{Z}/(p)$. Пусть $a \in C$ — образующая центра, $b \in G$ — такой элемент, что смежный класс bC является образующей в G/C. Тогда любой элемент группы имеет вид $b^k a^m$. Поскольку $a \in C$, любые два таких элемента коммутируют.

упр. 17.1. $(w_i, w_j) = \Big(\sum\limits_{\alpha} c_{\alpha i} v_\alpha\,,\, \sum\limits_{\beta} c_{\beta j} v_\beta\Big) = \sum\limits_{\alpha,\beta} c_{\alpha i} \cdot (v_\alpha, v_\beta) \cdot c_{\beta j} = \sum\limits_{\alpha} c^t_{i\alpha} \cdot \sum\limits_{\beta} (v_\alpha, v_\beta) \cdot c_{\beta j}$
или короче: $Bw = w^t w = C^t_{cw} v^t v\, C_{cw} = C^t_{cw} v^t B_v C_{cw}$.

упр. 17.2. первое следует из равенства $\beta(v+w, v+w) = \beta(v,v) + \beta(w,w) + \beta(v,w) + \beta(w,v)$, второе — из равенства $\beta(v,v) = -\beta(v,v)$

упр. 17.3. Это размерности пространства симметричных и кососимметричных матриц размера $n \times n$, равные $n(n \pm 1)/2$.

упр. 17.5. Переход к другому базису заключается в линейной однородной замене координат, в результате которой многочлены остаются многочленами (хотя и *меняются*). Если поле $\Bbbk$ конечно, то пространство функций $V \xrightarrow{\Bbbk}$ тоже конечно, а кольцо многочленов бесконечно. Поэтому гомоморфизм, сопоставляющий многочлену функцию должен иметь ненулевое ядро. Над бесконечным полем единственный многочлен от n переменных, тождественно равный нулю во всех точках $\Bbbk^n$ — это нулевой многочлен. Докажем это индукцией по $n = \dim V$. Ненулевой многочлен $f(x)$ от одной переменной не может иметь больше, чем $\deg f$ корней. Поэтому, если $f(p) = 0$ для бесконечного множества точек $p \in \Bbbk$, то $f(x) = 0$ в $\Bbbk[x]$. Многочлен от n переменных является многочленом от одной переменной x_n с коэффициентами из $\Bbbk[x_1, x_2, \dots, x_{n-1}]$:

$$f(x_1, x_2, \dots, x_n) = \sum_{\nu=0}^{d} \varphi_\nu(x_1, x_2, \dots, x_{n-1}) \cdot x_n^{d-\nu}\ .$$

Вычисляя коэффициенты φ_ν в произвольной точке $(p_1, p_2, \dots, p_{n-1}) \in \Bbbk^{n-1}$, мы получаем многочлен от x_n с постоянными коэффициентами, задающий тождественно нулевую функцию на прямой

$$(x_1, x_2, \dots, x_{n-1}) = (p_1, p_2, \dots, p_{n-1})\ ,$$

и потому нулевой. Тем самым, все многочлены φ_ν являются тождественно нулевыми функциями на $\Bbbk^{n-1}$. По предположению индукции, они являются нулевыми многочленами.

упр. 17.6. Переход к другому базису заключается в линейной однородной замене координат, в результате которой однородный многочлен второй степени останется однородным многочленом второй степени.

<u>упр. 17.7</u>. Зафиксируем в V какой-нибудь базис $e_1, e_2, \dots, e_n$, разложим v и w по этому базису как $v = \sum x_i e_i$ и $w = \sum y_i e_i$ и запишем q в виде (17-9). Тогда

$$q(v+w) - q(v) - q(w) = (x+y)B(x^t - y^t) - xBx^t - yBy^t = xBy^t + yBx^t = 2\,xBy^t\ .$$

(в последнем переходе мы воспользовались тем, что число yBx^t, будучи матрицей размера 1×1, совпадает со своей транспонированной версией, и в силу симметричности матрицы B равно $yBx^t = (yBx^t)^t = xB^t y^t = xBy^t$). Остальные утверждения проверяются аналогично.

<u>упр. 17.8</u>. $\sigma_{f(e)}$ тождественно действует на $f(e)^\perp$ и переводит $f(e)$ в $-f(e) = f(-e)$. Композиция $f \circ \sigma_e \circ f^{-1}$ действует точно также, посколькуf^{-1} переводит $f(e)^\perp$ в $e^\perp$ в силу изометричности оператора f.

<u>упр. 17.11</u>. Согласно n° 17.2.2, гиперболиность формы $x_1^2 + x_2^2$ равносильна тому, что -1 является квадратом в $\mathbb{F}_p$. Как мы видели в n° 4.4.4, это происходит в точности при $p \equiv 1 \pmod 4$. Рассуждение про вторую форму аналогично.

<u>упр. 17.13</u>. $\det \omega = \det(-\omega^t) = (-1)^{\dim V} \det \omega^t = (-1)^{\dim V} \det \omega$.

<u>упр. 18.1</u>. Каждая проходящая через начало координат прямая в $\mathbb{R}^{n+1}$ пересекает единичную сферу с центром в нуле по двум диаметрально противоположным точкам. Беря вместо единичной сферы её замкнутую полусферу (скажем, заданную условием $x_0 \geqslant 0$, мы можем отождествить $\mathbb{P}_n(\mathbb{R})$ с n-мерной замкнутой полусферой, у которой попарно склеены все диаметрально противоположные точки границы. Если воспринимать n-мерную полусферу как (заполненный) шар в $\mathbb{R}^n$, то можно эквивалентным образом сказать, что $\mathbb{P}_n(\mathbb{R})$ гомеоморфно n-мерному шару, у которого склеены вместе каждые две диаметрально противоположные точки ограничивающей его сферы.

При $n = 3$ получаем группу $\mathrm{SO}_3(\mathbb{R})$, элементы которой тоже можно непрерывно запараметризовать точками трёхмерного шара радиуса π с центром в нуле и склеенными диаметрально противоположными точками грницы: точке P шара отвечает поворот вокруг прямой OP на угол $|OP|$ по ЧС, если смотреть от O к P (диаметральным точкам сферы радиуса π при этом соответствуют одинаковые повороты на $180°$).

При $n = 2$ пространство $\mathbb{P}_2(\mathbb{R})$ получается склеиванием диаметрально противоположных точек границы у диска или, что то же самое, у квадрата. Если вначале склеить по этому правилу пару противолежащих сторон, то получится лента Мёбиуса. Дальнейшая склейка предписывает отождествить диаметрально противоположные точки её границы, что равносильно заклеиванию границы диском.

<u>упр. 18.2</u>. $\binom{n+d}{d} - 1$.

<u>упр. 18.3</u>. Любая прямая в проективном пространстве имеет непустое пересечение с любой гиперплоскостью.

<u>упр. 18.4</u>. Объединение $\cup \mathrm{Ann}\,(a_i) \subset V^*$ конечного числа векторных подпространств коразмерности 1 не может совпадать со всем пространством V^*, поскольку содержится в множестве нулей ненулевого многочлена $\prod a_i$ (произведение линейных форм a_i, задающих гиперплоскости $\mathrm{Ann}\,(a_i) \subset V^*$), который по упр. 17.5 не может обращаться в нуль во всех точках V^*. Поэтому существует $\xi \in V^*$, такой что $\langle \xi, a_i \rangle \neq 0$ для всех i .

упр. 19.1. Если прямая касается квадрики в точке b и пересекает её ещё в какой-нибудь точке $a \neq b$, то такая прямая целиком лежит на квадрике, поскольку матрица Грама векторов a, b тождественно нулевая. Тем самым, точка лежащая в пересечении всех касательных пространств, такова, что всякая проходящая через неё прямая либо больше уже нигде не пересекает квадрику, либо лежит на ней целиком. По лем. 19.1 это особая точка. Наоборот, любой элемент из $\ker \widehat{q}$ лежит в пересечении всех $\operatorname{Ann} \widehat{q}(b)$.

упр. 19.2. Первое следует из того, что проективное пространство $\mathbb{P}(S^2V^*)$ квадрик на $\mathbb{P}_3 = \mathbb{P}(V)$ имеет размерность 9, и любые 9 гиперплоскостей в $\mathbb{P}_9$ имеют непустое пересечение. Второе — из того, что прямая, пересекающая квадрику в трёх различных точках, лежит на ней целиком. Третье — из того, что ни на одной из квадрик в $\mathbb{P}_3$, кроме гиперболической квадрики Сегре нет трёх попарно скрещивающихся прямых.

упр. 19.4. Конус $C = P \cap T_pP$ имеет вершину в p и состоит из всех прямых, проходящих через p и лежащих на P. Фиксируем 3-мерную гиперплоскость $H \subset T_pP$, которая не содержит p. Тогда $G = C \cap H$ есть невырожденная квадрика на H. Таким образом, любая прямая, проходящая через p, имеет вид $(pp') = \pi_\alpha \cap \pi_\beta$, где $p' \in G$ и плоскости π_α, π_β натянутые на p и две прямые, проходящие через p' в G (см. рис. 19◇1).

упр. 19.5. Каждая прямая, которая проходит через p и не касается Q, пересекает квадрику ещё ровно в одной отличной от p точке, координвты которой, по теореме Виета, рационально зависят от прямой.

упр. 19.7. Воспользуйтесь тем, что точка a лежит на поляре точки b, если и только если точка b лежит на поляре точки a

упр. 19.8. Точка (a, b) переходит в прямую $ax + by = 1$ и наоборот.

упр. 19.9. Переход к другому реперу заключается в аффинной замене координат, которая представляет собой композицию параллельного переноса и линейного преобразования пространства V. От такой замены координат многочлен второй степени останется многочленом второй степени.

