А. Л. Городенцев*

А Л Г Е Б Р А

1-й курс

Факультет математики НИУ ВШЭ
2024/25 уч. год

* ВШЭ, ИТЭФ, НМУ, e-mail:gorod@itep.ru , http://gorod.bogomolov-lab.ru/

Оглавление

Оглавление 2

О множествах и отображениях 4

0.1 Множества 4
0.2 Отображения 5
0.3 Слои отображений 7
0.4 Классы эквивалентности 10
0.5 Композиции отображений 13
0.6 Группы преобразований 16
0.7 Частично упорядоченные множества 16
0.8 Вполне упорядоченные множества 18
0.9 Лемма Цорна 19

§1 Поля, коммутативные кольца и абелевы группы 21

1.1 Определения и примеры 21
1.2 Делимость в кольце целых чисел 24
1.3 Взаимная простота 27
1.4 Кольцо вычетов 28
1.5 Гомоморфизмы 30
1.6 Прямые произведения 34
1.7 Китайская теорема об остатках 35

§2 Многочлены и расширения полей 37

2.1 Ряды и многочлены 37
2.2 Делимость в кольце многочленов 40
2.3 Корни многочленов 43
2.4 Поле комплексных чисел 47
2.5 Конечные поля 50

§3 Дроби и ряды 54

3.1 Кольца частных 54
3.2 Рациональные функции 56
3.3 Логарифм и экспонента 60
3.4 Действие рядов от d/dt на многочлены от t 63

§4 Идеалы, факторкольца и разложение на множители 67

4.1 Идеалы 67
4.2 Фактор кольца 69
4.3 Области главных идеалов 72
4.4 Факториальность 73
4.5 Многочлены над факториальным кольцом 76
4.6 Разложение многочленов с целыми коэффициентами 78

§5 Векторы и матрицы 81

5.1 Модули над коммутативными кольцами 81
5.2 Алгебры над коммутативными кольцами 89

5.3 Матричный формализм 94
§6 Конечно порождённые модули над областью главных идеалов 102
6.1 Метод Гаусса 102
6.2 Инвариантные множители 111
6.3 Элементарные делители 114
§7 Конечно порождённые абелевы группы 120
7.1 Фробениусово и жорданово представления 120
7.2 Группы, заданные образующими и соотношениями 123
7.3 Общие замечания о полупростоте 126
§8 Грассмановы многочлены и определители 128
8.1 Длина, знак и чётность перестановки 128
8.2 Определитель 130
8.3 Грассмановы многочлены 132
8.4 Присоединённая матрица 138
8.5 Результант 141
§9 Пространство с оператором 143
9.1 Классификация пространств с оператором 143
9.2 Специальные классы операторов 154
9.3 Функции от операторов 160
9.4 Перестановочные операторы и разложение Жордана 165
§10 Группы 168
10.1 Группы, подгруппы, циклы 168
10.2 Группы фигур 171
10.3 Гомоморфизмы групп 174
10.4 Действие группы на множестве 178
10.5 Смежные классы и факторизация 183
10.6 Коммутант 186
§11 Композиционные факторы, произведения и силовские подгруппы 188
11.1 Простые группы 188
11.2 Композиционные факторы 190
11.3 Полупрямые произведения 193
11.4 p-группы и теоремы Силова 196
§12 Задание групп образующими и соотношениями 199
12.1 Свободные группы и соотношения 199
12.2 Пример: группы платоновых тел 202
12.3 Образующие и соотношения группы S_{n+1} 206
12.4 Порядок Брюа на симметрической группе 207
Ответы и указания к некоторым упражнениям 210

О множествах и отображениях

В этом разделе собраны некоторые факты о множествах и отображениях, которые будут использоваться в нашем курсе. Я надеюсь, что многие из них знакомы читателю из школы или вводных летних занятий «Матфак — предисловие», ну а те, что не знакомы, будут в самое ближайшее время изучены в параллельном нашему курсе теории множеств и топологии. Нет нужды «учить» данный раздел *перед* тем, как браться за курс алгебры. Но к нему стоит выборочно обращаться всякий раз, когда Вы почувствуете себя неуверенно в тех или иных рассуждениях, использующих множества, отображения, отношения или незнакомую Вам комбинаторику.

0.1. Множества. В наши цели не входит построение логически строгой теории множеств. Для понимания этого курса достаточно школьного интуитивного представления о множестве как «абстрактной совокупности элементов произвольной природы». Элементы множеств мы часто будем называть *точками*. Все точки в любом множестве, по определению, различны.

Множество X задано, как только про любой объект можно сказать, является он элементом множества X 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 $\varnothing$. Если множество X конечно, то мы обозначаем через $|X|$ количество точек в нём.

Множество X называется *подмножеством* множества Y, если каждый его 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. Подмножества, отличные от всего множества, называются *собственными*. В частности, пустое подмножество непустого множества собственное. Если надо указать, что X является собственным подмножеством в Y, используется обозначение $X \subsetneq Y$.

Упражнение 0.1. Сколько всего подмножеств (включая пустое и несобственное) имеется у множества, состоящего из n элементов?

Для заданных множеств X, Y их *объединение* $X \cup Y$ состоит из всех элементов, принадлежащих хотя бы одному из множеств X, Y; *пересечение* $X \cap Y$ состоит из всех элементов, принадлежащих одновременно каждому из множеств X, Y; *разность* $X \setminus Y$ состоит из всех элементов множества X, которые не содержатся в Y.

Упражнение 0.2. Проверьте, что операция пересечения выражается через разность по формуле $X \cap Y = X \setminus (X \setminus Y)$. 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 по определению являются всевозможные пары (x, y) с $x \in X$, $y \in Y$, называется *декартовым* (или *прямым*) *произведением* множеств X и Y.

0.2. Отображения. Отображение $f : X \to Y$ из множества X в множество Y есть правило, однозначно сопоставляющее каждой точке $x \in X$ некоторую точку $y = f(x) \in Y$, которая называется *образом* точки x при отображении f. Множество всех таких точек $x \in X$, образ которых равен заданной точке $y \in Y$, называется *полным прообразом* точки y или *слоем* отображения f над y и обозначается

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

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* $f : X \to Y$ и обозначается

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

Два отображения $f : X \to Y$ и $g : X \to Y$ *равны*, если $f(x) = g(x)$ для всех $x \in X$. Множество всех отображений из множества X в множество Y обозначается $\operatorname{Hom}(X, Y)$.

Отображение $f : X \to Y$ называется *наложением* (а также *сюръекцией* или *эпиморфизмом*), если $\operatorname{im}(f) = Y$, т. е. когда прообраз каждой точки $y \in Y$ не пуст. Мы будем изображать сюръективные 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 изображаются стрелками $X \hookrightarrow Y$.

Упражнение 0.3. Перечислите все отображения $\{0, 1, 2\} \to \{0, 1\}$ и $\{0, 1\} \to \{0, 1, 2\}$. Сколько среди них вложений и сколько наложений?

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

Упражнение 0.4. Из отображений: а) $\mathbb{N} \to \mathbb{N} : x \mapsto x^2$ б) $\mathbb{Z} \to \mathbb{Z} : x \mapsto x^2$ в) $\mathbb{Z} \to \mathbb{Z} : x \mapsto 7x$ г) $\mathbb{Q} \to \mathbb{Q} : x \mapsto 7x$ выделите все инъекции, все сюръекции и все биекции.

Отображения $X \to X$ из множества X в себя обычно называют *эндоморфизмами* множества X. Множество всех эндоморфизмов обозначается $\operatorname{End}(X) \stackrel{\text{def}}{=} \operatorname{Hom}(X, X)$.

Упражнение 0.5 (принцип Дирихле). Покажите, что следующие три условия на множество X равносильны: а) X бесконечно б) существует вложение $X \hookrightarrow X$, не являющееся наложением в) существует наложение $X \twoheadrightarrow X$, не являющееся вложением.

Взаимно однозначные эндоморфизмы $X \xrightarrow{\sim} X$ называются *автоморфизмами* X. Множество всех автоморфизмов обозначается через $\operatorname{Aut}(X)$. Автоморфизмы можно воспринимать как *перестановки* элементов множества X. У всякого множества X имеется *тождественный автоморфизм* $\operatorname{Id}_X : X \to X$, который переводит каждый элемент в самого себя: $\forall\, x \in X\ \operatorname{Id}_X(x) = x$.

Упражнение 0.6. Счётно[1] ли множество $\operatorname{Aut}(\mathbb{N})$?

[1] Множество M называется *счётным* если существует биекция $\mathbb{N} \xrightarrow{\sim} M$.

Пример 0.1 (запись отображений словами)
Рассмотрим множества $X = \{1, 2, \dots, n\}$ и $Y = \{1, 2, \dots, m\}$, сопоставим каждому отображению $f : X \to Y$ последовательность его значений:

$$w(f) \stackrel{\text{def}}{=} \big(f(x_1), f(x_2), \dots, f(x_n)\big) \tag{0-1}$$

и будем воспринимать её как n-буквенное слово, написанное при помощи m-буквенного алфавита Y. Так, отображениям $f : \{1, 2\} \to \{1, 2, 3\}$ и $g : \{1, 2, 3\} \to \{1, 2, 3\}$, действующим по правилам $f(1) = 3$, $f(2) = 2$ и $g(1) = 1$, $g(2) = 2$, $g(3) = 2$, сопоставятся слова $w(f) = (3, 2)$ и $w(g) = (1, 2, 2)$, составленные из букв алфавита $\{1, 2, 3\}$. Запись отображения словом задаёт биекцию

$$w : \ \mathrm{Hom}(X, Y) \xrightarrow{\sim} \{\text{слова из } |X| \text{ букв в алфавите } Y\}, \quad f \mapsto w(f). \tag{0-2}$$

Инъективные отображения записываются при этом словами, в которых нет повторяющихся букв, а сюръективные отображения — словами, в которых используются все без исключения буквы алфавита Y. Взаимно однозначным отображениям отвечают слова, в которых каждая буква алфавита Y встречается ровно один раз.

Предложение 0.1
Если множества X и Y конечны, то $|\mathrm{Hom}(X, Y)| = |Y|^{|X|}$.

Доказательство. Пусть X состоит из n элементов, а Y — из m, как в прим. 0.1 выше. Нас интересует количество всех n-буквенных слов, которые можно написать при помощи алфавита из m букв. Обозначим его через $W_m(n)$ и выпишем все эти слова на m страницах, поместив на i-ю страницу все слова, начинающиеся на i-ю букву алфавита. В результате на каждой странице окажется ровно по $W_m(n-1)$ слов. Поэтому $W_m(n) = m \cdot W_m(n-1) = m^2 \cdot W(n-2) = \dots = m^{n-1} \cdot W_m(1) = m^n$. □

Замечание 0.1. В виду предл. 0.1 множество $\mathrm{Hom}(X, Y)$ всех отображений $X \to Y$ часто обозначают Y^X. В доказательстве предл. 0.1 мы молчаливо предполагали, что оба множества непусты. Если $X = \varnothing$, то для любого множества Y множество $\mathrm{Hom}(\varnothing, Y)$ по определению состоит из единственного элемента — вложения $\varnothing$ в Y в качестве пустого подмножества или, что то же самое, пустого слова в алфавите Y. В этом случае предл. 0.1 остаётся в силе: $|\mathrm{Hom}(\varnothing, Y)| = 1 = |Y|^0$. В частности, $\mathrm{Hom}(\varnothing, \varnothing)$ тоже состоит из одного элемента[1] — тождественного автоморфизма $\mathrm{Id}_\varnothing$. Если $Y = \varnothing$, а $X \neq \varnothing$, то $\mathrm{Hom}(X, \varnothing) = \varnothing$, что тоже согласуется с предл. 0.1, ибо $0^{|X|} = 0$ при $|X| > 0$.

Предложение 0.2
Если $|X| = n$, то $|\mathrm{Aut}(X)| = n! \stackrel{\text{def}}{=} n \cdot (n-1) \cdot \ldots \cdot 1$.

Доказательство. Пусть $X = \{x_1, \dots, x_n\}$. Биекции $X \xrightarrow{\sim} X$ записываются n-буквенными словами в n-буквеном алфавите $x_1, \dots, x_n$, содержащими каждую букву x_i ровно по одному разу. Обозначим количество таких слов через $V(n)$ и выпишем их по алфавиту на n

[1] Т. е. 0^0 в этом контексте оказывается равным 1.

страницах, поместив на i-тую страницу все слова, начинающиеся на x_i. Тогда на каждой странице будет ровно $V(n-1)$ слов, откуда $V(n) = n \cdot V(n-1) = n \cdot (n-1) \cdot V(n-2) = = \ldots = n \cdot (n-1) \cdot \ldots \cdot 2 \cdot V(1) = n!$. □

Замечание 0.2. Число $n! = n \cdot (n-1) \cdot \ldots \cdot 1$ называется *n-факториал*. Так как множество $\mathrm{Aut}(\varnothing)$ состоит из одного элемента $\mathrm{Id}_\varnothing$, мы полагаем $0! \stackrel{\text{def}}{=} 1$.

0.3. Слои отображений. Задание отображения $f : X \to Y$ равносильно указанию подмножества $\mathrm{im}(f) \subset Y$ и разбиению множества X в дизъюнктное объединение непустых подмножеств $f^{-1}(y)$, занумерованных точками $y \in \mathrm{im}(f)$:

$$X = \bigsqcup\nolimits_{y \in \mathrm{im}(f)} f^{-1}(y)\,. \tag{0-3}$$

Такой взгляд на отображения часто оказывается полезным при подсчёте количества элементов в том или ином множестве. Например, когда все непустые слои отображения $f : X \to Y$ состоят из одного и того же числа точек $m = |f^{-1}(y)|$, число элементов в образе отображения f связано с числом элементов в множестве X соотношением

$$|X| = m \cdot |\,\mathrm{im}\, f\,|\,, \tag{0-4}$$

которое при всей своей простоте имеет много разнообразных применений.

Пример 0.2 (мультиномиальные коэффициенты)
При раскрытии скобок в выражении $(a_1 + \ldots + a_m)^n$ получится сумма одночленов вида $a_1^{k_1} \ldots a_m^{k_m}$, где каждый показатель k_i заключён в пределах $0 \leqslant k_i \leqslant n$, а общая степень $k_1 + \ldots + k_m = n$. Коэффициент, возникающий при таком одночлене после приведения подобных слагаемых, называется *мультиномиальным коэффициентом* и обозначается $\binom{n}{k_1 \ldots k_m}$. Таким образом,

$$(a_1 + \ldots + a_m)^n = \sum_{\substack{k_1+\ldots+k_m=n \\ \forall i\ 0 \leqslant k_i \leqslant n}} \binom{n}{k_1 \ldots k_m} \cdot a_1^{k_1} \ldots a_m^{k_m}\,, \tag{0-5}$$

Чтобы явно выразить $\binom{n}{k_1 \ldots k_m}$ через $k_1, \ldots, k_m$, заметим, что раскрытие n скобок

$$(a_1 + \ldots + a_m)(a_1 + \ldots + a_m) \ldots (a_1 + \ldots + a_m)$$

заключается в выборе внутри каждой из скобок какой-нибудь одной буквы и выписывании их слева направо друг за другом в одно n-буквенное слово. Это надо сделать всеми возможными способами и сложить все полученные слова. Подобные слагаемые, вносящие вклад в коэффициент при $a_1^{k_1} a_2^{k_2} \ldots a_m^{k_m}$, суть слова, состоящие ровно из k_1 букв a_1, k_2 букв a_2, … , k_m букв a_m. Количество таких слов легко подсчитать по формуле (0-4). А именно, сделаем на время k_1 букв a_1 попарно разными, снабдив каждую из них дополнительным верхним индексом; аналогично поступим с k_2 буквами a_2, k_3 буквами

a_3 и т. д. В результате получим $n = k_1 + \ldots + k_m$ попарно разных букв:

$$\underbrace{a_1^{(1)}, a_1^{(2)}, \ldots, a_1^{(k_1)}}_{k_1 \text{ меченых букв } a_1}, \underbrace{a_2^{(1)}, a_2^{(2)}, \ldots, a_2^{(k_2)}}_{k_2 \text{ меченых букв } a_2}, \ \ldots\ldots\ldots\ , \underbrace{a_m^{(1)}, a_m^{(2)}, \ldots, a_m^{(k_m)}}_{k_m \text{ меченых букв } a_m}.$$

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 k_1 одинаковых букв a_1, k_2 одинаковых букв a_2, и т. д. и рассмотрим отображение $f : X \to Y$, стирающее верхние индексы у всех букв. Оно эпиморфно, и полный прообраз каждого слова $y \in Y$ состоит из $k_1! \cdot k_2! \cdot \ \ldots\ \cdot k_m!$ слов, которые получаются из y всевозможными расстановками k_1 верхних индексов у букв a_1, k_2 верхних индексов у букв a_2, и т. д. По формуле (0-4)

$$\binom{n}{k_1 \ldots k_m} = \frac{n!}{k_1! \cdot k_2! \cdot \ \ldots\ \cdot k_m!}. \tag{0-6}$$

Тем самым, разложение (0-5) имеет вид

$$(a_1 + \ldots + a_m)^n = \sum_{\substack{k_1+\ldots+k_m=n \\ \forall i\ 0 \leqslant k_i \leqslant n}} \frac{n! \cdot a_1^{k_1} \ldots a_m^{k_m}}{k_1! \cdot \ldots \cdot k_m!}. \tag{0-7}$$

Упражнение 0.7. Сколько всего слагаемых в правой части формулы (0-7) ?

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

$$(a + b)^n = \sum_{k=0}^{n} \frac{n!}{k!(n-k)!}\, a^k b^{n-k}. \tag{0-8}$$

При $m = 2$ мультиномиальный коэффициент $\binom{n}{k,n-k}$ принято обозначать $\binom{n}{k}$ или C_n^k и называть k-тым *биномиальным коэффициентом* степени n или *числом сочетаний* из n по k. Он равен

$$\binom{n}{k} = C_n^k = \frac{n \cdot (n-1) \cdot \ldots \cdot (n-k+1)}{k \cdot (k-1) \cdot \ldots \cdot 1}$$

(сверху и снизу стоит по k последовательно убывающих сомножителей).

Пример 0.3 (диаграммы Юнга)
Разбиение конечного множества $X = \{1, 2, \ldots, n\}$ в объединение непересекающихся подмножеств

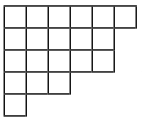
$$X = X_1 \sqcup X_2 \sqcup \ \ldots\ \sqcup X_k \tag{0-9}$$

[1] Это частный случай *формулы Ньютона*, которую мы обсудим в полной общности, когда будем заниматься степенными рядами.

можно кодировать следующим образом. Занумеруем подмножества в порядке нестрогого убывания их размера и обозначим количество элементов в i-том подмножестве через $\lambda_i = |X_i|$. Получим невозрастающую последовательность чисел

$$\lambda = (\lambda_1, \dots, \lambda_k), \quad \lambda_1 \geqslant \lambda_2 \geqslant \dots \geqslant \lambda_k,$$

которая называется *формой* разбиения (0-9). Форму разбиения удобно изображать *диаграммой Юнга* — картинкой вида

 , (0-10)

составленной из выровненных по левому краю горизонтальных клетчатых полосок, занумерованных сверху вниз, так что в i-й сверху полоске λ_i клеток. Общее число клеток в диаграмме λ называется её *весом* и обозначается $|\lambda|$, а количество строк называется *длиной* и обозначается $\ell(\lambda)$. Так, диаграмма Юнга (0-10) отвечает разбиению формы $\lambda = (6, 5, 5, 3, 1)$, имеет вес $|\lambda| = 20$ и длину $\ell(\lambda) = 5$.

Упражнение 0.8. Подсчитайте количество всех диаграмм Юнга, умещающихся в прямоугольнике размером $k \times n$ клеток с левым верхним углом в левом верхнем углу диаграммы (включая пустую диаграмму и сам прямоугольник).

Будем называть *заполнением* диаграммы λ множеством X из $|X| = |\lambda|$ элементов произвольную расстановку этих элементов в клетки диаграммы по одному элементу в каждую клетку. Таким образом, всякая диаграмма λ веса n имеет $n!$ различных заполнений заданным n-элементным множеством X.

Объединяя элементы, стоящие в i-й строке диаграммы в одно подмножество X_i, мы получаем разбиение множества X в дизъюнктное объединение k непересекающихся подмножеств $X_1, \dots, X_k$. Поскольку любое разбиение (0-9) заданной формы λ можно получить таким образом, возникает сюръективное 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 $m_i = m_i(\lambda)$ число строк длины[1] i в диаграмме λ, то перестановок первого типа будет $\prod \lambda_i! = \prod_{i=1}^{n} (i!)^{m_i}$ штук, а второго типа — $\prod_{i=1}^{n} m_i!$ штук. Так как все эти перестановки действуют независимо друг от друга, каждый слой нашего отображения состоит из $\prod_{i=1}^{n} (i!)^{m_i} m_i!$ элементов. Из формулы (0-4) вытекает

Предложение 0.3
Число разбиений n-элементного множества X в дизъюнктное объединение m_1 1-элементных, m_2 2-элементных, … , m_n n-элементных подмножеств равно

$$\frac{n!}{\prod_{i=1}^{n} m_i! \cdot (i!)^{m_i}}. \tag{0-11}$$

[1] Отметим, что многие $m_i = 0$, поскольку $|\lambda| = n = m_1 + 2m_2 + \dots + nm_n$.

0.4. Классы эквивалентности. Альтернативный способ разбить заданное множество 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 любое подмножество

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

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

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

$$\text{равенство} \qquad x_1 \underset{R}{\sim} x_2 \overset{\text{def}}{\iff} x_1 = x_2 \tag{0-12}$$

$$\text{предшествование} \qquad x_1 \underset{R}{\sim} x_2 \overset{\text{def}}{\iff} x_1 \leqslant x_2 \tag{0-13}$$

$$\text{делимость} \qquad x_1 \underset{R}{\sim} x_2 \overset{\text{def}}{\iff} x_1 | x_2 \tag{0-14}$$

$$\text{сравнимость по модулю } n \qquad x_1 \underset{R}{\sim} x_2 \overset{\text{def}}{\iff} x_1 \equiv x_2 \pmod{n} \tag{0-15}$$

(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 $x_1 - x_2$ делится на n).

Определение 0.1
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 бинарных отношений (0-12) – (0-15) первое и последнее являются эквивалентностями, а (0-13) и (0-14) не являются (они не симметричны).

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 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). Любые 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 эквивалентности R. Сюрьекция

$$f : X \twoheadrightarrow X/R\,, \quad x \mapsto [x]_R\,, \tag{0-16}$$

сопоставляющая каждому элементу $x \in X$ его класс эквивалентности $[x]_R \in X/R$, называется *отображением факторизации*. Слои этого отображения суть классы эквивалентных элементов. Наоборот, любое сюрьективное отображение $f : X \twoheadrightarrow Y$ является отображением факторизации по отношению эквивалентности $x_1 \sim x_2$, означающему, что $f(x_1) = f(x_2)$.

Пример 0.4 (классы вычетов)
Фиксируем ненулевое целое число $n \in \mathbb{Z}$. Фактор множества целых чисел $\mathbb{Z}$ по отношению сравнимости по модулю n из (0-15) обозначается $\mathbb{Z}/(n)$. Мы будем записывать его элементы символами $[z]_n$, где $z \in \mathbb{Z}$, и опускать индекс n, когда понятно чему он равен. Класс эквивалентности

$$[z]_n \stackrel{\text{def}}{=} \{x \in \mathbb{Z} \mid (z - x) \vdots n\} \tag{0-17}$$

называется *классом вычетов по модулю* n. Отображение факторизации

$$\mathbb{Z} \twoheadrightarrow \mathbb{Z}/(n)\,, \quad z \mapsto [z]_n$$

называется *приведением по модулю* n. Множество $\mathbb{Z}/(n)$ состоит из n различных классов

$$[0]_n\,,\ [1]_n\,,\ \ldots\,,\ [n-1]_n\,.$$

При желании их можно воспринимать как остатки от деления на n, но в практических вычислениях удобнее работать с ними именно как с *подмножествами* в $\mathbb{Z}$, поскольку возможность по-разному записывать один и тот же класс часто упрощает вычисления. Например, остаток от деления 12^{100} на 13 можно искать как

$$\left[12^{100}\right]_{13} = [12]_{13}^{100} = [-1]_{13}^{100} = \left[(-1)^{100}\right]_{13} = [1]_{13}\,. \tag{0-18}$$

Упражнение 0.9. Докажите правомочность этого вычисления: проверьте, что классы вычетов $[x+y]_n$ и $[xy]_n$ не зависят от выбора чисел $x \in [x]_n$ и $y \in [y]_n$, т. е. правила

$$[x]_n + [y]_n \stackrel{\text{def}}{=} [x+y]_n \tag{0-19}$$

$$[x]_n \cdot [y]_n \stackrel{\text{def}}{=} [xy]_n \tag{0-20}$$

корректно определяют на множестве $\mathbb{Z}/(n)$ операции сложения и умножения[1].

[1] Именно такое умножение $[12]^{100} = \underbrace{[12] \cdot [12] \cdot \ldots \cdot [12]}_{100} = \left[12^{100}\right]$ было использовано в (0-18).

0.4.1. Неявное задание эквивалентности. Для любого семейства отношений эквивалентности $R_\nu \subset X \times X$ пересечение $\bigcap_\nu R_\nu \subset X \times X$ также является отношением эквивалентности. В самом деле, если каждое из множеств $R_\nu \subset X \times X$ содержит диагональ

$$\Delta = \{(x, x) \mid x \in X\} \subset X \times X\,,$$

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 $\bigcap_\nu R_\nu$ 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.

Упражнение 0.10. Проверьте, что $(x, y) \in \overline{R}$ если и только если в X существует такая конечная последовательность точек $x = z_0, z_1, z_2, \ldots, z_n = y$, что $(z_{i-1}, z_i) \in R$ или $(z_i, z_{i-1}) \in R$ при каждом $i = 1, 2, \ldots, n$.

К сожалению, по данному подмножеству $R \subset X \times X$ не всегда легко судить о том, как устроена порождённая им эквивалентность $\overline{R}$. Даже выяснить, не окажутся ли в результате все точки эквивалентными друг другу может быть не просто.

Пример 0.5 (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* понимается класс эквивалентности упорядоченных пар (a, b), где $a \in \mathbb{Z}$, $b \in \mathbb{Z} \smallsetminus 0$, по минимальному отношению эквивалентности, содержащему все отождествления

$$(a, b) \sim (ac, bc) \quad \text{с произвольными } c \in \mathbb{Z} \smallsetminus \{0\}\,. \tag{0-21}$$

Отношения (0-21) выражают собою равенства дробей $a/b = (ac)/(bc)$, но сами по себе не образуют эквивалентности. Например, при $a_1 b_2 = a_2 b_1$ в двухшаговой цепочке отождествлений $(a_1, b_1) \sim (a_1 b_2, b_1 b_2) = (a_2 b_1, b_1 b_2) \sim (a_2, b_2)$ самый левый и самый правый элементы могут не отождествляться напрямую по правилу (0-21), как, например, $3/6$ и $5/10$. Поэтому эквивалентность, порождённая отождествлениями (0-21), обязана содержать все отождествления

$$(a_1, b_1) \sim (a_2, b_2) \quad \text{при} \quad a_1 b_2 = a_2 b_1\,. \tag{0-22}$$

Оказывается, что к этим отношениям больше уже ничего добавлять не надо.

Упражнение 0.11. Проверьте, что набор отношений (0-22) рефлексивен, симметричен и транзитивен.

Тем самым, он является минимальным отношением эквивалентности, содержащим все отождествления (0-21). Отметим, что если в отношениях (0-21) разрешить нулевые c, то все пары (a, b) окажутся эквивалентны паре $(0, 0)$.

0.5. Композиции отображений. Отображение $X \to Z$, получающееся в результате последовательного выполнения двух отображений $f : X \to Y$ и $g : Y \to Z$ называется *композицией* отображений g и f и обозначается $g \circ f$ или просто gf. Таким образом, композиция gf определена если и только если образ f содержится в множестве, на котором определено отображение g, и $gf : X \to Z$, $x \mapsto g(f(x))$.

Хотя композицию и принято записывать точно так же, как умножение чисел, единственным общим свойством этих операций является их *ассоциативность* или *сочетательный закон*: композиция трёх последовательных отображений

$$X \xrightarrow{f} Y \xrightarrow{g} Z \xrightarrow{h} T\,,$$

как и произведение трёх чисел, не зависит от того, в каком порядке перемножаются последовательные пары элементов, т. е. $(hg)f = h(gf)$, если хотя бы одна из двух частей этого равенства определена. Действительно, в этом случае вторая часть тоже определена, и обе части действуют на каждую точку $x \in X$ по правилу $x \mapsto h(g(f(x)))$.

В остальном алгебраические свойства композиции весьма далеки от привычных свойств умножения чисел. Если композиция fg определена, то противоположная композиция gf часто бывает не определена. Даже если $f, g : X \to X$ являются эндоморфизмами одного и того же множества X, так что обе композиции fg и gf определены, равенство $fg = gf$ может не выполняться.

Упражнение 0.12. 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 $\sigma_1\sigma_2 = \sigma_2\sigma_1$?

Общие множители тоже бывает нельзя сокращать, т. е. ни равенство $fg = fh$, ни равенство $gf = hf$, вообще говоря, не влекут равенства $g = h$.

Пример 0.6 (эндоморфизмы двухэлементного множества)
Двухэлементное множество $X = \{1, 2\}$ имеет ровно четыре эндоморфизма. Если кодировать отображение $f : X \to X$ двубуквенным словом $(f(1), f(2))$, как в прим. 0.1 на стр. 6, то эти четыре эндоморфизма запишутся словами $(1,1)$, $(1,2) = \mathrm{Id}_X$, $(2,1)$ и $(2,2)$. Все композиции между ними определены, и таблица композиций gf имеет вид:

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

(0-23)

Обратите внимание на то, что $(2,2)\circ(1,1) \neq (1,1)\circ(2,2)$ и что $(1,1)\circ(1,2) = (1,1)\circ(2,1)$, хотя $(1,2) \neq (2,1)$, и $(1,1) \circ (2,2) = (2,1) \circ (2,2)$, хотя $(1,1) \neq (2,1)$.

Лемма 0.1 (левые обратные отображения)
Если $X \neq \varnothing$, то следующие условия на отображение $f : X \to Y$ эквивалентны:

1) f инъективно

2) существует такое отображение $g : Y \to X$, что $gf = \mathrm{Id}_X$

3) для любых отображений $g_1, g_2 : Z \to X$ из равенства $fg_1 = fg_2$ вытекает равенство $g_1 = g_2$.

Доказательство. Импликация (1) ⇒ (2): для точек $y = f(x) \in \operatorname{im} f$ положим $g(y) = x$, а в точках $y \notin \operatorname{im} f$ зададим g как угодно[1]. Импликация (2) ⇒ (3): если $fg_1 = fg_2$, то умножая обе части слева на любое такое отображение $g : Y \to X$, что $gf = \mathrm{Id}_X$, получаем $g_1 = g_2$. Импликация (3) ⇒ (1) доказывается от противного. Пусть $x_1 \neq x_2$, но $f(x_1) = f(x_2)$. Положим $g_1 = \mathrm{Id}_X$, и пусть $g_2 : X \xrightarrow{\sim} X$ переставляет между собою точки x_1, x_2, а все остальные точки оставляет на месте. Тогда $g_1 \neq g_2$, но $fg_1 = fg_2$. □

Определение 0.2
Отображение $f : X \to Y$, удовлетворяющее лем. 0.1, называется *обратимым слева*, и всякое такое отображение $g : Y \to X$, что $gf = \mathrm{Id}_X$, называется *левым обратным* к f или *ретракцией* Y на $f(X)$.

Упражнение 0.13. В условиях лем. 0.1 убедитесь, что вложение f тогда и только тогда имеет несколько различных левых обратных, когда оно не сюръективно.

0.5.1. Правое обратное отображение и аксиома выбора. Стремление к гармонии вызывает желание иметь «правую» версию лем. 0.1 — хочется, чтобы следующие три свойства отображения $f : X \to Y$ тоже были эквивалентны:

1) f сюръективно

2) существует такое отображение $g : Y \to X$, что $fg = \mathrm{Id}_Y$

3) для любых отображений $g_1, g_2 : Y \to Z$ из равенства $g_1 f = g_2 f$ вытекает равенство $g_1 = g_2$.

Отображение f, удовлетворяющее свойству (2), называется *обратимым справа*, а такое отображение $g : Y \to X$, что $fg = \mathrm{Id}_Y$, называется *правым обратным* к f или *сечением* эпиморфизма f. Второе название связано с тем, что отображение g, удовлетворяющее свойству (2), переводит каждую точку $y \in Y$ в точку $g(y) \in f^{-1}(y)$, лежащую в слое отображения f над точкой y.

В строгой теории множеств, углубления в которую мы пытаемся избежать, импликация (1) ⇒ (2) постулируется в качестве одной из аксиом. Эта аксиома называется *аксиомой выбора* и утверждает, что в каждом слое любого сюръективного отображения можно выбрать по элементу[2].

[1] Например, отобразим их все в одну и ту же произвольно выбранную точку $x \in X$.

[2] Иными словами, если имеется множество попарно непересекающихся множеств, то в каждом из них можно выбрать по элементу.

Доказательство импликации (2) ⇒ (3) полностью симметрично доказательству аналогичной импликации из лем. 0.1: применяя отображения, стоящие в обеих частях равенства $g_1 f = g_2 f$, вслед за таким отображением $g : Y \to X$, что $fg = \mathrm{Id}_Y$, получаем равенство $g_1 = g_2$.

Импликация (3) ⇒ (1) доказывается, как в лем. 0.1, от противного: при $y \notin \operatorname{im} f$ свойство (3) не выполняется для $g_1 = \mathrm{Id}_Y$ и любого отображения $g_2 : Y \to Y$, переводящего точку y в какую-нибудь точку из $\operatorname{im} f$ и оставляющего на месте все остальные точки.

Таким образом, перечисленные выше свойства (1) – (3) действительно эквивалентны друг другу, если включить аксиому выбора в список свойств, определяющих множества.

0.5.2. Обратимые отображения. Если отображение $g : X \xrightarrow{\sim} Y$ биективно, то прообраз $g^{-1}(y) \subset X$ каждой точки $y \in Y$ состоит ровно из одной точки. В этом случае правило $y \mapsto g^{-1}(y)$ определяет отображение $g^{-1} : Y \to X$, которое является одновременно и левым, и правым обратным к g в смысле опр. 0.2 и n° 0.5.1, т. е.

$$g \circ g^{-1} = \mathrm{Id}_Y \qquad \text{и} \qquad g^{-1} \circ g = \mathrm{Id}_X \tag{0-24}$$

Отображение g^{-1} называется *обратным* к биективному отображению g.

Предложение 0.4
Следующие условия на отображение $g : X \to Y$ эквивалентны друг другу:

1) g взаимно однозначно

2) существует такое отображение $g' : Y \to X$, что[1] $g \circ g' = \mathrm{Id}_Y$ и $g' \circ g = \mathrm{Id}_X$

3) g обладает левым и правым обратными отображениями[2].

При выполнении этих условий все левые и правые обратные к g отображения равны друг другу и отображению g^{-1}, описанному перед формулировкой предложения.

Доказательство. Импликация (1) ⇒ (2) уже была установлена. Очевидно, что (2) ⇒ (3). Докажем, что (3) ⇒ (2). Если у отображения $g : X \to Y$ есть левое обратное $f : Y \to X$ и правое обратное $h : Y \to X$, то $f = f \circ \mathrm{Id}_Y = f \circ (g \circ h) = (f \circ g) \circ h = \mathrm{Id}_X \circ h = h$ и условие (2) выполнено для $g' = f = h$. Остаётся показать, что (2) ⇒ (1), и $g' = g^{-1}$. Так как $g(g'(y)) = y$ для любого $y \in Y$, прообраз $g^{-1}(y)$ каждой точки $y \in Y$ содержит точку $g'(y)$. С другой стороны, поскольку для всех $x \in g^{-1}(y)$ выполнено равенство $x = \mathrm{Id}_X(x) = g'(g(x)) = g'(y)$, прообраз $f^{-1}(y)$ состоит из единственной точки $g'(y)$, т. е. g — биекция, и $g' = g^{-1}$. □

[1] Т. е. g' *двусторонне* обратно к g.

[2] Обратите внимание, что совпадения левого обратного отображения с правым обратным отображением не требуется.

0.6. 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.

Пример 0.7 (группы перестановок)
Множество $\mathrm{Aut}(X)$ всех взаимно однозначных отображений $X \to X$ 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 $\{1, 2, \ldots, n\}$ обозначается S_n и называется n-й *симметрической группой*. Согласно предл. 0.2 на стр. 6 порядок $|S_n| = n!$. Перестановки

$$\sigma : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$$

принято записывать строчками $\sigma = (\sigma_1, \ldots, \sigma_n)$ их значений $\sigma_i \stackrel{\text{def}}{=} \sigma(i)$, как в прим. 0.1 на стр. 6. Например, перестановки $\sigma = (3, 4, 2, 1)$ и $\tau = (2, 3, 4, 1)$ представляют собою отображения

$$\begin{array}{cccc} 1 & 2 & 3 & 4 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 3 & 4 & 2 & 1 \end{array} \quad \text{и} \quad \begin{array}{cccc} 1 & 2 & 3 & 4 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 2 & 3 & 4 & 1 \end{array}$$

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

Упражнение 0.14. Составьте таблицу умножения шести элементов группы S_3, аналогичную таблице (0-23) на стр. 13.

Пример 0.8 (абелевы группы)
Группа G, в которой любые два элемента $f, g \in G$ перестановочны, т. е. удовлетворяют соотношению $fg = gf$, 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 $n \geqslant 2$ повороты на углы, кратные $2\pi/n$, образуют в группе SO_2 конечную подгруппу. Она называется *циклической группой порядка* n.

0.7. Частично упорядоченные множества. Бинарное отношение[1] $x \leqslant y$ на множестве Z называется *частичным порядком*, если оно рефлексивно и транзитивно[2], но в отличие от эквивалентности не симметрично, а *кососимметрично*, т. е. из $x \leqslant y$ и $y \leqslant x$ вытекает равенство $x = y$. Если на множестве задан частичный порядок, мы пишем

[1] См. n° 0.4 на стр. 10.
[2] Ср. с опр. 0.1 на стр. 10.

$x < y$, когда $x \leqslant y$ и $x \neq y$. Частичный порядок на множестве Z называется *линейным* (или просто *порядком*), если любые два элемента сравнимы, т. е. для всех $x, y \in Z$ выполняется одно из трёх альтернативных условий: или $x < y$, или $x = y$, или $y < x$. Например, обычное неравенство между числами является линейным порядком на множестве натуральных чисел $\mathbb{N}$, тогда как отношение делимости $n \mid m$, означающее, что n делит m, задаёт на $\mathbb{N}$ частичный порядок, который не является линейным. Другим важным примером частичного, но не линейного порядка является отношение включения $X \subseteq Y$ на множестве $\mathcal{S}(M)$ всех подмножеств заданного множества M.

Упражнение 0.15 (предпорядок). *Предпорядком* на множестве Z называется любое рефлексивное транзитивное бинарное отношение $x \prec y$. Убедитесь, что для каждого предпорядка бинарное отношение $x \sim y$, означающее, что одновременно $x \prec y$ и $y \prec x$, является отношением эквивалентности, и на факторе $Z/\sim$ корректно определено[1] бинарное отношение $[x] \leqslant [y]$, означающее, что $x \prec y$, которое является частичным порядком. Продумайте, как всё это работает для отношения делимости $n \mid m$ на множестве целых чисел $\mathbb{Z}$.

Множество P с зафиксированным на нём частичным порядком называется *частично упорядоченным множеством*, сокращённо — чумом. Если порядок линейный, чум P называется *линейно упорядоченным*. Всякое подмножество X любого чума P также является чумом по отношению к частичному порядку, имеющемуся на P. Если этот индуцированный с P порядок на X оказывается линейным, подмножество $X \subset P$ называют *цепью* в чуме P. Элементы x, y чума P называются *сравнимыми*, если $x \leqslant y$ или $y \leqslant x$. Если же ни одно из этих условий не выполняется, то x и y называются *несравнимыми*. Несравнимые элементы автоматически различны. Частичный порядок линеен тогда и только тогда, когда любые два элемента сравнимы.

Отображение $f : M \to N$ между чумами M, N называется *сохраняющим порядок*[2] или *морфизмом* чумов, если $f(x) \leqslant f(y)$ для всех $x \leqslant y$. Два чума M, N называются *изоморфными*, если имеется сохраняющая порядок биекция $M \xrightarrow{\sim} N$. В таком случае мы пишем $M \simeq N$. Отображение f называется *строго возрастающим*, если $f(x) < f(y)$ для всех $x < y$. Всякое сохраняющее порядок вложение является строго возрастающим. Обратное справедливо для возрастающих отображений из линейного упорядоченного множества, однако неверно в общем случае.

Элемент y чума P называется *верхней гранью* подмножества $X \subset P$, если $x \leqslant y$ для всех $x \in X$. Если при этом $y \notin X$, то верхняя грань y называется *внешней*. В таком случае для всех $x \in X$ выполнено строгое неравенство $x < y$.

Элемент $m^* \in X$ называется *максимальным* в подмножестве $X \subset P$, если для $x \in X$ неравенство $m^* \leqslant x$ выполняется только при $x = m^*$. Заметьте, что максимальный элемент не обязан быть сравним со всеми элементами $x \in X$ и, тем самым, может не являться верхней гранью для X. Частично упорядоченное множество может иметь несколько различных максимальных элементов или не иметь их вовсе, как, например, чум $\mathbb{N}$ по отношению к делимости или к обычному неравенству между числами. Линей-

[1] Т. е. выполнение или невыполнение условия $x \precsim y$ не зависит от выбора представителей x и y в классах $[x]$ и $[y]$.

[2] А также *неубывающим* или *нестрого возрастающим*.

но упорядоченный чум имеет не более одного максимального элемента, и если такой элемент существует, то он является верхней гранью.

Симметричным образом, элемент $m_* \in X$ называется *минимальным* в X, если для $x \in X$ неравенство $m_* \geqslant x$ выполняется только при $x = m_*$. Аналогично определяются и нижние грани, и всё сказанное выше о максимальных элементах и верхних гранях в равной степени относится и к минимальным элементам и нижним граням.

0.8. Вполне упорядоченные множества. Линейно упорядоченное множество W называется *вполне упорядоченным*, если каждое непустое подмножество $S \subset W$ содержит такой элемент $s_* \in S$, что $s_* \leqslant s$ для всех $s \in S$. Этот элемент автоматически единствен и называется *начальным элементом* подмножества S. Например, множество натуральных чисел $\mathbb{N}$ со стандартным отношением неравенства между числами вполне упорядочено, как и любое дизъюнктное объединение вида $\mathbb{N} \sqcup \mathbb{N} \sqcup \mathbb{N} \sqcup \ldots$, в котором все элементы каждой копии множества $\mathbb{N}$ полагаются строго большими всех элементов всех предыдущих копий. Пустое множество тоже вполне упорядочено. Напротив, множество $\mathbb{Q}$ со стандартным отношением неравенства между числами не является вполне упорядоченным.