упр. 19.10. Запишем многочлен второй степени $q(t) \in \Bbbk[x_1, x_2, \dots, x_n]$ в виде

$$q_2(x) + q_1(x) + q_0 \,,$$

где q_i однородны степени i. Линейной заменой координат приведём квадратичную форму q_2 к виду $q_2(t) = a_1t_1^2 + a_2t_2^2 + \dots + a_kt_k^2$. Пусть линейная форма q_1 в результате такой замены приобрела вид $q_1(t) = \sum c_\nu t_\nu$. Заменим все переменные t_ν с $1 \leqslant \nu \leqslant k$ на $t_\nu + \frac{c_\nu}{2a_\nu}$. Это не изменит вида квадратичной части. Если в результате сделанной замены $q_1 + q_0$ перестанет зависеть от t, то мы пришли к первой из написанных форм, если не перестанет, то обозначим $q_1(t) + q_0$ через t_{k+1} и придём ко второй форме. Дальнейшее упрощение над $\mathbb{R}$ и над $\mathbb{C}$ достигается делением уравнения на свободный член (если он не нуль) и перескалированием переменных.

упр. 20.2. Пусть $|v| = |w| = 1$. Поскольку $(e^{i\varphi}v, e^{i\psi}w) = e^{i(\varphi-\psi)}(v, w)$, абсолютная величина эрмитова произведения $|(v, w)|$ не зависит от выбора векторов v И w на единичных окружностях, образованных векторами длины 1 в $\mathbb{C}$-линейных оболочках u и v. Покажем, что эта величина равна косинусу наименьшего евклидова угла между векторами с концами на рассматриваемых двух окружностях в в вещественном пространстве $\mathbb{R}^4 \simeq \mathbb{C}\cdot v \oplus \mathbb{C}\cdot w$, относительно евклидовой структуры на этом пространстве, однозначно определяемой тем, что евклидова длина любого вектора равна его эрмитовой длине. Для этого рассмотрим в отдельно вещественную и мнимую части эрмитова скалярного произведения: $(u_1, u_2) = g(u_1, u_2) + i\omega(u_1, u_2)$, где

$$g(u_1, u_2) \stackrel{\text{def}}{=} \operatorname{Re}(u_1, u_2) \quad \text{и} \quad \omega(u_1, u_2) \stackrel{\text{def}}{=} \operatorname{Im}(u_1, u_2)\,.$$

Форма $g(u_1, u_2)$ является положительно определённой вещественно билинейной симметричной формой со свойством $g(u, u) = (u, u)\ \forall\, u$, и тем самым, задаёт интересующую нас евклидову структуру, а форма $\omega(u_1, u_2)$ является кососимметричной невырожденной вещественно билинейной формой[1]. Когда векторы v, w пробегают свои единичные окружности, сумма $g^2(v, w) + \omega^2(v, w) = |(v, w)|^2$ постоянна, и минимальному евклидову углу соответствует максимальное значение квадрата его косинуса, равное $g^2(v, w)$, или, эквивалентно, минимальное значение $\omega^2(v, w)$. Но последнее равно нулю и достигается, поскольку форма ω невырождена и, тем самым, вещественное подпространство $v^{\perp}_{\omega} = \{u \mid \omega(v, u) = 0\}$ 3-мерно и имеет в $\mathbb{R}^4$ ненулевое пересечение с вещественно 2-мерным подпространством $\mathbb{C}\cdot w$.

<u>упр. 20.3</u>. Поскольку унитарный оператор F взаимно однозначен, всякий вектор w можно записать в виде $F^{-1}u$ для некоторого u. Поэтому выполнение для любых векторов v, w равенства $(Fv, Fw) = (v, w)$ равносильно выполнению для любых векторов v и $u = Fw$ равенства $(Fv, u) = (v, F^{-1}u)$.

<u>упр. 20.5</u>. Ответ: $a(t)\cdot\left(\frac{d}{dt}\right)^2 - (b(t) - 2a'(t))\cdot\frac{d}{dt} + (c(t) - b'(t) + a''(t))$.

<u>упр. 20.6</u>. Рассмотрим $\operatorname{Mat}_n(\mathbb{C})$ как вещественное n^2-мерное векторное пространство с базисом E_{ij} и iE_{ij}, где E_{ij} — матрица с единицей в i-той строке j-того столбца и нулями в остальных местах. В координатах (x_{ij}, y_{ij}) относительно этого базиса матричное уравнение $F^t\cdot\overline{F} = E$, задающее унитарные матрицы $(F_{ij}) = (x_{ij}) + i\cdot(y_{ij})$, запишется системой системой квадратичных уравнений $\sum\limits_{\nu}(x_{\nu i}^2 + y_{\nu i}^2) = 1$ (для каждого $i = 1, \dots, n$) и $\sum\limits_{\nu}(x_{\nu i}x_{\nu j} + y_{\nu i}y_{\nu j}) = \sum\limits_{\nu}(y_{\nu i}x_{\nu j} - x_{\nu i}y_{\nu j}) = 0$ (для всех $1 \leqslant i < j \leqslant n$). Поэтому множество U_n замкнуто. Складывая все уравнения первого типа, видим, что U_n находятся внутри единичного шара радиуса $\sqrt{n}$ с центром в начале координат, и значит, компактно. Диагональная матрица D с диагональными элементами вида $e^{i\vartheta}$ очевидно соединяется с единичной матрицей гладким путём $\gamma : [0, 1] \longrightarrow \mathrm{U}_n$, образ которого целиком состоит из диагональных матриц того же вида (надо просто согласованно устремить все ϑ к нулю). Поскольку произвольная унитарная матрица F записывается как $F = CDC^{-1}$ для некоторого $C \in \mathrm{U}_n$, путь $t \mapsto C\cdot\gamma(t)\cdot C^{-1}$ будет целиком лежать в U_n и соединять F с E.

<u>упр. 20.7</u>. При помощи лем. 20.3 норма остатка экспоненциального ряда мажорируется сходящейся геометрической прогрессией со сколь угодно малой суммой точно также, как это делается в курсе анализа для числовых экспонент.

<u>упр. 21.1</u>. Проверки ассоциативности и дистрибутивности умножения векторов на числа, как формальные буквенные выражения, дословно совпадают с проверками ассоциативности и дистрибутивности умножения в поле $\mathbb{C}$, определённом как фактор кольцо $\mathbb{R}[x]/(x^2 + 1)$.

[1] все эти свойства подробно обсуждаются в n° 21.5 на стр. 379

упр. 21.3. Выберем в собственном подпространстве $W_\lambda \subset V_{\mathbb{C}}$ оператора $F_{\mathbb{C}}$ базис $w_1, w_2, \dots, w_m$. Из того что вектор $w_\nu = u_\nu + iv_\nu$ собственный для $F_{\mathbb{C}}$ с вещественным собственным значением λ, вытекает, что оба вектора u_ν, $v_\nu \in V$ собственные для F с собственным значением λ. Поэтому вещественная линейная оболочка векторов $u_1, u_2, \dots, u_m$, $v_1, v_2, \dots, v_m$ лежит в собственном подпространстве V_λ оператора F. Следовательно, комплексификация $\mathbb{C} \otimes V_\lambda$ содержит собственное подпространство W_λ оператора $F_{\mathbb{C}}$, а значит, совпадает с ним, поскольку все векторы из $\mathbb{C} \otimes V_\lambda$, очевидно, собственные для $F_{\mathbb{C}}$ с собственным значением λ, т. е. лежат в W_λ.

упр. 21.4. Используйте то же рассуждение, что в доказательстве сл. 21.2. Разница будет состоять в том, что пара комплексно сопряжённых собственных векторов с собственными значениями $\cos\vartheta \pm i\sin\vartheta$ порождает комплексификацию двумерного вещественного инвариантного подпространства, на котором оператор F действует поворотом на угол ϑ.

упр. 21.5. Блочно диагональная матрица, по главной диагонали которой стоят вещественные 2×2-матрицы вида (21-6), отвечающие парам комплексно сопряжённых собственных чисел оператора, и 1×1-матрицы, с вещественными собственными числами оператора.

упр. 21.6. См. комментарий к упр. 21.1.

упр. 22.1. Для невырожденных матриц $\eta^\times = \det(\eta)\eta^{-1}$, откуда

$$(\eta\zeta)^\times = \det(\eta\zeta)(\eta\zeta)^{-1} = \det\zeta\zeta^{-1}\eta^{-1}\det\eta = \zeta^\times\eta^\times \,.$$

Поскольку невырожденные матрицы всюду плотны, рассматриваемое нами полиномиальное соотношение верно для всех матриц.

упр. 22.2. Ответ: ненулевые элементы матрицы Грама исчерпываются произведениями

$$\widetilde{\det}(E_{11}, E_{22}) = \widetilde{\det}(E_{22}, E_{11}) = 1 \quad \text{и} \quad \widetilde{\det}(E_{12}, E_{21}) = \widetilde{\det}(E_{21}, E_{12}) = -1\,,$$

где E_{11}, E_{12}, E_{21}, E_{22} — стандартный базис из матричных единиц.

упр. 22.5. Первая строчка формулы (22-9) показывает, что скалярное произведение связано с кватернионным умножением формулами $(p,q) = \operatorname{Re}(p \cdot q^*) = \operatorname{Re}(p^* \cdot q)$, откуда сразу следуют равенства $(\boldsymbol{e}, \boldsymbol{i}) = (\boldsymbol{e}, \boldsymbol{j}) = (\boldsymbol{e}, \boldsymbol{k}) = 0$.

упр. 22.6. Это запись в координатах соотношения $||p||^2 \cdot ||q||^2 = ||pq||^2$.

упр. 22.7. Из $\boldsymbol{i}^2 = \boldsymbol{j}^2 = \boldsymbol{k}^2 = -1$ вытекает, что все три кватерниона имеют норму 1 и антисамосопряжены (ср. с упр. 22.9 ниже). Равенства $\boldsymbol{i} \cdot \boldsymbol{j} = \boldsymbol{k} = -\boldsymbol{j} \cdot \boldsymbol{i}$ по сл. 22.1 означают, что $\boldsymbol{k}$ перпендикулярен $\boldsymbol{i}$ и $\boldsymbol{j}$. Последнее утверждение следует из лем. 22.1.

упр. 22.9. Из $\boldsymbol{n}^2 = -1$ следует, что $||\boldsymbol{n}||^2 = 1$ и $\boldsymbol{n}^{-1} = -\boldsymbol{n}$. Первое означает, что $||\boldsymbol{n}|| = 1$, второе — что $\boldsymbol{n}^* = -\boldsymbol{n}$.

упр. 23.1. Из единственности подъёма полилинейной формы $V_1 \times V_2 \times \cdots \times V_n \longrightarrow \Bbbk$ до линейной формы $V_1 \otimes V_2 \otimes \cdots \otimes V_n \longrightarrow \Bbbk$ вытекает, что единственная линейная форма $V_1 \otimes V_2 \otimes \cdots \otimes V_n \longrightarrow \Bbbk$, обращающая в нуль на всех разложимых тензорах, это нулевая форма. Поэтому разложимые тензоры не содержатся ни в каком собственном подпространстве.

упр. 23.3. Дословно годится рассуждение, использованное в n° 19.2.1 перед формулой (19-14) на стр. 339

упр. 23.4. Модуль билинейных отображений $\mathbb{Z} \times A \longrightarrow W$ изоморфен $\mathrm{Hom}(A, W)$. Изоморфизм задаётся сопоставлением билинейному отображению φ его ограничения на $1 \times A$.

упр. 24.1. Для любого линейного отображения $V \xrightarrow{f} A$ отображение

$$V \times V \times \cdots \times V \longrightarrow A\,,$$

переводящее $(v_1, v_2, \dots, v_n)$ в произведение $\varphi(v_1) \cdot \varphi(v_2) \cdot \cdots \cdot \varphi(v_n) \in A$ полилинейно, и значит, корректно определяет для каждого $n \in \mathbb{N}$ линейное отображение $V^{\otimes n} \longrightarrow A$, которые все вместе задают гомоморфизм алгебр $\mathsf{T}V \longrightarrow A$, продолжающий f, причём всякий гомоморфизм $\mathsf{T}V \longrightarrow A$, продолжающий f, должен переводить разложимый тензор $v_1 \otimes v_2 \otimes \cdots \otimes v_n \in V^{\otimes n}$ в $\varphi(v_1) \cdot \varphi(v_2) \cdot \cdots \cdot \varphi(v_n) \in A$, и стало быть, должен совпадать с построенным продолжением. Это доказывает выполнение универсального свойства. Тот факт, что SV и ι однозначно определяются этим универсальным свойством, доказывается дословно также, как в лем. 23.1 на стр. 405.

упр. 24.2. Поскольку разложимые тензоры линейно порождают $V^{*\otimes n}$ и формула

$$i_v \varphi(w_1, w_2, \dots, w_{n-1}) = \varphi(v, w_1, w_2, \dots, w_{n-1})$$

линейна по v и по φ, достаточно проверять её для форм φ, переводимых изоморфизмом (24-6) в разложимые тензоры вида $\xi_1 \otimes \xi_2 \otimes \cdots \otimes \xi_n$, а для таких форм она очевидна из построения.

упр. 24.3. Для любых v, w имеем

$$0 = \varphi(\dots, (v+w), \dots, (v+w), \dots) = \varphi(\dots, v, \dots, w, \dots) + \varphi(\dots, w, \dots, v, \dots)$$

Наоборот, равенство $\varphi(\dots, v, \dots, v, \dots) = -\varphi(\dots, v, \dots, v, \dots)$ влечёт равенство $\varphi(\dots, v, \dots, v, \dots) = 0$, если $1 \neq -1$.

упр. 24.4. Годятся дословно те же формальные соображения, что и в доказательстве лем. 23.1 на стр. 405

упр. 24.5. Ответ: $\binom{n+d-1}{d-1}$, или число решений уравнения $m_1 + m_2 + \cdots + m_d = n$ в неотрицательных целых числах $m_1, m_2, \dots, m_d$.

упр. 24.6. Для любого линейного отображения $V \xrightarrow{f} A$ отображение

$$V \times V \times \cdots \times V \longrightarrow A\,,$$

переводящее $(v_1, v_2, \dots, v_n)$ в произведение $\prod \varphi(v_i)$ в A полилинейно и симметрично, и значит, корректно определяет для каждого $n \in \mathbb{N}$ линейное отображение $S^n V \longrightarrow A$, которые все вместе задают гомоморфизм алгебр $SV \longrightarrow A$, продолжающий f. Наоборот, любой гомоморфизм $SV \longrightarrow A$, продолжающий f, должен переводить разложимый тензор $\prod v_i \in S^n V$ в $\prod \varphi(v_i) \in A$, и стало быть, будет совпадать с построенным продолжением. Это доказывает выполнение универсального свойства. Тот факт, что SV и ι однозначно определяются этим универсальным свойством, доказывается дословно также, как в лем. 23.1 на стр. 405.

упр. 24.7. Первое вытекает из равенства $0 = (v+w) \otimes (v+w) = v \otimes w + w \otimes v$, второе — из того, что равенство $v \otimes v + v \otimes v = 0$ при $1 + 1 \neq 0$ влечёт равенство $v \otimes v = 0$.

<u>УПР. 24.8</u>. Модифицируйте доказательство предл. 24.1 на стр. 423.

<u>УПР. 25.1</u>. Стабилизатор каждого слагаемого в симметрической группе S_n состоит из $m_1!\,m_2!\,\cdots\,m_d!$ независимых перестановок одинаковых сомножителей между собою. Остаётся применить формулу для длины орбиты (см. теор. 15.1).

<u>УПР. 25.2</u>. Для $t \in V^{\otimes n}$ и $g \in S_n$ обозначим через $g(t)$ результат действия g на t перестановкой тензорных сомножителей, как в (25-1). Утверждения (а) и (б) вытекают из того, что для каждого $h \in S_n$ выполняются равенства

$$h\Big(\sum_{g\in S_n} g(t)\Big) = \sum_{g\in S_n} hg(t) = \sum_{g'\in S_n} g'(t)$$

$$h\Big(\sum_{g\in S_n} \mathrm{sgn}(g)\cdot g(t)\Big) = \mathrm{sgn}(h)\cdot \sum_{g\in S_n} \mathrm{sgn}(hg)\cdot hg(t) = \mathrm{sgn}(h)\cdot \sum_{g'\in S_n} \mathrm{sgn}(g)\cdot g'(t)$$

(ибо отображение $g \mapsto g' = hg$ взаимно однозначно), мы заключаем, что

$$h(\mathrm{sym}_n(t)) = \mathrm{sym}_n(t) \quad \text{и} \quad h(\mathrm{alt}_n(t)) = \mathrm{sgn}(h)\cdot \mathrm{alt}_n(t)\,.$$

Утверждения (в) и (г) очевидны (обе суммы состоят из $n!$ одинаковых слагаемых). В (д) суммы по чётным и по нечётным перестановкам будут состоять из одних и тех же (и одинаковых внутри каждой из сумм) слагаемых, отличающихся знаком.

<u>УПР. 25.3</u>. Первое проверяется прямым вычислением. Что касается второго, то из равенства $\mathrm{sym}_3 + \mathrm{alt}_3 + p = E$ вытекает, что образы $\mathrm{im}\,(\mathrm{sym}_3) = \mathrm{Sym}^3(V)$, $\mathrm{im}\,(\mathrm{alt}_3) = \mathrm{Skew}^3(V)$ и $\mathrm{im}\,(p)$ линейно порождают $V^{\otimes 3}$, поскольку любой $t \in V^{\otimes 3}$ представляется как $t = E(t) = \mathrm{sym}_3(t) + \mathrm{alt}_3(t) + p(t)$. Эта сумма прямая в силу того, что, с одной стороны, каждый из трёх операторов являются проектором и действует на своём образе тождественно, а с другой стороны, аннулирует образы двух оставшихся операторов в следствие равенств $p\circ\mathrm{alt}_3 = \mathrm{alt}_3\circ p = p\circ\mathrm{sym}_3 = \mathrm{sym}_3\circ p = 0$ и равенств $\mathrm{sym}_3\circ\mathrm{alt}_3 = \mathrm{alt}_3\circ\mathrm{sym}_3 = 0$, вытекающих из упр. 25.2. Например, если $t \in \mathrm{im}\,(p) \cap \big(\mathrm{im}\,(\mathrm{sym}_3) + \mathrm{im}\,(\mathrm{alt}_3)\big)$, то $t = p(t)$, а записывая t как $\mathrm{sym}_3(t_1) + \mathrm{alt}_3(t_2)$, получим $p(t) = 0$, откуда $t = 0$.