Вполне упорядоченные множества замечательны тем, что их элементы можно рекурсивно перебрать точно также, как и элементы множества $\mathbb{N}$. А именно, пусть некоторое утверждение $\Phi(w)$ зависит от элемента w вполне упорядоченного множества W. Если $\Phi(w)$ истинно для начального элемента w_* множества W, и для каждого $w \in W$ истинность утверждения $\Phi(x)$ при всех $x < w$ влечёт за собою истинность утверждения $\Phi(w)$, то $\Phi(w)$ истинно для всех $w \in W$.

Упражнение 0.16. Убедитесь в этом.

Такой способ доказательства утверждения $\Phi(w)$ для всех $w \in W$ называется *трансфинитной индукцией*. Используемые для индуктивного перехода подмножества, состоящие из всех элементов, предшествующих данному элементу w, называются *начальными интервалами* частично упорядоченного множества W и обозначаются

$$[w) \stackrel{\text{def}}{=} \{x \in W \mid x < w\}.$$

Элемент $w \in W$ называется *точной верхней гранью* начального интервала $[w) \subset W$ и однозначно восстанавливается по интервалу $[w)$ как начальный элемент множества $W \smallsetminus [w)$. Отметим, что начальный элемент $w_* \in W$ является точной верхней гранью пустого начального интервала $[w_*) = \varnothing$.

Упражнение 0.17. Покажите, что собственное подмножество $I \subsetneq W$ тогда и только тогда является начальным интервалом вполне упорядоченного множества W, когда $[x) \subset I$ для каждого $x \in I$, и в этом случае точная верхняя грань интервала I однозначно восстанавливается по I как начальный элемент дополнения $W \smallsetminus I$.

Между вполне упорядоченными множествами имеется отношение порядка $U \leqslant W$, означающее, что U можно биективно и с сохранением порядка отобразить на W или на какой-нибудь начальный интервал $[w) \subset W$. Если при этом U и W не изоморфны, мы пишем $U < W$. Хорошим упражнением на трансфинитную индукцию является

Упражнение 0.18. Убедитесь, что для любой пары вполне упорядоченных множеств U, W выполнено ровно одно из соотношений: или $U < W$, или $U \simeq W$, или $W < U$.

Классы изоморфных вполне упорядоченных множеств называют *ординалами*. Множество $\mathbb{N}$ со стандартным порядком можно воспринимать как множество всех конечных ординалов. Все остальные ординалы, включая $\mathbb{N}$, называются *трансфинитными*.

0.9. Лемма Цорна. Рассмотрим произвольное частично упорядоченное множество P и обозначим через $\mathcal{W}(P)$ множество всех подмножеств $W \subset P$, которые вполне упорядочены имеющимся на P отношением $x \leqslant y$. Множество $\mathcal{W}(P)$ непусто и содержит пустое подмножество $\varnothing \subset P$, а также все конечные цепи[1] $C \subset P$, в частности, все элементы множества P.

Лемма 0.2
Не существует такого отображения $\varrho : \mathcal{W}(P) \to P$, что $\varrho(W) > w$ для всех $W \in \mathcal{W}(P)$ и $w \in W$.

Доказательство. Пусть такое отображение ϱ существует. Назовём вполне упорядоченное подмножество $W \subset P$ рекурсивным, если $\varrho([w)) = w$ для всех $w \in W$. Например, подмножество

$$\Big\{ \varrho(\varnothing),\ \varrho\big(\{\varrho(\varnothing)\}\big),\ \varrho\Big(\big\{\varrho(\varnothing),\ \varrho(\{\varrho(\varnothing)\})\big\}\Big),\ \dots \Big\}$$

рекурсивно и его можно расширять дальше вправо, пока P не исчерпается, что противоречит наложенному на ϱ условию. Уточним сказанное. Если два рекурсивных вполне упорядоченных подмножества имеют общий начальный элемент, то либо они совпадают, либо одно из них является начальным интервалом другого.

Упражнение 0.19. Докажите это.

Обозначим через $U \subset P$ объединение всех рекурсивных вполне упорядоченных подмножеств в P с начальным элементом $\varrho(\varnothing)$.

Упражнение 0.20. Убедитесь, что подмножество $U \subset P$ вполне упорядочено и рекурсивно.

Поскольку элемент $\varrho(U)$ строго больше всех элементов из U, он не лежит в U. С другой стороны, множество $W = U \cup \{\varrho(U)\}$ вполне упорядочено, рекурсивно, и его начальным элементом является $\varrho(\varnothing)$. Следовательно, $W \subset U$, откуда $\varrho(U) \in U$. Противоречие. □

Предложение 0.5
Если каждое вполне упорядоченное подмножество чума P имеет верхнюю грань[2], то в P есть максимальный элемент[3] (возможно не единственный).

Доказательство. Если максимального элемента нет, то для любого $p \in P$ имеется такой элемент $p' \in P$, что $p < p'$. Тогда для каждого вполне упорядоченного подмножества $W \subset P$ найдётся такой элемент $w^* \in P$, что $w < w^*$ для всех $w \in W$. Сопоставляя каждому $W \in \mathcal{W}$ один[4] из таких элементов w^*, мы получаем отображение $\varrho : \mathcal{W} \to P$,

[1] Т. е. конечные линейно упорядоченные подмножества.

[2] Т. е. для любого вполне упорядоченного $W \subset P$ найдётся такой $p \in P$, что $w \leqslant p$ для всех $w \in W$.

[3] Т. е. такой $p^* \in P$, что неравенство $p^* \leqslant x$ выполняется в P только для $x = p^*$, см. последние два абзаца перед n° 0.8 на стр. 18.

[4] Для этого придётся воспользоваться аксиомой выбора из n° 0.5.1 на стр. 14.

которого не может быть по лем. 0.2. □

Определение 0.3 (полные чумы)
Частично упорядоченное множество называется *полным*, если каждая его цепь имеет верхнюю грань.

Следствие 0.1 (лемма Цорна)
В каждом полном чуме есть максимальный элемент (возможно не единственный). □

Упражнение 0.21 (лемма Бурбаки – Витта о неподвижной точке). Пусть отображение из полного чума в себя $f : P \to P$ таково, что $f(x) \geqslant x$ для всех $x \in P$. Покажите, что существует такое $p \in P$, что $f(p) = p$.

Упражнение 0.22 (теорема Цермелло). Докажите, что каждое множество можно вполне упорядочить.

Упражнение 0.23 (теорема Хаусдорфа о максимальной цепи). Докажите, что в любом чуме каждая цепь содержится в некоторой максимальной по включению цепи.

§1. Поля, коммутативные кольца и абелевы группы

1.1. Определения и примеры. Говоря вольно, поле представляет собою числовую область, где определены четыре стандартные арифметические операции: сложение, вычитание, умножение и деление, которые обладают теми же свойствами, что и соответствующие действия над рациональными числами. Точный перечень этих свойств идёт ниже.

Определение 1.1
Множество $\mathbb{F}$ с двумя операциями $\mathbb{F}\times\mathbb{F}\to\mathbb{F}$: *сложением* $(a,b)\mapsto a+b$ и *умножением* $(a,b)\mapsto ab$ называется *полем*, если выполняются следующие три набора аксиом:

свойства сложения

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

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

наличие нуля: $\exists\, 0\in\mathbb{F}:\quad a+0=a \quad \forall\, a\in\mathbb{F}$ (1-3)

наличие противоположных: $\forall\, a\in\mathbb{F} \quad \exists\,(-a)\in\mathbb{F}:\quad a+(-a)=0$ (1-4)

свойства умножения

коммутативность: $ab=ba \quad \forall\, a,b\in\mathbb{F}$ (1-5)

ассоциативность: $a\,(bc)=(ab)\,c \quad \forall\, a,b,c\in\mathbb{F}$ (1-6)

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

наличие обратных: $\forall\, a\in\mathbb{F}\smallsetminus 0 \quad \exists\, a^{-1}\in\mathbb{F}:\quad aa^{-1}=1$ (1-8)

свойства, связывающие сложение с умножением

дистрибутивность: $a(b+c)=ab+ac \quad \forall\, a,b,c\in\mathbb{F}$ (1-9)

нетривиальность: $0\neq 1$ (1-10)

Пример 1.1 (поле из двух элементов)
Простейший объект, удовлетворяющий всем аксиомам из опр. 1.1 — это поле $\mathbb{F}_2$, состоящее только из двух таких элементов 0 и 1, что $0+1=1\cdot 1=1$, а все остальные суммы и произведения равны нулю.

Упражнение 1.1. Проверьте, что $\mathbb{F}_2$ действительно является полем.

Элементы этого поля можно воспринимать как классы вычетов по модулю 2, т. е. «чётное» $=0$ и «нечётное» $=1$, со сложением и умножением, заданными формулами (0-19) – (0-20) на стр. 11. С другой стороны, элементы поля $\mathbb{F}_2$ могут интерпретироваться как «ложь» $=0$ и «истина» $=1$, сложение — как логическое «исключающее или»[1], а умножение — как логическое «и»[2]. При такой интерпретации алгебраические вычисления в поле $\mathbb{F}_2$ превращаются в логические манипуляции с высказываниями.

Упражнение 1.2. Напишите многочлен от x с коэффициентами из поля $\mathbb{F}_2$, равный «не x», а

[1] Т. е. высказывание $A+B$ истинно тогда и только тогда, когда истинно *ровно одно* из высказываний A, B. На языке формул: $0+1=1+0=1$, а $0+0=1+1=0$.

[2] Т. е. высказывание $A\cdot B$ истинно если и только если истинны *оба* высказывания A и B : $1\cdot 1=1$, но $0\cdot 1=1\cdot 0=0\cdot 0=0$.

также многочлен от x и y, равный «x или[1] y».

Пример 1.2 (рациональные числа)
Напомню[2], что поле рациональных чисел $\mathbb{Q}$ можно определить как множество дробей a/b, где под «дробью» понимается класс эквивалентности упорядоченной пары (a,b) с $a,b\in\mathbb{Z}$ и $b\neq 0$ по отношению $(a_1,b_1)\sim(a_2,b_2)$ при $a_1b_2=a_2b_1$, которое является минимальным отношением эквивалентности[3], содержащим все отождествления

$$\frac{a}{b}=\frac{ac}{bc}\quad\forall\, c\neq 0\,.$$

Сложение и умножение дробей определяется формулами

$$\frac{a}{b}+\frac{c}{d}\overset{\text{def}}{=}\frac{ad+bc}{bd}\,,\qquad \frac{a}{b}\cdot\frac{c}{d}\overset{\text{def}}{=}\frac{ac}{bd}\,. \tag{1-11}$$

Упражнение 1.3. Проверьте, что эти операции определены корректно (результат не зависит от выбора представителей в классах) и удовлетворяют аксиомам поля.

Пример 1.3 (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 полагаем, что читатель знаком с этими определениями и понимает, как они связаны друг с другом, либо скоро узнает об этом из курса анализа. Какое бы описание множества $\mathbb{R}$ ни использовалось, задание на нём сложения и умножения, равно как и проверка аксиом из опр. 1.1, требуют определённой умственной работы, также традиционно проделываемой в курсе анализа.

1.1.1. Коммутативные кольца. Множество K с операциями сложения и умножения называется *коммутативным кольцом с единицей*, если эти операции обладают всеми свойствами из опр. 1.1 на стр. 21 за исключением свойства (1-8) существования мультипликативно обратных элементов и условия $0\neq 1$. Если, кроме этих двух аксиом из списка аксиом поля исключается требование наличия единицы (1-7), 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.

1.1.2. Абелевы группы. Множество A *с одной* операцией $A\times A\to A$, удовлетворяющей первым четырём аксиомам сложения из опр. 1.1, называется *абелевой группой*. Таким образом, всякое коммутативное кольцо K является абелевой группой относительно операции сложения. Эта группа называется *аддитивной группой кольца*. Пример абелевой группы, не являющейся кольцом, доставляют *векторы*.

[1] 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.

[2] См. прим. 0.5 на стр. 12.

[3] См. n° 0.4.1 на стр. 12.

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

Пример 1.4 (геометрические векторы)
Будем называть *геометрическим вектором* класс направленного отрезка (на плоскости или в пространстве) по отношению эквивалентности, отождествляющему между собой все отрезки, которые 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 видны из рис. 1⋄1 и рис. 1⋄2.

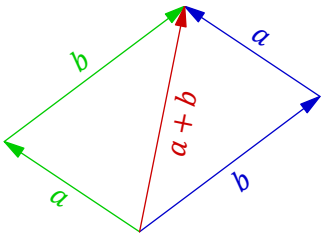


Рис. 1⋄1. Правило параллелограмма.

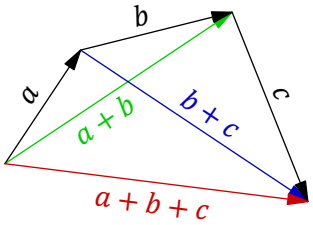


Рис. 1⋄2. Правило четырёхугольника.

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

Пример 1.5 (мультипликативная группа поля)
Четыре аксиомы умножения из опр. 1.1 на стр. 21 утверждают, то множество $\mathbb{F}^\times \stackrel{\text{def}}{=} \mathbb{F} \setminus 0$ всех *ненулевых* элементов поля $\mathbb{F}$ является абелевой группой относительно операции умножения. Эту группу называют *мультипликативной группой поля*. Роль нуля из аддитивной группы $\mathbb{F}$ в мультипликативной группе $\mathbb{F}^\times$ исполняет единица. В абстрактной абелевой группе такой элемент называется *нейтральным*. Мультипликативным аналогом перехода к противоположному элементу является переход к обратному элементу.

Лемма 1.1
В любой абелевой группе A нейтральный элемент единствен, и для каждого $a \in A$ противоположный к a элемент $-a$ определяется по a однозначно. В частности, $-(-a) = a$.

Доказательство. Будем записывать операцию в A аддитивно. Если есть два нулевых элемента 0_1 и 0_2, то $0_1 = 0_1 + 0_2 = 0_2$ (первое равенство выплнено, так как 0_2 является нулевым элементом, второе — поскольку нулевым элементом является 0_1). Если есть два элемента $-a$ и $-a'$, противоположных к a, то $-a = (-a) + 0 = (-a) + \big(a + (-a')\big) = \big((-a) + a\big) + (-a') = 0 + (-a') = -a'$. □

Лемма 1.2
В любом коммутативном кольце для любого элемента a выполняется равенство $0 \cdot a = 0$, а в любом коммутативном кольце с единицей — равенство $(-1) \cdot a = -a$.

Доказательство. Так как $a \cdot 0 = a\,(0 + 0) = a \cdot 0 + a \cdot 0$, прибавляя к обеим частям элемент, противоположный к $a \cdot 0$, получаем $0 = a \cdot 0$. Второе утверждение проверяется выкладкой $(-1) \cdot a + a = (-1) \cdot a + 1 \cdot a = ((-1) + 1) \cdot a = 0 \cdot a = 0$. □

Замечание 1.1. Если в коммутативном кольце K с единицей выполняется равенство $0 = 1$, то K состоит из одного нуля, так как для каждого $a \in K$ имеем $a = a \cdot 1 = a \cdot 0 = 0$. Образование, состоящее из одного нуля, согласно предыдущим определениям, является коммутативным кольцом с единицей, но не полем.

1.1.3. Вычитание и деление. Из лем. 1.1 вытекает, что в любой абелевой группе корректно определена *разность* любых двух элементов

$$a - b \stackrel{\text{def}}{=} a + (-b)\,. \tag{1-12}$$

В частности, операция вычитания имеется в аддитивной группе любого коммутативного кольца. В поле ненулевые элементы образуют абелеву группу по умножению. Поэтому в любом поле имеется ровно один единичный элемент, и для любого ненулевого элемента a обратный к нему элемент a^{-1} однозначно определяется по a. Тем самым, в любом поле помимо сложения, умножения и вычитания (1-12) имеется операция *деления* на любые ненулевые элементы

$$a/b \stackrel{\text{def}}{=} ab^{-1}\,, \quad b \neq 0\,. \tag{1-13}$$

1.2. Делимость в кольце целых чисел. Основным отличием коммутативных колец с единицей от полей является отсутствие обратных элементов к некоторым ненулевым элементам кольца. 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) и только они.

Говорят, что элемент a *делится* на элемент b, если в кольце существует такой элемент q, что $a = bq$. Это записывается как $b|a$ (читается «b делит a») или как $a \vdots b$ (читается «a делится на b»). Отношение делимости тесно связано с решением линейных уравнений.

1.2.1. Уравнение $ax + by = k$, НОД и НОК. Зафиксируем какие-нибудь целые числа a и b и обозначим через

$$(a, b) \stackrel{\text{def}}{=} \{ax + by \mid x, y \in \mathbb{Z}\} \tag{1-14}$$

множество всех целых чисел, представимых в виде $ax + by$ с целыми x, y. Это множество замкнуто относительно сложения и вместе с каждым своим элементом содержит все его целые 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). Обозначим через d наименьшее положительное число в (a, b). Остаток от деления любого числа $z \in (a, b)$ на d лежит в (a, b), поскольку представляется в виде $z - kd$, где и z и $-kd$ лежат в (a, b). Так как этот остаток строго меньше d, он равен нулю. Следовательно, (a, b) 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. При этом произвольное число $k \in \mathbb{Z}$ представляется в виде $k = ax + by$ если и только если оно делится на d. Число d называется *наибольшим общим делителем* чисел $a, b \in \mathbb{Z}$ и обозначается нод(a, b).

Упражнение 1.4. Обобщите проделанные только что рассуждения: для любого конечного набора чисел $a_1, \ldots, a_m \in \mathbb{Z}$ укажите число $d \in \mathbb{Z}$, которое делит все a_i, делится на любой их общий делитель и представляется в виде $d = a_1x_1 + \cdots + a_mx_m$ с целыми x_i. Покажите также, что уравнение $n = a_1x_1 + \cdots + a_mx_m$ разрешимо относительно x_i в кольце $\mathbb{Z}$ если и только если $n \vdots d$.

Записывая числа a и b как $a = \alpha d$, $b = \beta d$, где $d = \text{нод}(a, b)$, мы заключаем, что число

$$c = \alpha\beta d = \beta a = \alpha b \tag{1-15}$$

делится на a и на b. Покажем, что c делит все общие кратные чисел a и b. Пусть $m = ka = \ell b$. Так как $\text{нод}(\alpha, \beta) = 1$, существуют такие $x, y \in \mathbb{Z}$, что $\alpha x + \beta y = 1$. Умножая обе части этого равенства на m, мы заключаем, что $m = m\alpha x + m\beta y = \ell b\alpha x + ka\beta y = c(\ell x + ky)$, как и утверждалось. Число c называется *наименьшим общим кратным* чисел a и b и обозначается $\text{нок}(a, b)$.

Упражнение 1.5. Убедитесь, что все целые решения (x, y) уравнения $ax + by = k$ имеют вид $x = x_0 + n\beta$, $y = y_0 - n\alpha$, где α и β те же, что и выше, (x_0, y_0) — какое-то одно решение, а $n \in \mathbb{Z}$ — любое.

1.2.2. Алгоритм Евклида – Гаусса. Найти $\text{нод}(a, b)$ для данных $a, b \in \mathbb{Z}$ и представить его в виде $\text{нод}(a, b) = ax + by$ с целыми x, y можно следующим образом. Составим таблицу

$$\begin{pmatrix} a & 1 & 0 \\ b & 0 & 1 \end{pmatrix} \tag{1-16}$$

и будем преобразовывать её строки, поэлементно прибавляя к одной строке другую, умноженную на подходящее целое число так, чтобы один из элементов первого столбца каждый раз строго уменьшался по абсолютной величине. Это возможно до тех пор, пока один из элементов в первом столбце не обнулится. После этого, меняя при необходимости строки местами и/или меняя знак у всех элементов одной из строк, можем переписать полученную таблицу в виде

$$\begin{pmatrix} d & x & y \\ 0 & k & \ell \end{pmatrix}, \tag{1-17}$$

где $x, y, k, \ell \in \mathbb{Z}$ и $d \in \mathbb{N}$. Это означает, что $\text{нод}(a, b) = d = ax + by$, а $\text{нок}(a, b) = |ka| = |\ell b|$, причём $\text{нод}(k, \ell) = 1$. Например, для чисел $a = 5\,073$ и $b = 1\,064$ получаем[1]:

$$\begin{pmatrix} 5\,073 & 1 & 0 \\ 1\,064 & 0 & 1 \end{pmatrix} \qquad (1) \mapsto (1) - 5 \cdot (2)$$

$$\begin{pmatrix} -247 & 1 & -5 \\ 1\,064 & 0 & 1 \end{pmatrix} \qquad (2) \mapsto (2) + 4 \cdot (1)$$

$$\begin{pmatrix} -247 & 1 & -5 \\ 76 & 4 & -19 \end{pmatrix} \qquad (1) \mapsto (1) + 3 \cdot (2)$$

$$\begin{pmatrix} -19 & 13 & -62 \\ 76 & 4 & -19 \end{pmatrix} \qquad (2) \mapsto (2) + 4 \cdot (1)$$

$$\begin{pmatrix} -19 & 13 & -62 \\ 0 & 56 & -267 \end{pmatrix} \qquad (1) \mapsto -(1)$$

$$\begin{pmatrix} 19 & -13 & 62 \\ 0 & 56 & -267 \end{pmatrix}.$$

Тем самым, $\text{нод}(5\,073,\ 1\,064) = 19 = -13 \cdot 5\,073 + 62 \cdot 1\,064$, $\text{нок}(5\,073,\ 1\,064) = 5\,073 \cdot 56 = 1\,064 \cdot 267$.

[1] Запись вроде $(1) \mapsto (1) - 5 \cdot (2)$ означает, что к 1-й строке прибавляется 2-я, умноженная на -5.

Упражнение 1.6. Убедитесь, что в каждой возникающей по ходу вычисления таблице

$$\begin{pmatrix} m & x & y \\ n & s & t \end{pmatrix}$$

кроме, может быть, итоговой (полученной перестановкой строк и/или сменой знака в одной из строк) выполняются равенства $m = xa + by$, $n = as + bt$ и $xt - ys = 1$.

Из упражнения вытекает, что элементы возникающей в конце вычисления таблице вида

$$\begin{pmatrix} d' & x & y \\ 0 & s & t \end{pmatrix} \quad \text{или} \quad \begin{pmatrix} 0 & s & t \\ d' & x & y \end{pmatrix}$$

(где $d' \in \mathbb{Z}$ может отличаться от итогового $d \in \mathbb{N}$ лишь знаком) выполняются равенства

$$d' = ax + by\,, \quad sa = -tb\,, \quad tx - sy = 1\,. \tag{1-18}$$

Из первого следует, что d' делится на все общие делители чисел a и b. Умножая последнее равенство на a и на b и пользуясь первыми двумя равенствами, заключаем, что

$$a = atx - asy = atx + bty = td' \quad \text{и} \quad b = btx - bsy = -asx - bsy = -sd'$$

оба делятся на d', откуда $d = |d'| = \text{нод}(a, b)$. Второе равенство (1-18) показывает, что число $c' = sa = -tb$ является общим кратным a и b. Умножая третье равенство (1-18) на любое общее кратное $m = ka = \ell b$ чисел a и b, убеждаемся, что $m = mtx - msy = \ell btx - kasy = -c'(\ell x + ky)$ делится на c', откуда $c = |c'| = \text{нок}(a, b)$.

Замечание 1.2. С вычислительной точки зрения отыскание $\text{нод}(a, b)$ и $\text{нок}(a, b)$ по алгоритму Евклида – Гаусса *несопоставимо* быстрее разложения чисел a и b на простые множители. Читателю предлагается убедиться в этом, попробовав вручную разложить на простые множители числа 10 203 и 4 687. Вычисление по алгоритму Евклида – Гаусса занимает 6 строк:

$$\begin{aligned}
&\begin{pmatrix} 10\,203 & 1 & 0 \\ 4\,687 & 0 & 1 \end{pmatrix} && (1) \mapsto (1) - 2 \cdot (2) \\
&\begin{pmatrix} 829 & 1 & -2 \\ 4\,687 & 0 & 1 \end{pmatrix} && (2) \mapsto (2) - 6 \cdot (1) \\
&\begin{pmatrix} 829 & 1 & -2 \\ -287 & -6 & 13 \end{pmatrix} && (1) \mapsto (1) + 3 \cdot (2) \\
&\begin{pmatrix} -32 & -17 & 37 \\ -287 & -6 & 13 \end{pmatrix} && (2) \mapsto (2) - 9 \cdot (1) \\
&\begin{pmatrix} -32 & -17 & 37 \\ 1 & 147 & -320 \end{pmatrix} && (1) \mapsto (1) + 32 \cdot (2) \\
&\begin{pmatrix} 0 & 4\,687 & 10\,203 \\ 1 & 147 & -320 \end{pmatrix}, &&
\end{aligned} \tag{1-19}$$

откуда $\text{нод}(10\,203, 4\,687) = 1 = 147 \cdot 10\,203 - 320 \cdot 4\,687$, $\text{нок}(10\,203, 4\,687) = 10\,203 \cdot 4\,687$. Если известно произведение двух *очень* больших простых чисел, то извлечь из него сами эти числа за разумное время не под силу даже мощным компьютерам. Это обстоятельство лежит в основе многих популярных систем шифрования данных.

1.3. Взаимная простота. Выше мы видели, что в кольце $\mathbb{Z}$ условие нод$(a, b) = 1$ равносильно разрешимости в целых числах уравнения $ax + by = 1$. Числа a, b, обладающие этим свойством, называются *взаимно простыми*. В произвольном коммутативном кольце K с единицей из разрешимости уравнения $ax + by = 1$ также вытекает отсутствие у элементов a и b необратимых общих делителей: если $a = d\alpha$, $b = d\beta$, и $ax + by = 1$, то $d(\alpha + \beta) = 1$ и d обратим. Однако, отсутствие у a и b необратимых общих делителей, вообще говоря, не гарантирует разрешимости уравнения $ax + by = 1$. Например, в кольце $\mathbb{Q}[x, y]$ многочленов с рациональными коэффициентами от двух переменных x, y одночлены x и y не имеют общих делителей, отличных от констант, однако равенство $f(x, y) \cdot x + g(x, y) \cdot y = 1$ невозможно ни при каких $f, g \in \mathbb{Q}[x, y]$.

Упражнение 1.7. Объясните почему.

Оказывается, что именно разрешимость уравнения $ax + by = 1$ влечёт за собою наличие у элементов a, b многих приятных свойств, которыми обладают взаимно простые целые числа.

Определение 1.2
Элементы a и b произвольного коммутативного кольца K с единицей называются *взаимно простыми*, если уравнение $ax + by = 1$ разрешимо в K относительно x и y.

Лемма 1.3
В произвольном коммутативном кольце K с единицей 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 $b_1, \dots, b_n$, то он взаимно прост и с их произведением $b_1 \dots b_n$.

Доказательство. Умножая обе части равенства $ax + by = 1$ на c, получаем соотношение

$$c = acx + bcy\,,$$

из которого вытекают обе импликации (1), (2). Если $\forall\, i\ \exists\, x_i, y_i \in K:\ ax_i + b_i y_i = 1$, то перемножая все эти равенства и раскрывая скобки, получим в левой части сумму, в которой все слагаемые, кроме $(b_1 \dots b_n) \cdot (y_1 \dots y_n)$, делятся на a. Вынося a за скобку, приходим к соотношению $a \cdot X + (b_1 \dots b_n) \cdot (y_1 \dots y_n) = 1$. □

Упражнение 1.8. Пользуясь лем. 1.3, докажите следующую теорему об однозначности разложения на простые множители в кольце $\mathbb{Z}$: всякое необратимое целое число $z \neq 0$ является произведением конечного числа простых[1], причём любые два таких представления

$$p_1 \dots p_k = z = q_1 \dots q_m$$

имеют одинаковое число сомножителей $k = m$, и эти сомножители можно перенумеровать так, чтобы $p_i = \pm q_i$ для всех i.

Замечание 1.3. (нод и нок в произвольном кольце) В произвольном коммутативном кольце K принято называть *наибольшим общим делителем* элементов $a, b \in K$ любой элемент $d \in K$,

[1]Напомним, что ненулевое необратимое целое число называется *простым*, если оно не раскладывается в произведение двух необратимых целых чисел.

который делит a и b и делится на все их общие делители. Это определение не гарантирует ни существования, ни единственности наибольшего общего делителя, ни его представимости в виде $d = ax + by$. Аналогично, *наименьшим общим кратным* элементов $a, b \in K$ называется любой элемент $c \in K$, который делится на a и b и делит все их общие кратные. Такого элемента тоже может не быть, а если он есть, то не обязательно единствен.

1.4. Кольцо вычетов $\mathbb{Z}/(n)$. Напомню[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[2] 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 $a \in \mathbb{Z}$. Такое обозначение не однозначно: разные числа $x \in \mathbb{Z}$ и $y \in \mathbb{Z}$ задают один и тот же класс $[x]_n = [y]_n$ если и только если $x = y + dn$ для некоторого $d \in \mathbb{Z}$. Всего в $\mathbb{Z}/(n)$ имеется n различных классов: $[0]_n$, $[1]_n$, … , $[(n-1)]_n$. Сложение и умножение классов вычетов задаётся правилами:

$$[a] + [b] \stackrel{\text{def}}{=} [a + b]\,, \quad [a] \cdot [b] \stackrel{\text{def}}{=} [ab]\,. \tag{1-20}$$

Согласно упр. 0.9 на стр. 11, эти операции определены корректно[3]. Они очевидным образом удовлетворяют аксиомам коммутативного кольца с единицей — формулы (1-20) сводят операции над вычетами к операциям над целыми числами, для которых аксиомы выполнены.

1.4.1. 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 $[2]^3 = [8] = [0]$. Элемент a произвольного коммутативного кольца K называется *делителем нуля*, если $ab = 0$ для некоторого ненулевого $b \in K$. Тривиальным делителем нуля является нуль. Обратимый элемент $a \in K$ не может быть делителем нуля, поскольку, умножая обе части равенства $ab = 0$ на a^{-1}, мы получаем $b = 0$. Тем самым, кольцо с ненулевыми делителями нуля не может быть полем. Кольцо с единицей без ненулевых делителей нуля называется *целостным*.

Элемент a кольца K называется *нильпотентом*, если $a^n = 0$ для некоторого $n \in \mathbb{N}$. Тривиальным нильпотентом является нуль. Всякий нильпотент автоматически делит нуль. Кольцо с единицей без ненулевых нильпотентов называется *приведённым*. Например, каждое целостное кольцо приведено.

1.4.2. 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 равносильно наличию таких $x, y \in \mathbb{Z}$, что $mx + ny = 1$ в $\mathbb{Z}$. Тем самым, класс $[m]_n$ обратим в $\mathbb{Z}/(n)$ если и только если нод$(m, n) = 1$ в кольце $\mathbb{Z}$.

Проверить, обратим ли данный класс $[m]_n$, и если да, вычислить $[m]_n^{-1}$, можно при помощи алгоритма Евклида – Гаусса[4]. Так, проделанное в форм. (1-19) на стр. 26 вычисление 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 $4\,687^{-1} = -320 \pmod{10\,203}$.

[1] См. прим. 0.4 на стр. 11.

[2] См. n° 0.4 на стр. 10.

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

[4] См. n° 1.2.2 на стр. 25.

Обратимые элементы кольца $\mathbb{Z}/(n)$ образуют мультипликативную абелеву группу. Она называется *группой обратимых вычетов* по модулю n и обозначается $\mathbb{Z}/(n)^\times$. Порядок этой группы равен количеству натуральных чисел, меньших n и взаимно простых с n. Он обозначается

$$\varphi(n) \stackrel{\text{def}}{=} \left|\mathbb{Z}/(n)^\times\right|$$

и называется *функцией Эйлера* числа $n \in \mathbb{Z}$.

Пример 1.6 (теорема Эйлера и порядок обратимого вычета)
Умножение на фиксированный обратимый вычет $[a] \in \mathbb{Z}/(n)^\times$ задаёт биекцию[1]

$$a:\ \mathbb{Z}/(n)^\times \xrightarrow{\sim} \mathbb{Z}/(n)^\times, \quad [x] \mapsto [ax], \tag{1-21}$$

обратной к которой является умножение на вычет $[a]^{-1}$. Последовательно применяя отображение (1-21) к произвольному элементу $[z] \in \mathbb{Z}/(n)^\times$, получаем цепочку его образов

$$[z] \overset{a}{\mapsto} [az] \overset{a}{\mapsto} [a^2z] \overset{a}{\mapsto} [a^3z] \overset{a}{\mapsto} \dots, \tag{1-22}$$

которые начнут повторяться, ибо множество вычетов конечно. В силу биективности отображения (1-21), самым первым повторно встретившимся элементом цепочки (1-22) станет её начальный элемент $[z]$, т. е. цепочка (1-22) является циклом. В силу всё той же биективности отображения (1-21) два таких цикла, проходящие через классы $[x]$ и $[y]$, либо не пересекаются, либо полностью совпадают. Кроме того, все циклы имеют одинаковую длину.

Упражнение 1.9. Убедитесь, что отображения умножения на $[x]^{-1}[y]$ и на $[y]^{-1}[x]$ суть взаимно обратные биекции между циклами, проходящими через классы $[x]$ и $[y]$.

Мы заключаем, что $\mathbb{Z}/(n)^\times$ распадается в объединение непересекающихся циклов (1-22) *одинаковой длины* m, которая таким образом является делителем числа $\varphi(n) = |\mathbb{Z}/(n)^\times|$. Умножая обе части равенства $[z] = [a]^m[z]$ на $[z]^{-1}$, получаем $[a^m] = [1]$, откуда и $[a^{\varphi(n)}] = [1]$. Иными словами, для любых взаимно простых целых чисел a и n выполняется сравнение $a^{\varphi(n)} \equiv 1 \pmod{n}$. Этот факт известен как *теорема Эйлера*. Число m однозначно характеризуется как наименьшее такое $k \in \mathbb{N}$, что $[a]^k = 1$, и называется *порядком* обратимого вычета $[a] \in \mathbb{Z}/(n)^\times$. Как мы видели, порядок каждого обратимого вычета в $\mathbb{Z}/(n)^\times$ делит $\varphi(n)$.

1.4.3. Поля вычетов $\mathbb{F}_p = \mathbb{Z}/(p)$. Из сказанного в начале n° 1.4.2 вытекает, что 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 $[m], [k] \in \mathbb{Z}/(n)$ делят нуль и не могут быть обратимы. Напротив, если p простое, то $\text{нод}(m, p) = 1$ для всех m, не кратных p, и значит, каждый ненулевой класс $[m] \in \mathbb{Z}/(p)$ обратим. Поле $\mathbb{Z}/(p)$, где p простое, принято обозначать $\mathbb{F}_p$.

Пример 1.7 (бином Ньютона по модулю p)
В поле $\mathbb{F}_p = \mathbb{Z}/(p)$ выполняется замечательное равенство

$$\underbrace{1 + 1 + \dots + 1}_{p \text{ раз}} = 0\,. \tag{1-23}$$

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

$$(a + b)^p = a^p + b^p\,. \tag{1-24}$$

[1] См. n° 0.5.2 на стр. 15.

В самом деле, раскрывая скобки в биноме $(a+b)^p$, мы для каждого k получим $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ одночленов $a^k b^{p-k}$, сумма которых равна $(1+\ldots+1)\cdot a^k b^{p-k}$, где внутри скобок складываются $\binom{p}{k}$ единиц поля $\mathbb{F}_p$. Такая сумма равна нулю при $0 < k < p$ в силу следующей леммы.

Лемма 1.4
При простом p и любом натуральном k в пределах $1 \leqslant k \leqslant (p-1)$ биномиальный коэффициент $\binom{p}{k}$ делится на p.

Доказательство. Так как число p взаимно просто со всеми числами от 1 до $p-1$, оно по лем. 1.3 взаимно просто с произведением $k!(p-k)!$. Поскольку $p!$ делится на $k!(p-k)!$, из той же лем. 1.3 следует, что $(p-1)!$ делится на $k!(p-k)!$, а значит, $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ делится на p. □

Следствие 1.1 (малая теорема Ферма)
Для любого $a \in \mathbb{Z}$ и любого простого $p \in \mathbb{N}$ выполняется сравнение $a^p \equiv a \pmod p$.

Доказательство. Надо показать, что $[a^p] = [a]$ в поле $\mathbb{F}_p$. Согласно (1-24)

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

□

Упражнение 1.10. Выведите малую теорему Ферма из теоремы Эйлера[1].

Упражнение 1.11. Покажите, что $\binom{mp^n}{p^n} \equiv m \pmod p$ для всех $m, n \in \mathbb{N}$ и простых $p \nmid m$.

1.5. Гомоморфизмы. Отображение абелевых групп $\varphi : A \to B$ называется *гомоморфизмом*, если для любых $a_1, a_2 \in A$ в группе B выполнено соотношение

$$\varphi(a_1 + a_2) = \varphi(a_1) + \varphi(a_2)\,. \tag{1-25}$$

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

Упражнение 1.12. Убедитесь, что композиция[2] гомоморфизмов — это тоже гомоморфизм.

Любой гомоморфизм $\varphi : A \to B$ переводит нулевой элемент группы A в нулевой элемент группы B, так как из равенств $\varphi(0) = \varphi(0+0) = \varphi(0) + \varphi(0)$ вытекает, что $0 = \varphi(0)$. Выкладка

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

показывает, что $\varphi(-a) = -\varphi(a)$. Тем самым, *образ* $\operatorname{im}\varphi = \varphi(A) \subset B$ любого гомоморфизма $\varphi : A \to B$ является абелевой подгруппой в B.

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

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

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

$$\varphi(a_1 \pm a_2) = \varphi(a_1) \pm \varphi(a_2) = 0 \pm 0 = 0\,.$$

[1] См. прим. 1.6 на стр. 29.
[2] См. n° 0.5 на стр. 13.

Предложение 1.1
Каждый непустой слой[1] гомоморфизма абелевых групп $\varphi\colon A \to B$ является сдвигом его ядра:

$$\varphi^{-1}(\varphi(a)) = a + \ker\varphi = \{a + a' \mid a' \in \ker\varphi\} \text{ для всех } a \in A.$$

В частности, все непустые слои находятся в биекции друг с другом, и инъективность гомоморфизма φ равносильна равенству $\ker\varphi = \{0\}$.

Доказательство. Равенства $\varphi(a_1) = \varphi(a_2)$ и $\varphi(a_1 - a_2) = \varphi(a_1) - \varphi(a_2) = 0$ равносильны. Поэтому элементы $a_1, a_2 \in A$ переходят в один и тот же элемент из B тогда и только тогда, когда $a_1 - a_2 \in \ker(\varphi)$. □

Пример 1.8 (квадраты в поле $\mathbb{F}_p$)
Зафиксируем простое $p > 2$. Отображение $\varphi\colon \mathbb{F}_p^\times \to \mathbb{F}_p^\times$, $x \mapsto x^2$, является гомоморфизмом мультипликативной группы ненулевых элементов поля $\mathbb{F}_p$ в себя. Его ядро состоит из таких $x \in \mathbb{F}_p^\times$, что $x^2 = 1$. Поскольку в поле равенство $x^2 - 1 = (x+1)(x-1) = 0$ возможно только для $x = \pm 1$, мы заключаем, что $\ker\varphi = \{\pm 1\}$, и все непустые слои гомоморфизма φ состоят из двух элементов. Поэтому $|\operatorname{im}\varphi| = (p-1)/2$, т. е. ровно половина ненулевых элементов поля $\mathbb{F}_p$ является квадратами. Узнать, является ли квадратом заданное число $a \in \mathbb{F}_p^\times$ можно при помощи другого гомоморфизма $\psi\colon \mathbb{F}_p^\times \to \mathbb{F}_p^\times$, $x \mapsto x^{\frac{p-1}{2}}$. По малой теореме Ферма[2] все $(p-1)/2$ ненулевых квадратов лежат в его ядре. Поэтому $|\operatorname{im}\psi| \leqslant 2$.

Упражнение 1.13. Покажите, что ненулевой многочлен степени m с коэффициентами в произвольном поле $\Bbbk$ имеет в этом поле не более m различных корней.

Из упражнения вытекает, что равенство $x^{\frac{p-1}{2}} = 1$ не может выполняться сразу для всех $p-1$ элементов группы $\mathbb{F}_p^\times$. Поэтому $|\operatorname{im}\psi| = 2$ и $|\ker\psi| = (p-1)/2$. Мы заключаем, что $\ker\psi$ состоит в точности из ненулевых квадратов поля $\mathbb{F}_p$. Иными словами, $a \in \mathbb{F}_p^\times$ является квадратом если и только если $a^{\frac{p-1}{2}} = 1$. Например, -1 является квадратом в поле $\mathbb{F}_p$ если и только если $(p-1)/2$ чётно.

Упражнение 1.14. Покажите, что $\operatorname{im}\psi = \{\pm 1\}$.

1.5.2. Группа гомоморфизмов. Для абелевых групп A, B через $\operatorname{Hom}(A,B)$ мы обозначаем множество всех *гомоморфизмов* $A \to B$. Это множество является абелевой группой относительно операции поточечного сложения значений, т. е. $\varphi_1+\varphi_2\colon a \mapsto \varphi_1(a)+\varphi_2(a)$. Нулевым элементом группы $\operatorname{Hom}(A,B)$ является *нулевой гомоморфизм*, отображающий все элементы группы A в нулевой элемент группы B.

1.5.3. Гомоморфизмы колец. Отображение колец $\varphi\colon A \to B$ называется *гомоморфизмом колец*, если для любых $a_1, a_2 \in A$ в кольце B выполнены соотношения:

$$\begin{aligned} f(a_1 + a_2) &= f(a_1) + f(a_2) \\ f(a_1 a_2) &= f(a_1) f(a_2)\,. \end{aligned} \tag{1-26}$$

Поскольку гомоморфизм колец $\varphi\colon A \to B$ является гомоморфизмом аддитивных абелевых групп, он обладает всеми свойствами гомоморфизмов абелевых групп. В частности, $\varphi(0) = 0$,

[1] Ср. с n° 0.3 на стр. 7.
[2] См. сл. 1.1 на стр. 30.

$\varphi(-a) = -\varphi(a)$, и все непустые слои φ являются сдвигами слоя над нулём: если $\varphi(a) = b$, то $\varphi^{-1}(b) = a + \ker\varphi = \{a + a' \mid a' \in \ker\varphi\}$. Поэтому гомоморфизм φ инъективен тогда и только тогда, когда $\ker\varphi = \{0\}$. Ядро гомоморфизма колец $\varphi\colon A \to B$ вместе с каждым элементом $a \in \ker\varphi$ содержит и все кратные ему элементы aa', поскольку $\varphi(aa') = \varphi(a)\varphi(a') = 0$. В частности, ядро $\ker\varphi$ является подкольцом в A. Образ гомоморфизма колец $\varphi\colon A \to B$ является подкольцом в B, но он может не содержать единицы, и $1 \in A$ может не перейти в $1 \in B$.

Упражнение 1.15. Убедитесь, что отображение $\mathbb{Z}/(2) \to \mathbb{Z}/(6)$, $[0] \mapsto [0]$, $[1] \mapsto [3]$, является гомоморфизмом колец.

Предложение 1.2
Любой ненулевой гомоморфизм произвольного кольца с единицей в любое целостное[1] кольцо переводит единицу в единицу.

Доказательство. Из равенств $\varphi(1) = \varphi(1 \cdot 1) = \varphi(1) \cdot \varphi(1)$ вытекает, что $\varphi(1)\big(1 - \varphi(1)\big) = 0$. В целостном кольце такое возможно либо при $\varphi(1) = 1$, либо при $\varphi(1) = 0$. Во втором случае $\varphi(a) = \varphi(1 \cdot a) = \varphi(1) \cdot \varphi(a) = 0$ для всех $a \in A$. □

1.5.4. Гомоморфизмы полей. Если кольца A и B являются полями, то всякий ненулевой гомоморфизм колец $\varphi\colon A \to B$ является гомоморфизмом мультипликативных групп этих полей. В частности, $\varphi(1) = 1$ и $\varphi(a/b) = \varphi(a)/\varphi(b)$ для всех a и всех $b \neq 0$.

Предложение 1.3
Любой ненулевой гомоморфизм из поля в произвольное кольцо является вложением.

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

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

Поэтому любой ненулевой гомоморфизм из поля имеет нулевое ядро. □

1.5.5. Характеристика. Для любого кольца K с единицей имеется канонический гомоморфизм колец $\varkappa\colon \mathbb{Z} \to K$, заданный правилом

$$\varkappa(\pm n) = \pm\underbrace{(1 + \ldots + 1)}_{n}, \quad \text{где} \quad n \in \mathbb{N}\,. \tag{1-27}$$

Его образ $\operatorname{im}\varkappa$ является наименьшим по включению подкольцом в K с единицей, равной единице кольца K. Если гомоморфизм $\varkappa$ инъективен, то говорят, что кольцо K имеет *характеристику нуль*. В противном случае *характеристикой* $\operatorname{char}(K)$ кольца K называют наименьшее $m \in \mathbb{N}$, для которого $\underbrace{1 + 1 + \cdots + 1}_{m} = 0$. Равенство

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

[1] Напомню, что *целостным* называется кольцо с единицей без ненулевых делителей нуля, см. n° 1.4.1 на стр. 28.

показывает, что характеристика целостного кольца либо равна нулю, либо является простым числом. Для целостного кольца K характеристики $p > 0$ гомоморфизм $\varkappa$ переводит все числа, кратные p, в нуль и корректно факторизуется до гомоморфизма поля вычетов

$$\varkappa_p : \mathbb{Z}/(p) \to K\,, \quad a \,(\mathrm{mod}\ p) \mapsto \varkappa(a)\,. \tag{1-28}$$

По предл. 1.3 гомоморфизм (1-28) инъективен, и значит, $\operatorname{im}\varkappa = \operatorname{im}\varkappa_p \simeq \mathbb{F}_p$. Таким образом, наименьшее содержащее единицу подкольцо целостного кольца K положительной характеристики является полем, изоморфным полю вычетов $\mathbb{Z}/(p)$ по простому модулю $p \in \mathbb{N}$, равному характеристике $\operatorname{char} K$.

1.5.6. Простое подполе. Пусть теперь $K = \mathbb{F}$ является полем. Его наименьшее по включению подполе называется *простым подполем* в $\mathbb{F}$. В силу своего определения простое подполе содержит образ $\operatorname{im}(\varkappa)$ гомоморфизма (1-27). Если $\operatorname{char}(\mathbb{F}) = p > 0$, то простое подполе совпадает с $\operatorname{im}\varkappa = \operatorname{im}\varkappa_p$ и изоморфно полю вычетов $\mathbb{Z}/(p)$. Если $\operatorname{char}(\mathbb{F}) = 0$, то гомоморфизм $\varkappa$ инъективно вкладывает $\mathbb{Z}$ в $\mathbb{F}$. Так как простое подполе содержит обратные ко всем элементам из $\operatorname{im}\varkappa$, правило $p/q \mapsto \varkappa(p)/\varkappa(q)$ продолжает $\varkappa$ до вложения полей $\varkappa : \mathbb{Q} \hookrightarrow \mathbb{F}$, образ которого совпадает с простым подполем. Тем самым, простое подполе поля характеристики нуль изоморфно полю рациональных чисел $\mathbb{Q}$.

Упражнение 1.16. Покажите, что а) каждый ненулевой гомоморфизм из поля в себя тождественно действует на простом подполе б) между полями разной характеристики не существует ненулевых гомоморфизмов.

Пример 1.9 (автоморфизмы поля $\mathbb{R}$)
Покажем, что каждый ненулевой гомоморфизм $\varphi : \mathbb{R} \to \mathbb{R}$ тождествен. Поскольку неравенство $x_1 < x_2$ равносильно тому, что $x_2 - x_1 = a^2$ для некоторого $a \neq 0$, мы заключаем, что для всех $x_1 < x_2$ выполняется неравенство $\varphi(x_1) < \varphi(x_2)$, ибо $\varphi(x_2) - \varphi(x_1) = \varphi(x_2 - x_1) = \varphi(a^2) = \varphi(a)^2 > 0$. Таким образом, φ является строго монотонной функцией, совпадающей с тождественным отображением $\varphi(x) = x$ на простом подполе $\mathbb{Q} \subset \mathbb{R}$.

Упражнение 1.17 (по анализу). Покажите, что строго монотонная функция $\mathbb{R} \to \mathbb{R}$, совпадающая с функцией $\varphi(x) = x$ на подмножестве $\mathbb{Q} \subset \mathbb{R}$, совпадает с нею всюду.

Пример 1.10 (гомоморфизм Фробениуса)
В поле $\mathbb{F}$ характеристики $\operatorname{char}(\mathbb{F}) = p > 0$ отображение возведения в p-тую степень

$$F_p : \mathbb{F} \to \mathbb{F}\,, \quad x \mapsto x^p\,, \tag{1-29}$$

является гомоморфизмом, поскольку $\forall\, a, b \in \mathbb{F}$ выполняются равенства $(ab)^p = a^p b^p$ и

$$(a+b)^p = a^p + b^p + \sum_{k=1}^{p-1} \underbrace{(1 + 1 + \cdots + 1)}_{\binom{p}{k}} \cdot a^k b^{p-k} = a^p + b^p$$

(ср. с прим. 1.7 и лем. 1.4 на стр. 30). Гомоморфизм (1-29) называется *гомоморфизмом Фробениуса*. Как и всякий ненулевой гомоморфизм из поля в себя, он тождественно действует на простом подполе $\mathbb{F}_p \subset \mathbb{F}$, что ещё раз доказывает малую теорему Ферма[1].

[1] См. сл. 1.1 на стр. 30.

1.6. Прямые произведения. Прямое произведение абелевых групп $A_1, \dots, A_m$

$$\prod_\nu A_\nu = A_1 \times \dots \times A_\nu \stackrel{\text{def}}{=} \{(a_1, \dots, a_m) \mid a_\nu \in A_\nu \ \forall\, \nu\} \tag{1-30}$$

состоит из упорядоченных наборов $(a_1, \dots, a_m)$ элементов $a_\nu \in A_\nu$ и наделяется структурой абелевой группы посредством покомпонентных операций:

$$(a_1, \dots, a_m) + (b_1, \dots, b_m) \stackrel{\text{def}}{=} (a_1 + b_1, \dots, a_m + b_m)\,. \tag{1-31}$$

Упражнение 1.18. Проверьте, что так определённая операция коммутативна и ассоциативна, нулевым элементом для неё является набор нулей $(0, \dots, 0)$, а противоположным к набору $(a_1, \dots, a_m)$ является набор $(-a_1, \dots, -a_m)$.

Абелева группа (1-30) называется *прямым произведением* абелевых групп A_i. Если все группы A_i конечны, прямое произведение (1-30) тоже конечно и имеет порядок

$$\left|\prod A_i\right| = \prod |A_i|\,.$$

Прямое произведение имеет смысл не только для конечного набора, но и для произвольного семейства абелевых групп A_x, занумерованных элементами $x \in X$ какого-нибудь множества X. Такое произведение обозначается через $\prod_{x\in X} A_x$.

Аналогичным образом, для любого семейства коммутативных колец $\{K_x\}_{x\in X}$ определено прямое произведение $\prod K_x$, элементами которого являются семейства $(a_x)_{x\in X}$, где каждый элемент a_x лежит в своём кольце K_x. Операции сложения и умножения определяются также покомпонентно:

$$(a_x)_{x\in X} + (b_x)_{x\in X} \stackrel{\text{def}}{=} (a_x + b_x)_{x\in X}\ , \qquad (a_x)_{x\in X} \cdot (b_x)_{x\in X} \stackrel{\text{def}}{=} (a_x \cdot b_x)_{x\in X}\ .$$

Упражнение 1.19. Убедитесь, что $\prod K_x$ является кольцом, причём если все кольца K_x имеют единицы, то $\prod K_x$ тоже имеет единицу $(1, \dots, 1)$.

Например, если $X = \mathbb{R}$ и все $K_x = \mathbb{R}$, т. е. перемножается континуальное семейство одинаковых экземпляров поля $\mathbb{R}$, занумерованных действительными числами $x \in \mathbb{R}$, то прямое произведение $\prod_{x\in\mathbb{R}} \mathbb{R}_x$ изоморфно кольцу функций $f : \mathbb{R} \to \mathbb{R}$ с обычными операциями поточечного сложения и умножения значений функций. Этот изоморфизм переводит семейство вещественных чисел $(f_x) \in \prod_{x\in\mathbb{R}} \mathbb{R}_x$, занумерованное вещественным числом x, в функцию $f : \mathbb{R} \to \mathbb{R}$, значение которой в точке $x \in \mathbb{R}$ равно x-тому элементу семейства: $f(x) = f_x$.

В прямом произведении колец любой ненулевой элемент, имеющий хотя бы одну нулевую компоненту, является делителем нуля. Например, $(0, 1, \dots, 1)$ делит нуль:

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

Поэтому произведение нескольких колец никогда не является полем. Например, произведение $\mathbb{F}_p \times \mathbb{F}_q$ конечных полей $\mathbb{F}_p$ и $\mathbb{F}_q$ из p и q элементов состоит из $(p-1)(q-1)$ обратимых пар (a, b), образующих мультипликативную группу $\mathbb{F}_p^\times \times \mathbb{F}_q^\times$, и $p + q - 1$ делителей нуля вида $(a, 0)$ или $(0, b)$.

В общем случае элемент $a = (a_1, \dots, a_m) \in K_1 \times \dots \times K_m$ обратим если и только если 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:

$$\left(\prod K_\nu\right)^\times = \prod K_\nu^\times \tag{1-32}$$

1.7. Китайская теорема об остатках. Пусть целое число $n = n_1 \dots n_m$ является произведением попарно взаимно простых чисел $n_1, \dots, n_m \in \mathbb{Z}$. Отображение, переводящее вычет $z \pmod n$ в набор вычетов $z \pmod{n_i}$:

$$\varphi : \mathbb{Z}/(n) \to \mathbb{Z}/(n_1) \times \dots \times \mathbb{Z}/(n_m), \quad [z]_n \mapsto \bigl([z]_{n_1}, \dots, [z]_{n_m}\bigr), \tag{1-33}$$

корректно определено, поскольку при выборе другого представителя $z_1 \equiv z_2 \pmod n$ разность $z_1 - z_2$ делится на произведение $n = n_1 \dots n_m$, и $[z_1]_{n_i} = [z_2]_{n_i}$ при всех i. Легко видеть, что φ перестановочно со сложением:

$$\begin{aligned}\varphi\bigl([z]_n + [w]_n\bigr) = \varphi\bigl([z+w]_n\bigr) = \bigl([z+w]_{n_1}, \dots, [z+w]_{n_m}\bigr) = \\ = \bigl([z]_{n_1} + [w]_{n_1}, \dots, [z]_{n_m} + [w]_{n_m}\bigr) = \\ = \bigl([z]_{n_1}, \dots, [z]_{n_m}\bigr) + \bigl([w]_{n_1}, \dots, [w]_{n_m}\bigr) = \varphi\bigl([z]_n\bigr) + \varphi\bigl([w]_n\bigr).\end{aligned}$$

Аналогично проверяется, что φ перестановочно с умножением, т. е. является гомоморфизмом колец. Если $[z]_n \in \ker\varphi$, то z делится на каждое n_i, а значит, по лем. 1.3 на стр. 27, делится и на их произведение $n = n_1 \dots n_m$, откуда $[z]_n = 0$. Так как гомоморфизм с нулевым ядром инъективен и в кольцах $\mathbb{Z}/(n)$ и $\prod \mathbb{Z}/(n_i)$ одинаковое число элементов $n = n_1 \dots n_m$, отображение (1-33) биективно. Этот факт известен как *китайская теорема об остатках*.

На житейском языке он означает, что для любого набора остатков $r_1, \dots, r_m$ от деления на попарно взаимно простые числа $n_1, \dots, n_m$ всегда найдётся число z, имеющее остаток r_i от деления на n_i одновременно для всех i, причём любые два таких числа z_1, z_2 различаются на целое кратное числа $n = n_1 \dots n_k$. Практическое отыскание такого z осуществляется с помощью алгоритма Евклида – Гаусса следующим образом. Из взаимной простоты числа n_i с остальными числами n_ν вытекает[1], что n_i взаимно просто с произведением $m_i = \prod_{\nu \neq i} n_\nu$. Поэтому 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 $\nu \neq i$. Число $z = r_1 b_1 + \dots + r_m b_m$ решает задачу.

Пример 1.11

Найдём 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 число, обратное к $91 \cdot 179$ по модулю 57: замечаем, что $91 \cdot 179 \equiv 34 \cdot 8 \equiv -13 \pmod{57}$, применяем алгоритм Евклида – Гаусса[2] к $a = 57$ и $b = 13$ и приходим к равенству $22 \cdot 13 - 5 \cdot 57 = 1$. Таким образом, число

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

даёт при делении на 57, 91 и 179 остатки $(1,\ 0,\ 0)$. Аналогично находим числа

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

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

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

[1] По всё той же лем. 1.3 на стр. 27.

[2] См. n° 1.2.2 на стр. 25.

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

§2. Многочлены и расширения полей

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

2.1. Ряды и многочлены. Бесконечное выражение вида

$$f(x) = \sum_{\nu \geqslant 0} a_\nu x^\nu = a_0 + a_1 x + a_2 x^2 + \dots \text{, где } a_i \in K, \tag{2-1}$$

называется *формальным степенным рядом* от x с коэффициентами в кольце K. Ряды

$$\begin{aligned} f(x) &= a_0 + a_1 x + a_2 x^2 + \dots \\ g(x) &= b_0 + b_1 x + b_2 x^2 + \dots \end{aligned} \tag{2-2}$$

равны, если $a_i = b_i$ для всех i. Сложение и умножение рядов (2-2) осуществляется по стандартным правилам раскрытия скобок и приведения подобных слагаемых: коэффициенты s_m и p_m рядов $s(x) = f(x) + g(x) = s_0 + s_1 x + s_2 x^2 + \dots$ и $p(x) = f(x)g(x) = p_0 + p_1 x + p_2 x^2 + \dots$ суть[1]

$$\begin{aligned} s_m &= a_m + b_m \\ p_m &= \sum_{\alpha+\beta=m} a_\alpha b_\beta = a_0 b_m + a_1 b_{m-1} + \dots + a_{m-1} b_1 + a_m b_0 \end{aligned} \tag{2-3}$$

Упражнение 2.1. Убедитесь, что эти две операции удовлетворяют аксиомам коммутативного кольца с единицей.

Кольцо формальных степенных рядов от переменной x с коэффициентами в кольце K обозначается через $K[\![x]\!]$. Начальный коэффициент a_0 ряда (2-1) называется *свободным членом* этого ряда. Самый левый ненулевой коэффициент в (2-1) называется *младшим* коэффициентом ряда f, а его номер — *порядком* ряда f и обозначается $\operatorname{ord} f$. 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 тоже является целостным и $\operatorname{ord}(fg) = \operatorname{ord}(f) + \operatorname{ord}(g)$.

Кольцо $K[\![x_1, \dots, x_n]\!]$ формальных степенных рядов от n переменных определяется по индукции: $K[\![x_1, \dots, x_n]\!] \stackrel{\text{def}}{=} K[\![x_1, \dots, x_{n-1}]\!][\![x_n]\!]$ представляет собою множество формальных сумм вида $F(x) = \sum_{\nu_1, \dots, \nu_n \in \mathbb{Z}_{\geqslant 0}} a_{\nu_1 \dots \nu_n} x_1^{\nu_1} \cdots x_n^{\nu_n}$.

2.1.1. Алгебраические операции над рядами. Назовём *n-арной алгебраической операцией* в $K[\![x]\!]$ правило, сопоставляющее n рядам $f_1, \dots, f_n$ новый ряд f так, что каждый коэффициент ряда f вычисляется по коэффициентам рядов $f_1, \dots, f_n$ при помощи конечного числа[2] операций в K. Например, сложение и умножение рядов — это бинарные алгебраические операции, а подстановка вместо x численного значения $\alpha \in K$ алгебраической операцией обычно не является[3].

[1] Говоря формально, операции, о которых тут идёт речь, являются операциями над *последовательностями* (a_ν) и (b_ν) элементов кольца K. Буква x служит лишь для облегчения их восприятия.

[2] Которое может зависеть от номера коэффициента.

[3] Очевидным исключением из этого правила служит вычисление значения ряда $f(x)$ при $x = 0$, дающее в качестве результата свободный член этого ряда. Однако при произвольных α и f вычисление $f(\alpha)$ требует, вообще говоря, выполнения бесконечно большого количества сложений.

Пример 2.1 (замена переменной)
Подстановка в ряд (2-1) вместо x любого ряда $g(x) = b_1x + b_2x^2 + \dots$ с нулевым свободным членом является бинарной алгебраической операцией, дающей на выходе ряд

$$f(g(x)) = a_0 + a_1(b_1x + b_2x^2 + \dots) + a_2(b_1x + b_2x^2 + \dots)^2 + a_3(b_1x + b_2x^2 + \dots)^3 + \dots = \\ = a_0 + (a_1b_1)\cdot x + (a_1b_2 + a_2b_1^2)\cdot x^2 + (a_1b_3 + 2\,a_2b_1b_2 + a_3b_1^3)\cdot x^3 + \dots\,,$$

в котором на коэффициент при x^m влияют лишь начальные члены первых m слагаемых в f.

Пример 2.2 (обращение)
Покажем, что ряд $f(x) = a_0 + a_1x + a_2x^2 + \dots \in K[\![x]\!]$ обратим в $K[\![x]\!]$ если и только если его свободный член a_0 обратим в K, и в этом случае обращение $f \mapsto f^{-1}$ является унарной алгебраической операцией над обратимым рядом f. Пусть

$$(a_0 + a_1x + a_2x^2 + \dots)\cdot(b_0 + b_1x + b_2x^2 + \dots) = 1\,.$$

Приравнивая коэффициенты при одинаковых степенях x в левой и правой части, получаем бесконечную систему уравнений

$$\begin{aligned} a_0b_0 &= 1 \\ a_0b_1 + a_1b_0 &= 0 \\ a_0b_2 + a_1b_1 + a_2b_0 &= 0 \\ \dots\dots\dots\dots\dots\dots\dots\dots \end{aligned} \tag{2-4}$$

на коэффициенты b_i. Разрешимость первого уравнения равносильна обратимости a_0, и в этом случае $b_0 = a_0^{-1}$ и $b_k = -a_0^{-1}(a_1b_{k-1} + a_2b_{k-2} + \dots + a_kb_0)$ при всех $k \geqslant 1$.

Упражнение 2.2. Вычислите в $\mathbb{Q}[\![x]\!]$ а) $(1-x)^{-1}$ б) $(1-x^2)^{-1}$ в) $(1-x)^{-2}$.

2.1.2. Многочлены. Ряды с конечным числом ненулевых коэффициентов называются *многочленами*. Многочлены от $x_1, \dots, x_n$ с коэффициентами в K образуют в кольце степенных рядов подкольцо, которое обозначается $K[x_1, \dots, x_n] \subset K[\![x_1, \dots, x_n]\!]$. Многочлен от одной переменной x представляет собою формальное выражение вида $f(x) = a_0 + a_1x + \dots + a_nx^n$. Самый правый ненулевой коэффициент в нём называется *старшим*, а его номер — *степенью* многочлена f и обозначается $\deg f$. Многочлены со старшим коэффициентом 1 называются *приведёнными*, а многочлены степени нуль — *константами*.

Так как старший коэффициент произведения равен произведению старших коэффициентов сомножителей, для многочленов f_1, f_2 с коэффициентами в целостном[1] кольце K выполняется равенство $\deg(f_1f_2) = \deg(f_1) + \deg(f_2)$. В частности, кольцо $K[x]$ тоже целостное, и обратимыми элементами в нём являются только обратимые константы.

Упражнение 2.3. Покажите, что $y^n - x^n$ делится в $\mathbb{Z}[x, y]$ на $y - x$ и найдите частное.

2.1.3. Дифференциальное исчисление. Заменим в $f(x) = a_0 + a_1x + a_2x^2 + \dots$ переменную x на $x + t$, где t — ещё одна переменная. Получим ряд

$$f(x + t) = a_0 + a_1(x + t) + a_2(x + t)^2 + \dots \in K[\![x, t]\!]\,.$$

[1] Т. е. с единицей и без делителей нуля.

Раскроем в нём все скобки, затем сгруппируем слагаемые по степеням переменной t и обозначим через $f_m(x) \in K[\![x]\!]$ ряд, возникающий как коэффициент при t^m:

$$f(x+t) = f_0(x) + f_1(x)\cdot t + f_2(x)\cdot t^2 + f_3(x)\cdot t^3 + \ldots = \sum_{m\geqslant 0} f_m(x)\cdot t^m\,. \tag{2-5}$$

Упражнение 2.4. 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' 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 при помощи упр. 2.3 как результат подстановки $t = 0$ в ряд

$$\frac{f(x+t)-f(x)}{t} = \sum_{k\geqslant 1} a_k \frac{(x+t)^k - x^k}{t} = \sum_{k\geqslant 1} a_k\big((x+t)^{k-1} + (x+t)^{k-2}x + \ldots + x^{k-1}\big)\,,$$

что даёт

$$f'(x) = \sum_{k\geqslant 1} k\,a_k x^{k-1} = a_1 + 2a_2 x + 3a_3 x^2 + \ldots\,. \tag{2-6}$$

Пример 2.3 (ряды с нулевой производной)
Из формулы (2-6) вытекает, что производная от константы равна нулю. Если[1] $\operatorname{char} K = 0$, то верно и обратное: $f' = 0$ тогда и только тогда, когда $f = a_0$. Но если $\operatorname{char} K = p > 0$, то производная от каждого монома вида x^{kp} занулится, поскольку коэффициент m при x^{m-1} в формуле (2-6) представляет собою сумму m единиц кольца K. Мы заключаем, над целостным кольцом K характеристики $p > 0$ равенство $f'(x) = 0$ означает, что $f(x) = g(x^p)$ для некоторого $g \in K[\![x]\!]$.

Упражнение 2.5. Покажите, что при простом $p \in \mathbb{N}$ для любого ряда $g \in \mathbb{F}_p[\![x]\!]$ выполняется равенство $g(x^p) = g(x)^p$.

Предложение 2.1 (правила дифференцирования)
Для любого $\alpha \in K$ и любых $f, g \in K[\![x]\!]$ справедливы равенства

$$(\alpha f)' = \alpha\cdot f'\,,\quad (f+g)' = f'+g'\,,\quad (fg)' = f'\cdot g + f\cdot g'\,. \tag{2-7}$$

Кроме того, если ряд g не имеет свободного члена, то

$$\big(f(g(x))\big)' = g'(x)\cdot f'\big(g(x)\big)\,, \tag{2-8}$$

а если ряд f обратим, то

$$\frac{d}{dx}f^{-1} = -f'/f^2\,. \tag{2-9}$$

Доказательство. Первые два равенства в (2-7) вытекают прямо из формулы (2-6). Для доказательства третьего перемножим ряды

$$f(x+t) = f(x) + t\cdot f'(x) + (\text{члены, делящиеся на } t^2)$$
$$g(x+t) = g(x) + t\cdot g'(x) + (\text{члены, делящиеся на } t^2)\,.$$

[1] См. n° 1.5.5 на стр. 32.

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 (2-8) доказывается похожим образом: подставляя в $f(x)$ вместо x ряд $g(x+t)$, получаем $f\big(g(x+t)\big) = f\big(g(x) + t\cdot g'(x) + (\text{члены, делящиеся на } t^2)\big)$. Полагая $\tau(x,t) \stackrel{\text{def}}{=} g(x+t) - g(x) = t\cdot g'(x) + (\text{члены, делящиеся на } t^2)$ и переписывая правую часть предыдущего ряда как

$$\begin{aligned} f\big(g(x+t)\big) = f\big(g(x) + \tau(x,t)\big) = \\ = f(g(x)) + \tau(x,t)\cdot f'(g(x)) + (\text{члены, делящиеся на } \tau(x,t)^2) = \\ = f(g(x)) + t\cdot g'(x)\cdot f'(g(x)) + (\text{члены, делящиеся на } t^2)\,, \end{aligned}$$

заключаем, что $\big(f(g(x))\big)' = g'(x)\cdot f'\big(g(x)\big)$. Для доказательства формулы (2-9) достаточно продифференцировать обе части равенства $f\cdot f^{-1} = 1$. □

Упражнение 2.6. Покажите, что при $\operatorname{char}\Bbbk = 0$ в разложении (2-5) каждый ряд $f_m(x)$ равен $\frac{1}{m!}\big(\frac{d}{dx}\big)^m f(x)$, где $\big(\frac{d}{dx}\big)^m$ означает m-кратное применение операции $\frac{d}{dx}$.

2.2. Делимость в кольце многочленов. Школьный алгоритм «деления уголком» работает для многочленов с коэффициентами в произвольном коммутативном кольце с единицей при условии, что многочлен-делитель имеет обратимый старший коэффициент.

Предложение 2.2 (деление с остатком)
Пусть K — произвольное коммутативное кольцо с единицей, и старший коэффициент многочлена $u\in K[x]$ обратим. Тогда для любого $f\in K[x]$ существуют такие $q, r\in K[x]$, что $f = uq + r$ и $\deg(r) < \deg(u)$ или $r = 0$. Если кольцо K целостное, то q и r однозначно определяются этими свойствами по f и u.

Доказательство. Пусть $f = a_n x^n + \ldots + a_1 x + a_0$ и $u = b_k x^k + \ldots + b_1 x + b_0$, где b_k обратим. Если $n < k$, можно взять $q = 0$ и $r = f$. Если $k = 0$, т. е. $u = b_0$, можно взять $r = 0$, $q = b_0^{-1} f$. Пусть $n \geqslant k > 0$ и предложение справедливо для всех многочленов f с $\deg f < n$. Тогда многочлен $f - a_n b_k^{-1} x^{n-k} u$ имеет степень, строго меньшую чем n, и по индукции представляется в виде $qu + r$, где $\deg r < \deg u$ или $r = 0$. Тем самым, $f = (q + a_n b_k^{-1} x^{n-k})\cdot u + r$, как и утверждалось. Если кольцо K целостное и $p, s\in K[x]$ таковы, что $\deg(s) < \deg(u)$ и $up + s = f = uq + r$, то $u(q-p) = r - s$. При $p - q \neq 0$ степень левой части не менее $\deg u$, что строго больше степени правой. Поэтому, $p - q = 0$, откуда и $r - s = 0$. □

Определение 2.1
Многочлены q и r, удовлетворяющие условиям предл. 2.2 называются *неполным частным* и *остатком* от деления f на u в $K[x]$.

Следствие 2.1
Для любых многочленов f, g с коэффициентами в любом поле $\Bbbk$ существует единственная такая пара многочленов $q, r\in\Bbbk[x]$, что $f = g\cdot q + r$ и $\deg(r) < \deg(g)$ или $r = 0$. □

Пример 2.4 (вычисление значения многочлена в точке)
Остаток от деления многочлена $f(x) = a_n x^n + \ldots + a_1 x + a_0$ на линейный двучлен $x - \alpha$ имеет степень нуль и равен значению $f(\alpha)$ многочлена f при $x = \alpha$, в чём легко убедиться, подставляя

$x = \alpha$ в равенство $f(x) = (x - \alpha) \cdot q(x) + r$. При «делении уголком» значение $f(\alpha)$ вычисляется в виде

$$f(\alpha) = \alpha\Big(\dots \alpha\big(\alpha(\alpha a_n + a_{n-1}) + a_{n-2}\big) + \dots\Big) + a_0\,,$$

что гораздо эффективнее «лобовой подстановки» значения $x = \alpha$ в $a_n x^n + \dots + a_1 x + a_0$.

Предложение 2.3
Над произвольным полем $\Bbbk$ для любого набора многочленов $f_1, \dots, f_n \in \Bbbk[x]$ 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. Он представляется в виде

$$d = f_1 h_1 + \dots + f_n h_n\,, \quad \text{где} \quad h_i \in \Bbbk[x]\,. \tag{2-10}$$

Произвольный многочлен $g \in \Bbbk[x]$ представим в виде (2-10) если и только если $d | g$.

Доказательство. Единственность очевидна: два многочлена, каждый из которых делится на другой, имеют равные степени и могут различаться лишь постоянным множителем, который равен единице, коль скоро оба многочлена приведены. Существование доказывается тем же рассуждением, что и в n° 1.4.2 на стр. 28. Обозначим множество всех многочленов $g \in \Bbbk[x]$, представимых в виде (2-10), через $(f_1, \dots, f_n) \stackrel{\text{def}}{=} \big\{ f_1 h_1 + \dots + f_n h_n \;\big|\; h_i \in \Bbbk[x] \big\}$. Это подкольцо в $\Bbbk[x]$, содержащее вместе с каждым многочленом g и все кратные ему многочлены hg с любым $h \in \Bbbk[x]$. Кроме того, $(f_1, \dots, f_n)$ содержит каждый из многочленов f_i, и все многочлены из $(f_1, \dots, f_n)$ делятся на любой общий делитель всех многочленов f_i. Возьмём в качестве d приведённый многочлен наименьшей степени в $(f_1, \dots, f_n)$. Для любого $g \in (f_1, \dots, f_n)$ остаток $r = g - qd$ от деления g на d лежит в $(f_1, \dots, f_n)$, и так как неравенство $\deg r < \deg d$ невозможно, мы заключаем, что $r = 0$, т. е. все $g \in (f_1, \dots, f_n)$ делятся на d. □

Определение 2.2
Многочлен d из предл. 2.3 называется *наибольшим общим делителем*[1] многочленов f_i и обозначается нод$(f_1, \dots, f_n)$.

2.2.1. Взаимная простота. Из предл. 2.3 вытекает, что для любого поля $\Bbbk$ взаимная простота[2] многочленов $f_1, \dots, f_m \in \Bbbk[x]$, т. е. наличие таких $h_1, \dots, h_m \in \Bbbk[x]$, что $h_1 f_1 + \dots + h_n f_n = 1$, равносильна отсутствию у многочленов $f_1, \dots, f_n$ общих делителей положительной степени — точно также, как это происходит в кольце целых чисел $\mathbb{Z}$.

Определение 2.3
Необратимый многочлен $f \in K[x]$ с коэффициентами в целостном[3] кольце K называется *неприводимым*, если из равенства $f = gh$ вытекает, что g или h является обратимой константой.

Упражнение 2.7. Пусть $\Bbbk$ — любое поле. Пользуясь лем. 1.3, докажите следующую теорему об однозначности разложения на простые множители в кольце $\Bbbk[x]$: каждый многочлен f положительной степени является произведением конечного числа неприводимых многочленов, причём в любых двух таких представлениях $p_1 \dots p_k = f = q_1 \dots q_m$ одинаковое количество множителей $k = m$, и их можно перенумеровать так, чтобы $p_i = \lambda_i q_i$ при всех i для некоторых ненулевых констант $\lambda_i \in \Bbbk$.

[1] Ср. с зам. 1.3. на стр. 27.
[2] См. опр. 1.2 на стр. 27.
[3] Т. е. с единицей и без делителей нуля.

2.2.2. Алгоритм Евклида – Гаусса из n° 1.2.2 также применим к многочленам с коэффициентами из любого поля $\Bbbk$. Покажем, как он работает, вычислив нод(f,g) для

$$f = x^7 + 3x^6 + 4x^5 + x^4 + 5x^2 + 3x^3 + 3x + 4 \text{ и } g = x^5 + 5x^4 + 11x^3 + 12x^2 + 7x + 4\,.$$

Как и в n° 1.2.2 на стр. 25, составляем таблицу

$$\begin{pmatrix} f & 1 & 0 \\ g & 0 & 1 \end{pmatrix} = \begin{pmatrix} x^7 + 3x^6 + 4x^5 + x^4 + 3x^3 + 5x^2 + 3x + 4 & 1 & 0 \\ x^5 + 5x^4 + 11x^3 + 12x^2 + 7x + 4 & 0 & 1 \end{pmatrix}.$$

и преобразуем её строки, умножая какую-нибудь из них на ненулевую константу и прибавляя к результату другую строку, умноженную на подходящий многочлен, так, чтобы степень одного из многочленов в левом столбце строго уменьшалась, пока один из них не обнулится:

$$\begin{aligned}
(1) \mapsto (1) - x^2\,(2): &\quad \begin{pmatrix} -2x^6 - 7x^5 - 11x^4 - 4x^3 + x^2 + 3x + 4 & 1 & -x^2 \\ x^5 + 5x^4 + 11x^3 + 12x^2 + 7x + 4 & 0 & 1 \end{pmatrix} \\
(1) \mapsto (1) + 2x\,(2): &\quad \begin{pmatrix} 3x^5 + 11x^4 + 20x^3 + 15x^2 + 11x + 4 & 1 & -x^2 + 2x \\ x^5 + 5x^4 + 11x^3 + 12x^2 + 7x + 4 & 0 & 1 \end{pmatrix} \\
(1) \mapsto (1) - 3\,(2): &\quad \begin{pmatrix} -4x^4 - 13x^3 - 21x^2 - 10x - 8 & 1 & -x^2 + 2x - 3 \\ x^5 + 5x^4 + 11x^3 + 12x^2 + 7x + 4 & 0 & 1 \end{pmatrix} \\
(2) \mapsto 4\,(2) + x\,(1): &\quad \begin{pmatrix} -4x^4 - 13x^3 - 21x^2 - 10x - 8 & 1 & -x^2 + 2x - 3 \\ 7x^4 + 23x^3 + 38x^2 + 20x + 16 & x & -x^3 + 2x^2 - 3x + 4 \end{pmatrix} \\
(2) \mapsto 4\,(2) + 7\,(1): &\quad \begin{pmatrix} -4x^4 - 13x^3 - 21x^2 - 10x - 8 & 1 & -x^2 + 2x - 3 \\ x^3 + 5x^2 + 10x + 8 & 4x + 7 & -4x^3 + x^2 + 2x - 5 \end{pmatrix} \\
(1) \mapsto (1) + 4x\,(2): &\quad \begin{pmatrix} 7x^3 + 19x^2 + 22x - 8 & 16x^2 + 28x + 1 & -16x^4 + 4x^3 + 7x^2 - 18x - 3 \\ x^3 + 5x^2 + 10x + 8 & 4x + 7 & -4x^3 + x^2 + 2x - 5 \end{pmatrix} \\
(1) \mapsto (1) - 7\,(2): &\quad \begin{pmatrix} -16x^2 - 48x - 64 & 16x^2 - 48 & -16x^4 + 32x^3 - 32x + 32 \\ x^3 + 5x^2 + 10x + 8 & 4x + 7 & -4x^3 + x^2 + 2x - 5 \end{pmatrix} \\
(2) \mapsto (2) + x\,(1)/16: &\quad \begin{pmatrix} x^2 + 3x + 4 & -x^2 + 3 & x^4 - 2x^3 + 2x - 2 \\ 2x^2 + 6x + 8 & x^3 + x + 7 & -x^5 + 2x^4 - 4x^3 - x^2 + 4x - 5 \end{pmatrix} \\
(2) \mapsto (2) - 2\,(1): &\quad \begin{pmatrix} x^2 + 3x + 4 & -x^2 + 3 & x^4 - 2x^3 + 2x - 2 \\ 0 & x^3 + 2x^2 + x + 1 & -x^5 - x^2 - 1 \end{pmatrix}
\end{aligned}$$

Полученный результат означает, что нод$(f,g) = x^2+3x+4 = -(x^2-3)\cdot f + (x^4-2x^3+2x-2)\cdot g$, а нок$(f,g) = (x^3+2x^2+x+1)\cdot f = (x^5+x^2+1)\cdot g$.

Упражнение 2.8. Убедитесь, что в каждой возникающей по ходу вычисления таблице

$$\begin{pmatrix} p & r & s \\ q & u & w \end{pmatrix}$$

выполняются равенства $p = rf + sg$, $q = uf + wg$, а многочлен $rw - us$ является ненулевой константой, и выведите из них, что в итоговой таблице вида

$$\begin{pmatrix} d' & h_1 & h_2 \\ 0 & m_1 & m_2 \end{pmatrix} \quad \text{или} \quad \begin{pmatrix} 0 & m_1 & m_2 \\ d' & h_1 & h_2 \end{pmatrix}$$

многочлен $d' = fh_1 + gh_2$ делит f и g, а многочлен $c' = fm_1 = -gm_2$ делит любое общее кратное f и g.

2.3. Корни многочленов. Число $\alpha \in K$ называется *корнем* многочлена $f \in K[x]$, если $f(\alpha) = 0$. Как мы видели в прим. 2.4 на стр. 40, это равносильно тому, что $f(x)$ делится в $K[x]$ на $x - \alpha$.

Упражнение 2.9. Пусть $\Bbbk$ — поле. Проверьте, что многочлен степени 2 или 3 неприводим в $\Bbbk[x]$ если и только если у него нет корней в поле $\Bbbk$.

Предложение 2.4
Пусть K — целостное кольцо и $f \in K[x]$ имеет s различных корней $\alpha_1, \dots, \alpha_s \in K$. Тогда f делится в $K[x]$ на произведение $\prod_i (x - \alpha_i)$. В частности, $\deg(f) \geqslant s$ или $f = 0$.

Доказательство. Так как в K нет делителей нуля и $(\alpha_i - \alpha_1) \neq 0$ при $i \neq 1$, подставляя в равенство $f(x) = (x - \alpha_1) \cdot q(x)$ значения $x = \alpha_2, \dots, \alpha_s$, убеждаемся, что они являются корнями многочлена $q(x)$, и применяем индукцию. □

Следствие 2.2
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. Так как $\deg(f - g) \leqslant n$, и у $f - g$ больше n корней, $f - g = 0$. □

Пример 2.5 (интерполяционный многочлен Лагранжа)
Пусть $\Bbbk$ — поле. По сл. 2.2 для любых наборов из $n + 1$ различных чисел $a_0, a_1, \dots, a_n \in \Bbbk$ и произвольных значений $b_0, b_1, \dots, b_n \in \Bbbk$ имеется не более одного многочлена $f \in \Bbbk[x]$ степени $\leqslant n$ со значениями $f(a_i) = b_i$ при всех i. Единственный такой многочлен всегда существует и называется *интерполяционным многочленом Лагранжа*. Чтобы выписать его явно заметим, что произведение $\prod_{\nu \neq i} (x - a_\nu)$ зануляется во всех точках a_ν кроме i-той, где его значение отлично от нуля. Деля на него, получаем многочлен $f_i(x) = \prod_{\nu \neq i} (x - a_\nu) / \prod_{\nu \neq i} (a_i - a_\nu)$ со значениями $f_i(a_\nu) = 0$ при $\nu \neq i$ и $f_i(a_i) = 1$. Искомый многочлен Лагранжа имеет вид

$$\sum_{i=0}^{n} b_i f_i(x) = \sum_{i=0}^{n} b_i \prod_{\nu \neq i} \frac{x - a_\nu}{a_i - a_\nu}.$$

2.3.1. Присоединение корней. Зафиксируем произвольный отличный от константы многочлен $f \in \Bbbk[x]$. Кольцо вычетов $\Bbbk[x]/(f)$ определяется аналогично кольцу[1] $\mathbb{Z}/(n)$. А именно, обозначим через $(f) = \{fh \mid h \in \Bbbk[x]\}$ подкольцо в $\Bbbk[x]$, состоящее из всех многочленов, делящихся на f. Сдвиги этого подкольца на всевозможные элементы $g \in \Bbbk[x]$ обозначаются

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

и называются *классами вычетов* по модулю f. Два таких класса $[g_1]_f$ и $[g_2]_f$ либо не пересекаются, либо совпадают, причём последнее означает, что $g_1 - g_2 \in (f)$.

Упражнение 2.10. Убедитесь, что отношение $g_1 \equiv g_2 \pmod f$, означающее, что $g_1 - g_2 \in (f)$, является эквивалентностью[2].

Множество классов вычетов обозначается через $\Bbbk[x]/(f)$. Сложение и умножение в нём задаётся формулами $[g]_f + [h]_f \stackrel{\text{def}}{=} [g + h]_f$, $[g]_f \cdot [h]_f \stackrel{\text{def}}{=} [gh]_f$.

[1] См. n° 1.4 на стр. 28.
[2] См. опр. 0.1 на стр. 10.

Упражнение 2.11. Проверьте корректность[1] этого определения и выполнение в $\Bbbk[x]/(f)$ всех аксиом коммутативного кольца с единицей.

Нулём кольца $\Bbbk[x]/(f)$ является класс $[0]_f = (f)$, единицей — класс $[1]_f = 1 + (f)$. Так как константы не делятся на многочлены 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 классы чисел $c \in \Bbbk$ обычно записываются как c, а не $[c]_f$.

Упражнение 2.12. Покажите, что для любого $\alpha \in \Bbbk$ кольцо $\Bbbk[x]/(x-\alpha)$ изоморфно полю $\Bbbk$.

Каждый многочлен $g \in \Bbbk[x]$ однозначно представляется в виде $g = fh + r$, где $\deg r < \deg f$. Поэтому в каждом классе $[g]_f$ есть ровно один многочлен $r \in [g]_f$ с $\deg(r) < \deg(f)$. Таким образом, каждый элемент кольца $\Bbbk[x]/(f)$ однозначно записывается в виде

$$[a_0 + a_1 x + \ldots + a_{n-1}x^{n-1}]_f = a_0 + a_1\vartheta + \ldots + a_{n-1}\vartheta^{n-1}\,,\ \text{где } \vartheta = [x]_f \text{ и } a_i \in \Bbbk\,.$$

Класс $\vartheta = [x]_f$ удовлетворяет в кольце $\Bbbk[x]/(f)$ уравнению $f(\vartheta) = 0$, ибо

$$f(\vartheta) = f\left([x]_f\right) = [f(x)]_f = [0]_f\,.$$

В таких обозначениях сложение и умножение вычетов представляет собою формальное сложение и умножение записей $a_0 + a_1\vartheta + \ldots + a_{n-1}\vartheta^{n-1}$ по стандартным правилам раскрытия скобок и приведения подобных слагаемых с учётом соотношения $f(\vartheta) = 0$. По этой причине кольцо $\Bbbk[x]/(f)$ часто обозначают через $\Bbbk[\vartheta]$, где $f(\vartheta) = 0$, и называют *расширением* поля $\Bbbk$ путём *присоединения* к нему корня ϑ многочлена $f \in \Bbbk[x]$.