<u>УПР. 25.4</u>. Утверждение задачи равносильно тому, что $\mathrm{im}\,(p) \subset V^{\otimes 3}$ является аннулятором образа оператора $\mathrm{Id} + T + T^2 : V^{*\otimes 3} \longrightarrow V^{*\otimes 3}$:

$$\mathrm{im}\,(p) = \{t \in V^{\otimes 3} \mid \langle(\mathrm{Id} + T + T^2)\xi, t\rangle = 0\ \forall\, \xi \in V^{*\otimes 3}\}\,,$$

где $\langle *, * \rangle$ означает полную свёртку между $V^{*\otimes 3}$ и $V^{\otimes 3}$. Легко видеть, что для любых $g \in S_n$, $\xi \in V^{*\otimes n}$, $t \in V^{\otimes n}$ выполняется равенство $\langle g\xi, t\rangle = \langle \xi, g^{-1}t\rangle$. Поэтому утверждение задачи равносильно тому, что образ p совпадает с ядром оператора

$$\mathrm{Id}^{-1} + T^{-1} + T^{-2} = \mathrm{Id} + T^2 + T = 3(\mathrm{alt}_3 + \mathrm{sym}_3)\,,$$

действующего на $V^{\otimes 3}$. Но из решения упр. 25.3 видно, что $\mathrm{alt}_3 + \mathrm{sym}_3$ — это проектор $V^{\otimes 3}$ на подпространство $\mathrm{Sym}^3 V \oplus \mathrm{Skew}^3 V$ вдоль подпространства $\mathrm{im}\,(p)$.

<u>УПР. 25.6</u>. Поскольку утверждение линейно по v, f и g достаточно проверить его для $v = e_i$, $f = x_1^{m_1} \dots x_d^{m_d}$, $g = x_1^{k_1} \dots x_d^{k_d}$, что делается прямо по определению.

<u>УПР. 25.7</u>. Это следует из равенства $\widetilde{f}(v, x, \dots, x) = \frac{1}{n}\cdot \partial_v f(x)$, где $n = \deg f$.

упр. 25.9. Это аналогично упр. 25.6.

упр. 25.10. Фиксируем в U базис $e_1, e_2, \dots, e_m$. Если $\omega \notin \Lambda^m U$, то в ω есть моном e_I, не содержащий какого-нибудь базисного вектора — скажем, e_i. Тогда $e_i \wedge \omega \neq 0$, поскольку будет содержать ненулевой моном $e_{i \sqcup I}$, возникающий только из произведения e_i на e_I и, стало быть, не способный ни с чем сократиться. Наоборот, если $\omega \in \Lambda^m U$, то $\omega = \lambda \cdot e_1 \wedge e_2 \wedge \cdots \wedge e_m$ и $e_i \wedge \omega = 0\ \forall\, i$, а значит, $u \wedge \omega = 0\ \forall u \in U$.

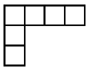
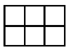
упр. 26.3. Поскольку Δ_δ обращается в нуль при подстановке $x_i = x_j$, он делится в кольце $\mathbb{Z}[x_1, x_2, \dots, x_n]$ на $(x_i - x_j)$. Так как каждая из разностей $(x_i - x_j)$ неприводима, f делится на $\prod\limits_{i<j}(x_i - x_j)$. Сравнивая лексикографически старшие мономы в этом произведении и в Δ_δ, заключаем, что частное равно 1.

упр. 26.4. См. предл. 15.2 на стр. 276.

упр. 26.5. В правом нижнем углу матрицы $(h_{\lambda_i + j - i})$, начиная с позиции $(m+1, m+1)$, где m — высота диаграммы λ, будет стоять верхняя унитреугольная матрица, левее которой все элементы в строках будут нулевые.

упр. 26.6. См. сл. 27.3 на стр. 478

упр. 27.1. Устойчивое паросочетание между i-тым и $(i+1)$-м солбцом устанавливается так: последовательно перебираем шарики в $(i+1)$-ом столбце двигаясь снизу вверх и назначаем очередному шарику $ш$ партнёром самый верхний шар i-того столбца, лежащий строго ниже $ш$ и ещё не назначенный никому партнёром, а если таких шаров нет, объявляем $ш$ свободным. После того, как все шары $(i+1)$-го столбца разделены на свободные и имеющие партнёров, все шары i-того столбца, не являющиеся ни чьими партнёрами, тоже объявляются свободными. Операция L_i перемещает на одну клетку влево самый верхний свободный шар $(i+1)$-го столбца или ничего не делает, если свободных шаров в $(i+1)$-ом столбце нет. Операция R_i перемещает на одну клетку вправо самый нижний свободный шар i-го столбца или ничего не делает, если в i-ом столбце нет свободных шаров.

упр. 27.4. Диаграммы  и  несравнимы по отношению $\trianglerighteq$.

упр. 27.5. $s_{(1)} \cdot s_{(1,1)} = s_{(2,1)} + s_{(1,1,1)} = s_{(1,1)} \cdot s_{(1)}$

упр. 27.6. При вычислении $s_\lambda \cdot e_k$ к диаграмме λ надо дописать k клеток без повторений заполненных числами от 1 до k, и если 2 из них попадают в одну строку, то возникает противоречие либо с табличным ограничением, либо с ограничением Ямaнучи. При вычислении $s_\lambda \cdot h_k$ к диаграмме λ надо дописать k клеток заполненных единицами, никакие две из которых не могут попасть в один столбец в силу табличного ограничения.

Предметный указатель

автоморфизм, 6
  гладкой коники, 352
  группы
    внешний, 275
    внутренний, 275
  квадрики, 333
  множества, 6
аксиома
  выбора, 20
  нетривиальности, 21
алгебра
  ассоциативная, 149
    свободная, 416
  внешняя, 423
  грассманова, 178, 423
  грассмановых многочленов, 178
  кватернионов, 390
  коммутативная, 149
    свободная, 422
  конечно порождённая, 91
  над полем, 149
  с единицей, 149
  симметрическая, 421
  тензорная, 416
  целая, 200
алгебраическая операция, 70
алгебраический элемент алгебры, 153
алгебраическое дополнение, 181
алгебраическое число, 58
алгебраичность, 67
алгоритм
  Евклида, 32, 55
  Кронекера, 97
альтернатива Фредгольма, 118
альтернирование, 430
аннулятор, 128
антиавтоморфизм, 391
антигомоморфизм, 361
антилинейный оператор, 361
аргумент комплексного числа, 25
асимптотическое направление, 320
ассоциативность, 15, 21, 266
аффинизация, 246
аффинная алгебраическая геометрия, 101
аффинная группа, 285
аффинная карта, 315
  на грассманиане, 142
аффинная квадрика, 347
аффинное пространство, 246
аффинный конус, 318

базис
  векторного пространства, 108
  гиперболический, 300
  двойственный, 124
    слева, 294
    справа, 294
  детерминантный, 446
  жорданов, 219, 221
  мономиальный, 446
  ортогональный, 237
  ортонормальный, 237, 356
  пространства функций, 109
  свободного модуля, 190
  симплектический, 308
  стандартный в $\Bbbk^n$, 105
  циклический, 219
базисы
  взаимные, 202
  евклидово двойственные, 241
барицентрическая комбинация, 247
  выпуклая, 248
биекция, 6
  бирациональная, 325
билинейная форма, 292
  вырожденная, 294
  кососимметричная, 296
  невырожденная, 294
  неразложимая, 314
  симметричная, 295
бинарное отношение, 11
бином Ньютона, 10
  по модулю p, 38
  с показателем в поле, 80

вектор, 104
- вещественный, 373
- геометрический, 23
- изотропный, 300
- на координатной плоскости, 39
- нулевой, 104
- противоположный, 104
- собственный, 120, 222, 374
- чисто мнимый, 373

векторизация, 246
векторное пространство, 104
- конечномерное, 112

векторы
- линейно зависимые, 110
- линейно независимые, 110
- ортогональные, 237
- порождающие, 108, 190
- сонаправленные, 240

верхнее полупространство Зигеля, 385
верхняя грань, 20
вершинное пространство, 337
вес, 247
- диаграммы Юнга, 10
- массива
  - столбцовый, 460
  - строчный, 460
- мультииндекса, 488

вещественная структура, 373
- σ на $\mathrm{Mat}_2(\mathbb{C})$, 390

взаимная простота, 33
- идеалов, 102
- многочленов, 55
- элементов кольца, 89

взаимные базисы модулей, 202
видимый контур, 438
вложение, 5
- Веронезе, 436
- Плюккера, 442

внешнее произведение, 421
внешнее умножение, 423
внешняя алгебра, 423
внешняя степень, 421
- матрицы, 180

внутреннее произведение, 418
возведение в степень, 79
выбором ориентации, 240
выпуклая оболочка, 248
выпуклая фигура, 248
вырожденный тензор, 419
вычет, 37
- квадратичный, 61
- обратимый, 38

вычитание, 24

гармоническая четвёрка точек, 329
гауссовы числа, 30, 94
геометрическая прогрессия, 71
геометрическое описание норм, 252
геометрия
- конечная, 39

гиперболический параболоид, 350
гиперболический поворот, 302
гиперболоид
- двуполостный, 350
- однополостный, 350
- эллиптический, 350

гиперплоскость
- аффинная, 254
- бесконечно удалённая, 315
- векторная, 107

гиперповерхность
- особая, 437
- проективная, 318

гладкая коника, 336
гомоморфизм
- абелевых групп, 42
- билинейных форм, 292
- векторных пространств, 105
- вычисления, 100, 103
- групп, 269
- колец, 43
- модулей, 192
- нулевой, 42, 43
- подъёма, 129
- полей, 44
- тривиальный, 42
- факторизации, 87, 285
- Фробениуса, 47

гомотетия, 327
- поворотная, 26

грассманиан, 142

Gr(2, 4), 343
изотропный, 382, 396
грассманов многочлен, 423
грассманова алгебра, 178
грассманово умножение, 423
грассмановы переменные, 178
группа, 265
p-группа, 287
абелева, 18, 23, 266
аффинная, 285
внутренних автоморфизмов, 275
гомотетий, 327
диэдра, 262
додекаэдра, 265, 272
дробно линейная, 327
знакопеременная, 272
икосаэдра, 265
бинарная, 401
кватернионных единиц, 278
Клейна, 262
коммутативная, 18, 266
корней из единицы, 29
куба, 270
линейная проективная, 327
обратимых вычетов, 38
октаэдра, 265
ортогональная, 244
квадратичной формы, 302
собственная, 244
перестановок, 18
полная линейная, 150
поля
аддитивная, 23
мультипликативная, 23
преобразований, 18, 260
простая, 286
сдвигов, 39
симметрическая, 18, 171
симплектическая, 309
специальная
линейная, 177
ортогональная, 244
унитарная, 358
тетраэдра, 263
треугольника, 263
унитарная, 358
фигуры
полная, 261
собственная, 261
циклическая, 18, 60, 199, 267
чётных перестановок, 272

двойная прямая, 335
двойная точка, 335
двойное отношение, 35, 327
на гладкой конике, 352
двойственные базисы, 124
двойственные пространства
векторные, 123
проективные, 324
двойственные решётки, 199
двойственный оператор, 129
двуугольник, 262
действие $\mathbb{Q}[[d/dx]]$ на $\mathbb{Q}[x]]$, 83
действие S_n на массивах, 470
действие группы, 273
диагональное, 281
присоединённое, 274
регулярное
левое, 274
правое, 274
свободное, 273
точное, 274
транзитивное, 273
эффективное, 274
действительная часть, 24
декартов квадрат, 467
декартово произведение, 5
деление, 24
кватернионов, 392
деление с остатком, 13
в евклидовом кольце, 87
многочленов, 52
делимость, 31
делитель нуля, 37
в модуле, 191
диагональ матрицы
главная, 154, 163
побочная, 154, 163
диагональное действие, 281
диаграмма

коммутативная, 146
циклов, 269
Юнга, 10
диаметр фигуры, 259
дизъюнктное объединение, 5
дискриминант, 66, 458
дистрибутивность, 21
дифференциал, 249
аффинного отображения, 248
длина
вектора
евклидова, 237, 239
эрмитова, 356
орбиты, 260
додекаэдр, 261
доминирование, 472
дополнение
к теореме Силова, 289
ортогональное, 358
дополнительное подпространство
векторное, 116
проективное, 324
дробно линейное преобразование, 327
дробь, 14
несократимая, 63
простейшая, 65

евклидова структура, 236
стандартная на $\mathbb{R}^n$, 236
евклидово пространство, 236
единица, 21
алгебры, 149
группы, 266
кольца, 161
симплектическая, 308
единичная подматрица, 135

жорданова клетка, 220
нильпотентная, 219
жорданова нормальная форма, 221
жорданова цепочка, 219

закон
квадратичной взаимности, 50
переместительный, 16
сочетательный, 15

замена координат, 160
замыкание, 250
проективное, 319
заполнение диаграммы Юнга, 10
звёздочка Ходжа, 426
зигелево полупространство, 385
знак перестановки, 172
значение многочлена, 53

идеал, 85, 190
главный, 85, 87
максимальный, 103, 197
порождённый элементами, 85
тривиальный, 85
идемпотент, 48, 223
изометрия, 243
гиперболической плоскости, 302
изоморфизм
аффинных квадрик, 347
билинейных форм, 292
векторных пространств, 105
групп, 261
линейных операторов, 215
множеств, 6
проективный, 326
проективных квадрик, 333
изотропный грассманиан, 382, 396
икосаэдр, 261
инвариантные множители, 201
инверсная пара, 171
инволюция, 223, 279, 280, 330
антилинейная, 362, 373
на гладкой конике, 353
индекс
инерции
отрицательный, 307
положительный, 307
квадратичной формы, 307
пересечения, 437
подгруппы, 282
интеграл степенного ряда, 77
интерполяционный многочлен, 227
Лагранжа, 97
инъекция, 5

карта аффинная на $\mathbb{P}(V)$, 315

касательная
к квадрике, 338
к проективной гиперповерхности, 437
касательное пространство, 338, 437
квадрат декартов, 467
квадратичная форма
анизотропная, 299
вещественная, 307
вырожденная, 299
гиперболическая, 299
над полем $\mathbb{F}_p$, 306
невырожденная, 299
от двух переменных, 299
отрицательно определённая, 307
положительно определённая, 307
квадратичный вычет, 61
квадратичный закон взаимности, 50
квадрика
аффинная, 347
гиперболическая, 334
гладкая, 333
вещественная, 334
над алгебраически замкнутым полем, 334
невырожденная, 333
Плюккера, 342, 425
проективная, 333
пустая, 347
Сегре, 339, 353, 397
эллиптическая, 334
квадрики
аффинно эквивалентные, 347
на $\mathbb{P}_1$ и на $\mathbb{P}_2$, 335
проективно эквивалентные, 333
квазимногочлены, 234
кватернион, 390
вещественный, 391
чисто мнимый, 391, 401
кватернионное сопряжение, 391
кватернионы, 390
келерова тройка, 380
келеровы тройки
на пространстве кватернионов, 399
с заданным ω, 382
с заданным g, 380
китайская теорема об остатках, 45, 64, 89
класс
вычетов
по модулю n, 13
вычетов, 37
по модулю идеала, 86
по модулю многочлена, 57
эквивалентности, 12
клетка
жорданова, 220
Шуберта, 142
ковектор, 127
кокуб, 256
кольцо, 160
гауссовых чисел, 30
главных идеалов, 87
евклидово, 87
коммутативное, 30
с единицей, 30
локальное, 199
нётерово, 89
нормальное, 200
приведённое, 37
противоположное, 188
регулярных функций, 99
с единицей, 161
симметрических функций, 457
структурное, 99
факториальное, 93
целозамкнутое, 200
целостное, 37
комбинаторный тип подпространства, 141
коммутативная диаграмма, 146
коммутативное произведение, 420
коммутативное умножение, 421
коммутативность, 16, 21, 266
коммутатор, 166
комплекс
Де Рама, 443
Кошуля, 443
комплексификация

билинейной формы, 375
вещественного пространства, 372
линейного оператора, 374
комплексная структура, 378
сопряжённая, 387
комплексное сопряжение, 27
векторов, 373
комплексное число, 24
композиция, 15
конечномерная линейная алгебра, 101
конечные геометрии, 39
коника, 335
Веронезе, 336
гладкая, 318, 336
распавшаяся, 335
константа, 51
конус, 350
эллиптический, 350
координатная плоскость, 39
координаты
аффинные, 246
локальные, 316
барицентрические, 258
вектора, 109
Дарбу, 180
однородные, 316
корень
бинарной формы, 321
из единицы, 29
многочлена, 56
кратный, 73
общий, 57
первообразный
из единицы, 29
по модулю n, 48
корневое разложение, 224
корреляция, 337
левая, 293
правая, 293
кососимметричность, 170
коэффициент
биномиальный, 79
гауссов, 120
младший, 51
мультиномиальный, 9
старший, 52
коядро, 147, 148
кривая
Веронезе, 321
гладкая, 331
особая, 331
рациональная, 331
нормальная, 321, 331
критерий
Сильвестра, 308
Эйзенштейна, 99
круговой многочлен, 29, 67
куб, 251, 254, 261

левый модуль, 188
левый сдвиг, 282
левый смежный класс, 282
лемма
Витта, 304
Гаусса
о квадратичных вычетах, 50
о многочленах, 96
Гаусса-Кронекера-Дедекинда, 200
Накаямы, 199
о змее, 148
о коммутировании уплотняющих операций, 462
о пяти гомоморфизмах, 147
Цорна, 20, 103, 111, 197
линейная зависимость, 110, 190
линейная комбинация, 108
линейная оболочка, 114
линейная система гиперповерхностей, 320
линейная форма, 123
линейное выражение, 108
линейное отображение, 189
изометрическое, 292
симплектическое, 309
линейное проективное преобразование, 326
линейное рекуррентное уравнение, 75, 230
линейное соединение, 337
линейные соотношения, 190
линейный носитель

грассманова многочлена, 440
многочлена, 435
тензора, 419
линейный оператор, 105
антисамосопряжённый, 361
двойственный, 129
диагонализуемый, 218, 226
идемпотентный, 223
изометрический, 292
инволютивный, 121, 223
канонический, 313
косоэрмитов, 361
неразложимый, 215
нильпотентный, 121, 218
нормальный, 364, 369
ортогональный, 243
несобственный, 244
собственный, 244
полупростой, 121, 226
разложимый, 215
самосопряжённый, 361
симплектический, 309
сопряжённый, 129
унитарный, 357
эрмитов, 361
линейный функционал, 123
логарифм, 77
логарифмическая производная, 77
локальные координаты, 316

малая теорема Ферма, 39
массив, 460
биплотный, 464
плотный, 464
матрица
верхнетреугольная, 163
Грама, 238, 292
квадратичной формы, 298
диагонализуемая, 427
единичная
симплектическая, 308
кососимметричная, 185
над некоммутативным кольцом, 161
невырожденная, 177
нижнетреугольная, 163
нильпотентная, 166
обратимая, 154
оператора, 106, 113
ортогональная, 244
перехода, 158
присоединённая, 183
симплектическая, 309
стандартная базисная, 107
транспонированная, 131
унипотентная, 166
унитарная, 358
унитреугольная, 163
эрмитово кососимметричная, 362
эрмитово симметричная, 356, 362
матричные единицы, 107
медиана, 258
метод Гаусса
над кольцом главных идеалов, 204
над полем, 135
обращения матрицы, 154
метрика, 250
метрическая топология, 250
минимальный многочлен
матрицы, 165
оператора, 122, 217
элемента алгебры, 153
элемента поля, 67
минор, 180
главный, 187
угловой, 307
дополнительный, 181
мнимая часть, 24
многообразие
Сегре, 408
спиноров, 396
многочлен, 52, 433
Аппеля, 83
гармонический, 368
грассманов, 423
интерполяционный, 227
Лагранжа, 97
кососимметрический, 445
круговой, 29, 67
минимальный
матрицы, 165