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

$$(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2}$$
$$(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (cb + ad)\sqrt{2}\,.$$

Упражнение 2.13. Проверьте, что $\mathbb{Q}[\sqrt{2}]$ является полем, и выясните, являются ли полями кольца $\mathbb{Q}[\vartheta]$, в которых а) $\vartheta^3 + 1 = 0$ б) $\vartheta^3 + 2 = 0$.

Предложение 2.5
Пусть $\Bbbk$ — произвольное поле и $f \in \Bbbk[x]$. Кольцо $\Bbbk[x]/(f)$ является полем если и только если f неприводим в $\Bbbk[x]$.

Доказательство. Если $f = gh$, где степени f и g строго меньше $\deg f$, ненулевые классы $[g]$, $[h]$ являются делителями нуля в кольце $\Bbbk[x]/(f)$, что невозможно в поле. Если f неприводим, то $\text{нод}(f, g) = 1$ для любого $g \notin (f)$, и значит, $fh + gq = 1$ для некоторых $h, q \in \Bbbk[x]$, откуда $[q]\cdot[g] = [1]$, т. е. класс $[g]$ обратим в $\Bbbk[x]/(f)$. □

Упражнение 2.14. Найдите $(1+\vartheta)^{-1}$ в поле $\mathbb{Q}[\vartheta]$, где $\vartheta^2 + \vartheta + 1 = 0$.

[1] Т. е. независимость классов $[g+h]_f$ и $[gh]_f$ от выбора представителей $g \in [g]_f$ и $h \in [h]_f$.

Теорема 2.1
Для любого поля $\Bbbk$ и произвольного $f \in \Bbbk[x]$ существует такое поле $\mathbb{F} \supset \Bbbk$, что в кольце $\mathbb{F}[x]$ многочлен f разлагается в произведение $\deg f$ линейных множителей.

Доказательство. Индукция по $n = \deg f$. Пусть для любого поля $\Bbbk$ и каждого многочлена степени $< n$ из $\Bbbk[x]$ искомое поле имеется[1]. Рассмотрим многочлен f степени n. Если он приводим, т. е. $f = gh$ и $\deg g, \deg h < n$, то по индуктивному предположению существует поле $\mathbb{L} \supset \Bbbk$ над которым g полностью разлагается на линейные множители, а также поле $\mathbb{F} \supset \mathbb{L}$ над которым полностью разлагается h, а с ним и f. Если f неприводим, рассмотрим поле $\mathbb{L} = \Bbbk[x]/(f)$. Оно содержит $\Bbbk$ в качестве классов констант, и многочлен f делится в $\mathbb{L}[x]$ на $(x - \vartheta)$, где $\vartheta = [x]_f \in \mathbb{L}$. Частное от этого деления имеет степень $n-1$ и по индукции раскладывается на линейные множители над некоторым полем $\mathbb{F} \supset \mathbb{L}$. Тем самым и f полностью раскладывается над $\mathbb{F}$. □

Теорема 2.2 (китайская теорема об остатках)
Пусть многочлен $f = f_1 \dots f_m \in \Bbbk[x]$ является произведением m попарно взаимно простых многочленов $f_i \in \Bbbk[x]$. Тогда отображение

$$\varphi : \frac{\Bbbk[x]}{(f)} \to \frac{\Bbbk[x]}{(f_1)} \times \dots \times \frac{\Bbbk[x]}{(f_m)}, \quad [g]_f \mapsto ([g]_{f_1}, \dots, [g]_{f_m}), \tag{2-11}$$

корректно определено и является изоморфизмом колец.

Доказательство. Проверка того, что отображение (2-11) корректно определено[2], является гомоморфизмом колец и имеет нулевое ядро, дословно та же, что в n° 1.7 на стр. 35, и мы оставляем её читателям. Докажем, что гомоморфизм (2-11) сюръективен. Для каждого i обозначим через $F_i = f/f_i$ произведение всех многочленов f_ν кроме i-го. Так как f_i взаимно прост с каждым f_ν при $\nu \neq i$, многочлены F_i и f_i взаимно просты по лем. 1.3 на стр. 27. Поэтому существует такой многочлен $h_i \in \Bbbk[x]$, что $[1]_{f_i} = [F_i]_{f_i}[h_i]_{f_i} = [F_i h_i]_{f_i}$ в $\Bbbk[x]/(f_i)$. Мы заключаем, что класс многочлена $F_i h_i$ нулевой во всех кольцах $\Bbbk[x]/(f_\nu)$ с $\nu \neq i$ и равен единице в $\Bbbk[x]/(f_i)$. Поэтому для любого набора классов $[r_i]_{f_i} \in \Bbbk[x]/(f_i)$ многочлен $g = \sum_i r_i F_i h_i$ таков, что $[g]_{f_i} = [r_i]_{f_i}$ сразу для всех i. □

2.3.2. Общие корни нескольких многочленов $f_1, \dots, f_m \in \Bbbk[x]$ с коэффициентами в поле $\Bbbk$ искать обычно проще, чем корни каждого из многочленов f_i в отдельности, так как общие корни являются корнями многочлена $\text{нод}(f_1, \dots, f_m)$, который находится при помощи алгоритма Евклида и как правило имеет меньшую степень, чем любой из f_i. Отметим, что при $\text{нод}(f_1, \dots, f_m) = 1$ многочлены f_i не имеют общих корней не только в поле $\Bbbk$, но и ни в каком большем кольце $K \supset \Bbbk$, поскольку существуют такие $h_i \in \Bbbk[x]$, что $f_1 h_1 + \dots + f_m h_m = 1$.

2.3.3. Кратные корни. Пусть $\Bbbk$ — произвольное поле. Число $\alpha \in \Bbbk$ называется m-кратным корнем многочлена $f \in \Bbbk[x]$, если $f(x) = (x-\alpha)^m \cdot g(x)$ и $g(\alpha) \neq 0$. Корни кратности $m = 1$ называются *простыми*, а более высоких кратностей — *кратными*.

Предложение 2.6
Число α является кратным корнем многочлена f если и только если $f(\alpha) = f'(\alpha) = 0$.

[1] Заметим, что при $n = 2$ это так: достаточно взять $\mathbb{F} = \Bbbk$.
[2] Т. е. $\varphi([g]_f) = \varphi([h]_f)$ при $[g]_f = [h]_f$.

Доказательство. Если корень α кратный, то $f(x) = (x-\alpha)^2 g(x)$. Дифференцируя, получаем

$$f'(x) = (x-\alpha)\big(2g(x) + (x-\alpha)g'(x)\big),$$

откуда $f'(\alpha) = 0$. Если корень α не кратный, то $f(x) = (x-\alpha)g(x)$, где $g(\alpha) \neq 0$. Подставляя $x = \alpha$ в $f'(x) = (x-\alpha)g'(x) + g(x)$, получаем $f'(\alpha) = g(\alpha) \neq 0$. □

Предложение 2.7
Если $\operatorname{char}\Bbbk = 0$, то $\alpha \in \Bbbk$ является m-кратным корнем многочлена $f \in \Bbbk[x]$ если и только если

$$f(\alpha) = \frac{d}{dx}f(\alpha) = \ldots = \frac{d^{m-1}}{dx^{m-1}}f(\alpha) = 0 \quad \text{и} \quad \frac{d^m}{dx^m}f(\alpha) \neq 0\,.$$

Доказательство. Если $f(x) = (x-\alpha)^m g(x)$, то $f'(x) = (x-\alpha)^{m-1}\big(mg(x) + (x-\alpha)g'(x)\big)$. При $g(\alpha) \neq 0$ второй множитель в последнем равенстве ненулевой при $x = \alpha$. Поэтому α является m-кратным корнем f если и только если α является $(m-1)$-кратным корнем f'. □

2.3.4. Сепарабельность. Многочлен $f \in \Bbbk[x]$ называется *сепарабельным*, если он взаимно прост со своей производной. Это равносильно отсутствию у f кратных корней в любом кольце $K \supset \Bbbk$. В самом деле, если $\deg \operatorname{нод}(f, f') \geqslant 1$ или $f' = 0$, то по теор. 2.1 $\operatorname{нод}(f, f')$ или, соответственно, сам f имеет корень в некотором поле $\mathbb{F} \supset \Bbbk$, и по предл. 2.6 этот корень кратный для f. Наоборот, если $\operatorname{нод}(f, f') = 1$, то $pf + qf' = 1$ для подходящих $p, q \in \Bbbk[x]$, и поэтому f и f' не могут одновременно обратиться в нуль ни в каком расширении $K \supset \Bbbk$.

Пример 2.6 (сепарабельность и несепарабельность неприводимых многочленов)
Если многочлен $f \in \Bbbk[x]$ неприводим, то он взаимно прост со всеми ненулевыми многочленами меньшей степени. Поэтому $\operatorname{нод}(f, f') = 1$, если $f' \neq 0$ в $\Bbbk[x]$. Поскольку над полем характеристики нуль каждый многочлен положительной степени имеет ненулевую производную, все неприводимые многочлены над таким полем сепарабельны. Если $\operatorname{char}\Bbbk = p > 0$, то $f' = 0$ если и только если[1] $f(x) = g(x^p)$ для некоторого $g(x) = b_m x^m + \ldots + b_1 x + b_0 \in \Bbbk[x]$. Так как в характеристике p возведение в p-тую степень является гомоморфизмом колец[2] и тождественно действует на простом поле $\mathbb{F}_p$, для любого многочлена g с коэффициентами в простом конечном поле $\Bbbk = \mathbb{F}_p$ выполняются равенства

$$g(x^p) = b_m x^{pm} + \ldots + b_1 x^p + b_0 = b_m^p x^{pm} + \ldots + b_1^p x^p + b_0^p = \\ = (b_m x^m + \ldots + b_1 x + b_0)^p = g^p(x)\,.$$

Поэтому в $\mathbb{F}_p[x]$ каждый многочлен с нулевой производной является чистой p-той степенью и тем самым приводим. Мы заключаем, что в $\mathbb{F}_p[x]$ все неприводимые многочлены тоже сепарабельны.

Упражнение 2.15*. Покажите, что неприводимый многочлен над любым конечным полем сепарабелен.

Неприводимый многочлен над бесконечным полем положительной характеристики не обязательно сепарабелен. Например, можно показать, что над полем $\Bbbk = \mathbb{F}_p(t)$ рациональных функций от одной переменной t с коэффициентами в поле $\mathbb{F}_p$ многочлен $f(x) = x^p - t$ неприводим, но поскольку $f' = 0$, многочлен f не сепарабелен.

[1] См. прим. 2.3 на стр. 39.
[2] См. прим. 1.7 на стр. 29.

2.4. Поле комплексных чисел $\mathbb{C} \stackrel{\text{def}}{=} \mathbb{R}[t]/(t^2+1)$ получается из поля $\mathbb{R}$ присоединением корня неприводимого над $\mathbb{R}$ многочлена $t^2+1=0$ и состоит из элементов $x+iy$, где $x, y \in \mathbb{R}$, а $i \stackrel{\text{def}}{=} [t]$ удовлетворяет соотношению $i^2 = -1$. Обратным к ненулевому числу $x+yi$ является число

$$\frac{1}{x+yi} = \frac{x-iy}{(x+iy)(x-iy)} = \frac{x}{x^2+y^2} - \frac{y}{x^2+y^2}\cdot i\,.$$

Комплексное число $z = x+yi$ удобно изображать на плоскости $\mathbb{R}^2$ с фиксированной прямоугольной системой координат (x, y) *радиус вектором* z, ведущим из начала координат в точку $z = (x, y)$, как на рис. 2◇1. Координаты (x, y) называются *действительной* и *мнимой* частями числа $z \in \mathbb{C}$ и обозначаются через $\operatorname{Re}(z)$ и $\operatorname{Im}(z)$, а длина $|z| \stackrel{\text{def}}{=} \sqrt{x^2+y^2}$ называется *модулем* или *абсолютной величиной* комплексного числа z. Множество всех таких $\vartheta \in \mathbb{R}$, что поворот плоскости вокруг нуля на угол ϑ совмещает направление координатной оси x с направлением вектора z, называется *аргументом* числа z и обозначается $\operatorname{Arg}(z) = \{\alpha + 2\pi k \mid k \in \mathbb{Z}\}$, где $\alpha \in \mathbb{R}$ — ориентированная длина какой-нибудь дуги единичной окружности, ведущей из точки $(1, 0)$ в точку[1] $z/|z|$. Таким образом, каждое комплексное число имеет вид $z = |z|\cdot(\cos\alpha + i\cdot\sin\alpha)$, где $\alpha \in \operatorname{Arg}(z)$, и $\operatorname{Re}(z) = |z|\cdot\cos\alpha$, а $\operatorname{Im}(z) = |z|\cdot\sin\alpha$.

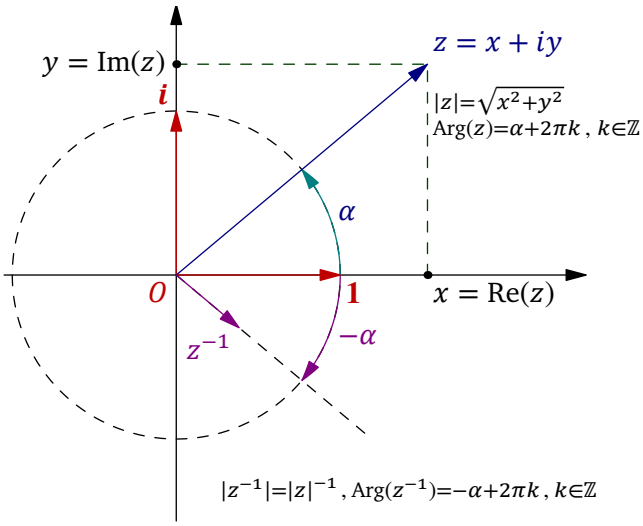


Рис. 2◇1. Числа $z = |z|\cdot(\cos\alpha + i\sin\alpha)$ и $z^{-1} = |z|^{-1}(\cos\alpha - i\sin\alpha)$.

На множестве векторов в $\mathbb{R}^2$ имеется своя внутренняя операция сложения векторов, относительно которой радиус векторы точек $z \in \mathbb{R}^2$ образуют абелеву группу. Зададим на множестве векторов в $\mathbb{R}^2$ операцию умножения требованием, чтобы длины перемножаемых векторов перемножались, а аргументы — складывались, т. е.

$$\begin{gathered} |z_1 z_2| = |z_1|\cdot|z_2| \\ \operatorname{Arg}(z_1 z_2) = \operatorname{Arg}(z_1) + \operatorname{Arg}(z_2) \stackrel{\text{def}}{=} \{\vartheta_1 + \vartheta_2 \mid \vartheta_1 \in \operatorname{Arg}(z_1),\ \vartheta_2 \in \operatorname{Arg}(z_2)\}\,. \end{gathered} \tag{2-12}$$

Упражнение 2.16. Проверьте корректность нижней формулы, т. е. убедитесь, что любые два числа в правом множестве отличаются на целое кратное 2π.

[1] Любые две таких дуги отличаются друг от друга на целое число оборотов, а «ориентированность» означает, что длину дуги следует брать со знаком «+», если движение вдоль неё происходит против часовой стрелки, и со знаком «−» если по часовой стрелке.

Лемма 2.1
Множество радиус векторов точек z евклидовой координатной плоскости $\mathbb{R}^2$ с описанными выше сложением и умножением является полем. Отображение $\mathbb{C} \to \mathbb{R}^2$, сопоставляющее комплексному числу $x + iy \in \mathbb{C}$ точку $z = (x, y) \in \mathbb{R}^2$, является изоморфизмом полей.

Доказательство. Радиус векторы точек плоскости образуют абелеву группу по сложению. Очевидно также, что ненулевые векторы образуют абелеву группу относительно операции умножения, задаваемой формулами (2-12). Единицей этой группы служит единичный направляющий вектор оси x, а обратный к ненулевому z вектор z^{-1} имеет $|z^{-1}| = 1/|z|$ и $\operatorname{Arg}(z^{-1}) = -\operatorname{Arg}(z)$ (см. рис. 2⋄1). Для проверки дистрибутивности заметим, что для любого $a \in \mathbb{R}^2$ отображение

$$a\colon \mathbb{R}^2 \to \mathbb{R}^2, \quad z \mapsto az,$$

состоящее в умножении всех векторов на a по формулам (2-12), представляет собою *поворотную гомотетию*[1] плоскости $\mathbb{R}^2$ относительно начала координат на угол $\operatorname{Arg}(a)$ с коэффициентом $|a|$. Аксиома дистрибутивности $a(b + c) = ab + ac$ утверждает, что поворотная гомотетия перестановочна со сложением векторов[2]. Но это действительно так, поскольку и повороты и гомотетии переводят параллелограммы в параллелограммы. Таким образом, радиус векторы точек евклидовой координатной плоскости $\mathbb{R}^2$ образуют поле. Векторы, параллельные горизонтальной координатной оси, составляют в нём подполе, изоморфное полю $\mathbb{R}$. Если обозначить через i единичный направляющий вектор вертикальной координатной оси, то радиус вектор каждой точки $z = (x, y) \in \mathbb{R}^2$ однозначно запишется в виде $z = x + iy$, где числа $x, y \in \mathbb{R}$ понимаются как векторы, параллельные горизонтальной координатной оси, а сложение и умножение происходят по правилам поля $\mathbb{R}^2$. При этом $i^2 = -1$ и для любых векторов $z_1 = x_1 + iy_1$ и $z_2 = x_2 + iy_2$ выполняются равенства $z_1 + z_2 = (x_1 + x_2) + i(y_1 + y_2)$ и

$$z_1 z_2 = (x_1 x_2 - y_1 y_2) + i(x_1 y_2 + x_2 y_1),$$

которыми описывается сложение и умножение вычетов $[x + yt]$ в поле $\mathbb{C} = \mathbb{R}[t]/(t^2 + 1)$. □

2.4.1. Комплексное сопряжение. Числа $z = x + iy$ и $\overline{z} \stackrel{\text{def}}{=} x - iy$ называются *комплексно сопряжёнными*. В терминах комплексного сопряжения обратное к ненулевому $z \in \mathbb{C}$ число можно записать как $z^{-1} = \overline{z}/|z|^2$. На геометрическом языке комплексное сопряжение $z \mapsto \overline{z}$ представляет собою симметрию комплексной плоскости относительно вещественной оси x. С алгебраической точки зрения сопряжение является инволютивным[3] автоморфизмом поля $\mathbb{C}$, т. е. $\overline{\overline{z}} = z$ для всех $z \in \mathbb{C}$, и $\overline{z_1 + z_2} = \overline{z}_1 + \overline{z}_2$, $\overline{z_1 z_2} = \overline{z}_1 \overline{z}_2$ для всех $z_1, z_2 \in \mathbb{C}$.

2.4.2. Тригонометрия. Почти вся школьная тригонометрия представляет собою трудно для восприятия закодированную запись заурядных алгебраических вычислений с комплексными числами, лежащими на единичной окружности.

Пример 2.7 (формулы сложения аргументов)
Произведение $z_1 z_2$ чисел $z_1 = \cos\varphi_1 + i\sin\varphi_1$ и $z_2 = \cos\varphi_2 + i\sin\varphi_2$ согласно лем. 2.1 равно $\cos(\varphi_1 + \varphi_2) + i\sin(\varphi_1 + \varphi_2)$, а лобовое перемножение этих чисел путём раскрытия скобок

[1] *Поворотной гомотетией* относительно точки 0 на угол α с коэффициентом $\varrho > 0$ называется композиция поворота на угол α вокруг точки 0 и растяжения в ϱ раз относительно 0. Так такие растяжения и повороты коммутируют друг с другом, неважно в каком порядке выполняется эта композиция.

[2] Т. е. является гомоморфизмом аддитивных групп.

[3] Эндоморфизм $\iota\colon X \to X$ произвольного множества X называется *инволюцией*, если $\iota \circ \iota = \mathrm{Id}_X$. По предл. 0.4 на стр. 15 всякая инволюция автоматически биективна.

даёт $z_1z_2 = (\cos\varphi_1\cos\varphi_2 - \sin\varphi_1\sin\varphi_2) + i(\cos\varphi_1\sin\varphi_2 + \sin\varphi_1\cos\varphi_2)$, откуда $\cos(\varphi_1+\varphi_2) = \cos\varphi_1\cos\varphi_2 - \sin\varphi_1\sin\varphi_2$ и $\sin(\varphi_1+\varphi_2) = \cos\varphi_1\sin\varphi_2 + \sin\varphi_1\cos\varphi_2$. Таким образом мы *доказали* тригонометрические формулы сложения аргументов.

Пример 2.8 (тригонометрические функции кратных углов)
По лем. 2.1 число $z = \cos\varphi + i\sin\varphi \in \mathbb{C}$ имеет $z^n = \cos(n\varphi) + i\sin(n\varphi)$. Раскрывая скобки в биноме $(\cos\varphi + i\sin\varphi)^n$ по форм. (0-8) на стр. 8, получаем равенство

$$\begin{aligned}\cos(n\varphi) + i\sin(n\varphi) &= (\cos\varphi + i\sin\varphi)^n = \\ &= \cos^n\varphi + i\binom{n}{1}\cos^{n-1}\varphi\sin\varphi - \binom{n}{2}\cos^{n-2}\varphi\sin^2\varphi - i\binom{n}{3}\cos^{n-3}\varphi\sin^3\varphi + \ldots = \\ &= \left(\binom{n}{0}\cos^n\varphi - \binom{n}{2}\cos^{n-2}\varphi\sin^2\varphi + \binom{n}{4}\cos^{n-4}\varphi\sin^4\varphi - \cdots\right) + \\ &\quad + i\cdot\left(\binom{n}{1}\cos^{n-1}\varphi\sin\varphi - \binom{n}{3}\cos^{n-3}\varphi\sin^3\varphi + \binom{n}{5}\cos^{n-5}\varphi\sin^5\varphi - \cdots\right)\end{aligned}$$

заключающее в себе сразу все мыслимые формулы для кратных углов:

$$\begin{aligned}\cos(n\varphi) &= \binom{n}{0}\cos^n\varphi - \binom{n}{2}\cos^{n-2}\varphi\sin^2\varphi + \binom{n}{4}\cos^{n-4}\varphi\sin^4\varphi - \cdots \\ \sin(n\varphi) &= \binom{n}{1}\cos^{n-1}\varphi\sin\varphi - \binom{n}{3}\cos^{n-3}\varphi\sin^3\varphi + \binom{n}{5}\cos^{n-5}\varphi\sin^5\varphi - \cdots\end{aligned}$$

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

Упражнение 2.17. Выразите $\sin(2\pi/5)$ и $\cos(2\pi/5)$ через радикалы от рациональных чисел.

2.4.3. Корни из единицы и круговые многочлены. Решим в поле $\mathbb{C}$ уравнение $z^n = 1$. Сравнивая модули левой и правой части, заключаем, что $|z| = 1$. Сравнивая аргументы, получаем $n\operatorname{Arg}(z) = \operatorname{Arg}(1) = \{2\pi k \mid k \in \mathbb{Z}\}$. С точностью до прибавления целых кратных 2π существует ровно n различных вещественных чисел, попадающих при умножении на n в множество $\{2\pi k \mid k \in \mathbb{Z}\}$. Это все геометрически различные углы $2\pi k/n$ с $0 \leqslant k \leqslant n-1$. Мы заключаем, что уравнение $z^n = 1$ имеет ровно n корней

$$\zeta_k = \cos(2\pi k/n) + i\sin(2\pi k/n), \quad \text{где} \quad k = 0, 1, \ldots, (n-1), \tag{2-13}$$

расположенных в вершинах правильного n-угольника, вписанного в единичную окружность так, что его вершина ζ_0 находится в точке 1, см. рис. 2⋄2 и рис. 2⋄3.

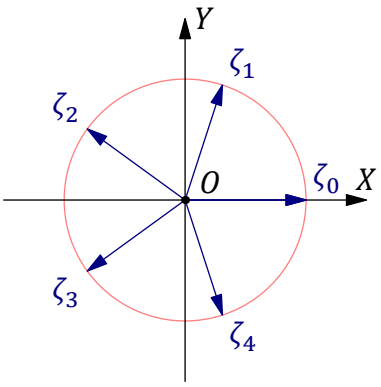


Рис. 2⋄2. Группа $\boldsymbol{\mu}_5$.

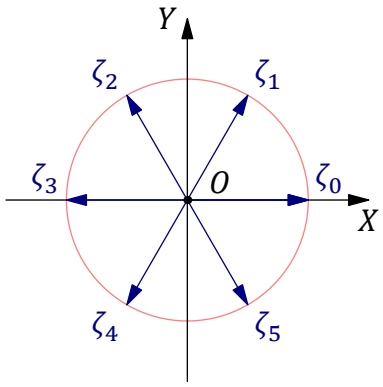


Рис. 2⋄3. Группа $\boldsymbol{\mu}_6$.

Корни (2-13) образуют абелеву группу относительно операции умножения. Эта группа обозначается $\boldsymbol{\mu}_n$ и называется *группой корней n-й степени из единицы*. 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, первообразным является корень $\zeta_1 = \cos(2\pi/n) + i\sin(2\pi/n)$, имеющий наименьший положительный аргумент. Но бывают и другие: на рис. 2⋄2 все четыре отличных от 1 элемента группы $\boldsymbol{\mu}_5$ являются первообразными корнями, тогда как в группе $\boldsymbol{\mu}_6$ на рис. 2⋄3 первообразными являются только ζ_1 и $\zeta_5 = \zeta_1^{-1} = \zeta_1^5$. Множество всех первообразных корней обозначается через $R_n \subset \boldsymbol{\mu}_n$.

Упражнение 2.18. Покажите, что $\zeta_1^k = \cos(2\pi k/n) + i\sin(2\pi k/n) \in R_n$ если и только если $\text{нод}(k, n) = 1$.

Приведённый многочлен $\Phi_n(z) = \prod_{\zeta \in R_n}(z - \zeta)$, корнями которого являются все первообразные корни n-й степени из единицы и только они, называется n-тым *круговым* или *циклотомическим* многочленом. Например, пятый и шестой круговые многочлены имеют вид

$$\Phi_5(z) = (z-\zeta_1)(z-\zeta_2)(z-\zeta_3)(z-\zeta_4) = z^4 + z^3 + z^2 + z + 1$$
$$\Phi_6(z) = (z-\zeta_1)(z-\zeta_4) = z^2 - z + 1\,.$$

Упражнение 2.19*. Попытайтесь доказать, что при всех $n \in \mathbb{N}$ многочлен Φ_n имеет целые коэффициенты и неприводим[1] в $\mathbb{Q}[x]$.

Пример 2.9 (уравнение $z^n = a$)
Число $z = |z| \cdot (\cos\varphi + i\sin\varphi) \in \mathbb{C}$ является корнем уравнения $z^n = a$ если и только если $|z|^n = |a|$ и $n\varphi \in \operatorname{Arg}(a)$. При $a \neq 0$ имеется ровно n таких чисел. Они выражаются через $r = |a|$ и $\alpha \in \operatorname{Arg} a$ по формуле

$$z_k = \sqrt[n]{r} \cdot \left(\cos\frac{\alpha + 2\pi k}{n} + i\,\sin\frac{\alpha + 2\pi k}{n}\right), \quad 0 \leqslant k \leqslant n-1\,,$$

и располагаются в вершинах правильного n-угольника, вписанного в окружность радиуса $\sqrt[n]{r}$ с центром в нуле так, что радиус вектор одной из его вершин образует с осью x угол α/n.

2.5. Конечные поля можно строить присоединяя к $\mathbb{F}_p = \mathbb{Z}/(p)$ корень какого-нибудь неприводимого многочлена $f \in \mathbb{F}_p[x]$. Если $\deg f = n$, то получающееся таким образом поле вычетов $\mathbb{F}_p[x]/(f)$ состоит из p^n элементов вида $a_0 + a_1\vartheta + \ldots + a_{n-1}\vartheta^{n-1}$, где $a_i \in \mathbb{F}_p$ и $f(\vartheta) = 0$.

Пример 2.10 (поле $\mathbb{F}_9$)
Многочлен $x^2 + 1 \in \mathbb{F}_3[x]$ неприводим, так как не имеет корней в $\mathbb{F}_3$. Присоединяя к $\mathbb{F}_3$ его корень, получаем поле $\mathbb{F}_9 \stackrel{\text{def}}{=} \mathbb{F}_3[x]/(x^2+1)$, состоящее из девяти элементов вида $a + bi$, где $a, b \in \mathbb{F}_3 = \{-1, 0, 1\}$ и $i^2 = -1$. Расширение $\mathbb{F}_3 \subset \mathbb{F}_9$ похоже на расширение $\mathbb{R} \subset \mathbb{C}$. Аналогом комплексного сопряжения в поле $\mathbb{F}_9$ является гомоморфизм Фробениуса[2] $F_3 : \mathbb{F}_9 \to \mathbb{F}_9, z \mapsto z^3$, тождественно действующий на простом подполе $\mathbb{F}_3 \subset \mathbb{F}_9$ и переводящий i в $-i$.

Упражнение 2.20. Составьте для поля $\mathbb{F}_9$ таблицы умножения и обратных элементов, перечислите в $\mathbb{F}_9$ все квадраты и кубы и убедитесь, что мультипликативная группа $\mathbb{F}_9^\times$ изоморфна $\boldsymbol{\mu}_8$.

[1] Т. е. не являются произведениями многочленов строго меньшей степени.
[2] См. прим. 1.10 на стр. 33.

Пример 2.11 (поле $\mathbb{F}_4$)
Многочлен $x^2+x+1 \in \mathbb{F}_2[x]$ неприводим, так как не имеет корней в $\mathbb{F}_2$. Присоединяя к $\mathbb{F}_2$ его корень, получаем поле $\mathbb{F}_4 \stackrel{\text{def}}{=} \mathbb{F}_2[x]/(x^2+x+1)$, состоящее из 0, 1, $\omega = [x]$ и $1+\omega = \omega^2 = \omega^{-1}$, причём[1] $\omega^2+\omega+1 = 0$. Расширение $\mathbb{F}_2 \subset \mathbb{F}_4$ тоже похоже на $\mathbb{R} \subset \mathbb{C}$, если понимать второе расширение как результат присоединения к $\mathbb{R}$ первообразного комплексного кубического корня ω из единицы, который также удовлетворяет уравнению $\omega^2+\omega+1=0$. В поле $\mathbb{F}_4$ аналогом комплексного сопряжения $\mathbb{C} \to \mathbb{C}$, переводящего $\omega \in \mathbb{C}$ в $\overline{\omega} = \omega^2$, также является гомоморфизм Фробениуса[2] $F_2 : \mathbb{F}_4 \to \mathbb{F}_4$, $z \mapsto z^2$, который тождественно действует на простом подполе $\mathbb{F}_2 \subset \mathbb{F}_4$ и переводит корни многочлена x^2+x+1 друг в друга.

Упражнение 2.21. Убедитесь, что мультипликативная группа $\mathbb{F}_4^\times$ изоморфна $\boldsymbol{\mu}_3$.

Теорема 2.3
Для каждого $n \in \mathbb{N}$ и простого $p \in \mathbb{N}$ существует конечное поле $\mathbb{F}_q$ из $q = p^n$ элементов.

Доказательство. Рассмотрим в $\mathbb{F}_p[x]$ многочлен $f(x) = x^q - x$. По теор. 2.1 существует такое поле $\mathbb{F} \supset \mathbb{F}_p$, что f полностью раскладывается в $\mathbb{F}[x]$ в произведение q линейных множителей. Так как $f'(x) = -1$, многочлен f сепарабелен[3], и все эти множители различны. Таким образом, в поле $\mathbb{F}$ имеется ровно q таких чисел α, что $\alpha^q = \alpha$. Обозначим множество этих чисел через $\mathbb{F}_q$ и покажем, что $\mathbb{F}_q \subset \mathbb{F}$ является подполем. Очевидно, что $0, 1 \in \mathbb{F}$ лежат в $\mathbb{F}_q$. Если $\alpha \in \mathbb{F}_q$, то $\alpha^{-1} \in \mathbb{F}_q$, так как $\left(\alpha^{-1}\right)^q = \left(\alpha^q\right)^{-1} = \alpha^{-1}$, и $-\alpha \in \mathbb{F}_q$, так как $(-\alpha)^q = -\alpha^q = -\alpha$ при $p \neq 2$, а в характеристике два $-\alpha = \alpha$. Если $\alpha, \beta \in \mathbb{F}_q$, то $(\alpha\beta)^q = \alpha^q\beta^q = \alpha\beta$, т. е. $\alpha\beta \in \mathbb{F}_q$. Поскольку $\operatorname{char}\mathbb{F} = p$, в поле $\mathbb{F}$ выполняется равенство[4] $(\alpha+\beta)^p = \alpha^p+\beta^p$. Применяя его n раз, заключаем, что $(\alpha+\beta)^q = (\alpha+\beta)^{p^n} = \alpha^{p^n}+\beta^{p^n} = \alpha+\beta$ для всех $\alpha, \beta \in \mathbb{F}_q$, откуда $\alpha+\beta \in \mathbb{F}_q$. □

Упражнение 2.22. Покажите, что число элементов в любом конечном поле является степенью его характеристики.

2.5.1. Конечные мультипликативные подгруппы поля. Рассмотрим абелеву группу A, операцию в которой будем записывать мультипликативно. Если группа A конечна, то среди степеней любого элемента $b \in A$ встречаются одинаковые, скажем $b^n = b^k$ с $n > k$. Умножая обе части этого равенства на b^{-k}, заключаем, что $b^{n-k} = 1$. Таким образом, для каждого $b \in A$ существует такое $m \in \mathbb{N}$, что $b^m = 1$. Наименьшее из этих m называется *порядком* элемента b и обозначается $\operatorname{ord} b$. Если $\operatorname{ord} b = n$, то элементы $b^0 = 1, b^1 = b, b^2, \ldots, b^{n-1}$ попарно различны, и каждая целая степень b^k совпадает с одним из них: если $k = nq + r$, где r — остаток от деления k на n, то $b^k = (b^n)^q b^r = b^r$. В частности, $b^m = 0$ если и только если $m \vdots \operatorname{ord} b$.

Упражнение 2.23. Покажите, что порядок любого элемента из конечной абелевой группы A делит $|A|$.

Группа A называется *циклической*, если она исчерпывается целыми степенями какого-нибудь элемента $a \in A$, т. е. $A = \{a^n \mid n \in \mathbb{Z}\}$. Для конечной группы A это равносильно равенству $\operatorname{ord} a = |A|$. Каждый обладающий этим свойством элемент $a \in A$ называется *образующей* циклической группы A. Например, группа $\boldsymbol{\mu}_n \subset \mathbb{C}$ комплексных корней n-й степени из единицы[5] циклическая, и её образующими являются первообразные корни.

[1] Отметим, что $-1 = 1$ в $\mathbb{F}_2$, что позволяет обходиться без минусов.
[2] См. прим. 1.10 на стр. 33.
[3] См. n° 2.3.4 на стр. 46.
[4] См. прим. 1.10 на стр. 33.
[5] См. n° 2.4.3 на стр. 49.

Предложение 2.8
Если порядки элементов мультипликативной абелевой группы A ограничены сверху, то максимальный из них делится на порядок любого элемента $a \in A$.

Доказательство. Достаточно для любых двух элементов $a_1, a_2 \in A$, имеющих порядки m_1, m_2, построить элемент $b \in A$, порядок которого равен нок(m_1, m_2). Если нод$(m_1, m_2) = 1$, положим $b = a_1 a_2$. Тогда $b^{m_1 m_2} = a^{m_1} a^{m_2} = 1$. Если $b^k = 1$, то $a_1^k = a_2^{-k}$, откуда $1 = a_1^{km_1} = a_2^{-km_1}$, и значит, $km_1 \vdots m_2$. Так как m_1 и m_2 взаимно просты, $k \vdots m_2$. Меня ролями a_1 и a_2, заключаем, что $k \vdots m_1$, а значит, $k \vdots m_1 m_2$. Тем самым, $\operatorname{ord}(b) = m_1 m_2 = \text{нок}(m_1, m_2)$.

Если нод$(m_1, m_2) \neq 1$, то для каждого простого $p \in \mathbb{N}$ обозначим через $\nu_i(p)$ показатель, с которым p входит в разложение числа m_i на простые множители[1]. Тогда

$$\text{нок}(m_1, m_2) = \prod\nolimits_p p^{\max(\nu_1(p), \nu_2(p))}.$$

Положим $\ell_1 = \prod p^{\nu_1(p)}$ по всем простым $p \in \mathbb{N}$ с $\nu_1(p) > \nu_2(p)$, и $\ell_2 = \text{нок}(m_1, m_2)/\ell_1$. Тогда нод$(\ell_1, \ell_2) = 1$ и $m_1 = k_1 \ell_1$, $m_2 = k_2 \ell_2$ для некоторых $k_1, k_2 \in \mathbb{N}$. Элементы $b_1 = a_1^{k_1}$, $b_2 = a_2^{k_2}$ имеют взаимно простые порядки ℓ_1, ℓ_2, и по уже доказанному их произведение $b = b_1 b_2$ имеет порядок $\ell_1 \ell_2 = \text{нок}(m_1, m_2)$. □

Следствие 2.3
Любая конечная подгруппа A в мультипликативной группе $\Bbbk^\times$ произвольного поля $\Bbbk$ является циклической.

Доказательство. Обозначим через m максимальный из порядков элементов группы A. Согласно предл. 2.8, все элементы группы A являются корнями многочлена $x^m - 1 = 0$. Поэтому их не более m и все они исчерпываются степенями имеющегося в A элемента m-того порядка. □

Теорема 2.4
Всякое конечное поле изоморфно одному из полей $\mathbb{F}_q$, построенных в теор. 2.3 на стр. 51.

Доказательство. Пусть поле $\mathbb{F}$ имеет характеристику p и состоит из q элементов. По сл. 2.3 мультипликативная группа $\mathbb{F}^\times$ является циклической. Обозначим её образующую через $\zeta \in \mathbb{F}^\times$. Тогда $\mathbb{F} = \{0, 1, \zeta, \zeta^2, \dots, \zeta^{q-2}\}$ и $\zeta^{q-1} = 1$. Чтобы доказать теорему, построим ещё одно поле из q элементов, изоморфное как полю $\mathbb{F}$, так и подходящему полю из теор. 2.3. Для этого обозначим через $g \in \mathbb{F}_p[x]$ приведённый многочлен минимальной степени с корнем ζ.

Упражнение 2.24. Убедитесь, что такой многочлен g существует, неприводим в $\mathbb{F}_p[x]$ и делит все многочлены $f \in \mathbb{F}_p[x]$ с корнем ζ.

Из упражнения вытекает, что кольцо $\mathbb{F}_p[x]/(g)$ является полем, а правило $[h]_g \mapsto h(\zeta)$ корректно задаёт ненулевой гомоморфизм колец $\mathbb{F}_p[x]/(g) \to \mathbb{F}$. Он инъективен по предл. 1.3 на стр. 32 и сюръективен, так как все ζ^m содержатся в его образе. Тем самым, $\mathbb{F} \simeq \mathbb{F}_p[x]/(g)$. В частности, поле $\mathbb{F}$ состоит из $q = p^n$ элементов $a_{n-1}\zeta^{n-1} + \dots + a_1\zeta + a_0$, где $a_i \in \mathbb{F}_p$, $n = \deg g$.

Так как ζ является корнем многочлена $f(x) = x^q - x$, из упр. 2.24 вытекает, что $f = gu$ для некоторого $u \in \mathbb{F}_p[x]$. Подставляя в это равенство q элементов поля $\mathbb{F}_q$, построенного в теор. 2.3 и состоящего в точности из q корней многочлена f, мы заключаем, что хотя бы один

[1] См. упр. 1.8 на стр. 27.

из них — назовём его $\xi \in \mathbb{F}_q$ — является корнем многочлена g. Правило $[h]_g \mapsto h(\xi)$ корректно задаёт вложение полей $\mathbb{F}_p[x]/(g) \hookrightarrow \mathbb{F}_q$, сюръективное, поскольку оба поля состоят из q элементов. Тем самым, $\mathbb{F}_p[x]/(g) \simeq \mathbb{F}_q$. □

Следствие 2.4 (из доказательства теор. 2.4)
Для каждого $n \in \mathbb{N}$ и простого $p \in \mathbb{N}$ в $\mathbb{F}_p[x]$ имеется неприводимый многочлен степени n. □

Следствие 2.5
Каждое конечное поле $\mathbb{F}$ состоит из p^n элементов, где простое $p = \operatorname{char}\mathbb{F}$, и для каждого $n \in \mathbb{N}$ и простого p имеется единственное с точностью до изоморфизма поле из p^n элементов. □

§3. Дроби и ряды

В этом параграфе мы продолжаем обозначать через K произвольное коммутативное кольцо с единицей, а через $\Bbbk$ — произвольное поле.

3.1. Кольца частных. Способ изготовления поля $\mathbb{Q}$ из кольца $\mathbb{Z}$ как множества дробей с целым числителем и ненулевым целым знаменателем[1] применим в любом коммутативном кольце K с единицей. Подмножество $S \subset K$ называется *мультипликативным*, если $1 \in S$ и $st \in S$ для всех $s, t \in S$. Например, множество всех целых неотрицательных степеней q^k любого элемента $q \in K$ мультипликативно[2]. Множество $K^\circ \subset K$, состоящее из всех не делящих нуль ненулевых элементов, тоже мультипликативно. В частности, множество всех ненулевых элементов любого целостного кольца мультипликативно. Каждое мультипликативное подмножество $S \subset K$ задаёт на множестве упорядоченных пар $K \times S$ отношение эквивалентности $\sim_S$, порождённое[3] отождествлениями $(a, s) \sim_S (at, st)$ для всех $t \in S$. Класс эквивалентности пары (a, s) по модулю этого отношения называется *дробью* со знаменателем в S и обозначается a/s. Множество всех таких дробей обозначается KS^{-1} или $K[S^{-1}]$ и называется *кольцом частных* или *локализацией* кольца K со знаменателями в S.

Пример 3.1
Пусть $K = \mathbb{Z}/(6)$ и $S = \{[1], [2], [-2]\}$. Каждая дробь в KS^{-1} имеет представление со знаменателем $[1]$: $[a]/[\pm 2] = [a][\mp 2]/[\pm 2][\mp 2] = [\mp a][2]/[1][2] = [\mp a]/[1]$. В частности, $[0]/[\pm 2] = [0]/[1]$. Далее, $[\pm 2]/[1] = [\pm 2][2]/[1][2] = [\mp 1][2]/[1][2] = [\mp 1]/[1]$. Наконец, $[3]/[1] = [3][2]/[1][2] = = [0]/[2] = [0]/[1]$. Тем самым, KS^{-1} исчерпывается дробями $[0]/[1]$, $[1]/[1]$ и $[-1]/[1]$.

Упражнение 3.1. Убедитесь, что эти три дроби различны.

Лемма 3.1
$a/s = b/t$ в KS^{-1} если и только если $atu = bsu$ в K для некоторого $u \in S$.