оператора, 122, 217
элемента алгебры, 103, 153
элемента поля, 67
неприводимый, 30, 55
приведённый, 52, 67
симметрический, 119, 445
мономиальный, 446
Ньютона, 450
полный, 449
элементарный, 448, 473
характеристический, 76, 187, 194
оператора, 221
целозначный, 198
циклотомический, 29
Шура, 447, 471
стандартный, 471
множество
DU-множество, 469
замкнутое, 250
особых точек, 337
открытое, 250
пустое, 4
частично упорядоченное, 20
полное, 20
модуль
без кручения, 191
комплексного числа, 24
конечно порождённый, 190
левый, 188
неразложимый, 195
полилинейных отображений, 402
полупростой, 198
правый, 188
свободный, 190
точный, 200
унитальный, 188
момент силы, 247
мономорфизм, 5
мультиномиальный коэффициент, 9
мультипликативный характер, 49

набор элементарных делителей
модуля, 209
оператора, 217
наибольший общий делитель
в кольце главных идеалов, 88
в факториальном кольце, 95
многочленов, 55
чисел, 32
элементов кольца, 33
наименьшее общее кратное, 33
наложение, 5
направление асимптотическое, 320
неполное частное, 52, 87
неприводимый элемент кольца, 92
неравенство
Коши – Буняковского – Шварца
евклидово, 239
эрмитово, 357
треугольника
евклидово, 240
эрмитово, 357
несократимое представление дроби, 63
нечётная перестановка, 171
нётерово кольцо, 89
нильпотент, 37
нильпотентная составляющая, 226
нильпотентный оператор, 121
нильрадикал, 102
норма, 250
алгебраического числа, 484
в евклидовом кольце, 87
в евклидовом пространстве, 253
стандартная в $\mathbb{R}^n$, 251
эрмитова, 356
нормализатор подгруппы, 291
нуль, 21

обобщённые элементарные преобразования, 203
оболочка
выпуклая, 248
линейная, 114
образ
гомоморфизма групп, 270
линейного отображения, 116
обратный, 99
отображения, 5
точки, 5
образующая
алгебры, 91

модуля, 190
циклической группы, 60, 267
обратный образ, 99
обращение Мёбиуса, 49
объединение множеств, 4
дизъюнктное, 5
объём, 169
евклидов, 240
симплекса, 255
эрмитов, 358
овеществление комплексного пространства, 370
однородные координаты, 316
ожерелья, 278
окрестность, 35
октаплекс, 256
октаэдр, 261
оператор
антилинейный, 361
дифференциальный, 127
комплексного сопряжения, 373
Лапласа, 367
линейный, 105
разностный, 83
Серра, 313
операторы
сопряжённые матрицей, 215
операция
алгебраическая, 70
вычитания, 24
деления, 24
композиции, 265
сложения, 21
умножения, 21
определитель, 154, 173
Вандермонда, 447
Грама, 238, 299
орбита, 260
DU-орбита, 469
ориентация, 169
базиса, 240
стандартная в $\mathbb{R}^n$, 240
ортогонал, 242
левый, 295
правый, 295
ортогонализация Грама-Шмидта, 237, 356
ортогональное дополнение, 242, 358
остаток от деления, 13
в евклидовом кольце, 87
многочленов, 52
отношение
бинарное, 11
делимости, 31
доминирования, 472
кососимметричное, 20, 167
рефлексивное, 12
симметричное, 12
сравнимости, 37
транзитивное, 12
частичного порядка, 20
эквивалентности, 11
двойное, 35, 327
отображение
n-линейное, 402
аффинное, 248
биективное, 6
бирациональное, 325
Веронезе, 321
взаимно однозначное, 6
возрастающее, 19
вычисления, 8
некоммутативное, 260
дифференцируемое, 249
инъективное, 5
линейное, 105, 189
мономорфное, 5
неубывающее, 19
обратное, 17
двустороннее, 17
левое, 16
правое, 17
Плюккера, 343, 442
полилинейное, 402
универсальное, 404
регулярное, 100
Сегре, 339, 408
факторизации, 12, 283
отражение, 258, 303
отрезок, 248

параболоид, 349
гиперболический, 350
эллиптический, 350
параллельный перенос, 246
параметризация Кэли, 257
первообразная, 77
первообразный корень
из единицы, 29
по модулю n, 48
переместительный закон, 16
пересечение множеств, 4
перестановка
инволютивная, 279
нечётная, 171
тасующая, 173, 181
чётная, 171
перечисление орбит, 276
перспективные треугольники, 330
планарность квадрики, 333
платоновы тела, 261
плоскость
α на $\mathrm{Gr}(2,4)$, 344
β на $\mathrm{Gr}(2,4)$, 344
координатная, 39
поворот, 13
гиперболический, 302
поворотная гомотетия, 26
подгруппа, 18, 266
инвариантная, 284
мультипликативная в поле, 61
нормальная, 284
силовская, 288
циклическая, 267
подмножество, 4
собственное, 4
подмодуль
дополнительный, 196
кручения, 191
собственный, 189
подобные операторы, 215
подпространства
дополнительные
векторные, 116
проективные, 324
трансверсальные, 115
подпространства на гладкой квадрике, 340
подпространство
анизотропное, 300
аффинное, 254
векторное, 104
дополнительное
векторное, 116
проективное, 324
изотропное, 300
инвариантное, 215
корневое, 224
лагранжево, 309
проективное, 322, 323
собственное, 120, 222
подрешётка соизмеримая, 207
поле, 21
$\mathbb{F}_p$, 38
вещественных чисел $\mathbb{R}$, 22
из двух элементов $\mathbb{F}_2$, 21
комплексных чисел $\mathbb{C}$, 24, 59
конечное $\mathbb{F}_p[\vartheta]$, 59
разложения, 67
рациональных функций, 63
рациональных чисел $\mathbb{Q}$, 22
частных, 62
полилинейное отображение
кососимметричное, 420
симметричное, 420
универсальное, 404
(косо) симметричное, 420
полная линейная группа, 150
полная свёртка, 417
полный прообраз, 5
полный флаг, 141
полупростая составляющая, 226
полупространство Зигеля, 385
полюс, 345
поляра, 345, 434
степени r, 438
поляризация
квадратичной формы, 297
полная, 433
грассманова многочлена, 438
поляритет, 345

полярное разложение, 365
порядок
группы, 18, 198, 260, 266
обратимого вычета, 48
элемента группы, 61, 212, 267
правила дифференцирования, 72
правило
Крамера, 178
Лейбница, 166
грассманово, 440
Литтлвуда – Ричардсона, 474
ниточек, 172
правый модуль, 188
правый сдвиг, 283
правый смежный класс, 283
представление группы, 273
преобразование
дробно линейное , 327
полярное, 345
сдвига, 39
приведение
квадратичной формы к нормальным осям, 386
по модулю n, 13, 98
принцип
Аронгольда, 443
Дирихле, 7
расщепления, 427
присоединение корня, 58
присоединённая матрица, 183
проективизация, 315
проективная гиперповерхность, 318
проективная квадрика, 333
проективное замыкание, 319
аффинной квадрики, 348
проективное линейное преобразование, 326
проективное пространство, 315
проектор, 121
проекция
из подпространства, 325
коники на прямую, 325
ортогональная, 242, 358
произведение
внешнее, 421
внутреннее, 418
декартово, 5
идеалов, 102
коммутативное, 420
матриц, 150
множеств, 5
послойное, 467
прямое
векторных пространств, 116
групп, 280
множеств, 5
расслоенное, 467
производная, 434
грассманова, 439
логарифмическая, 77
степенного ряда, 71
прообраз точки, 5
простое подполе, 46
простое число, 34
простой элемент кольца, 92
пространство
аффинное, 246
векторное, 104
вершинное, 337
гиперболическое, 300
гиперповерхностей, 320
двойственное
векторное, 123
проективное, 324
евклидово, 236
касательное
к квадрике, 338
к проективной гиперповерхности, 437
координатное, 105
линейных операторов, 112
линейных соотношений, 134
матриц, 107
метрическое, 250
многочленов, 108
направляющее, 254
подмножеств, 119
проективное, 315
симплектическое, 308
сопряжённое, 123

унитарное, 355
функций, 107
эрмитово, 355
прямая
двойная, 335
касательная
к квадрике, 338
к проективной гиперповерхности, 437
проективная, 316, 322
прямая сумма
векторных пространств, 116
подмодулей, 195
подпространств, 115
прямое произведение
векторных пространств, 116
групп, 41, 280
множеств, 5
пустое множество, 4
пучок фигур, 320
пфаффиан, 310

равенство
многочленов, 51
множеств, 4
отображений, 5
формальных степенных рядов, 51
радикал идеала, 102
радиус-вектор, 25, 246
разбиение, 82
развёртка массива, 465
разложение
в сумму двух квадратов, 50
Жордана, 225
корневое, 224
на множители в $\mathbb{Z}[x]$, 97
на неприводимые множители, 93
на простейшие дроби, 65
полярное, 365
спинорное, 425
Тейлора, 435
размерность
аффинного пространства, 246
векторного пространства, 112
пересечения подпространств, 114
проективного пространства, 315
разностный оператор, 83
верхний, 122
нижний, 122
разность множеств, 4
ранг
квадратичной формы, 298
матрицы, 131
свободного модуля, 196
тензора, 419
распавшаяся коника, 335
расслоение Хопфа, 400
расширение поля, 58
рациональная нормальная кривая, 321, 331
редукция по простому модулю, 98
результант, 186
репер, 246
рефлексивность, 12
ряд
биномиальный, 79
Кэмпбела – Хаусдорфа, 367
первообразнй, 77
степенной, 51
Тодда, 84
формальный, 51

свёртка
вектора и ковектора, 126
полная, 417
частичная, 418
свободная коммутативная алгебра, 422
свободные неизвестные, 139
свободный член, 51
свободный шар, 461
связанные неизвестные, 139
связка
прямых в $\mathbb{P}_3$, 344
α-связка, 344
β-связка, 344
фигур, 320
сдвиг, 246
сигнатура квадратичной формы, 307
силовская p-подгруппа, 288
символ Лежандра – Якоби, 50
симметризация, 430

симметрическая алгебра, 421
симметрическая группа, 18
симметрическая степень, 420
симметричность, 12
симплекс, 255
симплектическая единица, 308
системы линейных уравнений, 117, 138
скалярное произведение
  евклидово, 236
  на кольце симметрических функций, 477
  на пространстве многочленов, 256
  на пространстве функций, 237, 355
  эрмитово, 355
след, 166, 194
сложение векторов, 104
слой отображения, 5
смежный класс
  векторного подпространства, 132
  по модулю идеала, 86
  подгруппы
    левый, 282
    правый, 283
собственное
  значение, 120
  подмножество, 4
  подпространство, 120
собственное значение, 222
собственное число, 120, 222
собственный вектор, 120, 222, 374
содержание многочлена, 95
соизмеримые решётки, 207
соотношения, 91
  антикоммутирования, 178, 423
  коммутирования, 421
  Плюккера, 441
  Римана, 385
  Сильвестра, 181
сопряжение
  в симметрической группе, 275
  дифференциальных операторов, 363
  кватернионное, 391
  комплексное, 27
  линейных операторов, 129
    в евклидовом пространстве, 362
    в эрмитовом пространстве, 361, 374
  оператора автоморфизмом, 215
  элементом группы, 261, 274
сопряжённость
  силовских подгрупп, 288
  стабилизаторов, 261
сопряжённые диаграммы Юнга, 448, 476
сопряжённые комплексные структуры, 396
сопряжённые операторы, 129
  в евклидовом пространстве, 362
  в эрмитовом пространстве, 361
сопряжённые точки, 346
состав таблицы, 472
сочетательный закон, 15
спаривание, 126
  невырожденное, 126
спектр оператора, 222
специальная линейная группа, 177
спинорное разложение, 425
сравнимость по модулю, 11
  идеала, 86
  многочлена, 57
  целого числа, 37
стабилизатор
  подмножества, 288
  точки, 260
степень
  внешняя, 421
  многочлена, 52
  монома, 19
  плоской кривой, 322
  проективной гиперповерхности, 318
  симметрическая, 420
  тензорная, 416
строгий ступенчатый вид, 136
структура
  вещественная, 373
  евклидова, 236

стандартная на $\mathbb{R}^n$, 236
комплексная, 378
унитарная, 355
эрмитова, 355
стандартная на $\mathbb{C}^n$, 355
структурное кольцо, 99
струя функции, 230
сумма
идеалов, 102
подпространств, 114
прямая
векторных пространств, 116
подмодулей, 195
подпространств, 115
суммирование степеней, 84
суперкоммутативное умножение, 423
сфера, 254
схема Горнера, 54
сюрьектция, 5

таблица Юнга, 466
стандартная, 468
текст Яманучи, 466
тело, 392
тензор, 405
вырожденный, 419
Казимира, 413
кососимметрический, 429
разложимый, 405
симметрический, 429
тензорная алгебра, 416
тензорная степень, 416
тензорное произведение
DU-множеств, 474
векторов, 405
модулей, 405
операторов, 426
теорема
Брианшона, 353
Вильсона, 49
Гамильтона – Кэли, 194
Гильберта о базисе, 90
Дезарга, 330
Кантора – Бернштейна, 112
Кронекера – Капелли, 132
Лагранжа
о диагонализации квадратичной формы, 298
об индексе подгруппы, 282
о базисе векторного пространства, 111
о группировании масс, 248
о приведении к строгому ступенчатому виду, 136
о ранге матрицы, 131, 213
об инвариантных множителях, 201
об умножении на чужие алгебраические дополнения, 182
об элементарных делителях, 209
Паскаля, 353
Силова, 288
Ферма (малая), 39
Хелли, 258
Шура, 368
Эйлера
о вычетах, 47
о движениях, 246
о пятиугольных числах, 82
Юнга, 259
тетраэдр, 261
тождество
Гамильтона – Кэли, 194
Коши, 473, 478
параллелограмма, 253
Шура, 474
Эйлера, 392
Якоби, 431
Якоби – Труди, 476
топология
метрическая, 250
стандартная в $\mathbb{R}^n$, 251
точка, 4
внешняя, 250
внутренняя, 250
гладкая, 437
граничная, 251
собственная, 251
двойная, 335
кольца, 100
координатной плоскости, 39

множества, 4
особая, 437
точки
гармонические, 329
сопряжённые, 346
точная последовательность, 147
точная тройка, 147
транзитивность, 12
трансверсальные подпространства, 115
транспозиция, 171
транспонированная диаграмма Юнга, 448, 476
транспонированная матрица, 131
трансцендентный элемент алгебры, 153
тригонометрия, 27
тройка
келерова, 380
с заданным ω, 382
с заданным g, 380
точная, 147

угол между
векторами
евклидова пространства, 240
эрмитова пространства, 360
вектором и подпространством, 243
умножение
векторов на числа, 104
внешнее, 423
внутреннее, 415
грассманово, 423
коммутативное, 421
левое, 188
правое, 188
суперкоммутативное, 423
универсальное накрытие $\mathrm{SU}_2 = S^3 \twoheadrightarrow \mathrm{SO}_3(\mathbb{R})$, 394
универсальное свойство
базиса свободного модуля, 192
внешней алгебры, 423
поля частных, 63
свободной ассоциативной алгебры, 416
свободной коммутативной алгебры, 422
тензорного произведения, 404
уравнение
$ax + by = k$, 31
$z^n = a$, 30
линейное рекуррентное, 75, 230
треугольника, 471
условия
Коши – Римана, 371, 372
устойчивое паросочетание, 461

фактор
группа, 284
кольцо, 87
множество, 12
модуль, 189
по действию группы, 260
пространство, 132
решётки по подрешётке, 207
факторизация, 12
фигура выпуклая, 248
флаг
координатный, 141
многогранника, 256
форма
билинейная, 236, 292
вырожденная, 294
кососимметричная, 296
невырожденная, 294
неразложимая, 314
положительная, 236
симметричная, 236, 295
бинарная, 321
евклидова, 307
квадратичная, 297
анизотропная, 299
вещественная, 307
вырожденная, 299
гиперболическая, 299
над полем $\mathbb{F}_p$, 306
невырожденная, 299
отрицательно определённая, 307
положительно определённая, 307
линейная, 123
массива, 464

объёма, 169
полилинейная, 418
кососимметричная, 170, 420
симметричная, 420
разбиения, 10
симплектическая, 180
формальный степенной ряд, 51
формула
Джамбелли
вторая, 477
первая, 453
для длины орбиты, 261
Лагранжа, 57
Ньютона, 10, 80
Полиа – Бернсайда, 276
Пьери, 455, 475
разложения определителя, 182
формула Тейлора, 125
формулы
Виета, 66, 448
Джамбелли, 453, 477
Ньютона, 450
тригонометрические, 27
функционал
вычисления, 124, 125
координатный, 123
линейный, 123
функция
вещественно дифференцируемая, 371
высоты, 87
комплексно дифференцируемая, 371
комплекснозначная, 376
Мёбиуса, 49
перехода, 318
полиномиальная, 433
регулярная, 99
симметрическая, 456
характеристическая, 108
Эйлера, 38, 49

характеристика, 46
характеристическая функция, 108
характеристический многочлен
матрицы, 187, 194
оператора, 221
ходжева звёздочка, 426

целое замыкание, 200
целое расширение, 200
целозначный многочлен, 198
центр
векторизации, 246
грассмановой алгебры, 179
группы, 275
тяжести, 247
цикл (в группе перестановок), 268
цикловой тип
оператора, 219
перестановки, 269
цилиндр, 350
циркулянт, 458

частичная свёртка, 418
четырёхвершинник, 329
чётная перестановка, 171
чётность перестановки, 172
числа
Бернулли, 84
гауссовы, 30
Каталана, 80, 81
Костки, 472
Фиббоначчи, 75, 76, 231
число
алгебраическое, 58
комплексное, 24
простое, 34, 38
разбиений, 82, 457
собственное, 120, 222
член
младший, 51
свободный, 51
старший, 52
чум, 20, 167
полный, 20, 111

эйлеровы разложения, 35
эквивалентность, 11
экспонента, 78
грассманова, 444
от матрицы, 366

элемент
алгебраический, 67, 103, 153
бесконечного порядка, 267
единичный, 21
идемпотентный, 48
кручения, 191
множества, 4
нейтральный, 23
необратимый, 31
неприводимый, 92
нильпотентный, 37
нулевой, 21
обратимый, 31, 150
обратный, 21, 266
простой, 92
противоположный, 21
трансцендентный, 153
целый над кольцом, 200
элементарные делители, 209
элементарные операции над массивом, 460
элементарные преобразования, 136
обобщённые, 203
элементы
ассоциированные, 92
взаимно простые, 33
эллипсоид, 350
эллиптический конус, 350
эллиптический параболоид, 350
эндоморфизм, 5
множества, 5
тождественный, 5
эпиморфизм, 5
эрмитова норма, 356
эрмитово продолжение билинейной формы, 376
эффективное слово, 462

ядро
билинейной формы, 296
левое, 294
правое, 294
гомоморфизма
групп, 42, 270
модулей, 189
линейного отображения, 107, 116
язык теории множеств, 4