Доказательство. Положим $(a, s) \approx (b, t)$, если $atu = bsu$ для некоторого $u \in S$. Двухшаговая цепочка отождествлений $(a, s) \sim_S (atu, stu) = (bsu, tsu) \sim_S (b, t)$ показывает, что отношение $\approx$ содержится в отношении $\sim_S$. Остаётся проверить, что отношение $\approx$ является отношением эквивалентности — тогда оно совпадёт с $\sim_S$ в силу минимальности последнего. Рефлексивность и симметричность очевидны. Докажем транзитивность. Пусть $(a, s) \approx (b, t)$ и $(b, t) \approx (c, r)$, т. е. существуют такие $u, w \in S$, что $atu = bsu$ и $brw = ctw$. Тогда

$$ar(tuw) = (atu)rw = (bsu)rw = (brw)su = (ctw)su = cs(tuw)\,,$$

т. е. $(a, s) \approx (c, r)$. □

Лемма 3.2
Операции $\frac{a}{r} + \frac{b}{s} \stackrel{\text{def}}{=} \frac{as+br}{rs}$ и $\frac{a}{r} \cdot \frac{b}{s} \stackrel{\text{def}}{=} \frac{ab}{rs}$ корректно задают на KS^{-1} структуру коммутативного кольца с единицей $1/1$ и нулём $0/1$.

[1] См. прим. 0.5 на стр. 12 и прим. 1.2 на стр. 22.

[2] Мы по определению полагаем $q^0 = 1$.

[3] Т. е. наименьшее по включению отношение эквивалентности $R \subset (K \times S) \times (K \times S)$, содержащее все пары вида $\big((a, s), (at, st)\big)$, где $t \in S$, см. n° 0.4.1 на стр. 12.

Доказательство. Так как каждое отождествление $\sim_S$ является цепочкой элементарных отождествлений $(a,r) \sim_S (au,ru)$, где $u \in S$, достаточно проверить, что результаты операций не меняются при замене $\frac{a}{r}$ на $\frac{au}{ru}$, а $\frac{b}{s}$ — на $\frac{bw}{sw}$, где $u,w \in S$, что очевидно:

$$\frac{au}{ru} + \frac{bw}{sw} = \frac{ausw + bwru}{rusw} = \frac{(as+br)\cdot wu}{rs\cdot wu} = \frac{as+br}{rs}$$
$$\frac{au}{ru}\cdot\frac{bw}{sw} = \frac{aubw}{rusw} = \frac{(ab)\cdot wu}{rs\cdot wu} = \frac{ab}{rs}.$$

Проверку выполнения в KS^{-1} всех аксиом коммутативного кольца с единицей мы оставляем читателю в качестве упражнения. □

Следствие 3.1
Кольцо KS^{-1} нулевое если и только если S содержит нуль.

Доказательство. Если $0 \in S$, то любая дробь $a/s = (a\cdot 0)/(s\cdot 0) = 0/0 = (0\cdot 0)/(1\cdot 0) = 0/1$ эквивалентна нулю. С другой стороны, $1/1 = 0/1$ только если существует такой $s \in S$, что $1\cdot 1\cdot s = 0\cdot 1\cdot s = 0$, откуда $s = 0 \in S$. □

Теорема 3.1
Отображение $\iota_S\colon K \to KS^{-1}$, переводящее $a \in K$ в дробь $a/1 \in KS^{-1}$, является гомоморфизмом колец с ядром $\ker \iota_S = \{a \in K \mid \exists\, s \in S\colon as = 0\}$. Образ $\iota_S(s)$ любого элемента $s \in S$ обратим в KS^{-1}. Для любого гомоморфизма $\varphi\colon K \to R$ в целостное кольцо R, переводящего каждый элемент из S в обратимый элемент из R, существует единственный такой гомоморфизм колец $\varphi_S\colon KS^{-1} \to R$, что $\varphi = \varphi_S \circ \iota_S$.

Доказательство. Очевидно, что ι_S является гомоморфизмом. Дробь $\iota_S(a) = a/1$ равна $0/1$ если и только если найдётся такой $s \in S$, что $a\cdot 1\cdot s = 0\cdot 1\cdot s = 0$. Обратным к $\iota_S(s) = s/1$ элементом является дробь $1/s$. Остаётся доказать последнее утверждение. Для продолжения гомоморфизма $\varphi\colon K \to R$ до гомоморфизма $\varphi_S\colon KS^{-1} \to R$ нет иного выбора как положить $\varphi_S(1/s) = 1/\varphi(s)$, так как в кольце R должны выполняться равенства $\varphi_S(1/s)\cdot\varphi_S(s) = \varphi_S\bigl(s\cdot(1/s)\bigr) = \varphi(1) = 1$. Следовательно, искомое продолжение обязано задаваться формулой $\varphi_S(a/s) \stackrel{\text{def}}{=} \varphi(a)/\varphi(s)$. Она корректна, поскольку при замене $\frac{a}{s}$ на $\frac{au}{su}$ с $u \in S$ имеем $\varphi_S\left(\frac{au}{su}\right) = \frac{\varphi(au)}{\varphi(su)} = \frac{\varphi(a)\varphi(u)}{\varphi(s)\varphi(u)} = \frac{\varphi(a)}{\varphi(s)}$. Бесхитростную проверку того, что построенное отображение φ_S перестановочно со сложением и умножением, мы оставляем читателю. □

Упражнение 3.2. Пусть $K = \mathbb{Z}/(30)$, а $S = \{[2^k]_{30} \mid k = 0,\dots,4\}$. Покажите, что $KS^{-1} \simeq \mathbb{Z}/(15)$.

Пример 3.2 (поле частных целостного кольца)
Если кольцо K не имеет делителей нуля, его ненулевые элементы образуют мультипликативную систему. Кольцо частных со знаменателями в этой системе является полем. Оно называется *полем частных* целостного кольца K и обозначается Q_K. Равенство $a/b = c/d$ в Q_K равносильно равенству $ac = bd$ в K, а гомоморфизм $\iota\colon K \hookrightarrow Q_K$, $a \mapsto a/1$, инъективен, и любой гомоморфизм $\varphi\colon K \to R$ в целостное кольцо R, переводящий все ненулевые элементы из K в обратимые элементы кольца R, единственным способом продолжается до вложения поля частных $\widetilde{\varphi}\colon Q_K \hookrightarrow R$.

Пример 3.3 (поле $\mathbb{Q}$)
Полем частных целостного кольца $\mathbb{Z}$ является поле рациональных чисел $\mathbb{Q} = Q_{\mathbb{Z}}$, которое канонически вкладывается в любое поле характеристики нуль в качестве простого подполя[1].

[1] См. n° 1.5.6 на стр. 33.

Пример 3.4 (поле рядов Лорана)
Поле частных кольца формальных степенных рядов $\Bbbk[\![x]\!]$ с коэффициентами в произвольном поле $\Bbbk$ обозначается $\Bbbk(\!(x)\!) \stackrel{\text{def}}{=} Q_{\Bbbk[\![x]\!]}$. Так как любой ряд с ненулевым свободным членом обратим[1] в $\Bbbk[\![x]\!]$, каждая дробь $p(x)/q(x) \in \Bbbk(\!(x)\!)$ однозначно представляется в виде $x^m h(x)$, где $h \in \Bbbk[\![x]\!]$ имеет ненулевой свободный член, а показатель $m \in \mathbb{Z}$ равен разности показателей младших членов рядов p и q. Иначе говоря, поле $\Bbbk(\!(x)\!)$ состоит из формальных степенных рядов вида $f(x) = \sum_{k \geqslant m(f)} a_k x^k$, в которых допускается конечное число мономов отрицательной степени. Такие ряды называются *рядами Лорана*, а поле $\Bbbk(\!(x)\!)$ — *полем рядов Лорана*. Номер $m(f) \in \mathbb{Z}$ самого левого ненулевого коэффициента ряда Лорана f называется *порядком* ряда f.

3.2. Рациональные функции. Поле частных кольца $\Bbbk[x]$ обозначается через $\Bbbk(x)$ и называется *полем рациональных функций* от x. Его элементами являются дроби вида $p(x)/q(x)$ с $p, q \in \Bbbk[x]$.

Предложение 3.1
Если $g = g_1 \dots g_m$, где $g_i \in \Bbbk[x]$ и нод$(g_i, g_j) = 1$ при $i \neq j$, то при любом $f \in \Bbbk[x]$ дробь f/g единственным образом представляется в виде суммы

$$\frac{f}{g} = h + \frac{f_1}{g_1} + \dots + \frac{f_m}{g_m}, \tag{3-1}$$

где $h \in \Bbbk[x]$ и $\deg f_i < \deg g_i$ при всех i.

Доказательство. Деля f на g с остатком[2], заключаем, что $f/g = h + r/g$, где h — неполное частное, а остаток r имеет степень $\deg r < \deg g$. Если $g = g_1 g_2$ и нод$(g_1, g_2) = 1$, то $[g_2]_{g_1}$ обратим в $\Bbbk[x]/(g_1)$. Представим $[r]_{g_1} / [g_2]_{g_1} = [f_1]_{g_1}$ многочленом f_1 степени $\deg f_1 < \deg g_1$. Тогда $r = f_1 \cdot g_2 + f_2 \cdot g_1$ для некоторого $f_2 \in \Bbbk[x]$. Сравнивая степени, заключаем, что $\deg f_2 < \deg g_2$. Таким образом, $r/g = f_1/g_1 + f_2/g_2$ и к каждой из этих дробей применимо то же рассуждение, если её знаменатель является произведением взаимно простых многочленов. Это доказывает существование разложения (3-1). Для доказательства его единственности, умножим обе части разложения (3-1) на g. Получим равенство вида $f = hg + f_1 G_1 + \dots + f_m G_m$, где через $G_i = g/g_i$ обозначено произведение всех многочленов g_ν кроме i-го. Так как $\deg(f_1 G_1 + \dots + f_m G_m) < \deg g$, многочлен h является неполным частным, а $r = f_1 G_1 + \dots + f_m G_m$ — остатком от деления f на g. Каждый f_i является тем единственным многочленом степени $< \deg g_i$, класс которого в $\Bbbk[x]/(g_i)$ равен $[f]_{g_i} / [G_i]_{g_i}$. Таким образом, все ингредиенты формулы (3-1) однозначно определяются многочленами f и $g_1, \dots, g_n$. □

Предложение 3.2
Любую дробь вида f/g^m, в которой $\deg f < \deg g^m = m \deg g$, можно единственным образом представить в виде суммы

$$\frac{f}{g^m} = \frac{f_1}{g} + \frac{f_2}{g^2} + \dots + \frac{f_m}{g^m}, \tag{3-2}$$

где $\deg f_i < \deg g$ при всех i.

Доказательство. Представление (3-2) равносильно записи f в виде

$$f = f_1 g^{m-1} + f_2 g^{m-2} + \dots + f_{m-1} g + f_m, \tag{3-3}$$

[1] См. прим. 2.2 на стр. 38.
[2] См. n° 2.2 на стр. 40.

аналогичном записи целого числа f в g-ичной позиционной системе исчисления: f_m является остатком от деления f на g, f_{m-1} — остатком от деления частного $(f - f_m)/g$ на g, f_{m-2} — остатком от деления частного $\left(\frac{f-f_m}{g} - f_{m-1}\right)/g$ на g и т. д. □

3.2.1. Разложение на простейшие дроби. Из предыдущих двух предложений вытекает, что каждая дробь $f/g \in \Bbbk(x)$ допускает *единственное* представление в виде суммы неполного частного от деления f на g и дробей вида p/q^m, где q пробегает неприводимые делители знаменателя g, показатель m меняется от 1 до кратности вхождения q в разложение g на неприводимые множители, и в каждой из таких дробей $\deg p < \deg q$. Такое представление называется *разложением f/g на простейшие дроби* и бывает полезно в практических вычислениях с рациональными функциями.

Пример 3.5
Вычислим 2022-ю производную, а также первообразную[1] от $1/(1+x^2)$. Разложим эту дробь в поле $\mathbb{C}(x)$ на простейшие:

$$\frac{1}{1+x^2} = \frac{\alpha}{1+ix} + \frac{\beta}{1-ix}, \quad \text{где} \quad \alpha, \beta \in \mathbb{C}.$$

Подставляя $x = \pm i$ в равенство $1 = \alpha(1-ix) + \beta(1+ix)$, находим $\alpha = \beta = 1/2$, т. е.

$$\frac{1}{1+x^2} = \frac{1}{2}\left(\frac{1}{1+ix} + \frac{1}{1-ix}\right).$$

Теперь дифференцируем каждое слагаемое:

$$\left(\frac{d}{dx}\right)^{2022} \frac{1}{1+x^2} = \frac{2022!}{2}\left(\frac{(-i)^{2022}}{(1+ix)^{2023}} + \frac{i^{2022}}{(1-ix)^{2023}}\right) =$$
$$= -2022! \cdot \frac{1}{2}\frac{(1-ix)^{2023} + (1+ix)^{2023}}{(1+x^2)^{2023}} = 2022! \cdot \sum_{\nu=0}^{1011} \binom{2023}{2\nu} \cdot \frac{(-1)^{\nu+1} x^{2\nu}}{(1+x^2)^{2023}},$$

и интегрируем каждое слагаемое:

$$\int \frac{dx}{1+x^2} = \frac{1}{2}\int \frac{dx}{1+ix} + \frac{1}{2}\int \frac{dx}{1-ix} = \frac{\ln(1+ix) - \ln(1-ix)}{2i} = \frac{1}{2i}\ln\frac{1+ix}{1-ix} = \operatorname{arctg} x.$$

Подчеркнём, что все проделанные вычисления корректно определены в кольце $\mathbb{C}[\![x]\!]$, а все написанные равенства суть равенства между элементами этого кольца[2].

[1] Т. е. такой ряд f без свободного члена, что $f'(x) = 1/(1+x^2)$. Подробнее см. в n° 3.3 на стр. 60.

[2] В частности, последнее равенство вытекает из определения тангенса:

$$\operatorname{tg} t \stackrel{\text{def}}{=} \frac{\sin t}{\cos t} = \frac{1}{i} \cdot \frac{e^{it} - e^{-it}}{e^{it} + e^{-it}} = \frac{1}{i} \cdot \frac{e^{2it} - 1}{e^{2it} + 1} \in \mathbb{C}[\![t]\!].$$

Полагая $\operatorname{tg} t = x$, получаем $e^{2it} = \frac{1+ix}{1-ix}$. Про экспоненту и логарифм мы ещё подробно поговорим в n° 3.3 на стр. 60 ниже.

3.2.2. Разложение рациональной функции в степенной ряд. По теор. 3.1 на стр. 55 существует единственное вложение $\Bbbk(x) \hookrightarrow \Bbbk((x))$, переводящее каждый многочлен в себя. Иначе говоря, каждую рациональную функцию можно разложить в ряд Лорана. Если основное поле $\Bbbk$ алгебраически замкнуто[1], такое разложение описывается довольно явными формулами. Пусть $\deg f < \deg g$ и знаменатель дроби f/g имеет вид:

$$g(x) = 1 + a_1 x + a_2 x^2 + \ldots + a_n x^n = \prod (1 - \alpha_i x)^{m_i}, \tag{3-4}$$

где все числа $\alpha_i \in \Bbbk$ попарно различны.

Упражнение 3.3. Убедитесь, что числа α_i из разложения (3-4) суть корни многочлена

$$t^n + a_1 t^{n-1} + \ldots + a_{n-1} t + a_n = \prod (t - \alpha_i)^{m_i}.$$

По предл. 3.1 и предл. 3.2 функция f/g является суммой простейших дробей

$$\frac{\beta_{ij}}{(1 - \alpha_i x)^{k_{ij}}}, \tag{3-5}$$

где при каждом i показатели k_{ij} лежат в пределах $1 \leqslant k_{ij} \leqslant m_i$, а $\beta_{ij} \in \Bbbk$.

Если все кратности $m_i = 1$, то разложение на простейшие дроби имеет вид

$$\frac{f(x)}{(1 - \alpha_1 x) \ldots (1 - \alpha_n x)} = \frac{\beta_1}{1 - \alpha_1 x} + \ldots + \frac{\beta_n}{1 - \alpha_n x}.$$

Чтобы найти β_i, умножим обе части на общий знаменатель и подставим $x = \alpha_i^{-1}$. Получим

$$\beta_i = \frac{f\left(\alpha_i^{-1}\right)}{\prod_{\nu \neq i} \left(1 - (\alpha_\nu / \alpha_i)\right)} = \frac{\alpha_i^{n-1} f\left(\alpha_i^{-1}\right)}{\prod_{\nu \neq i} \left(\alpha_i - \alpha_\nu\right)}. \tag{3-6}$$

Мы заключаем, что когда все $m_i = 1$, дробь f/g является суммой $n = \deg g$ геометрических прогрессий:

$$\frac{f(x)}{g(x)} = \sum \left(\beta_1 \alpha_1^k + \beta_2 \alpha_2^k + \ldots + \beta_n \alpha_n^k\right) \cdot x^k, \tag{3-7}$$

где β_i находятся по формулам (3-6).

Простейшая дробь (3-5) с показателем $k_{ij} = m > 1$ раскладывается в ряд при помощи формулы Ньютона для бинома с отрицательным показателем

$$\frac{1}{(1 - x)^m} = \sum_{k \geqslant 0} \frac{(k + m - 1) \ldots (k + 2)(k + 1)}{(m - 1)!} \cdot x^k = \sum_{k \geqslant 0} \binom{k + m - 1}{m - 1} \cdot x^k, \tag{3-8}$$

которая получается $(m-1)$-кратным дифференцированием обеих частей разложения геометрической прогрессии $(1 - x)^{-1} = 1 + x + x^2 + x^3 + \ldots$.

Упражнение 3.4. Убедитесь, что $\left(\frac{d}{dx}\right)^n (1 - x)^{-1} = n! / (1 - x)^{n+1}$.

Таким образом, разложение простейшей дроби (3-5) имеет вид

$$\frac{\beta}{(1 - \alpha_i x)^m} = \beta \sum_{k \geqslant 0} \alpha_i^k \binom{k + m - 1}{m - 1} \cdot x^k. \tag{3-9}$$

[1] Т. е. каждый многочлен из $\Bbbk[x]$ полностью раскладывается в $\Bbbk[x]$ на линейные множители.

3.2.3. Решение линейных рекуррентных уравнений. Предыдущие вычисления можно использовать для отыскания «формулы k-того члена» последовательности z_k, заданной *линейным рекуррентным уравнением n-того порядка*:

$$z_k + a_1 z_{k-1} + a_2 z_{k-2} + \ldots + a_n z_{k-n} = 0\,, \tag{3-10}$$

где коэффициенты $a_1, \ldots, a_n \in \mathbb{C}$ — заданные числа. При $k \geqslant n$ уравнению (3-10) удовлетворяют коэффициенты z_k любого степенного ряда вида

$$z_0 + z_1 x + z_2 x^2 + \ldots = \frac{b_0 + b_1 x + \ldots + b_{n-1} x^{n-1}}{1 + a_1 x + a_2 x^2 + \ldots + a_n x^k}\,.$$

Если в числителе правой части подобрать коэффициенты $b_0, b_1, \ldots, b_{n-1} \in \mathbb{C}$ так, чтобы первые n коэффициентов $z_0, \ldots, z_{n-1}$ разложения полученной дроби в степенной ряд совпали с первыми n членами последовательности (3-10), то формулы (3-6) и (3-9) дадут явные выражения элементов последовательности z_k через k.

Пример 3.6 (числа Фибоначчи)
Найдём явное выражение через k для элементов последовательности z_k, в которой

$$z_0 = 0\,,\ z_1 = 1 \text{ и } z_k = z_{k-1} + z_{k-2} \text{ при } k \geqslant 2\,.$$

Рекуррентное уравнение $z_k - z_{k-1} - z_{k-2} = 0$ описывает коэффициенты ряда

$$x + z_2 x^2 + z_3 x^3 + \ldots = \frac{b_0 + b_1 x}{1 - x - x^2}\,,$$

у которого $z_0 = 0$ и $z_1 = 1$. Умножая обе части на знаменатель и сравнивая коэффициенты при x^0 и x^1, заключаем, что $b_0 = 0$, а $b_1 = 1$. Таким образом,

$$z(x) = \frac{x}{1 - x - x^2} = \frac{\beta_+}{1 - \alpha_+ x} + \frac{\beta_-}{1 - \alpha_- x}\,,$$

где $\alpha_\pm = (1 \pm \sqrt{5})/2$ суть корни многочлена $t^2 - t - 1$, а $\beta_+ = -\beta_- = 1/(\alpha_+ - \alpha_-) = 1/\sqrt{5}$ по формуле (3-6). Разложение $z(x)$ в ряд имеет вид

$$\frac{x}{1 - x - x^2} = \frac{1}{\sqrt{5}}\left(\frac{1}{1 - \alpha_+ x} - \frac{1}{1 - \alpha_- x}\right) = \sum_{k \geqslant 0} \frac{\alpha_+^k - \alpha_-^k}{\sqrt{5}} \cdot x^k\,,$$

т. е.

$$z_k = \frac{(1 + \sqrt{5})^k - (1 - \sqrt{5})^k}{2^k \sqrt{5}}\,.$$

Предложение 3.3
Если последовательность чисел $z_k \in \mathbb{C}$ удовлетворяет при $k \geqslant n$ рекуррентному уравнению

$$z_k + a_1 z_{k-1} + a_2 z_{k-2} + \ldots + a_n z_{k-n} = 0 \tag{3-11}$$

с постоянными коэффициентами $a_i \in \mathbb{C}$, то $z_k = \alpha_1^k \varphi_1(k) + \ldots + \alpha_r^k \varphi_r(k)$, где $\alpha_1, \ldots, \alpha_r$ — это все различные корни многочлена[1]

$$t^n + a_1 t^{n-1} + \ldots + a_n\,, \tag{3-12}$$

а $\varphi_i(x) \in \mathbb{C}[x]$ и $\deg \varphi_i$ строго меньше кратности соответствующего корня α_i.

[1] Он называется *характеристическим многочленом* рекуррентного уравнения (3-10).

Доказательство. Ряд $\sum z_k x^k \in \mathbb{C}[\![x]\!]$, коэффициенты которого решают уравнение (3-11), является суммой дробей вида $\beta(1-\alpha x)^{-m}$, где α пробегает различные корни многочлена (3-12), показатель m лежит в пределах от 1 до кратности соответствующего корня α, и для каждой пары α, m комплексное число $\beta = \beta(\alpha, m)$ однозначно вычисляется по α, m и первым n коэффициентам последовательности z_k. Согласно формуле (3-9) коэффициент при x^k у разложения дроби $(1-\alpha x)^{-m}$ в степенной ряд имеет вид $\alpha^k \varphi(k)$, где $\varphi(k) = \binom{k+m-1}{m-1}$ является многочленом степени $m-1$ от k. □

3.3. Логарифм и экспонента. Всюду в этом разделе мы рассматриваем ряды с коэффициентами в поле $\Bbbk$ характеристики $\operatorname{char}\Bbbk = 0$. В этом случае для любого ряда $f(x) = a_0 + a_1 x + a_2 x^2 + \dots$ существует единственный ряд без свободного члена, производная от которого равна $f(x)$. Он называется *первообразной* или *интегралом* от f и обозначается

$$\int f(x)\,dx \stackrel{\text{def}}{=} a_0 x + \frac{a_1}{2}x^2 + \frac{a_2}{3}x^3 + \dots = \sum_{k\geqslant 1} \frac{a_{k-1}}{k}\,x^k\,. \tag{3-13}$$

Первообразный ряд от знакопеременной геометрической прогрессии называется *логарифмом* и обозначается

$$\ln(1+x) \stackrel{\text{def}}{=} \int \frac{dx}{1+x} = \int \left(1 - x + x^2 - x^3 + \dots\right) dx = \\ = x - \frac{x^2}{2} + \frac{x^3}{3} - \frac{x^4}{4} + \frac{x^5}{5} - \dots = \sum_{k\geqslant 1} \frac{(-1)^{k-1}}{k} x^k\,. \tag{3-14}$$

Единственный ряд со свободным членом 1, совпадающий со своей производной, называется *экспонентой* и обозначается

$$e^x \stackrel{\text{def}}{=} \sum_{k\geqslant 0} x^k/k! = 1 + x + \frac{x^2}{2} + \frac{x^3}{6} + \frac{x^4}{24} + \frac{x^5}{120} + \dots\,. \tag{3-15}$$

3.3.1. Логарифмирование и экспоненцирование. Обозначим через $N = (x) \subset \Bbbk[\![x]\!]$ аддитивную абелеву группу всех рядов без свободного члена, а через $U = 1+N \subset \Bbbk[\![x]\!]$ — мультипликативную абелеву группу всех рядов с единичным свободным членом. Подстановка в аргумент логарифма вместо $1+x$ произвольного ряда $u(x) \in U$ означает подстановку в логарифмический ряд (3-14) вместо переменной x ряда $u(x) - 1$ без свободного члена и тем самым является алгебраической операцией[1]. Мы получаем отображение *логарифмирования*

$$\ln :\ U \to N\,, \quad u \mapsto \ln u\,. \tag{3-16}$$

Упражнение 3.5. Убедитесь, что $\frac{d}{dx}\ln u = u'/u$ и $\ln(1/u) = -\ln u$ для всех $u \in U$.

Подстановка в экспоненту (3-15) вместо x любого ряда $\tau(x) \in N$ даёт ряд $e^{\tau(x)}$ со свободным членом 1. Мы получаем *экспоненциальное отображение*

$$\exp :\ N \to U\,, \quad \tau \mapsto e^{\tau}\,. \tag{3-17}$$

Лемма 3.3
Для рядов $u, w \in U$ равенства $u = w$, $u' = w'$, $\ln(u) = \ln(w)$ и $u'/u = w'/w$ попарно эквивалентны друг другу.

[1] См. n° 2.1.1 на стр. 37.

Доказательство. Первое равенство влечёт за собой все остальные. Поскольку ряды с равными свободными членами совпадают если и только если совпадают их производные, первые два равенства и последние два равенства равносильны друг другу. Остаётся показать, что из последнего равенства следует первое. Но последнее равенство утверждает, что $u'/u - w'/w = (u'w - w'u)/uw = (w/u)\cdot(u/w)' = 0$ откуда $(u/w)' = 0$, т. е. $u/w = \mathrm{const} = 1$. □

Теорема 3.2
Экспоненциальное и логарифмическое отображения (3-17) и (3-16) являются взаимно обратными изоморфизмами абелевых групп, т. е. для любых рядов u, u_1, u_2 из U и τ, τ_1, τ_2 из N выполняются тождества $\ln e^{\tau} = \tau$, $e^{\ln u} = u$, $\ln(u_1u_2) = \ln(u_1) + \ln(u_2)$, $e^{\tau_1+\tau_2} = e^{\tau_1}e^{\tau_2}$.

Доказательство. Равенство $\ln e^{\tau} = \tau$ проверяется сравнением производных от обеих частей:

$$\left(\ln e^{\tau}\right)' = \frac{\left(e^{\tau}\right)'}{e^{\tau}} = \frac{e^{\tau}\tau'}{e^{\tau}} = \tau',$$

а равенство $e^{\ln u} = u$ — сравнением логарифмических производных:

$$\frac{\left(e^{\ln u}\right)'}{e^{\ln u}} = \frac{e^{\ln u}(\ln u)'}{e^{\ln u}} = \frac{u'}{u}.$$

Тем самым, экспоненцирование и логарифмирование являются взаимно обратными биекциями. Ряды $\ln(u_1u_2)$ и $\ln u_1 + \ln u_2$ совпадают, поскольку имеют нулевые свободные члены и равные производные:

$$\left(\ln(u_1u_2)\right)' = \frac{(u_1u_2)'}{u_1u_2} = \frac{u_1'u_2 + u_1u_2'}{u_1u_2} = \frac{u_1'}{u_1} + \frac{u_2'}{u_2} = \left(\ln u_1 + \ln u_2\right)'.$$

Поэтому логарифмирование — гомоморфизм, а значит, и обратное к нему экспоненцирование — тоже. □

Упражнение 3.6. Докажите в $\Bbbk[\![x, y]\!]$ равенство $e^{x+y} = e^x e^y$ непосредственным сравнением коэффициентов этих двух рядов.

3.3.2. Степенная функция и бином. В этом разделе мы продолжаем считать, что поле $\Bbbk$ имеет характеристику нуль. Для любого числа $\alpha \in \Bbbk$ 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 $\alpha \in \Bbbk$ получаем алгебраическую операцию *возведения в α-тую степень* $U \to U$, $u \mapsto u^{\alpha}$, обладающую всеми интуитивно ожидаемыми от степенной функции свойствами. В частности, для любых рядов $u, v \in U$ и чисел $\alpha, \beta \in \Bbbk$ выполняются равенства

$$u^{\alpha}\cdot u^{\beta} = e^{\alpha\ln u}e^{\beta\ln u} = e^{\alpha\ln u+\beta\ln u} = e^{(\alpha+\beta)\ln u} = u^{\alpha+\beta}$$
$$\left(u^{\alpha}\right)^{\beta} = e^{\beta\ln(u^{\alpha})} = e^{\beta\ln\left(e^{\alpha\ln u}\right)} = e^{\alpha\beta\ln u} = u^{\alpha\beta}$$
$$(uv)^{\alpha} = e^{\alpha\ln(uv)} = e^{\alpha(\ln u+\ln v)} = e^{\alpha\ln u+\alpha\ln v} = e^{\alpha\ln u}\cdot e^{\alpha\ln v} = u^{\alpha}v^{\alpha}.$$

Например, для любого ряда u с единичным свободным членом ряд $u^{1/n}$ представляет собою $\sqrt[n]{u}$ в том смысле, что $\left(u^{1/n}\right)^n = u$. Чтобы явно найти коэффициенты a_i биномиального ряда

$$(1+x)^{\alpha} = a_0 + a_1x + a_2x^2 + \ldots$$

рассмотрим его логарифмическую производную

$$\frac{\bigl((1+x)^\alpha\bigr)'}{(1+x)^\alpha} = \frac{d}{dx}\ln(1+x)^\alpha = \alpha\frac{d}{dx}\ln(1+x) = \frac{\alpha}{1+x}\,.$$

Умножая левую и правую части на $(1+x)^{\alpha+1}$, получаем равенство

$$\bigl(a_1 + 2a_2x + 3a_3x^2 + \ldots\bigr)\cdot(1+x) = \alpha\cdot(1 + a_1x + a_2x^2 + a_3x^3 + \ldots)\,.$$

Сравнивая коэффициенты при x^{k-1} в правой и левой части, приходим к рекуррентному соотношению $ka_k + (k-1)a_{k-1} = \alpha a_{k-1}$, из которого

$$a_k = \frac{\alpha-(k-1)}{k}\cdot a_{k-1} = \frac{(\alpha-(k-1))(\alpha-(k-2))}{k(k-1)}\cdot a_{k-2} = \ldots$$
$$\ldots = \frac{(\alpha-(k-1))(\alpha-(k-2))\cdots(\alpha-1)\alpha}{k!}\,.$$

Стоящая в правой части дробь имеет в числителе и 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

$$\binom{\alpha}{k} \stackrel{\text{def}}{=} \frac{\alpha(\alpha-1)\cdots(\alpha-k+1)}{k!} \tag{3-18}$$

Таким образом, для любого $\alpha\in\Bbbk$ справедлива *формула Ньютона*

$$(1+x)^\alpha = \sum_{k\geqslant 0}\binom{\alpha}{k}x^k = 1 + \alpha x + \frac{\alpha(\alpha-1)}{2}x^2 + \frac{\alpha(\alpha-1)(\alpha-2)}{6}x^3 + \ldots\,.$$

Пример 3.7 (бином с рациональным показателем)
Если $\alpha = n\in\mathbb{N}$, то при $k>n$ в числителе дроби (3-18) появится нулевой сомножитель. Поэтому разложение бинома в этом случае конечно и имеет вид

$$(1+x)^n = 1 + n\,x + \frac{n(n-1)}{2}\,x^2 + \ldots + x^n = \sum_{k=0}^{n}\binom{n}{k}\cdot x^k\,,$$

знакомый нам из форм. (0-8) на стр. 8. При $\alpha = -m$, где $m\in\mathbb{N}$, мы получаем разложение из форм. (3-8) на стр. 58

$$(1+x)^{-m} = 1 - m\,x + \frac{m(m+1)}{2}\,x^2 - \frac{m(m+1)(m+2)}{6}\,x^3 + \ldots = \sum_{k\geqslant 0}(-1)^k\binom{k+m-1}{k}\cdot x^k\,.$$

При $\alpha = 1/n$, где $n\in\mathbb{N}$, 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 $n = 2$ и $k \geqslant 1$ в качестве коэффициента при x^k получается дробь

$$(-1)^{k-1} \cdot \frac{1 \cdot 3 \cdot 5 \cdot \ldots \cdot (2k-3)}{2^k k!} = \frac{(-1)^{k-1}}{2k} \cdot \frac{1}{4^{k-1}} \cdot \binom{2k-2}{k-1},$$

т. е.

$$\sqrt{1+x} = 1 + \sum\nolimits_{k\geqslant 1} \frac{(-1)^{k-1}}{2k} \cdot \binom{2k-2}{k-1} \cdot \frac{x^k}{4^{k-1}}. \tag{3-19}$$

Пример 3.8 (числа Каталана)
Воспользуемся разложением (3-19) для получения явной формулы для *чисел Каталана*, часто возникающих в комбинаторных задачах. Вычислим произведение $n+1$ чисел

$$a_0 a_1 \ldots a_n, \tag{3-20}$$

делая за один шаг ровно одно из n умножений и заключая перемножаемые числа в скобки. В результате мы расставим n пар скобок в выражении (3-20). Количество различных расстановок скобок, возникающих таким образом, называется n-ым *числом Каталана* c_n. При $n = 1$ есть лишь одна расстановка скобок $(a_0 a_1)$, при $n = 2$ — две $(a_0(a_1 a_2))$ и $((a_0 a_1)a_2)$, при $n = 3$ — пять: $(a_0(a_1(a_2 a_3)))$, $(a_0((a_1 a_2)a_3))$, $((a_0 a_1)(a_2 a_3))$, $((a_0(a_1 a_2))a_3)$, $(((a_0 a_1)a_2)a_3)$. Множество всевозможных расстановок скобок в произведении (3-20) распадается в дизъюнктное объединение n подмножеств, в которых конфигурации наружных скобок имеют вид

$$(a_0(a_1 \ldots a_n)),\ ((a_0 a_1)(a_2 \ldots a_n)),\ \ldots,\ ((a_0 \ldots a_{n-2})(a_{n-1} a_n)),\ ((a_0 \ldots a_{n-1})a_n)$$

и которые состоят, соответственно, из c_{n-1}, $c_1 c_{n-2}$, $c_2 c_{n-3}$, …, $c_{n-2} c_1$, c_{n-1} элементов. Если дополнить последовательность чисел Каталана числом $c_0 \stackrel{\text{def}}{=} 1$, то получится соотношение

$$c_n = c_0 c_{n-1} + c_1 c_{n-2} + \ldots + c_{n-2} c_1 + c_{n-1} c_0,$$

означающее, что *ряд Каталана* $c(x) \stackrel{\text{def}}{=} \sum_{k\geqslant 0} c_k x^k = 1 + c_1 x + c_2 x^2 + \ldots \in \mathbb{Z}[\![x]\!]$ удовлетворяет уравнению $c(x)^2 = (c(x) - 1)/x$, т. е. является лежащим в кольце $\mathbb{Z}[\![x]\!]$ корнем квадратного трёхчлена $xt^2 - t - 1 = 0$ от переменной t. В поле рядов Лорана $\mathbb{Q}(\!(x)\!) \supset \mathbb{Z}[\![x]\!]$ корни находятся по стандартной школьной формуле $t = (1 \pm \sqrt{1-4x})/2x$. Так как $1 + \sqrt{1-4x}$ не делится на $2x$ в $\mathbb{Z}[\![x]\!]$, корень $(1 + \sqrt{1-4x})/(2x) \notin \mathbb{Z}[\![x]\!]$. Тем самым, $c(x) = (1 - \sqrt{1-4x})/(2x)$, откуда по формуле (3-19)

$$c_k = \frac{1}{k+1}\binom{2k}{k}.$$

Отметим, что даже не сразу понятно, что это число — целое.

3.4. Действие $\mathbb{Q}[[d/dt]]$ на $\mathbb{Q}[t]$. Рассмотрим кольцо формальных степенных рядов $\mathbb{Q}[\![x]\!]$ от переменной x и кольцо многочленов $\mathbb{Q}[t]$ от переменной t. Обозначим через

$$D = \frac{d}{dt} : \mathbb{Q}[t] \to \mathbb{Q}[t], \quad g \mapsto g',$$

оператор дифференцирования. Оператор D можно подставить вместо переменной x в любой степенной ряд $\Phi(x) = \sum_{k\geqslant 0} \varphi_k x^k \in \mathbb{Q}[\![x]\!]$. Результатом такой подстановки, по определению, является линейное отображение

$$\Phi(D) : \mathbb{Q}[t] \to \mathbb{Q}[t], \quad f \mapsto \sum_{k\geqslant 0} \varphi_k D^k f = \varphi_0 f + \varphi_1 f' + \varphi_2 f'' + \ldots. \tag{3-21}$$

Поскольку каждое дифференцирование уменьшает степень многочлена на единицу, все слагаемые в правой части (3-21) обратятся в нуль при $k > \deg f$. Таким образом, для каждого многочлена $f \in \mathbb{Q}[t]$, правая часть (3-21) является корректно определённым многочленом, каждый коэффициент которого вычисляется конечным числом действий с коэффициентами исходного многочлена f и первыми $\deg(f)$ коэффициентами ряда Φ. Линейность отображения (3-21) означает, что $\Phi(D)(\alpha f + \beta g) = \alpha\Phi(D)f + \beta\Phi(D)g$ для всех $\alpha, \beta \in \mathbb{Q}$ и $f, g \in \mathbb{Q}[t]$. Результатом подстановки оператора D в произведение рядов $\Phi(x)\Psi(x) \in \mathbb{Q}[\![x]\!]$ является *композиция* $\Phi(D) \circ \Psi(D) = \Psi(D) \circ \Phi(D)$ отображений $\Phi(D)$ и $\Psi(D)$.

Упражнение 3.7. Убедитесь в этом.

Таким образом, все отображения вида $\Phi(D)$ перестановочны друг с другом, и для биективности отображения $\Phi(D)$ необходимо и достаточно, чтобы степенной ряд $\Phi(x)$ был обратим[1] в кольце $\mathbb{Q}[\![x]\!]$. В силу линейности значение отображения $\Phi(D)$ на произвольном многочлене выражается через его значения $\Phi_m(t) \stackrel{\text{def}}{=} \Phi(D)t^m$ на базисных одночленах t^m:

$$\Phi(D)\left(a_0 + a_1 t + \ldots + a_n t^n\right) = a_0 + a_1\Phi_1(t) + \ldots + a_n\Phi_n(t)\,.$$

Многочлен $\Phi_m(t) \stackrel{\text{def}}{=} \Phi(D)t^m$ называется m-тым *многочленом Аппеля* ряда Φ. Его степень не превосходит m, а коэффициенты зависит лишь от первых $m+1$ коэффициентов ряда Φ.

Пример 3.9 (операторы сдвига)
Экспонента $e^D = 1 + D + D^2/2 + D^3/6 + \ldots$ имеет многочлены Аппеля

$$e^D t^m = \sum_{k\geqslant 0} \frac{1}{k!} D^k t^m = \sum_{k\geqslant 0} \frac{m(m-1)\ldots(m-k+1)}{k!}\, t^{m-k} = \sum_{k=0}^{m} \binom{m}{k} t^{m-k} = (t+1)^m\,.$$

Поэтому $e^D : f(t) \mapsto f(t+1)$ — это *оператор сдвига*. Так как ряды e^x и e^{-x} обратны друг другу в $\mathbb{Q}[\![x]\!]$, операторы e^D и e^{-D} тоже обратны друг другу, т. е. $e^{-D} : f(t) \mapsto f(t-1)$.

Упражнение 3.8. Убедитесь, что $e^{\alpha D} : f(t) \mapsto f(t+\alpha)$ при любом $\alpha \in \mathbb{Q}$.

Пример 3.10 (вычисление суммы степеней)
Для произвольно зафиксированного $m \in \mathbb{Z}_{\geqslant 0}$ рассмотрим сумму

$$S_m(n) \stackrel{\text{def}}{=} 0^m + 1^m + 2^m + 3^m + \ldots + n^m = \sum_{k=0}^{n} k^m \tag{3-22}$$

как функцию от n. При $m = 0, 1, 2, 3$ функции $S_m(n)$ достаточно известны:

$$\begin{aligned} S_0(n) &= 1 + \ldots + 1 = n \\ S_1(n) &= 1 + 2 + \ldots + n = n(n+1)/2 \\ S_2(n) &= 1^2 + 2^2 + \ldots + n^2 = n(n+1)(2n+1)/6 \\ S_3(n) &= 1^3 + 2^3 + \ldots + n^3 = n^2(n+1)^2/4 = S_1(n)^2\,. \end{aligned} \tag{3-23}$$

Чтобы получить для $S_m(t)$ явное выражение, применим к этой функции *разностный оператор*

$$\nabla : \varphi(t) \mapsto \varphi(t) - \varphi(t-1)\,.$$

[1] Т. е. имел ненулевой свободный член, см. прим. 2.2 на стр. 38.