Оглавление

Список стандартных сокращений 2

Раздел I
Множества, отображения, разбиения

§1. Множества и отображения 4
1.1. Множества 4
1.2. Отображения 5
1.3. Разбиения 7
1.4. Классы эквивалентности 11
1.5. Композиции отображений 15
1.6. Группы преобразований 18
Задачи для самостоятельного решения к §1 18

Раздел II
Числа и функции

§2. Числовые поля и кольца 21
2.1. Поля 21
2.2. Абелевы группы 23
2.3. Поле комплексных чисел 24
2.4. Коммутативные кольца 30
2.5. Делимость 31
2.6. Взаимная простота 33
Задачи для самостоятельного решения к §2 34
§3. Кольца и поля вычетов 37
3.1. Кольцо вычетов $\mathbb{Z}/(n)$ 37
3.2. Поле $\mathbb{F}_p = \mathbb{Z}/(p)$ 38
3.3. Прямые произведения 40
3.4. Гомоморфизмы 42
3.5. Китайская теорема об остатках 44
3.6. Простое подполе и характеристика 46
Задачи для самостоятельного решения к §3 47
§4. Многочлены и алгебраические числа 51
4.1. Ряды и многочлены 51
4.2. Деление с остатком 52
4.3. Корни многочленов 56
4.4. Кольцо вычетов $\Bbbk[x]/(f)$ 57
4.5. Поле частных целостного кольца 62
4.6. Поле рациональных функций $\Bbbk(x)$ 63
Задачи для самостоятельного решения к §4 65
§5. Формальные степенные ряды 70
5.1. Алгебраические операции над формальными рядами 70

5.2. Дифференциальное исчисление . . . 71
5.3. Разложение рациональных функций . . . 74
5.4. Логарифм и экспонента . . . 77
5.5. Бином Ньютона . . . 79
Задачи для самостоятельного решения к §5 . . . 82
§6. Фактор кольца и идеалы . . . 85
6.1. Идеалы . . . 85
6.2. Факторизация . . . 86
6.3. Кольца главных идеалов . . . 87
6.4. Нётеровы кольца . . . 89
6.5. Разложение на множители . . . 92
6.6. Гомоморфизмы подъёма и вычисления . . . 99
Задачи для самостоятельного решения к §6 . . . 101

Раздел III
Векторы и матрицы

§7. Векторы . . . 104
7.1. Векторные пространства . . . 104
7.2. Базисы . . . 108
7.3. Подпространства . . . 114
7.4. Линейные операторы . . . 116
Задачи для самостоятельного решения к §7 . . . 118
§8. Двойственность . . . 123
8.1. Двойственное пространство . . . 123
8.2. Аннуляторы . . . 127
8.3. Двойственные операторы . . . 129
8.4. Фактор пространства . . . 132
8.5. Метод Гаусса . . . 135
8.6. Расположение подпространства относительно базиса . . . 140
Задачи для самостоятельного решения к §8 . . . 144
§9. Матрицы . . . 149
9.1. Алгебры над полем . . . 149
9.2. Умножение матриц . . . 150
9.3. Матрицы перехода . . . 158
9.4. Некоммутативные кольца . . . 160
Задачи для самостоятельного решения к §9 . . . 164
§10. Определители . . . 169
10.1. Объём . . . 169
10.2. Знак перестановки . . . 171
10.3. Свойства определителей . . . 175
10.4. Грассмановы многочлены . . . 178
Задачи для самостоятельного решения к §10 . . . 184
§11. Модули . . . 188

11.1. Определение модулей . . . 188
11.2. Образующие и соотношения . . . 190
11.3. Матрицы гомоморфизмов . . . 193
11.4. Разложимость . . . 195
11.5. Ранг свободного модуля . . . 196
Задачи для самостоятельного решения к §11 . . . 198
§12. Конечно порождённые модули над кольцами главных идеалов . . . 201
12.1. Теорема об инвариантных множителях . . . 201
12.2. Пример: подрешётки в $\mathbb{Z}^m$. . . . 205
12.3. Теорема об элементарных делителях . . . 208
12.4. Пример: конечно порождённые абелевы группы . . . 211
Задачи для самостоятельного решения к §12 . . . 212
§13. Пространство с оператором . . . 215
13.1. Классификация операторов . . . 215
13.2. Аннулирующие многочлены . . . 221
13.3. Перестановочные операторы . . . 225
13.4. Функции от оператора . . . 227
Задачи для самостоятельного решения к §13 . . . 232

Раздел IV
Геометрические структуры

§14. Евклидовы пространства . . . 236
14.1. Евклидова структура . . . 236
14.2. Матрицы Грама . . . 238
14.3. Евклидова геометрия . . . 239
14.4. Двойственность . . . 241
14.5. Ортогональные операторы . . . 243
14.6. Аффинные пространства . . . 246
14.7. Метрики, нормы и топология . . . 249
Задачи для самостоятельного решения к §14 . . . 253
§15. Группы . . . 260
15.1. Группы преобразований . . . 260
15.2. Абстрактные группы . . . 265
15.3. Гомоморфизмы . . . 269
15.4. Действие группы на множестве . . . 273
Задачи для самостоятельного решения к §15 . . . 278
§16. Смежные классы . . . 282
16.1. Теорема Лагранжа . . . 282
16.2. Фактор группы . . . 283
16.3. Простые группы . . . 286
16.4. p-группы . . . 287
Задачи для самостоятельного решения к §16 . . . 290
§17. Ортогональная геометрия над произвольным полем . . . 292

17.1. Билинейные формы . . . 292
17.2. Симметричные билинейные и квадратичные формы . . . 297
17.3. Изометрии невырожденной симметричной формы . . . 302
17.4. Невырожденные кососимметричные формы . . . 308
Задачи для самостоятельного решения к §17 . . . 311
§18. Проективное пространство . . . 315
18.1. Проективизация векторного пространства . . . 315
18.2. Задание фигур уравнениями . . . 318
18.3. Подпространства . . . 322
18.4. Линейные проективные преобразования . . . 326
Задачи для самостоятельного решения к §18 . . . 330
§19. Квадрики . . . 333
19.1. Проективные квадрики . . . 333
19.2. Касательное пространство к квадрике . . . 338
19.3. Пример: $\mathrm{Gr}(2,4) \subset \mathbb{P}_5$ и прямые в $\mathbb{P}_3$ . . . 342
19.4. Поляритеты . . . 345
19.5. Аффинные квадрики . . . 347
Задачи для самостоятельного решения к §19 . . . 352

Раздел V
Комплексные и вещественные структуры

§20. Эрмитовы пространства . . . 355
20.1. Эрмитова геометрия . . . 355
20.2. Сопряжение операторов . . . 361
20.3. Нормальные операторы . . . 364
20.4. Полярное разложение . . . 365
Задачи для самостоятельного решения к §20 . . . 367
§21. Комплексификация и овеществление . . . 370
21.1. Овеществление . . . 370
21.2. Комплексификация . . . 372
21.3. Эрмитово продолжение евклидовой структуры . . . 376
21.4. Комплексные структуры . . . 378
21.5. Келеровы тройки (I, g, ω) . . . 379
Задачи для самостоятельного решения к §21 . . . 386
§22. Кватернионы . . . 389
22.1. Три инволюции на пространстве $\mathrm{Mat}_2(\mathbb{C})$ . . . 389
22.2. Тело кватернионов $\mathbb{H}$ . . . 390
22.3. Универсальное накрытие $S^3 = \mathrm{SU}_2 \twoheadrightarrow \mathrm{SO}_3(\mathbb{R})$ . . . 393
22.4. Два семейства комплексных структур на $\mathbb{H}$ . . . 395
22.5. Спиноры . . . 397
Задачи для самостоятельного решения к §22 . . . 401

Раздел VI
Полилинейная алгебра

§23. Тензорные произведения модулей 403
23.1. Полилинейные отображения 403
23.2. Универсальное полилинейное отображение 405
23.3. Тензорное произведение модулей 406
23.4. Изоморфизм $U^* \otimes V \simeq \mathrm{Hom}(U,V)$ и разложимые операторы . . 409
23.5. Тензорные произведения абелевых групп 411
23.6. Канонические изоморфизмы 412
Задачи для самостоятельного решения к §23 414
§24. Тензорная алгебра векторного пространства 417
24.1. Свободная ассоциативная алгебра $\mathsf{T}(V)$ 417
24.2. Двойственность и свёртки 418
24.3. Линейный носитель тензора 419
24.4. Соотношения (косо) симметричности 421
Задачи для самостоятельного решения к §24 425
§25. Поляризация полиномов 430
25.1. Симметрические и кососимметрические тензоры 430
25.2. Поляризация коммутативных многочленов 433
25.3. Производные и поляры 434
25.4. Поляризация грассмановых многочленов 439
Задачи для самостоятельного решения к §25 443

Раздел VII
Симметрические функции, массивы и таблицы Юнга

§26. Симметрические функции 446
26.1. Симметрические и кососимметрические многочлены 446
26.2. Элементарные симметрические многочлены 449
26.3. Полные симметрические многочлены 450
26.4. Степенные суммы Ньютона 451
26.5. Детерминантные тождества 453
26.6. Кольцо симметрических функций 457
Задачи для самостоятельного решения к §26 458
§27. Исчисление массивов, таблиц и диаграмм 461
27.1. Массивы и элементарные операции над ними 461
27.2. Уплотнение массивов 464
27.3. Действие симметрической группы на DU-множествах 470
27.4. Полиномы Шура 472
27.5. Правило Литтлвуда – Ричардсона 475
27.6. Скалярное произведение 478
Задачи для самостоятельного решения к §27 479
Ответы и указания к некоторым упражнениям 482

Предметный указатель 504
Оглавление 521