Функция $\nabla S_m(t)$ принимает при всех $t \in \mathbb{Z}_{\geqslant 0}$ те же значения, что и многочлен t^m. Если существует такой многочлен $S_m(t) \in \mathbb{Q}[t]$, что $S_m(0) = 0$ и $\nabla S_m(t) = t^m$, то его значения в точках $t = 0,\ 1,\ 2,\ \ldots$ последовательно вычисляются, начиная с $S_m(0) = 0$, по формуле

$$S_m(n) = S_m(n-1) + \nabla S_m(n) = S_m(n-1) + n^m$$

и совпадают с суммами (3-22). Покажем, что уравнение $\nabla S_m(t) = t^m$ имеет в $\mathbb{Q}[t]$ единственное решение $S_m(t)$ с $S_m(0) = 0$. Согласно прим. 3.9 оператор $\nabla\colon\ \mathbb{Q}[t] \to \mathbb{Q}[t]$ имеет вид

$$\nabla = 1 - e^{-D} = \frac{1 - e^{-D}}{D} \circ D\,.$$

Ряд $(1 - e^{-x})/x$ имеет свободный член 1 и обратим в $\mathbb{Q}[\![x]\!]$. Обратный ему ряд

$$\mathrm{td}(x) \stackrel{\text{def}}{=} \frac{x}{1 - e^{-x}} \in \mathbb{Q}[\![x]\!]$$

называется *рядом Тодда*. Подставляя $x = D$ в равенство $\mathrm{td}(x) \cdot (1 - e^{-x}) = x$, получаем соотношение $\mathrm{td}(D) \circ \nabla = D$. Стало быть, $DS_m(t) = \mathrm{td}(D)\nabla S_m(t) = \mathrm{td}(D)t^m = \mathrm{td}_m(t)$ является многочленом Аппеля ряда Тодда, а искомый нами многочлен $S_m(t) = \int \mathrm{td}_m(t)\,dt$ получается из него интегрированием. Запишем ряд Тодда в «экспоненциальной форме»

$$\mathrm{td}(x) = \sum_{k \geqslant 0} \frac{a_k}{k!}\, x^k. \tag{3-24}$$

Сумма m-тых степеней первых t натуральных чисел равна

$$S_m(t) = \int \Bigl(\sum_{k=0}^{m} \frac{a_k}{k!} D^k t^m\Bigr)\,dt = \int \Bigl(\sum_{k=0}^{m} \binom{m}{k} a_k t^{m-k}\Bigr)\,dt = \sum_{k=0}^{m} \binom{m}{k} \frac{a_k t^{m-k+1}}{m-k+1} =$$
$$= \frac{1}{m+1}\left(\binom{m+1}{1} a_m t + \binom{m+1}{2} a_{m-1} t^2 + \ldots + \binom{m+1}{m} a_1 t^m + \binom{m+1}{m+1} a_0 t^{m+1}\right).$$

Эту формулу часто символически пишут в виде

$$(m+1) \cdot S_m(t) = (a^{\downarrow} + t)^{m+1} - a_{m+1}\,,$$

где стрелка у $a^{\downarrow}$ предписывает при раскрытии бинома $(a+t)^{m+1}$ заменять a^k на a_k. Коэффициенты a_k рекурсивно вычисляются из равенства $\mathrm{td}(x) \cdot (1 - e^{-x})/x = 1$, которое имеет вид

$$\Bigl(1 + a_1 x + \frac{a_2}{2} x^2 + \frac{a_3}{6} x^2 + \frac{a_4}{24}\, x^4 + \ldots\Bigr) \cdot \Bigl(1 - \frac{1}{2}\, x + \frac{1}{6}\, x^2 - \frac{1}{24}\, x^3 + \frac{1}{120}\, x^4 - \ldots\Bigr) = 1\,.$$

Упражнение 3.9. Найдите первую дюжину чисел a_k, проверьте формулы (3-23), дополните их явными формулами для $S_4(n)$ и $S_5(n)$ и вычислите[1] $S_{10}(1000)$.

[1] Яков Бернулли (1654–1705), пользуясь лишь пером и бумагой, сложил 10-е степени первой тысячи натуральных чисел примерно за 7 минут, о чём не без гордости написал в своём манускрипте «Ars Conjectandi», изданном в 1713 году уже после его кончины.

Замечание 3.1. (числа Бернулли) Название «ряд Тодда» вошло в обиход во второй половине XX века после работ Хирцебруха и Гротендика, где он использовался для формулировки и доказательства теоремы Римана – Роха. Во времена Бернулли и Эйлера предпочитали пользоваться рядом $\mathrm{td}(-x) = x/(e^x - 1)$, который отличается от $\mathrm{td}(x)$ ровно в одном члене, поскольку

$$\mathrm{td}(x) - \mathrm{td}(-x) = \frac{x}{1-e^{-x}} + \frac{x}{1-e^{x}} = x \cdot \frac{2 - e^x - e^{-x}}{(1-e^{-x})\cdot(1-e^x)} = x\,.$$

Тем самым, коэффициенты при x в $\mathrm{td}(x)$ и в $\mathrm{td}(-x)$ равны соответственно $1/2$ и $-1/2$, а все прочие коэффициенты при нечётных степенях x^{2k+1} с $k \geqslant 1$ в обоих рядах нулевые. Коэффициенты B_k в экспоненциальном представлении

$$\frac{x}{e^x - 1} = \sum_{k\geqslant 0} \frac{B_k}{k!}\, x^k$$

называются *числами Бернулли*. Таким образом, $B_k = a_k$ при $k \neq 1$ и обращаются в нуль при всех нечётных $k \geqslant 3$, а $B_1 = -a_1 = -1/2$. Со времён своего открытия числа Бернулли вызывают неослабевающий интерес. Им посвящена обширная литература[1] и специальный интернет-ресурс[2], на котором среди прочего есть программа для быстрого вычисления чисел B_k в виде несократимых рациональных дробей. Однако, не смотря на множество красивых теорем о числах Бернулли, про явную зависимость B_n от n известно немного, и любой содержательный новый взгляд в этом направлении был бы интересен.

Упражнение 3.10. Получите для чисел Бернулли рекурсивную формулу

$$(n+1)B_n = -\sum_{k=0}^{n-1} \binom{n+1}{k} \cdot B_k\,.$$

[1] Начать знакомство с которой я советую с гл. 15 книги *К. Айрлэнд, М. Роузен*. «Классическое введение в современную теорию чисел» и § 8 гл. V книги *З. И. Боревич, И Р. Шафаревич*. «Теория чисел».

[2] http://www.bernoulli.org/

§4. Идеалы, факторкольца и разложение на множители

4.1. Идеалы. Подкольцо I коммутативного кольца K называется *идеалом*, если вместе с каждым своим элементом оно содержит и все его кратные. В n° 1.5.3 мы видели, что этим свойством обладает ядро любого гомоморфизма колец. Множество всех элементов кольца, кратных фиксированному элементу $a \in K$, также является идеалом. Он обозначается

$$(a) = \{ka \mid k \in K\}, \tag{4-1}$$

и называется *главным* идеалом, порождённым a. Главные идеалы использовались нами при построении колец вычетов[1] $\mathbb{Z}/(n)$ и $\Bbbk[x]/(f)$, где они возникали как ядра гомоморфизмов факторизации $\mathbb{Z} \twoheadrightarrow \mathbb{Z}/(n)$, $m \mapsto [m]_n$, и $\Bbbk[x] \twoheadrightarrow \Bbbk[x]/(f)$, $g \mapsto [g]_f$, переводящих целое число (соотв. многочлен) в класс его вычета. Среди главных идеалов имеются *тривиальный* идеал (0), состоящий только из нулевого элемента, и *несобственный* идеал (1), совпадающий со всем кольцом. Идеалы, отличные от всего кольца, называются *собственными*.

Упражнение 4.1. Покажите, что следующие условия на идеал I в коммутативном кольце K с единицей эквивалентны: а) $I = K$ б) $1 \in I$ в) I содержит обратимый элемент.

Предложение 4.1
Коммутативное кольцо K с единицей тогда и только тогда является полем, когда в нём нет нетривиальных собственных идеалов.

Доказательство. Из упр. 4.1 вытекает, что в поле таких идеалов нет. Наоборот, если в кольце нет нетривиальных собственных идеалов, то главный идеал (b), состоящий из всех кратных произвольно взятого элемента $b \neq 0$, совпадает со всем кольцом. В частности, он содержит единицу, т. е. $1 = ab$ для некоторого a. Тем самым, любой ненулевой элемент b обратим. □

4.1.1. Нётеровость. Любое подмножество $M \subset K$ порождает идеал $(M) \subset K$, состоящий из всех элементов кольца K, представимых в виде $b_1a_1 + \ldots + b_ma_m$, где $a_1, \ldots, a_m$ — произвольные элементы множества M, а $b_1, \ldots, b_m$ — произвольные элементы кольца K, и число слагаемых $m \in \mathbb{N}$ также произвольно.

Упражнение 4.2. Убедитесь, что $(M) \subset K$ является идеалом и совпадает с пересечением всех идеалов, содержащих множество M.

Любой идеал $I \subset K$ имеет вид (M) для подходящего множества образующих $M \subseteq I$: например, всегда можно положить $M = I$. Идеалы $I = (a_1, \ldots, a_k) = \{b_1a_1 + \ldots + b_ka_k \mid b_i \in K\}$, допускающие конечное множество образующих, называются *конечно порождёнными*. Мы встречались с такими идеалами, когда доказывали существование наибольшего общего делителя в кольцах целых чисел и многочленов с коэффициентами в поле.

Лемма 4.1
Следующие свойства коммутативного кольца K попарно эквивалентны:

1) любое подмножество $M \subset K$ содержит конечный набор элементов $a_1, \ldots, a_k \in M$, порождающий тот же идеал, что и M

2) любой идеал $I \subset K$ конечно порождён

[1] См. n° 1.4 на стр. 28 и n° 2.3.1 на стр. 43.

3) любая бесконечная возрастающая цепочка вложенных идеалов $I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots$ в K стабилизируется в том смысле, что найдётся такое $n \in \mathbb{N}$, что $I_\nu = I_n$ для всех $\nu \geqslant n$.

Доказательство. Ясно, что (1) влечёт (2). Чтобы получить (3) из (2), заметим, что объединение $I = \bigcup I_\nu$ всех идеалов цепочки тоже является идеалом. Согласно (2), идеал I порождён конечным набором элементов. Все они принадлежат некоторому идеалу I_n. Тогда $I_n = I = I_\nu$ при $\nu \geqslant n$. Чтобы вывести (1) из (3), будем по индукции строить цепочку идеалов $I_n = (a_1, \ldots, a_n)$, начав с произвольного элемента $a_1 \in M$ и добавляя на k-том шагу очередную образующую $a_k \in M \setminus I_{k-1}$ до тех пор, пока это возможно, т. е. пока $M \not\subset I_k$. Так как $I_{k-1} \subsetneq I_k$, этот процесс не может продолжаться бесконечно, и на каком-то шагу мы получим идеал, содержащий всё множество M, а значит, совпадающий с (M). □

Определение 4.1
Кольцо K, удовлетворяющее условиям лем. 4.1, называется *нётеровым*. Отметим, что любое поле нётерово.

Теорема 4.1 (теорема Гильберта о базисе идеала)
Если кольцо K нётерово, то кольцо многочленов $K[x]$ также нётерово.

Доказательство. Рассмотрим произвольный идеал $I \subset K[x]$ и обозначим через $L_d \subset K$ множество старших коэффициентов всех многочленов степени не выше d из I, а через $L_\infty = \bigcup_d L_d$ — множество старших коэффициентов вообще всех многочленов из I.

Упражнение 4.3. Убедитесь, что все L_d (включая L_∞) являются идеалами в K.

Поскольку кольцо K нётерово, все идеалы L_d конечно порождены. Для каждого d (включая $d = \infty$) обозначим через $f_1^{(d)}, \ldots, f_{m_d}^{(d)} \in K[x]$ многочлены, старшие коэффициенты которых порождают соответствующий идеал $L_d \subset K$. Пусть наибольшая из степеней многочленов $f_i^{(\infty)}$, старшие коэффициенты которых порождают идеал L_∞, равна D. Покажем, что идеал I порождается многочленами $f_i^{(\infty)}$ и $f_j^{(d)}$ с $d < D$.

Каждый многочлен $g \in I$ сравним по модулю многочленов $f_1^{(\infty)}, \ldots, f_{m_\infty}^{(\infty)}$ с многочленом, степень которого строго меньше D. В самом деле, поскольку старший коэффициент многочлена g лежит в идеале L_∞, он имеет вид $\sum \lambda_i a_i$, где $\lambda_i \in K$, а a_i — старшие коэффициенты многочленов $f_i^{(\infty)}$. При $\deg g \geqslant D$ все разности $\delta_i = \deg g - \deg f_i^{(\infty)} \geqslant 0$, и можно образовать многочлен $h = g - \sum \lambda_i \cdot f_i^{(\infty)}(x) \cdot x_i^{\delta_i}$, сравнимый с g по модулю I и имеющий $\deg h < \deg g$. Заменяем g на h и повторяем процедуру, пока не получим многочлен $h \equiv g \pmod{(f_1^{(\infty)}, \ldots, f_{m_\infty}^{(\infty)})}$ с $\deg h < D$. Теперь старший коэффициент многочлена h лежит в идеале L_d с $d < D$, и мы можем строго уменьшать его степень, тем же способом сокращая старший член путём вычитания из h подходящих комбинаций многочленов $f_j^{(d)}$ с $0 \leqslant d < D$. □

Следствие 4.1
Если K нётерово, то кольцо многочленов $K[x_1, \ldots, x_n]$ также нётерово. □

Упражнение 4.4. Покажите, что кольцо формальных степенных рядов над нётеровым кольцом нётерово.

Следствие 4.2
Любая система полиномиальных уравнений с коэффициентами в нётеровом кольце эквивалентна некоторой конечной своей подсистеме.

Доказательство. Если кольцо K нётерово, то кольцо $K[x_1,\dots,x_n]$ тоже нётерово, и в любом множестве многочленов $M \subset K[x_1,\dots,x_n]$ можно указать такой конечный набор многочленов $f_1,\dots,f_m \in M$, что каждый многочлен $g \in M$ представляется в виде $g = h_1f_1 + \dots + h_mf_m$ для некоторых $h_i \in K[x_1,\dots,x_n]$. Поэтому любое уравнение вида $g(x_1,\dots,x_n) = 0$ с $g \in M$ является следствием m уравнений $f_1(x_1,\dots,x_n) = \dots = f_m(x_1,\dots,x_n) = 0$. □

4.1.2. Примеры ненётеровых колец. Кольцо многочленов от счётного множества переменных $\mathbb{Q}[x_1, x_2, x_3, \dots]$, элементы которого суть конечные линейные комбинации с рациональными коэффициентами всевозможных мономов вида $x_{\nu_1}^{m_1}x_{\nu_2}^{m_2}\dots x_{\nu_s}^{m_s}$ не является нётеровым: его идеал $(x_1, x_2, \dots)$, состоящий из всех многочленов без свободного члена, нельзя породить конечным множеством многочленов.

Упражнение 4.5. Докажите это и выясните, является ли конечно порождённым идеал, образованный в кольце бесконечно гладких функций $\mathbb{R} \to \mathbb{R}$ всеми функциями, которые обращаются в нуле в нуль вместе со всеми своими производными.

Предостережение 4.1. Подкольцо нётерова кольца может не быть нётеровым. Например, кольцо формальных степенных рядов $\mathbb{C}[\![z]\!]$ нётерово по упр. 4.4, тогда как его подкольцо образованное рядами, сходящимися всюду в $\mathbb{C}$, нётеровым не является.

Упражнение 4.6. Приведите пример бесконечной возрастающей цепочки строго вложенных идеалов в кольце сходящихся всюду в $\mathbb{C}$ степенных рядов из $\mathbb{C}[\![x]\!]$.

4.2. Фактор кольца. Пусть на коммутативном кольце K задано отношение эквивалентности, разбивающее K в дизъюнктное объединение классов эквивалентных элементов. Обозначим множество классов через X и рассмотрим сюръективное отображение факторизации

$$\pi : K \twoheadrightarrow X, \quad a \mapsto [a], \tag{4-2}$$

переводящее элемент $a \in K$ в его класс эквивалентности $[a] \subset K$, являющийся элементом множества X. Мы хотим задать на множестве X структуру коммутативного кольца, определив сложение и умножение теми же сами правилами

$$[a] + [b] = [a + b], \quad [a] \cdot [b] = [ab], \tag{4-3}$$

которые мы использовали в кольцах вычетов. Если эти правила корректны, то аксиомы коммутативного кольца в X будут автоматически выполнены, как и для колец вычетов, поскольку формулы (4-3) сводят их проверку к проверке аксиом коммутативного кольца в K. В частности, нулевым элементом кольца X будет класс $[0]$. С другой стороны, если формулы (4-3) корректны, то они утверждают, что отображение (4-2) является гомоморфизмом колец. Но если это так, то согласно n° 1.5.3 на стр. 31 класс нуля $[0] = \ker\pi$, служащий ядром этого гомоморфизма, является идеалом в K, а класс $[a] \subset K$ произвольного элемента $a \in K$, служащий прообразом точки $[a] \in X$ при гомоморфизме (4-2), является аддитивным сдвигом ядра на элемент a:

$$[a] = \pi^{-1}(\pi(a)) = a + \ker\pi = a + [0] = \{a + b \mid b \in [0]\}.$$

Оказывается, что этих необходимых условий на классы также и достаточно для того, чтобы правила (4-3) были корректны, т. е. для любого идеала $I \subset K$ множество классов

$$[a]_I = a + I \stackrel{\text{def}}{=} \{a + b \mid b \in I\} \tag{4-4}$$

образует разбиение кольца K, и правила (4-3) корректно определяют на классах этого разбиения структуру коммутативного кольца с нулевым элементом $[0]_I = I$.

Упражнение 4.7. 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, и проверьте, что формулы (4-3) корректны.

Определение 4.2
Классы эквивалентности (4-4) называются *классами вычетов* (или *смежными классами*) по модулю идеала I. Множество этих классов с операциями (4-3) называется *факторкольцом* кольца K по идеалу I и обозначается K/I. Эпиморфизм $K \twoheadrightarrow K/I$, $a \mapsto [a]_I$, сопоставляющий каждому элементу кольца его класс вычетов, называется *гомоморфизмом факторизации*.

Пример 4.1 (кольца вычетов)
Рассматривавшиеся выше кольца $\mathbb{Z}/(n)$ и $\Bbbk[x]/(f)$ суть факторы кольца целых числел и кольца многочленов по главным идеалам $(n) \subset \mathbb{Z}$ и $(f) \subset \Bbbk[x]$ соответственно.

Пример 4.2 (образ гомоморфизма)
Согласно n° 1.5.3, для любого гомоморфизма коммутативных колец $\varphi\colon A \to B$ имеется канонический изоморфизм колец $\overline{\varphi}\colon A/\ker\varphi \xrightarrow{\sim} \operatorname{im}\varphi$, $[a]_{\ker\varphi} \mapsto \varphi(a)$, переводящий каждый класс

$$[a]_{\ker\varphi} = a + \ker\varphi = \varphi^{-1}(\varphi(a))$$

в его образ $\varphi(a) = \varphi([a])$ при гомоморфизме φ.

Пример 4.3 (максимальные идеалы и гомоморфизмы вычисления)
Идеал $\mathfrak{m} \subset K$ называется *максимальным*, если факторкольцо $K/\mathfrak{m}$ является полем. Название связано с тем, что собственный[1] идеал $\mathfrak{m} \subset K$ максимален, если и только если он не содержится ни в каком строго большем собственном идеале, т. е. является максимальным элементом в чуме[2] собственных идеалов кольца K, частично упорядоченных по включению. В самом деле, обратимость всех ненулевых классов $[a]_{\mathfrak{m}}$ в факторкольце $K/\mathfrak{m}$ означает, что для любого $a \notin \mathfrak{m}$ найдутся такие $b \in K$, $m \in \mathfrak{m}$, что $ab + m = 1$ в K. Последнее равносильно тому, что идеал $(\mathfrak{m}, a) \supsetneq \mathfrak{m}$, порождённый $\mathfrak{m}$ и элементом $a \notin \mathfrak{m}$, содержит 1 и совпадает с K, т. е. что идеал $\mathfrak{m}$ не содержится ни в каком строго большем собственном идеале.

Из леммы Цорна[3] вытекает, что любой собственный идеал произвольного коммутативного кольца с единицей содержится в некотором максимальном идеале. В самом деле, множество всех собственных идеалов, содержащих произвольно заданный идеал $I \subset K$, тоже составляет чум по включению.

Упражнение 4.8. Убедитесь, что он полный, т. е. для любого линейно упорядоченного множества[4] M содержащих I собственных идеалов в K существует собственный идеал J^*, содержащий все идеалы из M.

[1] Т. е. отличный от всего кольца.
[2] См. n° 0.7 на стр. 16.
[3] См. сл. 0.1 на стр. 20.
[4] В данном случае это означает, что для любых $J_1, J_2 \in M$ выполняется включение $J_1 \subseteq J_2$ или включение $J_2 \subseteq J_1$.

По лемме Цорна существует такой собственный идеал $\mathfrak{m} \supset I$, который не содержится ни в каком большем собственном идеале, содержащем I. Такой идеал $\mathfrak{m}$ автоматически максимален по включению и в чуме всех собственных идеалов кольца K.

Максимальные идеалы возникают в кольцах функций как ядра *гомоморфизмов вычисления*. А именно, пусть X — произвольное множество, $p \in X$ — любая точка, $\Bbbk$ — любое поле, и K — какое-нибудь подкольцо в кольце всех функций $X \to \Bbbk$, содержащее тождественно единичную функцию 1 и вместе с каждой функцией $f \in K$ содержащее и все пропорциональные ей функции cf, $c \in \Bbbk$. Гомоморфизм вычисления $\mathrm{ev}_p : K \to \Bbbk$ переводит функцию $f \in K$ в её значение $f(p) \in \Bbbk$. Поскольку он сюръективен, его ядро $\ker \mathrm{ev}_p = \{f \in K \mid f(p) = 0\}$ является максимальным идеалом в K.

Упражнение 4.9. Убедитесь, что: а) каждый максимальный идеал кольца $\mathbb{C}[x]$ имеет вид $\ker \mathrm{ev}_p$ для некоторого $p \in \mathbb{C}$ б) в кольце непрерывных функций $[0,1] \to \mathbb{R}$ каждый максимальный идеал имеет вид $\ker \mathrm{ev}_p$ для некоторой точки $p \in [0,1]$. в) Укажите в кольце $\mathbb{R}[x]$ максимальный идеал, отличный от всех идеалов вида $\ker \mathrm{ev}_p$, где $p \in \mathbb{R}$.

Пример 4.4 (простые идеалы и гомоморфизмы в поля)
Идеал $\mathfrak{p} \subset K$ называется *простым*, если в факторкольце $K/\mathfrak{p}$ нет делителей нуля. Иначе говоря, идеал $\mathfrak{p} \subset K$ прост, если и только если из $ab \in \mathfrak{p}$ вытекает, что $a \in \mathfrak{p}$ или $b \in \mathfrak{p}$. Например, главные идеалы $(p) \subset \mathbb{Z}$ и $(q) \subset \Bbbk[x]$, где $\Bbbk$ — поле, просты тогда и только тогда, когда число p просто, а многочлен q неприводим.

Упражнение 4.10. Убедитесь в этом.

Согласно определениям, всякий максимальный идеал прост. Обратное неверно: скажем, главный идеал $(x) \subset \mathbb{Q}[x,y]$ прост, так как кольцо $\mathbb{Q}[x,y]/(x) \simeq \mathbb{Q}[y]$ целостное, но не максимален, поскольку строго содержится в идеале (x,y) многочленов без свободного члена[1]. Простые идеалы кольца K являются ядрами гомоморфизмов из кольца K во всевозможные поля. В самом деле, образ любого такого гомоморфизма, будучи подкольцом в поле, не имеет делителей нуля. Наоборот, факторкольцо $K/\mathfrak{p}$ по простому идеалу $\mathfrak{p} \subset K$ является подкольцом своего поля частных $Q_{K/\mathfrak{p}}$, и композиция факторизации и вложения $K \twoheadrightarrow K/\mathfrak{p} \hookrightarrow Q_{K/\mathfrak{p}}$ задаёт гомоморфизм из K в поле $Q_{K/\mathfrak{p}}$ с ядром $\mathfrak{p}$.

Упражнение 4.11. Убедитесь, что пересечение конечного множества идеалов содержится в простом идеале $\mathfrak{p}$ только если хотя бы один из пересекаемых идеалов содержится в $\mathfrak{p}$.

Пример 4.5 (конечно порождённые коммутативные алгебры)
Пусть K — произвольное коммутативное кольцо с единицей. Всякое кольцо вида

$$A = K[x_1, \dots, x_n]/I\,,$$

где $I \subset K[x_1, \dots, x_n]$ — произвольный идеал, называется *конечно порождённой K-алгеброй*[2]. Классы $a_i = [x_i]_I$ 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 $a_1, \dots, a_n$

[1] Т. е. в ядре гомоморфизма вычисления в нуле: $\mathrm{ev}_{(0,0)} : \mathbb{Q}[x,y] \twoheadrightarrow \mathbb{Q}$, $f(x,y) \mapsto f(0,0)$.

[2] Или, более торжественно, *конечно порождённой коммутативной алгеброй* над кольцом K.

при помощи операций сложения и умножения, производимых с учётом полиномиальных соотношений $f(a_1, \dots, a_n) = 0$ для всех f из I. Из сл. 4.1 и идущего следом упр. 4.12:

Упражнение 4.12. Покажите, что факторкольцо нётерова кольца тоже нётерово.

мы получаем

Следствие 4.3
Всякая конечно порождённая коммутативная алгебра над нётеровым коммутативным кольцом нётерова, и все соотношения между её образующими являются следствиями конечного числа соотношений. □

4.3. Области главных идеалов. Целостное кольцо с единицей называется *областью главных идеалов*, если каждый его идеал является главным. Наблюдавшийся нами в §§ 1, 2 параллелизм между кольцами $\mathbb{Z}$ и $\Bbbk[x]$, где $\Bbbk$ — поле, объясняется тем, что оба кольца являются областями главных идеалов. Мы фактически установили это при построении наибольших общих делителей[1]. Ключевым элементом наших рассуждений было *деление с остатком*.

Пример 4.6 (евклидовы кольца)
Целостное кольцо K с единицей называется *евклидовым*, если на нём имеется *функция высоты*

$$\nu : K \to \mathbb{Z}_{\geqslant 0} = \mathbb{N} \cup \{0\},$$

с двумя свойствами: (1) $\nu(a) = 0 \iff a = 0$; (2) для любых ненулевых $a, b \in K$ найдётся такое $q \in K$, что $\nu(a - bq) < \nu(b)$. Все такие q называются *неполными частными*, а соответствующие разности $r = a - bq$ — *остатками* от деления a на b относительно высоты ν. Подчеркнём, что никакой их единственности для заданных a, b не предполагается. В каждом ненулевом идеале I евклидова кольца K имеется ненулевой элемент $d \in I$ наименьшей в I высоты. Поскольку для любого $a \in I$ найдётся такое $q \in K$, что $\nu(a - dq) < \nu(d)$, и при этом $a - dq \in I$, мы заключаем, что $a - dq = 0$ и, тем самым, $I = (d)$. Поэтому каждое евклидово кольцо K является областью главных идеалов.

Упражнение 4.13. Докажите евклидовость колец: а) $\mathbb{Z}$ с $\nu(z) = |z|$
б) $\Bbbk[x]$, где $\Bbbk$ — поле, с $\nu(f) = \deg f + 1$ при $f \neq 0$ и $\nu(0) = 0$
в) $\mathbb{Z}[i] \stackrel{\text{def}}{=} \{\, a + bi \in \mathbb{C} \mid a, b \in \mathbb{Z},\ i^2 = -1 \}$ с $\nu(z) = |z|^2$
г) $\mathbb{Z}[\omega] \stackrel{\text{def}}{=} \{a + b\omega \in \mathbb{C} \mid a, b \in \mathbb{Z},\ \omega^2 + \omega + 1 = 0\}$ с $\nu(z) = |z|^2$.

Функцию высоты $\nu : K \to \mathbb{Z}_{\geqslant 0}$ на любом евклидовом кольце K всегда можно выбрать так, чтобы для всех ненулевых $a, b \in K$ выполнялось дополнительное свойство $\nu(ab) \geqslant \nu(a)$. Для этого, задавшись какой-нибудь высотой ν', для всех ненулевых $a \in K$ положим

$$\nu(a) = \min\nolimits_{x \in K \setminus 0} \nu'(ax).$$

Тогда по определению $\nu(ab) \geqslant \nu(a)$ для всех ненулевых $a, b \in K$ и $\nu(a) = 0$, если и только если $a = 0$. Убедимся, что ν обладает и вторым свойством евклидовой высоты. Пусть $\nu(b) = \nu'(bc)$ для ненулевого $c \in K$. Поскольку существует такое $q \in K$, что $\nu'(ac - bcq) < \nu'(bc)$, мы заключаем, что $\nu(a - bq) \leqslant \nu'\big((a - bq)c\big) < \nu'(bc) = \nu(b)$, как и требовалось. Высота ν со свойством $\nu(ab) \geqslant \nu(a)$ для всех ненулевых $a, b \in K$ называется *приведённой*.

Упражнение 4.14. Покажите, что в евклидовом кольце с приведённой высотой ν равенство $\nu(ab) = \nu(a)$ выполняется для ненулевых a, b, если и только если b обратим.

[1] См. n° 1.2.1 на стр. 24 и предл. 2.3 на стр. 41.

Существуют области главных идеалов, не являющиеся евклидовыми кольцами. Например, таковым является кольцо всех чисел вида $a + b\zeta \in \mathbb{C}$, где $a, b \in \mathbb{Z}$, а $\zeta = (1 + \sqrt{-19})/2$, однако содержательное обсуждение этого примера выходят за рамки понятий, которыми мы пока владеем. В прим. 4.7 на стр. 75 будет дана характеризация областей главных идеалов в терминах высот с немного более слабыми свойствами, чем у евклидовой высоты.

4.3.1. НОД и взаимная простота. В кольце главных идеалов K идеал

$$(a_1, \dots, a_n) = \{x_1a_1 + \dots + x_na_n \mid x_i \in K\},$$

порождённый любым набором элементов $a_1, \dots, a_n$, является главным и имеет вид (d) для некоторого $d \in K$. Таким образом, элемент d представляется в виде $d = a_1b_1 + \dots + a_nb_n$, где $b_i \in K$, делит все элементы a_i и делится на любой общий делитель элементов a_i, т. е. является *наибольшим общим делителем*[1] элементов $a_1, \dots, a_n$. Отметим, что наибольший общий делитель определён не однозначно, а с точностью до умножения на произвольный обратимый элемент из K.

Упражнение 4.15. Убедитесь, что в любом целостном коммутативном кольце K главные идеалы (a) и (b) совпадают, если и только если $a = sb$ для некоторого обратимого $s \in K$.

Поэтому всюду далее обозначение нод$(a_1, \dots, a_n)$ подразумевает целый класс элементов, получающихся друг из друга умножениями на обратимые константы, и все формулы, которые будут писаться, относятся к произвольно выбранному конкретному представителю этого класса[2]. В частности, равенство нод$(a_1, \dots, a_n) = 1$ означает, что у элементов a_i нет необратимых общих делителей. Так как в этом случае $1 = a_1b_1 + \dots + a_nb_n$ с $b_i \in K$, отсутствие необратимых общих делителей у элементов a_i в кольце главных идеалов равносильно их *взаимной простоте* в смысле опр. 1.2 на стр. 27.

Упражнение 4.16. Проверьте, что идеалы $(x, y) \subset \mathbb{Q}[x, y]$ и $(2, x) \in \mathbb{Z}[x]$ не являются главными.

4.4. Факториальность. Всюду в этом разделе мы по умолчанию обозначаем через K *целостное* кольцо. Ненулевые элементы $a, b \in K$ называются *ассоциированными*, если b делится на a, и a делится на b или, что то же самое, если $(a) = (b)$. Из упр. 4.15 выше вытекает, что a и b ассоциированы, если и только если они получаются друг из друга умножением на обратимый элемент кольца. Например, целые числа a и b ассоциированы в кольце $\mathbb{Z}$, если и только если $a = \pm b$, а многочлены $f(x)$ и $g(x)$ с коэффициентами из поля $\Bbbk$ ассоциированы в $\Bbbk[x]$, если и только если $f(x) = cg(x)$, где $c \in \Bbbk^*$ — ненулевая константа.

4.4.1. Неприводимые элементы. Ненулевой необратимый элемент q называется *неприводимым*, если из равенства $q = mn$ вытекает, что m или n обратим. Другими словами, неприводимость элемента q означает, что главный идеал (q) собственный и не содержится строго ни в каком другом собственном главном идеале, т. е. максимален в частично упорядоченном отношением включения множестве собственных главных идеалов. Неприводимыми элементами в кольце $\mathbb{Z}$ являются простые числа, а в кольце $\Bbbk[x]$, где $\Bbbk$ — поле, — неприводимые многочлены.

В кольце главных идеалов любые два неприводимых элемента p, q либо взаимно просты[3], либо ассоциированы, поскольку идеал $(p, q) = (d)$ для некоторого $d \in K$, и в виду максимальности (p) и (q) включения $(p) \subset (d)$ и $(q) \subset (d)$ влекут либо равенство $(d) = (K) = (1)$, либо равенство $(d) = (p) = (q)$. Обратите внимание, что в произвольном целостном кольце два

[1] См. зам. 1.3. на стр. 27.

[2] Что, конечно же, требует проверки корректности всех таких формул, которую мы, как правило, будем оставлять читателю в качестве упражнения.

[3] В смысле опр. 1.2 на стр. 27, т. е. существуют такие $x, y \in K$, что $px + qy = 1$.

неассоциированных неприводимых элемента могут и не быть взаимно простыми. Например, в $\mathbb{Q}[x, y]$ неприводимые многочлены x и y не взаимно просты и не ассоциированы.

Предложение 4.2
В кольце главных идеалов K следующие свойства ненулевого элемента $p \in K$ эквивалентны:

1) идеал (p) максимален, т. е. факторкольцо $K/(p)$ является полем

2) идеал (p) прост, т. е. в факторкольце $K/(p)$ нет делителей нуля

3) p неприводим, т. е. из равенства $p = ab$ вытекает, что a или b обратим в K.

Доказательство. Импликация (1) $\Rightarrow$ (2) очевидна и имеет место в любом коммутативном кольце с единицей. Импликация (2) $\Rightarrow$ (3) имеет место в любом целостном кольце K. Действительно, из $p = ab$ следует, что $[a][b] = 0$ в $K/(p)$, и так как в $K/(p)$ нет делителей нуля, один из сомножителей, скажем $[a]$, равен $[0]$. Тогда $a = ps = abs$ для некоторого $s \in K$, откуда $a(1 - bs) = 0$. Поскольку в K нет делителей нуля, $bs = 1$, т. е. b обратим.

Покажем теперь, что в кольце главных идеалов (3) $\Rightarrow$ (1). Так как каждый собственный идеал в K главный, максимальность идеала (p) в чуме собственных главных идеалов означает его максимальность в чуме всех собственных идеалов. В прим. 4.3 на стр. 70 мы видели, что это равносильно тому, что $K/(p)$ поле. □

Предложение 4.3
Каждый ненулевой необратимый элемент целостного нётерова кольца 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 $(a_1) \subsetneq (a_2) \subsetneq (a_3) \subsetneq \ldots$, что противоречит нётеровости. □

Определение 4.3
Целостное кольцо K называется *факториальным*, если каждый его необратимый ненулевой элемент является произведением конечного числа неприводимых, причём любые два таких разложения $p_1 p_2 \ldots p_m = q_1 q_2 \ldots q_k$ состоят из одинакового числа $k = m$ сомножителей, после надлежащей перенумерации которых можно указать такие обратимые элементы $s_\nu \in K$, что $q_\nu = p_\nu s_\nu$ при всех ν.

4.4.2. Простые элементы. Ненулевой элемент $p \in K$ называется *простым*, если порождённый им главный идеал $(p) \subset K$ прост, т. е. в факторкольце $K/(p)$ нет делителей нуля. Это означает, что для любых $a, b \in K$ произведение ab делится на p только если a или b делится на p. Каждый 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. Согласно предл. 4.2 в кольце главных идеалов верно и обратное: все неприводимые элементы кольца главных идеалов просты. Однако в произвольном целостном кольце могут быть неприводимые непростые

элементы. Например, в кольце $\mathbb{Z}[\sqrt{5}] = \mathbb{Z}[x]/(x^2-5)$ таковым является число 2, так как в факторе $\mathbb{Z}[\sqrt{5}]/(2) \simeq \mathbb{Z}[x]/(2, x^2-5) = \mathbb{Z}[x]/(2, x^2+1) \simeq \mathbb{F}_2[x]/(x^2+1) \simeq \mathbb{F}_2[x]/\big((x+1)^2\big)$ есть нильпотент — класс $[x+1] \in \mathbb{Z}[x]/(2, x^2+5)$. Среди прочего это означает, что квадрат $(1+\sqrt{5})^2 = 6+2\sqrt{5}$ делится в кольце $\mathbb{Z}[\sqrt{5}]$ на 2, хотя $1+\sqrt{5}$ не делится на 2, при том что 2 и $\sqrt{5}+1$ неприводимы и не ассоциированы друг с другом в кольце $\mathbb{Z}[\sqrt{5}]$.

Упражнение 4.17. Убедитесь в этом, и покажите, что $2 \cdot 2 = 4 = \big(\sqrt{5}+1\big) \cdot \big(\sqrt{5}-1\big)$ суть два *различных* разложения числа 4 на неприводимые множители в $\mathbb{Z}[\sqrt{5}]$.

Предложение 4.4
Целостное нётерово кольцо K факториально, если и только если все его неприводимые элементы просты.

Доказательство. Покажем сначала, что если K факториально, то любой неприводимый элемент $q \in K$ прост. Пусть произведение ab делится на q. Тогда разложение ab на неприводимые множители содержит множитель, ассоциированный с q, и в силу своей единственности является произведением разложений a и b на неприводимые множители. Поэтому q ассоциирован с одним из неприводимых делителей a или b, т. е. a или b делится на q. Наоборот, пусть все неприводимые элементы в K просты. Тогда по предл. 4.3 на стр. 74 каждый элемент кольца K является произведением конечного числа простых. Покажем, что в целостном кольце равенство $p_1 \dots p_k = q_1 \dots q_m$, в котором все сомножители просты, возможно только если $k = m$ и после надлежащей перенумерации каждый $p_i = s_i q_i$, где s_i обратим. Поскольку произведение $q_1 \dots q_m$ делится на p_1, один из его сомножителей делится на p_1. Будем считать, что это $q_1 = sp_1$. Так как q_1 неприводим, элемент s обратим. Пользуясь целостностью K, сокращаем обе части равенства $p_1 \dots p_k = q_1 \dots q_m$ на p_1 и получаем более короткое равенство $p_2 p_3 \dots p_k = (sq_2)q_3 \dots q_m$, к которому применимы те же рассуждения. □

Следствие 4.4
Всякое кольцо главных идеалов факториально. □

Пример 4.7 (характеризация областей главных идеалов, продолжение прим. 4.6 на стр. 72)
Покажем, что целостное кольцо K является областью главных идеалов, если и только если на K имеется функция высоты $\nu : K \to \mathbb{Z}_{\geqslant 0} = \mathbb{N} \cup \{0\}$ со следующими двумя свойствами:

1) $\nu(a) = 0 \iff a = 0$; 2) если $a \notin (b)$, то найдутся $x, y \in K$ с $0 < \nu(ax+by) < \nu(b)$.

Действительно, пусть такая высота существует. Тогда в каждом идеале $I \subset K$ есть ненулевой элемент $d \in I$, на котором ν принимает наименьшее в I ненулевое значение. Если $a \in I \smallsetminus (d)$, то найдутся $x, y \in K$ с $0 < \nu(ax+dy) < \nu(d)$, что невозможно, ибо $ax+dy \in I$. Тем самым $I = (d)$ и K является областью главных идеалов. Наоборот, пусть K — область главных идеалов. Выберем в каждом классе ассоциированных простых элементов какого-нибудь представителя p и для каждого $a \in K$ обозначим через $\nu_p(a)$ показатель, с которым p входит в разложение a на простые множители: $a = \prod_p p^{\nu_p(a)}$. Положим $\nu(a) = 2^{\sum_p \nu_p(a)}$. Так как $\nu_p(a) = 0$ для всех p кроме конечного числа, это определение корректно. Если $b \nmid a$, то нод$(a, b) = \prod_p p^{\min(\nu_p(a), \nu_p(b))}$ имеет положительную высоту, строго меньшую, чем $\nu(b)$, и представляется в виде $ax+by$, что и требуется. Более того, построенная высота ν *приведена* в том смысле[1], что $\nu(a) \leqslant \nu(ab)$ для всех a и всех ненулевых b, причём равенство равносильно обратимости b.

[1] Ср. с прим. 4.6 на стр. 72.

Пример 4.8 (гауссовы числа и суммы двух квадратов)
Элементы кольца $\mathbb{Z}[i] = \mathbb{Z}[x]/(x^2+1) \simeq \{x+iy \in \mathbb{C} \mid x,y \in \mathbb{Z}\}$ из упр. 4.13 (в) на стр. 72 называются *целыми гауссовыми числами*.

Упражнение 4.18. Убедитесь, что: а) в $\mathbb{Z}[i]$ обратимы только ± 1 и $\pm i$ б) $z \in \mathbb{Z}$ прост, если и только если прост $\overline{z}$.

Из упражнения вытекает, что разложение вещественного целого числа $n \in \mathbb{Z}$ на простые множители в области $\mathbb{Z}[i]$, будучи инвариантным относительно комплексного сопряжения, вместе с каждым невещественным неприводимым множителем содержит и его сопряжённый. Поэтому вещественное простое $p \in \mathbb{Z}$ становится приводимым в $\mathbb{Z}[i]$, если и только если оно имеет вид $p = (a+ib)(a-ib) = a^2+b^2$ с ненулевыми $a, b \in \mathbb{Z}$. С другой стороны, неприводимость $p \in \mathbb{Z}[i]$ означает, что факторкольцо $\mathbb{Z}[i]/(p) \simeq \mathbb{Z}[x]/(p, x^2+1) \simeq \mathbb{F}_p[x]/(x^2+1)$ является полем[1], что равносильно неприводимости многочлена x^2+1 над $\mathbb{F}_p$. Последнее равносильно тому, что -1 не является квадратом в $\mathbb{F}_p$, и имеет место если и только если[2] $p = 4k+3$. Мы заключаем, что неприводимость простого $p \in \mathbb{Z}$ в области $\mathbb{Z}[i]$ равносильна тому, что $p = 4k+3$, и тому, что p не представляется в виде суммы двух квадратов целых чисел.

Упражнение 4.19. Покажите, что произвольное $n \in \mathbb{N}$ является квадратом или суммой двух квадратов натуральных чисел, если и только если в его разложении на простые множители в кольце $\mathbb{Z}$ простые числа $p = 4k+3$ присутствуют только в чётных степенях.

4.4.3. НОД в факториальном кольце. В любом факториальном кольце K у любого конечного набора чисел $a_1, \ldots, a_m \in K$ имеется наибольший общий делитель[3]. Он имеет следующее явное описание. Зафиксируем в каждом классе ассоциированных простых элементов кольца K некоторый представитель p и для каждого $a \in K$ обозначим через $\nu_p(a) \in \mathbb{Z}_{\geqslant 0}$ показатель, с которым p входит в разложение a на простые множители[4], как в прим. 4.7 выше. Тогда, с точностью до умножения на обратимые элементы, $\text{нод}(a_1, \ldots, a_m) = \prod_p p^{\min_i \nu_p(a_i)}$.

Упражнение 4.20. Убедитесь, что правая часть делит каждое a_i и делится на любой общий делитель всех a_i.

Отметим, что если K не является областью главных идеалов, то $\text{нод}(a_1, \ldots, a_m)$ может не представляться в виде линейной комбинации элементов a_i с коэффициентами из K. Например, элементы x, y факториального кольца[5] $\mathbb{Q}[x,y]$ имеют $\text{нод}(x,y) = 1$, но нет таких $f, g \in \mathbb{Q}[x,y]$, что $fx+gy = 1$, ибо подставляя в это равенство $x = y = 0$, получим $0 = 1$.

4.5. Многочлены над факториальным кольцом. Пусть K — факториальное кольцо. Обозначим через Q_K его поле частных. Кольцо $K[x]$ является подкольцом в $Q_K[x]$. Назовём *содержанием* многочлена $f = a_0 + a_1 x + \ldots + a_n x^n \in K[x]$ наибольший общий делитель его коэффициентов:

$$\text{cont}(f) \stackrel{\text{def}}{=} \text{нод}(a_0, a_1, \ldots, a_n)\,.$$

Лемма 4.2
$\text{cont}(fg) = \text{cont}(f) \cdot \text{cont}(g)$ для любых $f, g \in K[x]$.

[1] См. предл. 4.2 на стр. 74.
[2] См. прим. 1.8 на стр. 31.
[3] В смысле зам. 1.3. на стр. 27, т. е. число, которое делит все a_i и делится на любой их общий делитель.
[4] Обратите внимание, что для каждого a показатель $\nu_p(a) \neq 0$ только для конечного множества простых чисел p.
[5] См. сл. 4.6 на стр. 78.

Доказательство. Достаточно для каждого простого $q \in K$ убедиться в том, что q делит все коэффициенты произведения fg, если и только если q делит все коэффициенты хотя бы одного из многочленов f, g. Для этого положим $R = K/(q)$ и применим к произведению fg гомоморфизм

$$K[x] \to R[x], \quad a_0 + a_1 x + \ldots + a_n x^n \mapsto [a_0]_q + [a_1]_q x + \ldots + [a_n]_q x^n,$$

заменяющий коэффициенты каждого многочлена их вычетами по модулю q.

Упражнение 4.21. Проверьте, что это и в самом деле гомоморфизм колец.

В силу простоты q кольцо R целостное. Поэтому $R[x]$ тоже целостное, и $[fg]_q = [f]_q[g]_q = 0$, если и только если $[f]_q = 0$ или $[g]_q = 0$. □

Лемма 4.3 (приведённое представление)
Каждый $f \in Q_K[x]$ представляется в виде $f(x) = (a/b) \cdot f_{\text{red}}(x)$, где $f_{\text{red}} \in K[x]$, $a, b \in K$ и $\text{cont}(f_{\text{red}}) = \text{нод}(a, b) = 1$, причём a, b и f_{red} определяются по f однозначно с точностью до умножения на обратимые элементы кольца K.

Доказательство. Вынесем из коэффициентов f их общий знаменатель, потом вынесем из всех коэффициентов полученного многочлена их наибольший общий делитель. В результате мы получим многочлен содержания 1, умноженный на число из Q_K, которое запишем несократимой дробью a/b. Докажем единственность такого представления. Если $(a/b) \cdot f_{\text{red}}(x) = (c/d) \cdot g_{\text{red}}(x)$ в $Q_K[x]$, то $ad \cdot f_{\text{red}}(x) = bc \cdot g_{\text{red}}(x)$ в $K[x]$. Сравнивая содержание обеих частей, заключаем, что $ad = bc$, откуда $f_{\text{red}}(x) = g_{\text{red}}(x)$. В виду отсутствия общих неприводимых множителей у a и b и у c и d, равенство $ad = bc$ возможно лишь когда a ассоциирован с c, а b — с d. □

Следствие 4.5 (лемма Гаусса)
Многочлен $f \in K[x]$ содержания 1 неприводим в $Q_K[x]$, если и только если он неприводим в $K[x]$.

Доказательство. Пусть $f(x) = g(x) \cdot h(x)$ в $Q_K[x]$. Записывая многочлены g и h в приведённом виде из лем. 4.3 и сокращая возникающую дробь, приходим к равенству

$$f(x) = \frac{a}{b} \cdot g_{\text{red}}(x) \cdot h_{\text{red}}(x), \tag{4-5}$$

в котором $g_{\text{red}}, h_{\text{red}} \in K[x]$ имеют содержание 1, и $\text{нод}(a, b) = 1$. По лем. 4.2

$$\text{cont}(g_{\text{red}} h_{\text{red}}) = \text{cont}(g_{\text{red}}) \cdot \text{cont}(h_{\text{red}}) = 1,$$

т. е. правая часть в (4-5) является приведённым представлением многочлена f. В силу единственности приведённого представления элементы a и b обратимы в K, а $f = g_{\text{red}} h_{\text{red}}$ с точностью до умножения на обратимую константу. □

Теорема 4.2
Кольцо многочленов над факториальным кольцом факториально.

Доказательство. Будучи кольцом главных идеалов, кольцо $Q_K[x]$ факториально, и каждый многочлен $f \in K[x] \subset Q_K[x]$ раскладывается в $Q_K[x]$ в произведение неприводимых множителей $f_\nu \in Q_K[x]$. Записывая их в приведённом виде из лем. 4.3 и сокращая возникающую при этом числовую дробь, получаем равенство $f = \frac{a}{b} \prod f_{\nu,\text{red}}$, в котором $a, b \in K$ имеют $\text{нод}(a, b) = 1$, а

все $f_{\nu,\mathrm{red}} \in K[x]$ неприводимы в $Q_K[x]$ и $\mathrm{cont}(f_{\nu,\mathrm{red}}) = 1$. Тогда $\mathrm{cont}\left(\prod f_{\nu,\mathrm{red}}\right) = 1$ по лем. 4.3, и правая часть равенства является приведённым представлением многочлена $f = \mathrm{cont}(f) \cdot f_{\mathrm{red}}$. В силу единственности приведённого представления $b = 1$ и $f = a \prod f_{\nu,\mathrm{red}}$ с точностью до умножения на обратимые константы из K. 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 $K[x]$

$$a_1 \dots a_k \cdot p_1 \dots p_s = b_1 \dots b_m \cdot q_1 \dots q_r\,,$$

где $a_\alpha, b_\beta \in K$ — неприводимые константы, а $p_\mu, q_\nu \in K[x]$ — неприводимые многочлены. Поскольку неприводимые многочлены имеют содержание 1, сравнивая содержание обеих частей, приходим к равенству $a_1 \dots a_k = b_1 \dots b_m$ в K. Так как K факториально, мы заключаем, что $k = m$ и после надлежащей перенумерации сомножителей $a_i = s_i b_i$, где все $s_i \in K$ обратимы. Следовательно, с точностью до умножения на обратимую константу из K, в кольце $K[x]$ выполняется равенство $p_1 \dots p_s = q_1 \dots q_r$. Так как все p_i и q_i неприводимы в факториальном кольце $Q_K[x]$, мы заключаем, что $r = s$ и после надлежащей перенумерации сомножителей $p_i = q_i$ с точностью до постоянных множителей из поля Q_K. Из единственности приведённого представления[1] вытекает, что эти постоянные множители являются обратимыми константами из кольца K. □

Следствие 4.6
Кольцо многочленов $K[x_1, \dots, x_n]$ над факториальным кольцом[2] K факториально. □

4.6. Разложение многочленов 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 4.22. Покажите, что несократимая дробь $p/q \in \mathbb{Q}$ является корнем многочлена $a_0 + a_1 x + \dots + a_n x^n \in \mathbb{Z}[x]$ только если $p \mid a_0$ и $q \mid a_n$.

Точное знание комплексных корней многочлена f тоже весьма полезно.

Упражнение 4.23. Разложите $x^4 + 4$ в произведение двух квадратных трёхчленов из $\mathbb{Z}[x]$.

После того, как эти простые соображения будут исчерпаны, следует подключать более трудоёмкие способы.

4.6.1. Редукция коэффициентов $\mathbb{Z}[x] \to \mathbb{Z}/(m)\,[x]$, $f \mapsto [f]_m$, где

$$[f]_m \stackrel{\text{def}}{=} [a_0]_m + [a_1]_m x + \dots [a_n]_m x^n \text{ для } f = a_0 + a_1 x + \dots + a_n x^n\,, \tag{4-6}$$

приводит коэффициенты всех многочленов по модулю m и является гомоморфизмом колец[3]. Поэтому равенство $f = gh$ в $\mathbb{Z}[x]$ влечёт за собой равенства $[f]_m = [g]_n \cdot [h]_m$ во всех кольцах $\big(\mathbb{Z}/(m)\big)[x]$, и из неприводимости многочлена $[f]_m$ хотя бы при одном m вытекает его неприводимость в $\mathbb{Z}[x]$. Если число $m = p$ простое, кольцо коэффициентов $\mathbb{Z}/(m) = \mathbb{F}_p$ является полем, и кольцо многочленов $\mathbb{F}_p[x]$ в этом случае факториально. При малых p разложение многочлена небольшой степени на неприводимые множители в $\mathbb{F}_p[x]$ можно осуществить простым перебором, и анализ такого разложения может дать существенную информацию о возможном разложении в $\mathbb{Z}[x]$.

[1] См. лем. 4.3 на стр. 77.
[2] В частности, над полем или над областью главных идеалов.
[3] Мы уже пользовались этим в доказательстве лем. 4.2 на стр. 76, см. упр. 4.21.

Пример 4.9
Покажем, что многочлен $f(x) = x^5 + x^2 + 1$ неприводим в кольце $\mathbb{Z}[x]$. Поскольку у f нет целых корней, нетривиальное разложение $f = gh$ в $\mathbb{Z}[x]$ возможно только с $\deg(g) = 2$ и $\deg(h) = 3$. Сделаем редукцию по модулю 2. 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. Тем самым, $[f]_2$ неприводим над $\mathbb{F}_2$, а значит, и над $\mathbb{Z}$.

Пример 4.10 (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. Покажем, что f неприводим в $\mathbb{Z}[x]$. В силу сделанных об f предположений при редукции по модулю p от f остаётся только старший моном $[f(x)]_p = x^n$. Если $f(x) = g(x)h(x)$ в $\mathbb{Z}[x]$, то в силу единственности разложения на простые множители в $\mathbb{F}_p[x]$ оба сомножителя g, h тоже редуцируются в некоторые степени переменной: $[g]_p = x^k$ и $[h]_p = x^m$. Это означает, что все коэффициенты многочленов g и h кроме старшего делятся на p. Тогда младший коэффициент многочлена f, будучи произведением младших коэффициентов многочленов g и h, должен делиться на p^2, что не так.

Пример 4.11 (неприводимость кругового многочлена Φ_p)
Покажем, что при простом $p \in \mathbb{N}$ круговой многочлен $\Phi_p(x) = x^{p-1} + \ldots + x + 1 = (x^p - 1)/(x - 1)$ неприводим в $\mathbb{Z}[x]$. Для этого перепишем его как многочлен от переменной $t = x - 1$:

$$f(t) = \Phi_p(t+1) = (t+1)^p - 1/t = t^{p-1} + \binom{p}{1} t^{p-2} + \ldots + \binom{p}{p-1}.$$

Поскольку при простом p все биномиальные коэффициенты $\binom{p}{k}$ с $1 \leqslant k \leqslant p-1$ делятся[1] на p, а свободный член $\binom{p}{p-1} = p$ не делится на p^2, многочлен $f(t)$ неприводим по критерию Эйзенштейна из прим. 4.10. Поэтому и $\Phi_p(x) = f(x-1)$ неприводим.

4.6.2. Алгоритм Кронекера позволяет путём довольно трудоёмкого, но вполне конечного вычисления либо явно разложить многочлен $f \in \mathbb{Z}[x]$ на множители в кольце $\mathbb{Z}[x]$, либо убедиться, что f неприводим в $\mathbb{Z}[x]$. Пусть $\deg f = 2n$ или $\deg f = 2n+1$. Тогда в любом нетривиальном разложении $f = gh$ степень одного из делителей, пусть это будет h, не превосходит n. Чтобы выяснить, делится ли f в $\mathbb{Z}[x]$ на какой-нибудь многочлен степени не выше n, подставим в f произвольные $n+1$ различных чисел $z_0, \ldots, z_n \in \mathbb{Z}$ и выпишем все возможные наборы чисел $d_0, \ldots, d_n \in \mathbb{Z}$, в которых каждое d_i делит соответствующее $f(z_i)$. Таких наборов имеется конечное число, и если искомый многочлен h существует, то набор его значений $h(z_0), \ldots, h(z_n)$ на числах z_i является одним из выписанных наборов $d_0, \ldots, d_n$. Для каждого такого набора в $\mathbb{Q}[x]$ есть ровно один многочлен h степени не выше n с $h(z_i) = d_i$ при всех i — это *интерполяционный многочлен Лагранжа*[2]

$$h(x) = \sum_{i=0}^{n} d_i \cdot \prod_{\nu \neq i} \frac{(x - z_\nu)}{(z_i - z_\nu)}. \tag{4-7}$$

[1] См. сл. 1.1 на стр. 30.
[2] См. прим. 2.5 на стр. 43.

Таким образом, делитель h многочлена f, если он существует, совпадает с одним из тех многочленов (4-7), что имеют целые коэффициенты. Остаётся явно разделить f на все такие многочлены и либо убедиться, что они не делят f, либо обнаружить среди них делитель f.

§5. Векторы и матрицы

5.1. Модули над коммутативными кольцами. Аддитивная абелева группа[1] V называется *модулем* над коммутативным кольцом K или *K-модулем*, если задана операция умножения

$$K \times V \to V\,, \quad (x, v) \mapsto x \cdot v = xv\,,$$

с теми же свойствами, что известное из курса геометрии умножение векторов на числа[2]:

$$\forall\, x, y \in K \quad \forall\, v \in V \quad x(yv) = (xy)v \tag{5-1}$$

$$\forall\, x, y \in K \quad \forall\, v \in V \quad (x + y)v = xv + yv \tag{5-2}$$

$$\forall\, x \in K \quad \forall\, u, w \in V \quad x(u + w) = xu + xw\,. \tag{5-3}$$

Если в кольце K есть единица и выполняется дополнительное свойство

$$\forall\, v \in V \quad 1v = v\,, \tag{5-4}$$

то модуль V называется *унитальным*.

Упражнение 5.1. Выведите из свойств (5-1) – (5-3), что в любом K-модуле V для всех $v \in V$ и $x \in K$ выполняются равенства $0 \cdot v = 0$ и $x \cdot 0 = 0$, а в унитальном модуле над коммутативным кольцом с единицей — равенство[3] $(-1) \cdot v = -v$.

Всюду далее мы предполагаем, что K является коммутативным кольцом с единицей и по умолчанию считаем все модули унитальными. Унитальные модули над полями — это в точности векторные пространства. По этой причине мы часто будем называть элементы K-модулей *векторами*, элементы кольца K — *скалярами*, а операцию $K \times V \to V$ — *умножением векторов на скаляры*. Часто бывает удобно записывать произведение вектора $v \in V$ на скаляр $x \in K$ не как xv, а как vx. Мы по определению считаем эти две записи эквивалентными обозначениями

$$vx \stackrel{\text{def}}{=} xv$$

для одного и того же вектора из V.

Упражнение 5.2. Убедитесь, что «правые» версии равенств (5-1) – (5-4) тоже выполняются:

$$(vy)x = v(yx)\,, \quad v(x + y) = vx + vy\,, \quad (u + w)x = ux + wx\,, \quad v\,1 = v\,.$$

Аддитивная абелева подгруппа $U \subseteq V$ в K-модуле V называется *K-подмодулем*, если она образует K-модуль относительно имеющейся в V операции умножения векторов на скаляры. Для этого необходимо и достаточно, чтобы $xu \in U$ для всех $x \in K$ и $u \in U$. Подмодули $U \subsetneq V$ называются *собственными*. Собственный подмодуль 0, состоящий из одного нуля, называется *тривиальным*.

---

[1] См. n° 1.1.2 на стр. 22.

[2] См. лекцию http://gorod.bogomolov-lab.ru/ps/stud/geom_ru/2122/lec_01.pdf. При этом в роли «векторов» выступают элементы модуля V, а в роли «чисел» — элементы кольца K.

[3] Слева стоит произведение вектора $v \in V$ на скаляр $-1 \in K$, а справа — противоположный к v вектор $-v \in V$.

Пример 5.1 (кольцо как модуль над собой)
Каждое коммутативное кольцо K является модулем над самим собой: сложение векторов и их умножение на скаляры суть сложение и умножение в K. Если в K имеется единица, K-модуль K является унитальным. K-подмодули $I \subset K$ — это в точности идеалы кольца K. В частности, коммутативное кольцо K с единицей является полем если и только если в K-модуле K нет нетривиальных собственных подмодулей[1].

Пример 5.2 (координатный модуль K^r)
Декартово произведение r экземпляров кольца K обозначается $K^r = K \times \ldots \times K$ и состоит из строк $a = (a_1, \ldots, a_r)$, в которых $a_i \in K$. Сложение таких строк и их умножение их на скаляры $x \in K$ происходит покоординатно: для $a = (a_1, \ldots, a_r)$, $b = (b_1, \ldots, b_r)$ и $x \in K$ мы полагаем

$$a + b \stackrel{\text{def}}{=} (a_1 + b_1, \ldots, a_r + b_r) \quad \text{и} \quad xa \stackrel{\text{def}}{=} (xa_1, \ldots, xa_r)\,.$$

Пример 5.3 (модуль матриц $\mathrm{Mat}_{m\times n}(K)$)
Таблицы из m строк и n столбцов, заполненные элементами кольца K, называются $m\times n$ *матрицами с элементами из* K. Множество всех таких матриц обозначается $\mathrm{Mat}_{m\times n}(K)$. Элемент матрицы A, расположенный в i-й строке и j-м столбце, обозначается a_{ij}. Запись $A = (a_{ij})$ означает, что матрица A состоит из таких элементов a_{ij}. Например, матрица $A \in \mathrm{Mat}_{3\times 4}(\mathbb{Z})$ с элементами $a_{ij} = i - j$ имеет вид

$$\begin{pmatrix} 0 & -1 & -2 & -3 \\ 1 & 0 & -1 & -2 \\ 2 & 1 & 0 & -1 \end{pmatrix}.$$

Так же как и координатные строки, $m\times n$ матрицы $\mathrm{Mat}_{m\times n}(K)$ образуют K-модуль относительно поэлементного сложения и умножения на скаляры: сумма $S = (s_{ij})$ матриц $A = (a_{ij})$ и $B = (b_{ij})$ имеет $s_{ij} = a_{ij} + b_{ij}$, а произведение $P = xA$ матрицы A на число $x \in K$ имеет $p_{ij} = xa_{ij}$.

Пример 5.4 (абелевы группы как $\mathbb{Z}$-модули)
Каждая аддитивно записываемая абелева группа A может рассматриваться как унитальный $\mathbb{Z}$-модуль, в котором сложение векторов есть сложение в A, а умножение векторов на числа $\pm n$, где $n \in \mathbb{N}$, задаётся правилом $(\pm n)\cdot a \stackrel{\text{def}}{=} \pm(a + \ldots + a)$, где в скобках стоит n слагаемых, равных a.

Упражнение 5.3. Удостоверьтесь, что эти операции удовлетворяют аксиомам (5-1) – (5-4).

5.1.1. Гомоморфизмы модулей. Отображение $\varphi : M \to N$ между K-модулями M и N называется *K-линейным* или *гомоморфизмом K-модулей*, если оно перестановочно со сложением векторов и умножением векторов на скаляры, т. е. для всех $x \in K$ и $u, w \in M$

$$\varphi(u + w) = \varphi(u) + \varphi(w) \quad \text{и} \quad \varphi(xu) = x\varphi(u)\,. \tag{5-5}$$

Упражнение 5.4. Убедитесь, что композиция K-линейных отображений тоже K-линейна.

Гомоморфизмы K-модулей образуют K-модуль относительно операций сложения значений и умножения их на скаляры: отображения $\varphi+\psi$ и $x\varphi$, где $x \in K$, переводят каждый вектор $w \in M$, соответственно, в $\varphi(w) + \psi(w)$ и в $x\varphi(w) = \varphi(xw)$.

Упражнение 5.5. Убедитесь, что для любого $x \in K$ и K-линейных отображений $\varphi, \psi : M \to N$ отображения $\varphi + \psi$ и $x\varphi$ тоже K-линейны.

[1] См. предл. 4.1 на стр. 67.

Модуль K-линейных отображений $M \to N$ называется *модулем гомоморфизмов* из M в N и обозначается $\operatorname{Hom}(M, N)$ или $\operatorname{Hom}_K(M, N)$, если надо явно указать кольцо, над которым рассматриваются модули.

Так как K-линейные отображения $\varphi : M \to N$ являются гомоморфизмами абелевых групп, все они обладают перечисленными в n° 1.5 на стр. 30 свойствами таких гомоморфизмов. В частности, $\varphi(0) = 0$ и $\varphi(-w) = -\varphi(w)$ для всех $w \in M$, а каждый непустой слой φ является аддитивным сдвигом ядра $\ker\varphi = \varphi^{-1}(0) = \{u \in M \mid \varphi(u) = 0\}$, т. е. $\varphi^{-1}(\varphi(w)) = w + \ker\varphi$ для всех $w \in M$. В частности, инъективность φ равносильна тому, что $\ker\varphi = 0$ состоит из одного нуля.

Упражнение 5.6. Убедитесь, что ядро и образ K-линейного гомоморфизма $\varphi : M \to N$ являются подмодулями в M и в N соответственно.

Биективные гомоморфизмы модулей называются *изоморфизмами*. K-линейное отображение $\varphi : M \to N$ является изоморфизмом если и только если $\ker\varphi = 0$ и $\operatorname{im}\varphi = N$. Например, выписывание элементов матрицы в строку в произвольном порядке задаёт изоморфизм между модулем матриц $\operatorname{Mat}_{m\times n}(K)$ из прим. 5.3 и координатным K-модулем K^{mn} из прим. 5.2.

Пример 5.5 (дифференцирование)
Кольцо многочленов $K[x]$ с коэффициентами в коммутативном кольце K можно рассматривать и как K-модуль. Оператор дифференцирования $D = \frac{d}{dx} : K[x] \to K[x]$, $f(x) \mapsto f'(x)$, является гомоморфизмом K-модулей, поскольку перестановочен со сложением многочленов и умножением многочленов на константы, но не является гомоморфизмом колец, так как не перестановочен с умножением многочленов друг на друга.

Предостережение 5.1. Именуемое в школе «линейной функцией» отображение $\varphi : K \to K$, задаваемое правилом $\varphi(x) = ax + b$, где $a, b \in K$ фиксированы, является K-линейным в смысле предыдущего определения только при $b = 0$. Если же $b \neq 0$, то φ не перестановочно ни со сложением, ни с умножением на числа.

5.1.2. Прямые произведения и прямые суммы. Из любого семейства K-модулей M_ν, занумерованных элементами ν произвольного множества $\mathcal{N}$, можно образовать прямое произведение $\prod_{\nu\in\mathcal{N}} M_\nu$, состоящее из всевозможных семейств $v = (v_\nu)_{\nu\in\mathcal{N}}$ векторов $v_\nu \in M_\nu$, занумерованных элементами $\nu \in \mathcal{N}$, как в n° 1.6 на стр. 34. Такие семейства можно поэлементно складывать и умножать на скаляры точно также, как мы это делали в n° 1.6 в прямых произведениях абелевых групп и коммутативных колец. А именно, сумма $v + w$ семейств $v = (v_\nu)_{\nu\in\mathcal{N}}$ и $w = (w_\nu)_{\nu\in\mathcal{N}}$ имеет ν-тым членом элемент $v_\nu + w_\nu$, а на ν-тым членом произведения xv семейства $v = (v_\nu)_{\nu\in\mathcal{N}}$ на скаляр $x \in K$ является элемент xv_ν. Модуль $\prod_{\nu\in\mathcal{N}} M_\nu$ называется *прямым произведением* модулей M_ν, а его подмодуль $\bigoplus_{\nu\in\mathcal{N}} M_\nu$, состоящий из всех семейств $v = (v_\nu)_{\nu\in\mathcal{N}}$ с конечным числом ненулевых векторов v_ν, называется *прямой суммой* модулей M_ν. Для конечных множеств $\mathcal{N}$ прямые суммы совпадают с прямыми произведениями. Так, координатный модуль K^r из прим. 5.2 и модуль матриц $\operatorname{Mat}_{m\times n}(K)$ из прим. 5.3 являются прямыми суммами (и произведениями), соответственно, r и mn одинаковых экземпляров K-модуля K.

Пример 5.6 (многочлены и степенные ряды)
Обозначим через Kt^n множество одночленов вида at^n, где $a \in K$, а t — переменная. Каждое множество Kt^n является K-модулем, изоморфным модулю K. Прямая сумма $\bigoplus_{n\geqslant 0} Kt^n$ изоморфна модулю многочленов $K[t]$, а прямое произведение $\prod_{n\geqslant 0} Kt^n$ — модулю формальных степенных рядов $K[\![t]\!]$.

Пример 5.7 (модуль функций со значениями в модуле)
Отображения $Z \to M$ из любого множества Z в произвольный K-модуль M можно складывать и умножать на числа из K по тем же правилам, что выше: для $\varphi, \psi : Z \to M$ и $x \in K$ отображения $\varphi + \psi$ и $x\varphi$ переводят $z \in Z$ в $\varphi(z) + \psi(z)$ и $x\varphi(z)$ соответственно. Эти операции задают на множестве M^Z всех отображений $Z \to M$ структуру K-модуля, изоморфного прямому произведению $\prod_{z\in Z} M_z$ одинаковых копий $M_z = M$ модуля M, занумерованных элементами $z \in Z$. Этот изоморфизм сопоставляет отображению $\varphi : Z \to M$ семейство его значений $\big(\varphi(z)\big)_{z\in Z} \in \prod_{z\in X} M_z$. Если Z является K-модулем, то K-линейные отображения $Z \to M$ составляют подмодуль $\mathrm{Hom}_K(Z, N) \subset M^Z$.

Предложение 5.1
Для любого семейства K-модулей M_μ, занумерованных элементами μ произвольного множества $\mathcal{M}$, и любого K-модуля N имеется изоморфизмом K-модулей

$$\prod\nolimits_{\mu\in\mathcal{M}} \mathrm{Hom}_K(M_\mu, N) \xrightarrow{\sim} \mathrm{Hom}_K\Big(\bigoplus\nolimits_{\mu\in\mathcal{M}} M_\mu,\ N\Big), \tag{5-6}$$

который переводит семейство K-линейных гомоморфизмов $\varphi_\mu : M_\mu \to N$ в гомоморфизм

$$\bigoplus \varphi_\mu : \bigoplus\nolimits_{\mu\in\mathcal{M}} M_\mu \to N, \tag{5-7}$$

отображающий каждое семейство векторов $(w_\mu)_{\mu\in\mathcal{M}}$ с конечным числом ненулевых членов в сумму $\sum_{\mu\in\mathcal{M}} \varphi_\mu(w_\mu)$ с конечным числом ненулевых слагаемых.

Доказательство. Отображение (5-6) очевидно является K-линейным гомоморфизмом. Обратное к (5-6) отображение переводит каждый K-линейный гомоморфизм $\psi : \bigoplus_{\mu\in\mathcal{M}} M_\mu \to N$ в семейство гомоморфизмов $\varphi_\mu : M_\mu \to N$, где для каждого $\nu \in \mathcal{M}$ гомоморфизм $\varphi_\nu = \psi\iota_\nu$ является композицией ψ с вложением $\iota_\nu : M_\nu \hookrightarrow \bigoplus_{\mu\in\mathcal{M}} M_\mu$, которое отправляет каждый вектор $u \in M_\nu$ в семейство $(w_\mu)_{\mu\in\mathcal{M}}$ с единственным ненулевым элементом $w_\nu = u$. □

Пример 5.8 (продолжение прим. 5.6 на стр. 83)
В прим. 5.6 мы видели, что модуль многочленов $K[t] \simeq \bigoplus_{n\geqslant 0} Kt^n$ можно воспринимать как прямую сумму модулей $Kt^n \simeq K$. Применительно к этому случаю предл. 5.1 утверждает, что каждое K-линейное отображение $\varphi : K[t] \to K$ однозначно задаётся последовательностью K-линейных отображений $\varphi_n = \varphi|_{Kt^n} : Kt^n \to K$ — ограничениями отображения φ на подмодули $Kt^n \subset K[t]$. Каждое из отображений φ_n в свою очередь однозначно задаётся своим значением на базисном мономе t^n, т. е. числом $f_n = \varphi_n(t^n) \in K$. Последовательность чисел f_n может быть любой, и отвечающее такой последовательности K-линейное отображение $\varphi : K[t] \to K$ переводит многочлен $a(t) = a_0 + a_1 t + \ldots + a_m t^m$ в число $\varphi(a) = f_0 a_0 + f_1 a_1 + \ldots + f_m a_m$. Мы заключаем, что модуль $\mathrm{Hom}_K(K[t], K)$ изоморфен прямому произведению счётного множества копий модуля K, т. е. модулю формальных степенных рядов $K[\![x]\!]$. Изоморфизм сопоставляет последовательности (f_n) её *производящую функцию* $F(x) = \sum_{n\geqslant 0} f_n x^n \in K[\![x]\!]$. Например, для любого $\alpha \in K$ *гомоморфизм вычисления* $\mathrm{ev}_\alpha : K[t] \to K$, $f \mapsto f(\alpha)$, переводящий многочлены в их значения в точке $\alpha \in K$ и действующий на базисные мономы по правилу $t^n \mapsto \alpha^n$, имеет $f_n = \alpha^n$ и задаётся рядом $\sum_{n\geqslant 0} \alpha^n x^n = (1 - \alpha x)^{-1} \in K[\![x]\!]$.

Упражнение 5.7. В условиях предл. 5.1 постройте изоморфизм K-модулей

$$\bigoplus\nolimits_{\mu\in\mathcal{M}} \mathrm{Hom}_K(N, M_\mu) \xrightarrow{\sim} \mathrm{Hom}_K\Big(N, \bigoplus\nolimits_{\mu\in\mathcal{M}} M_\mu\Big). \tag{5-8}$$

5.1.3. Пересечения и суммы подмодулей. В произвольном K-модуле M пересечение любого множества подмодулей также является подмодулем в M. Пересечение всех подмодулей, содержащих заданное множество векторов $A \subset M$, называется *K-линейной оболочкой* множества A или K-подмодулем, *порождённым* множеством A, и обозначается $\operatorname{span}(A)$ или $\operatorname{span}_K(A)$, если надо указать, из какого кольца берутся константы. Линейная оболочка является наименьшим по включению K-подмодулем в M, содержащим A, и может быть иначе описана как множество всех конечных линейных комбинаций $x_1a_1 + \ldots + x_na_n$ векторов $a_i \in A$ с коэффициентами $x_i \in K$, ибо все такие линейные комбинации образуют подмодуль в M и содержатся во всех подмодулях, содержащих A. В противоположность пересечениям, объединения подмодулей почти никогда не являются подмодулями.

Упражнение 5.8. Покажите, что объединение двух подгрупп в абелевой группе является подгруппой если и только если одна из подгрупп содержится в другой.

K-линейная оболочка объединения произвольного множества подмодулей $U_\nu \subset M$ называется *суммой* этих подмодулей и обозначается $\sum_\nu U_\nu \stackrel{\text{def}}{=} \operatorname{span} \bigcup_\nu U_\nu$. Таким образом, сумма подмодулей представляет собою множество всевозможных конечных сумм векторов, принадлежащих этим подмодулям. Например,

$$U_1 + U_2 = \{u_1 + u_2 \mid u_1 \in U_1,\ u_2 \in U_2\}$$
$$U_1 + U_2 + U_3 = \{u_1 + u_2 + u_3 \mid u_1 \in U_1,\ u_2 \in U_2,\ u_3 \in U_3\}$$

и т. д. Если подмодули $U_1, \ldots, U_m \subset M$ таковы, что гомоморфизм сложения

$$U_1 \oplus \ldots \oplus U_n \to U_1 + \ldots + U_n \subset M, \quad (u_1, \ldots, u_n) \mapsto u_1 + \ldots + u_n, \tag{5-9}$$

является биекцией между $U_1 \oplus \ldots \oplus U_n$ и $U_1 + \ldots + U_n$, то сумму $U_1 + \ldots + U_n$ называют *прямой* и обозначают $U_1 \oplus \ldots \oplus U_n$, как в n° 5.1.2 выше. Биективность отображения (5-9) эквивалентна тому, что каждый вектор $w \in U_1 + \ldots + U_n$ имеет *единственное* разложение $w = u_1 + \ldots + u_n$, в котором $u_i \in U_i$ при каждом i.

Предложение 5.2
Сумма подмодулей $U_1, \ldots, U_n \subset V$ является прямой если и только если каждый из подмодулей имеет нулевое пересечение с суммой всех остальных. В частности, сумма $U+W$ двух подмодулей прямая тогда и только тогда, когда $U \cap W = 0$.

Доказательство. Обозначим через W_i сумму всех подмодулей U_ν за исключением i-того. Если пересечение $U_i \cap W_i$ содержит ненулевой вектор $u_i = u_1 + \ldots + u_{i-1} + u_{i+1} + \ldots + u_n$, где $u_i \in U_i$ при всех i, то у этого вектора имеется два различных представления[1]

$$0 + \ldots + 0 + u_i + 0 + \ldots + 0 = u_1 + \ldots + u_{i-1} + 0 + u_{i+1} + \ldots + u_n.$$

Поэтому такая сумма не прямая. Наоборот, если $U_i \cap W_i = 0$ при всех i, то переписывая равенство $u_1 + \ldots + u_n = w_1 + \ldots + w_n$, где $u_\nu, w_\nu \in U_\nu$ при всех i, в виде $u_i - w_i = \sum_{\nu \neq i}(w_\nu - u_\nu)$, заключаем, что этот вектор лежит в $U_i \cap W_i = 0$. Поэтому $u_i = w_i$ для каждого $i = 1, \ldots, n$. □

Следствие 5.1
Для того чтобы модуль M распадался в прямую сумму собственных подмодулей $L, N \subset M$ необходимо и достаточно, чтобы $L + N = M$ и $L \cap N = 0$. □

[1] В левом отлично от нуля только i-е слагаемое, а в правом оно нулевое.

5.1.4. Фактор модули. Для любых K-модуля M подмодуля $N \subseteq M$ можно образовать *фактормодуль* M/N, состоящий из классов $[m]_N = m\,(\mathrm{mod}\ N) = m + N = \{m' \in M \mid m' - m \in N\}$, которые являются аддитивными сдвигами подмодуля N на всевозможные элементы $m \in M$ или, что тоже самое, классами эквивалентности по отношению $m \equiv m'\ (\mathrm{mod}\ N)$ сравнимости по модулю N, означающему, что $m' - m \in N$. Сложение классов и их умножение на элементы кольца определяются обычными формулами $[m_1]_N + [m_2]_N \stackrel{\text{def}}{=} [m_1 + m_2]_N$ и $x \cdot [m]_N \stackrel{\text{def}}{=} [xm]_N$.

Упражнение 5.9. Проверьте, что отношение сравнимости по модулю N является эквивалентностью, а операции корректно определены и удовлетворяют аксиомам (5-1) – (5-4).

В частности, факторкольцо K/I кольца K по идеалу $I \subset K$ является фактором K-модуля K по его K-подмодулю I, ср. с прим. 5.1 выше.

Пример 5.9 (разложение гомоморфизма)
Любой гомоморфизм K-модулей $\varphi : M \to N$ является композицией сюръективного гомоморфизма факторизации $\pi_\varphi : M \twoheadrightarrow M/\ker\varphi$, $w \mapsto [w]_{\ker\varphi}$ и отображения

$$\iota_\varphi : M/\ker\varphi \hookrightarrow N\,, \quad [w]_{\ker\varphi} \mapsto \varphi(w)\,,$$

которое корректно определено и инъективно, так как равенство $\varphi(u) = \varphi(w)$ означает, что $u - w \in \ker\varphi$. Отображение ι_φ K-линейно, поскольку

$$\iota_\varphi(x[u] + y[w]) = \iota_\varphi([xu + yw]) = \varphi(xu + yw) = x\varphi(u) + y\varphi(w) = x\iota_\varphi([u]) + y\iota_\varphi([w])\,.$$

Тем самым, $\iota_\varphi : M/\ker\varphi \xrightarrow{\sim} \mathrm{im}\,\varphi$ является изоморфизмом K-модулей.

Упражнение 5.10. Пусть модуль M является прямой суммой своих подмодулей $L, N \subset M$. Покажите, что $M/N \simeq L$ и $M/L \simeq N$.

Пример 5.10 (дополнительные подмодули и разложимость)
Подмодули $L, N \subset M$ называются *дополнительными*, если $M = L \oplus N$. Согласно сл. 5.1 на стр. 85 для этого необходимо и достаточно, чтобы $L \cap N = 0$ и $L + N = M$. В такой ситуации модуль M называется *разложимым*, а про подмодули L, N говорят, что они *отщепляются* от M прямыми слагаемыми. Модуль M, не представимый в виде прямой суммы своих собственных подмодулей называется *неразложимым*. Например, $\mathbb{Z}$-модуль $\mathbb{Z}$ неразложим, хотя и имеет собственные $\mathbb{Z}$-подмодули. В самом деле, каждый собственный подмодуль $I \subset \mathbb{Z}$ представляет собою главный идеал $I = (d)$. Согласно упр. 5.10, разложение $\mathbb{Z} = (d) \oplus N$ означает наличие в $\mathbb{Z}$ подмодуля $N \subset \mathbb{Z}$, изоморфного $\mathbb{Z}$-модулю $\mathbb{Z}/(d)$, все элементы которого аннулируются умножением на число $d \in \mathbb{Z}$, тогда как в $\mathbb{Z}$-модуле $\mathbb{Z}$ умножение на число d действует инъективно.

Упражнение 5.11. Рассмотрим $\mathbb{Z}$-подмодуль $N \subset \mathbb{Z}^2$, порождённый векторами $(2,1)$ и $(1,2)$. Покажите, что $N \simeq \mathbb{Z}^2$, $M/N \simeq \mathbb{Z}/(3)$, и не существует такого $\mathbb{Z}$-подмодуля $L \subset \mathbb{Z}^2$, что $\mathbb{Z}^2 = L \oplus N$.

Пример 5.11 (фактор модуля по идеалу кольца)
Для произвольных K-модуля M и идеала $I \subset K$ обозначим через

$$IM \stackrel{\text{def}}{=} \{x_1a_1 + \ldots + x_na_n \in M \mid x_i \in I,\ a_i \in M,\ n \in \mathbb{N}\}$$

K-подмодуль, образованный всевозможными линейными комбинациями элементов модуля M с коэффициентами из идеала I.

Упражнение 5.12. Проверьте, что IM действительно является K-подмодулем в M.

Абелева факторгруппа M/IM, элементы которой — это классы

$$[w]_{IM} = w + IM = \{v \in M \mid v - w \in IM\},$$

является модулем над факторкольцом K/I. Умножение векторов на скаляры задаётся правилом

$$[x]_I \cdot [w]_{IM} = [xw]_{[IM]}.$$

Упражнение 5.13. Убедитесь, что оно корректно.

Если $M = N_1 \oplus \ldots \oplus N_m$ раскладывается с прямую сумму своих подмодулей $N_i \subset M$, то возникает аналогичное разложение $IM = IN_1 \oplus \ldots \oplus IN_m$ в сумму подмодулей $IN_i = N_i \cap IM$.

Упражнение 5.14. Убедитесь в этом.

Мы заключаем, что в этом случае $M/IM = (N_1/IN_1) \oplus \ldots \oplus (N_m/IN_m)$. В частности,

$$K^n/IK^n = (K/I)^n. \tag{5-10}$$

для любого идеала $I \subset K$.

Предложение 5.3

Для любых K-модулей M, N и подмодуля $L \subset M$ гомоморфизмы $\varphi: M \to N$, переводящие L в нуль, образуют подмодуль $\mathrm{Ann}_N(L) \stackrel{\text{def}}{=} \{\varphi: M \to N \mid \varphi(L) = 0\} \subset \mathrm{Hom}(M, N)$. Каждый гомоморфизм $\varphi \in \mathrm{Ann}_N(L)$ корректно задаёт K-линейное отображение $\varphi_L: M/L \to M$, $[v]_L \mapsto f(v)$. При этом отображение $\mathrm{Ann}_N(L) \to \mathrm{Hom}_K(M/L, N)$, $\varphi \mapsto \varphi_L$, является изоморфизмом K-модулей, и обратный к нему изоморфизм $\mathrm{Hom}_K(M/L, N) \to \mathrm{Ann}_N(L)$, $\psi \mapsto \psi\pi_L$, переводит гомоморфизм $\psi: M/L \to N$ в его композицию с эпиморфизмом факторизации $\pi_L: M \twoheadrightarrow M/L$.

Доказательство. Если $\varphi_1, \varphi_2: M \to N$ аннулируют L, то линейная комбинация $x_1\varphi_1 + y_1\varphi_2$ тоже аннулирует L. Поэтому $\mathrm{Ann}_N(L)$ является K-подмодулем в $\mathrm{Hom}_K(M, N)$. Если $\varphi \in \mathrm{Ann}_N(L)$, отображение $\varphi_L: [v]_L \mapsto \varphi(v)$ корректно определено, так как для любого вектора $w = v + \ell$ с $\ell \in L$ имеем $\varphi_L(w) = \varphi(v) + \varphi(\ell) = \varphi(v) = \varphi_L(v)$. Очевидно, что отображение φ_L, во-первых, само K-линейно, а во вторых, K-линейно зависит от φ. Поэтому отображение

$$\mathrm{Ann}_N(L) \to \mathrm{Hom}_K(M/L, N), \quad \varphi \mapsto \varphi_L,$$

является гомоморфизмом K-модулей. Поскольку для любого гомоморфизма $\psi: M/L \to M$ выполняется равенство $(\psi\pi_L)_L = \psi$, а для любого гомоморфизма $\varphi \in \mathrm{Ann}_N(L)$ — равенство $\varphi_L\pi_L = \varphi$, отображения $\varphi \mapsto \varphi_L$ и $\psi \mapsto \psi\pi_L$ обратны друг другу и тем самым биективны. □

5.1.5. Образующие и соотношения. Говорят, что вектор v из K-модуля M *линейно выражается* над K через векторы $w_1, \ldots, w_m$, если $v = x_1w_1 + \ldots + x_mw_m$ для некоторых $x_1, \ldots, x_m \in K$. Правая часть этой формулы называется *линейной комбинацией* векторов $w_i \in V$ с коэффициентами $x_i \in K$. Линейная комбинация, в которой все коэффициенты $x_i = 0$, называется *тривиальной*. Множество векторов $Z \subset M$ называется *линейно зависимым*, если некоторая нетривиальная конечная линейная комбинация векторов из Z обращается в нуль, т. е. $x_1u_1 + \ldots + x_ku_k = 0$ для некоторых $u_1, \ldots, u_k \in Z$ и $x_1, \ldots, x_k \in K$, таких что не все x_i равны нулю. Каждая такая линейная комбинация называется *линейным соотношением* на векторы из множества Z.

Мы говорим, что множество $Z \subset M$ *порождает* модуль M, если любой вектор $v \in M$ является линейной комбинацией конечного числа векторов из Z, т. е. $v = x_1u_1 + \ldots + x_mu_m$ для некоторых $x_i \in K$, $w_i \in G$ и $m \in \mathbb{N}$.

Множество $E \subset M$ называется *базисом* модуля M, если каждый вектор $v \in M$ единственным образом линейно выражается через векторы из E, т. е. $v = \sum_{e\in E} x_e e$, где все $x_e \in K$ и только конечное множество из них отлично от нуля, и равенство двух таких сумм $\sum_{e\in E} x_e e = \sum_{e\in E} y_e e$ с конечным числом ненулевых слагаемых равносильно равенству коэффициентов $x_e = y_e$ при каждом векторе $e \in E$.

Модуль M, обладающий базисом, называется *свободным*, и коэффициенты x_e единственного линейного выражения вектора v через базисные векторы $e \in E$ какого-либо базиса $E \subset M$ называются *координатами* вектора v в базисе E. Иначе можно сказать, что свободный модуль с базисом E представляет собою прямую сумму $\bigoplus_{e\in E} Ke$ одинаковых копий $Ke = K$ модуля K, занумерованных элементами $e \in E$.

Лемма 5.1
Множество векторов E составляет базис K-модуля M если и только если оно линейно независимо и линейно порождает M над K.

Доказательство. Пусть множество векторов E порождает K-модуль M. Если существует линейное соотношение $x_1e_1 + \ldots + x_ne_n = 0$, в котором $e_i \in E$ и $x_1 \neq 0$, то оно у нулевого вектора $0 \in M$ имеется два различных представления в линейной комбинации векторов из E: первое даётся указанным соотношением, второе имеет вид $0 = 0 \cdot e_1$. Наоборот, если множество E линейно независимо и имеется равенство $\sum_{e\in E} x_e e = \sum_{e\in E} y_e e$, в обоих частях которого имеется лишь конечное число ненулевых коэффициентов, то перенося все ненулевые слагаемые в одну часть, получаем конечное линейное соотношение $\sum_{e\in E}(x_e - y_e)\cdot e = 0$, возможное только если все коэффициенты нулевые, т. е. только когда $x_e = y_e$ при всех e. □

Предостережение 5.2. Если кольцо коэффициентов K не является полем, то линейная зависимость векторов, вообще говоря, не даёт возможности линейно выразить один из этих векторов через другие. Поэтому понятие размерности в том виде, как оно определяется для векторных пространств над полем, не переносится буквально на модули над произвольными коммутативными кольцами. Например, идеал $I \subset K$ порождается как модуль над K одним элементом если и только если он главный, т. е. $I = (d)$ для некоторого $d \in K$. Такой идеал является свободным K-модулем с базисом d если и только если d не делит нуль в K. Если же идеал $I \subset K$ не главный, то его нельзя линейно породить менее, чем двумя элементами, а любой набор, содержащий по меньшей мере два разных элемента кольца линейно зависим, так как $ab - ba = 0$ для любых $a, b \in K$. Поэтому в неглавном идеале заведомо нет базиса. Так, идеал $(x, y) \subset \mathbb{Q}[x, y]$, состоящий из всех многочленов с нулевым свободным членом, как модуль над кольцом $K = \mathbb{Q}[x, y]$ линейно порождается векторами $w_1 = x$ и $w_2 = y$, которые линейно зависимы над K, ибо $yw_1 - xw_2 = 0$, но ни один из них не выражается линейно через другой.

Пример 5.12 (задание модуля образующими и соотношениями)
Координатный модуль K^n из прим. 5.2 на стр. 82 свободен, так как каждый вектор $(x_1, \ldots, x_n)$ единственным образом представляется в виде линейной комбинации $x_1e_1 + \ldots + x_ne_n$ стандартных базисных векторов $e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$, где единственная ненулевая координата

равна 1 и стоит на i-том месте. Если некоторый K-модуль M линейно порождается над K векторами $w_1, \dots, w_m$, то имеется K-линейный эпиморфизм

$$\pi : K^m \twoheadrightarrow M\,, \quad (x_1, \dots, x_m) \mapsto x_1 w_1 + \dots + x_m w_m\,.$$

Его ядро $R = \ker \pi$ называется *модулем соотношений* между образующими w_i, поскольку оно состоит из всех тех строк $(x_1, \dots, x_n) \in K^m$, что являются коэффициентами линейных соотношений $x_1 w_1 + \dots + x_m w_m = 0$ между образующими w_i в модуле M. Таким образом, каждый конечно порождённый K-модуль M имеет вид $M = K^m/R$ для некоторого числа $m \in \mathbb{N}$ и некоторого подмодуля $R \subset K^m$.

5.1.6. Ранг свободного модуля. Модуль F называется *свободным модулем ранга* r если он обладает базисом из r векторов. Число r обозначается $\operatorname{rk} F$ и не зависит от выбора базиса в силу следующей теоремы.

Теорема 5.1
Все базисы свободного модуля F над коммутативным кольцом K с единицей равномощны.

Доказательство. Пусть множество векторов $E \subset F$ является базисом в F, т. е. $F = \bigoplus_{e\in E} Ke$. Рассмотрим произвольный максимальный идеал[1] $\mathfrak{m} \subset K$. В прим. 5.11 на стр. 86 мы видели, что фактормодуль $F/\mathfrak{m}F$ является векторным пространством над полем $\Bbbk = K/\mathfrak{m}$ и изоморфен $\bigoplus_{e\in E} \Bbbk \cdot [e]$ в силу форм. (5-10) на стр. 87. Таким образом классы $[e]$ векторов $e \in E$ составляют базис векторного пространства $F/\mathfrak{m}F$ над полем $\Bbbk = K/\mathfrak{m}$. Но из курса линейной алгебры известно[2], что все базисы векторного пространства имеют одинаковую мощность. □

5.2. Алгебры над коммутативными кольцами. Модуль A над коммутативным кольцом K называется *K-алгеброй* или *алгеброй над K*, если на нём задана операция умножения

$$A \times A \to A\,, \quad (a, b) \mapsto ab\,,$$

которая K-линейна по a при фиксированном b и K-линейна по b при фиксированном[3] a, т. е.

$$(x_1 a_1 + x_2 a_2)\, b = x_1 a_1 b + x_2 a_2 b \quad \text{и} \quad a\,(y_1 b_1 + y_2 b_2) = y_1 a b_1 + y_2 a b_2$$

для всех $a, b, a_i, b_j \in A$ и всех $x_i, y_j \in K$. Поскольку для всех $a \in A$ выполняются равенства

$$0 \cdot a = (0+0)\, a = 0 \cdot a + 0 \cdot a \quad \text{и} \quad a \cdot 0 = a\,(0+0) a = a \cdot 0 + a \cdot 0\,,$$

мы заключаем, что $0 \cdot a = 0 = a \cdot 0$ для всех $a \in A$ в любой K-алгебре A.

Алгебра A называется *ассоциативной*, если $(ab)c = a(bc)$ для всех $a, b, c \in A$, и *коммутативной* — если $ab = ba$ для всех $a, b \in A$. Алгебра A называется *алгеброй с единицей*, если в ней есть нейтральный элемент по отношению к умножению, т. е. такой $e \in A$, что $ea = ae = a$ для всех $a \in A$. Так как для любых элементов e', e'' с этим свойством выполняются равенства $e' = e' \cdot e'' = e''$, единица в алгебре единственна, если существует.

[1] См. прим. 4.3 на стр. 70.
[2] См. теор. 7.3 на стр. 93 лекции http://gorod.bogomolov-lab.ru/ps/stud/geom_ru/2122/lec_07.pdf.
[3] Такие функции от двух аргументов называются *билинейными*.

Отображение $\varphi : A \to B$ между K-алгебрами A и B называется *гомоморфизмом K-алгебр*, если оно K-линейно и перестановочно с умножением, т. е. $\varphi(a_1 a_2) = \varphi(a_1)\varphi(a_2)$. Будучи гомоморфизмами K-модулей, гомоморфизмы K-алгебр обладают всеми свойствами из n° 5.1.1 на стр. 82 выше.

Примерами *коммутативных* ассоциативных K-алгебр с единицами являются алгебра многочленов $K[x_1, \dots, x_n]$ и другие конечно порождённые коммутативные K-алгебры из прим. 4.5 на стр. 71. Основным модельным примером некоммутативной K-алгебры является

Пример 5.13 (алгебра K-линейных эндоморфизмов)
Модуль $\mathrm{Hom}_K(M, M)$ всех K-линейных отображений $M \to M$ обозначается $\mathrm{End}\, M$ или $\mathrm{End}_K M$ и называется *алгеброй эндоморфизмов*[1] K-модуля M, поскольку композиция эндоморфизмов

$$\mathrm{End}(M) \times \mathrm{End}(M) \to \mathrm{End}(M), \quad (\varphi, \psi) \mapsto (\varphi \circ \psi : w \mapsto \varphi(\psi(w))),$$

задаёт на $\mathrm{End}\, M$ структуру ассоциативной K-алгебры с единицей, в роли которой выступает тождественный эндоморфизм $\mathrm{Id}_M : w \mapsto w$.

Упражнение 5.15. Проверьте, что композиция отображений ассоциативна и линейно зависит от каждого из двух компонуемых отображений.

5.2.1. Алгебра матриц $\mathbf{Mat}_n(K)$. Рассмотрим свободный координатный модуль $M = K^n$ с базисом из векторов $e_1, \dots, e_n$. Каждый K-линейный эндоморфизм $\varphi : K^n \to K^n$ однозначно задаётся набором из n векторов $w_i = \varphi(e_i)$ — образами базисных векторов под действием эндоморфизма φ. В самом деле, поскольку любой вектор $w \in K^n$ единственным образом записывается в виде $w = x_1 e_1 + \dots + x_i e_i$, значение φ на нём вычисляется как

$$\varphi(w) = \varphi(x_1 e_1 + \dots + x_n e_n) = x_1 \varphi(e_1) + \dots + x_n \varphi(w_n) = x_1 w_1 + \dots + x_n w_n,$$

и наоборот, для любого набора векторов $w_1, \dots, w_n \in K^n$ отображение

$$\varphi_{w_1,\dots,w_n} : K^n \to K^n, \quad x_1 e_1 + \dots + x_n e_n \mapsto x_1 w_1 + \dots + x_n w_n,$$

является K-линейным и переводит каждый базисный вектор e_i в вектор w_i.

Упражнение 5.16. Убедитесь в этом.

Таким образом, мы получаем биекцию между K-линейными эндоморфизмами $K^n \to K^n$, т. е. элементами K-модуля $\mathrm{End}\, K^n$, и упорядоченными наборами $(w_1, \dots, w_n)$ из n векторов $w_i \in K^n$, т. е. элементами K-модуля $K^n \times \dots \times K^n \simeq K^{n^2}$.

Упражнение 5.17. Убедитесь в том, что эта биекция K-линейна, т. е. является изоморфизмом K-модулей.

Набор векторов $w_j = \varphi(e_j) \in K^n$, задающих эндоморфизм $\varphi : K^n \to K^n$, принято записывать в виде квадратной матрицы[2] Φ размера $n \times n$, помещая координаты j-го вектора w_j в j-й *столбец* этой таблицы:

$$w_1, w_2, \dots, w_n = \begin{pmatrix} \varphi_{11} \\ \vdots \\ \varphi_{n1} \end{pmatrix}, \begin{pmatrix} \varphi_{12} \\ \vdots \\ \varphi_{n2} \end{pmatrix}, \dots, \begin{pmatrix} \varphi_{1n} \\ \vdots \\ \varphi_{nn} \end{pmatrix} \dashrightarrow \Phi = \begin{pmatrix} \varphi_{11} & \varphi_{12} & \cdots & \varphi_{1n} \\ \vdots & \vdots & \dots & \vdots \\ \varphi_{n1} & \varphi_{n2} & \cdots & \varphi_{nn} \end{pmatrix}.$$

[1] Терминологию, относящуюся к отображениям множеств, см. на стр. 5.
[2] См. прим. 5.3 на стр. 82.

Матрица $\Phi = \left(\varphi_{ij}\right)$ в i-й строке и j-м столбце которой находится i-я координата вектора $\varphi(e_j)$, называется *матрицей* отображения $\varphi\colon K^n \to K^n$ в базисе $e_1, \dots, e_n$. Таким образом, сопоставляя эндоморфизму φ его матрицу Φ, мы получаем изоморфизм K-модулей

$$\operatorname{End}(K^n) \xrightarrow{\sim} \operatorname{Mat}_{n\times n}(K)\,, \quad \varphi \mapsto \Phi\,, \tag{5-11}$$

где $\operatorname{Mat}_n(K) \stackrel{\text{def}}{=} \operatorname{Mat}_{n\times n}(K)$ — модуль $n \times n$ матриц[1] с элементами из K. Изоморфизм (5-11) позволяет перенести на K-модуль матриц ассоциативное умножение с единицей, которое имеется в алгебре $\operatorname{End}(K^n)$ из прим. 5.13 выше и задаётся композицией отображений. Возникающая таким образом билинейная ассоциативная операция

$$\operatorname{Mat}_{n\times n}(K) \times \operatorname{Mat}_{n\times n}(K) \to \operatorname{Mat}_{n\times n}(K)\,, \quad (\Phi, \Psi) \mapsto \Phi\Psi\,,$$

где Φ и Ψ суть матрицы K-линейных отображений $\varphi, \psi\colon K^n \to K^n$, а $\Phi\Psi$ — матрица их композиции $\varphi\psi\colon K^n \to K^n$, $w \mapsto \varphi(\psi(w))$, называется *произведением матриц*. Элемент $p_{ij} \in K$ произведения $P = \Phi\Psi = (p_{ij})$ является i-й координатой вектора

$$\varphi(\psi(e_j)) = \varphi(\psi_{1j}e_1 + \dots + \psi_{nj}e_n) = \psi_{1j}\varphi(e_1) + \dots + \psi_{nj}\varphi(e_n)\,,$$

которая равна $\psi_{1j}\varphi_{i1} + \dots + \psi_{nj}\varphi_{in}$. Мы заключаем, что произведение $C = AB$ матриц $A = \left(a_{ij}\right)$ и $B = \left(b_{ij}\right)$ имеет в i-й строке и j-м столбце элемент

$$c_{ij} = \sum_k a_{ik}b_{kj} = a_{i1}b_{1j} + a_{i2}b_{2j} + \dots + a_{in}b_{nj}\,.$$

Единицей алгебры $\operatorname{Mat}_{n\times n}(K)$ является матрица тождественного отображения $\mathrm{Id}\colon K^n \to K^n$

$$E = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & 1 \end{pmatrix} \in \operatorname{Mat}_{n\times n}(K)\,, \tag{5-12}$$

(по диагонали стоят единицы, в остальных местах — нули). Как и композиция отображений, умножение матриц не коммутативно. Например,

$$\begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix} \cdot \begin{pmatrix} 3 & 0 \\ 4 & 5 \end{pmatrix} = \begin{pmatrix} 11 & 10 \\ 12 & 15 \end{pmatrix}$$
$$\begin{pmatrix} 3 & 0 \\ 4 & 5 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix} = \begin{pmatrix} 3 & 6 \\ 4 & 23 \end{pmatrix}.$$

Как модуль над K алгебра $\operatorname{Mat}_n(K)$ изоморфна координатному модулю K^{n^2} и тем самым свободна. Стандартный базис в $\operatorname{Mat}_n(K)$ состоит из матриц E_{ij}, единственным ненулевым элементом которых является единица, стоящая в i-й строке и j-м столбце. Произвольная матрица $A = (a_{ij})$ линейно выражается через этот базис по формуле $A = \sum_{i,j} a_{ij}E_{ij}$. Прообразами базисных матриц E_{ij} при изоморфизме (5-11) являются K-линейные отображения $E_{ij}\colon K^n \to K^n$, которые

[1] См. прим. 5.3 на стр. 82.

мы обозначаем также, как и базисные матрицы, и которые действуют на базисные векторы e_k координатного модуля K^n по правилам

$$E_{ij}(e_k) = \begin{cases} e_i & \text{при } k = j \\ 0 & \text{при } k \neq j. \end{cases}$$

Отсюда немедленно получается таблица умножения базисных матриц E_{ij}:

$$E_{ik}E_{\ell j} = \begin{cases} E_{ij} & \text{при } k = \ell \\ 0 & \text{при } k \neq \ell, \end{cases} \tag{5-13}$$

которая ещё раз показывает, что умножение матриц не коммутативно: $E_{12}E_{21} \neq E_{21}E_{12}$.

Упражнение 5.18. Составьте таблицу *коммутаторов* $[E_{ik}, E_{\ell j}] \stackrel{\text{def}}{=} E_{ik}E_{\ell j} - E_{\ell j}E_{ik}$.

Пример 5.14
Вычислим A^{2023} для матрицы $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Поскольку $A = E + E_{12}$ и матрицы E и E_{12} коммутируют, вычислить $(E + E_{12})^{2023}$ можно по формуле для раскрытия бинома[1], а так как $E_{12}^n = 0$ при $n > 1$, на ответ влияют только первые два члена:

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{2023} = (E + E_{12})^{2023} = E + 2023\,E_{12} = \begin{pmatrix} 1 & 2023 \\ 0 & 1 \end{pmatrix}.$$

Упражнение 5.19. Покажите, что $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$ при всех $n \in \mathbb{Z}$.

5.2.2. Обратимые элементы. Элемент a алгебры A с единицей $e \in A$ называется *обратимым*, если существует такой элемент $a^{-1} \in A$, что $aa^{-1} = a^{-1}a = e$. В ассоциативной алгебре A это требование можно ослабить до существования таких $a', a'' \in A$, что $a'a = aa'' = e$. В самом деле, тогда $a' = a'e = a'(aa'') = (a'a)a'' = ea'' = a''$. Это вычисление заодно показывает, что обратный к a элемент a^{-1}, если он существует, однозначно определяется по a равенствами $aa^{-1} = a^{-1}a = e$.

Пример 5.15 (обратимые 2×2-матрицы)
Выясним, какие 2×2-матрицы

$$\Phi = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

обратимы в алгебре $\mathrm{Mat}_{2\times 2}(K)$ из n° 5.2.1. Чтобы получить нули в правом верхнем и левом нижнем углах произведения

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix}$$

можно в качестве первого приближения к левой матрице взять матрицу со строками

$$(\alpha, \beta) = (d, -b) \quad \text{и} \quad (\gamma, \delta) = (-c, a).$$

[1] См. формулу (0-8) на стр. 8.

Тогда

$$\begin{pmatrix} d & -b \\ -c & d \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} ad-bc & 0 \\ 0 & ad-bc \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} d & -b \\ -c & d \end{pmatrix}.$$

Матрица

$$\Phi^\vee \stackrel{\text{def}}{=} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

называется *присоединённой* к матрице Φ, а число $\det\Phi \stackrel{\text{def}}{=} ad-bc \in K$ — *определителем* матрицы Φ. В этих обозначениях предыдущее равенство переписывается в виде

$$\Phi^\vee\Phi = \Phi\Phi^\vee = \det(\Phi)\cdot E\,.$$

Мы заключаем, что если $\det\Phi$ обратим в K, то матрица Φ обратима и $\Phi^{-1} = \det(\Phi)^{-1}\Phi^\vee$.

Упражнение 5.20. Убедитесь, что $(AB)^\vee = B^\vee A^\vee$ для любых $A, B \in \mathrm{Mat}_{2\times 2}(K)$.

Из упражнения вытекает, что для всех $A, B \in \mathrm{Mat}_{2\times 2}(K)$

$$\det(AB)\cdot E = AB(AB)^\vee = ABB^\vee A^\vee = A\cdot\det(B)\cdot E\cdot A^\vee = \det(B)\cdot AA^\vee = \det(A)\cdot\det(B)\cdot E\,,$$

откуда $\det(AB) = \det(A)\cdot\det(B)$. Мы заключаем, что если матрица Φ обратима, то

$$1 = \det E = \det(\Phi\Phi^{-1}) = \det(\Phi)\cdot\det(\Phi^{-1})\,,$$

и тем самым $\det\Phi$ обратим в K. Итак, 2×2 матрица Φ обратима если и только если обратим её определитель, и в этом случае $\Phi^{-1} = \det(\Phi)^{-1}\Phi^\vee$.

Пример 5.16 (обращение унитреугольной матрицы)
Диагональ, идущая из левого верхнего угла квадратной матрицы в правый нижний, называется *главной*. Если все стоящие под (соотв. над) главной диагональю элементы нулевые, матрица называется *верхней* (соотв. *нижней*) *треугольной*.

Упражнение 5.21. Проверьте, что верхние и нижние треугольные матрицы являются подалгебрами[1] в $\mathrm{Mat}_n(K)$.

Треугольные матрицы с единицами на главной диагонали называются *унитреугольными*. Покажем, что каждая верхняя унитреугольная матрица $A = (a_{ij})$ обратима[2] и обратная к ней матрица $B = A^{-1}$ тоже верхняя унитреугольная с наддиагональными элементами

$$b_{ij} = \sum_{s=0}^{j-i-1}(-1)^{s+1}\sum_{i<\nu_1<\ldots<\nu_s<j} a_{i\nu_1}a_{\nu_1\nu_2}a_{\nu_2\nu_3}\ \ldots\ a_{\nu_{s-1}\nu_s}a_{\nu_s j} =$$
$$= -a_{ij} + \sum_{i<k<j} a_{ik}a_{kj} - \sum_{i<k<\ell<j} a_{ik}a_{k\ell}a_{\ell j} + \sum_{i<k<\ell<m<j} a_{ik}a_{k\ell}a_{\ell m}a_{mj} - \ \ldots\ . \qquad (5\text{-}14)$$

Для этого запишем матрицу A в виде линейной комбинации базисных матриц E_{ij}:

$$A = E + \sum_{i<j} a_{ij}E_{ij} = E + N\,,$$

[1] Т. е. являются подмодулями, замкнутыми относительно умножения.

[2] Причём этот факт, как и приводимое здесь доказательство, остаётся в силе для матриц с элементами в произвольном (даже некоммутативном) ассоциативном кольце с единицей.

где матрица $N = \sum_{i<j} a_{ij}E_{ij}$ представляет собою наддиагональную часть матрицы A. Согласно форм. (5-13) на стр. 92 коэффициент при E_{ij} в матрице N^k равен нулю при $j - i < k$, а при $j - i \geqslant k$ представляет собою сумму всевозможных произведений[1]

$$\underbrace{a_{iv_1}a_{v_1v_2}\dots a_{v_{k-2}v_{k-1}}a_{v_{k-1}j}}_{k\text{ сомножителей}}, \quad \text{где} \quad i < v_1 < \dots < v_{k-1} < j\,.$$

В частности, он заведомо зануляется, когда k превышает размер матрицы A. Полагая $x = E$, $y = N$ в равенстве[2] $(x+y)(x^{m-1} - x^{m-2}y + \dots + (-1)^{m-1}y^{m-1}) = x^m - y^m$, при достаточно большом m мы получим матричное равенство $A(E - N + N^2 - N^3 + \dots) = E$, откуда

$$A^{-1} = E - N + N^2 - N^3 + \dots\,,$$

что и утверждалось.

5.3. Матричный формализм. Матрица из m строк и n столбцов, заполненная элементами какого-нибудь K-модуля R, называется $m \times n$ *матрицей* с элементами из R. Множество всех таких матриц обозначается $\mathrm{Mat}_{m\times n}(R)$ и тоже является K-модулем, изоморфным прямому произведению mn копий модуля R.

5.3.1. Умножение матриц. Пусть элементы K-модулей L и M можно билинейно перемножать со значениями в K-модуле N, т. е. задано такое отображение $L \times M \to N$, $(u, w) \to uw$, что $(x_1u_1 + x_2u_2)(y_1w_1 + y_2w_2) = x_1y_1u_1w_1 + x_1y_2u_1w_2 + x_2y_1u_2w_1 + x_2y_2u_2w_2$ для всех $u_i \in L$, $w_j \in M$ и $x_i, y_j \in K$. Тогда для всех $m, s, n \in \mathbb{N}$ определено *произведение матриц*

$$\mathrm{Mat}_{m\times s}(L) \times \mathrm{Mat}_{s\times n}(M) \to \mathrm{Mat}_{m\times n}(N)\,, \quad (A, B) \mapsto AB\,.$$

Обратите внимание, что в этом произведении ширина левой матрицы A должна быть равна высоте правой матрицы B, а само произведение имеет столько же строк, сколько левый сомножитель, и столько же столбцов, сколько правый. При $m = n = 1$ результатом умножения строки ширины s на столбец высоты s является матрица размера 1×1, т. е. один элемент, который определяется так:

$$(a_1, \dots, a_s)\begin{pmatrix} b_1 \\ \vdots \\ b_s \end{pmatrix} \stackrel{\text{def}}{=} a_1b_1 + \dots + a_sb_s = \sum_{k=1}^{s} a_kb_k\,. \tag{5-15}$$

Для произвольных m и n элемент c_{ij} матрицы $C = AB$ равен произведению i-й строки из A на j-й столбец из B, посчитанному по формуле (5-15):

$$c_{ij} = \begin{pmatrix} a_{i1}, \dots\ a_{is} \end{pmatrix} \cdot \begin{pmatrix} b_{1j} \\ \vdots \\ b_{sj} \end{pmatrix} = \sum_{k=1}^{s} a_{ik}b_{kj}\,. \tag{5-16}$$

[1] Продуктивно представлять себе E_{ij} как стрелку, ведущую из числа j в число i на числовой прямой. Произведение k сомножителей E_{ij} отлично от нуля если и только если конец каждой стрелки совпадает с началом предыдущей, и в этом случае такое произведение равно сумме всех перемножаемых стрелок, рассматриваемых как целочисленные векторы на числовой прямой. Таким образом, каждое ненулевое произведение k стрелок имеет длину как минимум k, а разложения элемента E_{ij} в произведение k таких элементов находятся в биекции со всевозможными способами пройти из j в i за k шагов.

[2] Поскольку матрицы E и N коммутируют друг с другом, в результате этой подстановки мы получим верное матричное равенство.

Иначе можно сказать, что в j-том столбце матрицы AB стоит линейная комбинация s столбцов матрицы A с коэффициентами из j-го столбца матрицы B. Это описание получается, если подставить в формулу (5-15) в качестве элементов b_i числа из j-го столбца матрицы B, а в качестве элементов a_j — столбцы матрицы A, интерпретируемые как элементы K-модуля L^m, записанные в виде координатных столбцов.

Упражнение 5.22. Удостоверьтесь, что это описание согласуется с формулой (5-16).

Например, для того, чтобы превратить матрицу

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \end{pmatrix} \tag{5-17}$$

в матрицу из четырёх столбцов, равных, соответственно, сумме 1-го столбца матрицы A со 2-м, умноженным на λ, сумме 1-го и 3-го столбцов матрицы A, сумме 3-го столбца матрицы A со 2-м, умноженным на μ, и сумме всех трёх столбцов матрицы A, умноженных на их номера, надо умножить матрицу A справа на матрицу

$$\begin{pmatrix} 1 & 1 & 0 & 1 \\ \lambda & 0 & \mu & 2 \\ 0 & 1 & 1 & 3 \end{pmatrix}$$

Упражнение 5.23. Проверьте это прямым вычислением по формуле (5-16).

Симметричным образом, если в формуле (5-15) взять в в качестве элементов a_j те, что стоят в i-й строке матрицы A, а в качестве b_i — строки матрицы B, интерпретируемые как элементы K-модуля M^n, записанные в виде координатных строк, то можно сказать, что i-й строкой матрицы AB является линейная комбинация строк матрицы B с коэффициентами, стоящими в i-й строке матрицы A. Например, если в той же матрице (5-17) 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 5.24. Проверьте это прямым вычислением по формуле (5-16).

Предыдущие два описания произведения AB получаются друг из друга одновременной перестановкой букв A, B и заменой слов «столбец» и «строка» друг на друга. Матрица $C^t = (c^t_{ij})$ размера $n \times m$, по строкам которой записаны столбцы $m \times n$ матрицы $C = (c_{ij})$, называется *транспонированной* к матрице C. Её элементы $c^t_{ij} = c_{ji}$ получаются отражением элементов матрицы C относительно биссектрисы левого верхнего угла матрицы.

Предложение 5.4
Для матриц с элементами из коммутативного кольца выполняется равенство $(AB)^t = B^t A^t$, т. е. транспонирование обращает порядок сомножителей в произведениях матриц, элементы которых коммутируют друг с другом.

Доказательство. Пусть $AB = C$, $B^t A^t = D$, тогда $c_{ij} = \sum\limits_k a_{ik} b_{kj} = \sum\limits_k a^t_{ki} b^t_{jk} = \sum\limits_k b^t_{jk} a^t_{ki} = d_{ji}$. □

Упражнение 5.25. Убедитесь, что если операция умножения $L \times M \to N$ билинейна, то произведение матриц $\mathrm{Mat}_{m\times s}(L) \times \mathrm{Mat}_{s\times n}(M) \to \mathrm{Mat}_{m\times n}(N)$ тоже билинейно, т. е.

$$(x_1A_1 + x_2A_2)B = x_1A_1B + x_2A_2B \quad \text{и} \quad A(y_1B_1 + y_2B_2) = y_1AB_1 + y_2AB_2$$

для всех $A, A_1, A_2 \in \mathrm{Mat}_{m\times s}(L)$, $B, B_1, B_2 \in \mathrm{Mat}_{m\times s}(M)$ и $x_i, y_j \in K$.

Предложение 5.5
Если на K-модулях $L_1, L_2, L_3, L_{12}, L_{23}, L_{123}$ заданы билинейные ассоциативные[1] умножения

$$L_1 \times L_2 \to L_{12}\,, \quad L_{12} \times L_3 \to L_{123}\,, \quad L_2 \times L_3 \to L_{23}\,, \quad L_1 \times L_{23} \to L_{123}\,,$$

то при всех $m, k, \ell, n \in \mathbb{N}$ умножения матриц

$$\mathrm{Mat}_{m\times k}(L_1) \times \mathrm{Mat}_{k\times \ell}(L_2) \to \mathrm{Mat}_{m\times \ell}(L_{12})\,, \quad \mathrm{Mat}_{m\times \ell}(L_{12}) \times \mathrm{Mat}_{\ell\times n}(L_3) \to \mathrm{Mat}_{m\times n}(L_{123})\,,$$
$$\mathrm{Mat}_{k\times \ell}(L_2) \times \mathrm{Mat}_{\ell\times n}(L_3) \to \mathrm{Mat}_{k\times n}(L_{23})\,, \quad \mathrm{Mat}_{m\times k}(L_1) \times \mathrm{Mat}_{k\times n}(L_{23}) \to \mathrm{Mat}_{m\times n}(L_{123})\,.$$

тоже ассоциативны, т. е. $(AB)C = A(BC)$ когда эти произведения определены.

Доказательство. Пусть $AB = P$, $BC = Q$. Проверим, что (i, j)-е элементы матриц PC и AQ равны:

$$\sum_k p_{ik}c_{kj} = \sum_k \Big(\sum_\ell a_{i\ell}b_{\ell k}\Big)c_{kj} = \sum_{k\ell}(a_{i\ell}b_{\ell k})c_{kj} =$$
$$= \sum_{k\ell} a_{i\ell}(b_{\ell k}c_{kj}) = \sum_\ell a_{i\ell}\Big(\sum_k b_{\ell k}c_{kj}\Big) = \sum_\ell a_{i\ell}q_{\ell j}\,.$$

Обратите внимание, что 2-е и 4-е равенства используют билинейность умножений. □

5.3.2. Матрицы перехода. Пусть в K-модуле M заданы два набора векторов:

$$\boldsymbol{u} = (u_1, \ldots, u_n) \quad \text{и} \quad \boldsymbol{w} = (w_1, \ldots, w_m)\,,$$

причём первый из них содержится в линейной оболочке второго, т. е. каждый вектор u_j имеет вид $u_j = w_1c_{1j} + w_2c_{2j} + \ldots + w_mc_{mj}$, где $c_{ij} \in K$. Эти n равенств собираются в одну матричную формулу $\boldsymbol{u} = \boldsymbol{w}\,C_{\boldsymbol{wu}}$, где $\boldsymbol{u} = (u_1, \ldots, u_n)$ и $\boldsymbol{w} = (w_1, \ldots, w_m)$ суть матрицы-строки с элементами из M, а матрица $C_{\boldsymbol{wu}} = \big(c_{ij}\big)$ получается подстановкой в матрицу $\boldsymbol{u}$ вместо каждого из векторов u_j столбца коэффициентов его линейного выражения через векторы w_i. Матрица $C_{\boldsymbol{wu}}$ называется *матрицей перехода* от векторов $\boldsymbol{u}$ к векторам $\boldsymbol{w}$. Название объясняется тем, что если имеется набор векторов $\boldsymbol{v} = (v_1, \ldots, v_k)$, линейно выражающихся через векторы $\boldsymbol{u}$ по формулам $\boldsymbol{v} = \boldsymbol{u}C_{\boldsymbol{uv}}$, то выражение векторов $\boldsymbol{v}$ через векторы $\boldsymbol{w}$ задаётся матрицей

$$C_{\boldsymbol{wv}} = C_{\boldsymbol{wu}}C_{\boldsymbol{uv}}\,, \tag{5-18}$$

которая возникает при подстановке $\boldsymbol{u} = \boldsymbol{w}C_{\boldsymbol{wu}}$ в разложение $\boldsymbol{v} = \boldsymbol{u}C_{\boldsymbol{uv}}$. В частности, если вектор $v \in \mathrm{span}(u_1, \ldots, u_n) \subset \mathrm{span}(w_1, \ldots, w_n)$ линейно выражается через векторы $\boldsymbol{u}$ по формуле $v = u_1x_1 + \ldots + u_nx_n = \boldsymbol{u}\boldsymbol{x}$, где $\boldsymbol{x} = (x_1, \ldots, x_n)^t \in K^n$ — столбец коэффициентов, то этот

[1] Т. е. $(ab)c = a(bc)$ всякий раз, когда произведения определены.

же вектор выражается через векторы $\boldsymbol{w}$ по формуле $v = w_1y_1 + \ldots + w_my_m = \boldsymbol{wy}$ со столбцом коэффициентов $\boldsymbol{y} = (y_1, \ldots, y_m)^t \in K^m$, который связан со столбцом $\boldsymbol{x}$ соотношением

$$\boldsymbol{y} = C_{\boldsymbol{wu}}\boldsymbol{x}\,.$$

Отметим, что когда набор векторов $\boldsymbol{w} = (w_1, \ldots, w_m)$ линейно зависим, у каждого вектора v из их линейной оболочки имеется много *разных* линейных выражений через векторы w_j. Поэтому обозначение $C_{\boldsymbol{wv}}$ в этой ситуации не корректно в том смысле, что элементы матрицы $C_{\boldsymbol{wv}}$ определяются наборами векторов $\boldsymbol{w}$ и $\boldsymbol{v}$ не однозначно. Тем не менее, равенство (5-18) вполне осмысленно и означает, что имея какие-нибудь линейные выражения $C_{\boldsymbol{wu}}$ и $C_{\boldsymbol{uv}}$ векторов $\boldsymbol{u}$ через $\boldsymbol{w}$ и векторов $\boldsymbol{v}$ через $\boldsymbol{u}$, мы можем явно предъявить одно из линейных выражений $C_{\boldsymbol{wv}}$ векторов $\boldsymbol{v}$ через векторы $\boldsymbol{w}$, перемножив матрицы $C_{\boldsymbol{wu}}$ и $C_{\boldsymbol{uv}}$.

Если же набор векторов $\boldsymbol{e} = (e_1, \ldots, e_n)$ является базисом своей линейной оболочки, то матрица перехода $C_{\boldsymbol{ew}}$, выражающая произвольный набор векторов $\boldsymbol{w} = (w_1, \ldots, w_m)$ через $\boldsymbol{e}$ однозначно определяется наборами $\boldsymbol{e}$ и $\boldsymbol{w}$, т. е. $\boldsymbol{u} = \boldsymbol{w}$ если и только если $C_{\boldsymbol{eu}} = C_{\boldsymbol{ew}}$. Отсюда получается следующий критерий обратимости матрицы с элементами из коммутативного кольца.

Предложение 5.6
Следующие условия на квадратную матрицу $C \in \mathrm{Mat}_n(K)$ эквивалентны:

1) матрица C обратима в $\mathrm{Mat}_n(K)$

2) столбцы матрицы C образуют базис свободного модуля K^n

3) строки матрицы C образуют базис свободного модуля K^n.

Доказательство. Последние два свойства равносильны, так как по предл. 5.4 на стр. 95 равенства $BC = CB = E$ при транспонировании превращаются в равенства $C^tB^t = B^tC^t = E$, и тем самым обратимость матрицы C влечёт обратимость транспонированной матрицы C^t и наоборот. Чтобы доказать равносильность первых двух условий, обозначим через $\boldsymbol{u} = (u_1, \ldots, u_n)$ набор столбцов матрицы C, рассматриваемых как векторы координатного модуля K^n. Тогда $C = C_{\boldsymbol{eu}}$ является матрицей перехода от векторов $\boldsymbol{u}$ к стандартному базису $\boldsymbol{e} = (e_1, \ldots, e_n)$ модуля K^n. Если векторы $\boldsymbol{u}$ образуют базис в K^n, то векторы $\boldsymbol{e}$ линейно через них выражаются: $\boldsymbol{e} = \boldsymbol{u}\,C_{\boldsymbol{ue}}$, где $C_{\boldsymbol{ue}} \in \mathrm{Mat}_n(K)$. Из формулы (5-18) вытекают равенства $C_{\boldsymbol{ee}} = C_{\boldsymbol{eu}}C_{\boldsymbol{ue}}$ и $C_{\boldsymbol{uu}} = C_{\boldsymbol{ue}}C_{\boldsymbol{eu}}$. Так как оба набора векторов являются базисами, $C_{\boldsymbol{ee}} = C_{\boldsymbol{uu}} = E$. Поэтому матрицы $C_{\boldsymbol{ue}}$ и $C_{\boldsymbol{eu}}$ обратны друг другу. Наоборот, если матрица $C_{\boldsymbol{eu}}$ обратима, то умножая обе части равенства $\boldsymbol{u} = \boldsymbol{e}C_{\boldsymbol{eu}}$ справа на $C_{\boldsymbol{eu}}^{-1}$, получаем линейное выражение $\boldsymbol{e} = \boldsymbol{u}\,C_{\boldsymbol{eu}}^{-1}$ векторов $\boldsymbol{e}$ через векторы $\boldsymbol{u}$. Поэтому последние линейно порождают модуль K^n. Пусть столбец $\boldsymbol{x} = (x_1, \ldots, x_n)^t \in K^n$ таков, что $\boldsymbol{ux} = 0$. Поскольку векторы $\boldsymbol{e}$ составляют базис в K^n и $\boldsymbol{e}\,C_{\boldsymbol{eu}}\boldsymbol{x} = \boldsymbol{ux} = 0$, столбец $C_{\boldsymbol{eu}}\boldsymbol{x} \in K^n$ является нулевым. Умножая его слева на $C_{\boldsymbol{eu}}^{-1}$, заключаем, что и столбец $\boldsymbol{x}$ нулевой, т. е. векторы $\boldsymbol{u}$ линейно независимы. □

Пример 5.17 (теорема об элементарных симметрических функциях)
Многочлен $f \in \mathbb{Z}[x_1, \ldots, x_n]$ называется *симметрическим*, если он не меняется при перестановках переменных, т. е. когда $f(x_1, \ldots, x_n) = f(x_{g(1)}, \ldots, x_{g(n)})$ для всех биекций

$$g\colon \{1, \ldots, n\} \xrightarrow{\sim} \{1, \ldots, n\}\,.$$

Иначе говоря, многочлен f симметрический если и только если вместе с каждым входящим в f мономом $x_1^{m_1}\dots x_n^{m_n}$ с тем же самым коэффициентом в f входят и все мономы $x_1^{m_{g(1)}}\dots x_n^{m_{g(n)}}$, которые получаются из него перестановками степеней. Так как среди них есть ровно один моном $x_1^{\lambda_1}\dots x_n^{\lambda_n}$ с невозрастающими показателями $\lambda_1 \geqslant \dots \geqslant \lambda_n$, мы заключаем, что однородные симметрические многочлены степени d образуют свободный $\mathbb{Z}$-модуль с базисом из многочленов

$$m_\lambda = (\text{сумма всех различных мономов вида } x_1^{\lambda_{g(1)}}\dots x_n^{\lambda_{g(n)}}), \tag{5-19}$$

где $\lambda = (\lambda_1, \dots, \lambda_n)$ пробегает диаграммы Юнга[1] из d клеток и n строк, часть из которых может быть нулевой длины. Многочлен (5-19) называется *мономиальным симметрическим*.

Упражнение 5.26. Сколько слагаемых в правой части (5-19)?

Симметрические многочлены $e_0 = 1$ и $e_k(x_1, \dots, x_n) = \sum_{i_1<\dots<i_k} x_{i_1}\dots x_{i_k}$, равный сумме всех произведений из k различных переменных, где $1 \leqslant k \leqslant n$, называются *элементарными*. Они появляются в *формулах Виета*: если $\alpha_1, \dots, \alpha_n$ — корни приведённого многочлена

$$t^n + a_1 t^{n-1} + \dots + a_n = \prod_{i=1}^{n}(x - \alpha_i), \tag{5-20}$$

то $a_i = (-1)^i e_i(\alpha_1, \dots, \alpha_n)$.

Упражнение 5.27. Убедитесь в этом.

Для каждой диаграммы Юнга $\mu = (\mu_1, \dots, \mu_n)$ положим $e_\mu \stackrel{\text{def}}{=} e_{\mu_1}\dots e_{\mu_n}$. Это лишь другое обозначение для монома $e_1^{m_1}\dots e_n^{m_n}$, каждый показатель m_i в котором равен количеству строк длины i в диаграмме μ.

Упражнение 5.28. Убедитесь, что диаграмма Юнга μ и набор $(m_1, \dots, m_n) \in \mathbb{Z}^n_{\geqslant 0}$ взаимно однозначно определяют друг друга из равенства $e_{\mu_1}\dots e_{\mu_n} = e_1^{m_1}\dots e_n^{m_n}$.

Многочлен e_μ однороден степени $m_1 + 2m_2 + \dots + nm_n$, а его лексикографически старший по переменным $x_1, \dots, x_n$ мономом является произведением старших мономов $x_1\dots x_{\mu_1}$ из e_{μ_1}, $x_1\dots x_{\mu_2}$ из e_{μ_2} и т. д. вплоть до $x_1\dots x_{\mu_n}$ из e_{μ_n}. Это произведение является результатом перемножения переменных x_i, вписанных в клетки диаграммы Юнга μ так, что номер переменной совпадает с номером столбца, в котором она стоит, и равно $x_1^{\mu_1^t}\dots x_n^{\mu_n^t}$, где $\mu^t = (\mu_1^t, \dots, \mu_n^t)$ — транспонированная к μ диаграмма Юнга[2]. Таким образом, разложение многочлена e_μ по базису (5-19) имеет вид:

$$e_\mu = m_{\mu^t} + (\text{лексикографически младшие члены}). \tag{5-21}$$

Если линейно упорядочить все диаграммы λ из d клеток и не более, чем n строк по лексикографическому возрастанию наборов чисел $(\lambda_1, \dots, \lambda_n)$, а все диаграммы μ из d клеток и не более, чем n столбцов — по лексикографическому возрастанию наборов чисел $(\mu_1^t, \dots, \mu_n^t)$, равных длинам строк транспонированных диаграмм μ^t, то согласно формуле (5-21) матрица перехода от многочленов e_μ к многочленам m_μ окажется верхней унитреугольной. В прим. 5.16 на стр. 93 мы видели, что такая матрица обратима в алгебре целочисленных матриц. Тем самым, по предл. 5.6 многочлены $e_\mu = e_1^{m_1}\dots e_n^{m_n}$, где $m_1 + 2m_2 + \dots + nm_n = d$, тоже составляют

[1] См. прим. 0.3 на стр. 8.

[2] Её строками являются столбцы диаграммы μ также, как при транспонировании матриц.

базис модуля однородных симметрических многочленов степени d над $\mathbb{Z}$. Это означает, что любой симметрический многочлен единственным образом представляется в виде многочлена от элементарных симметрических многочленов $e_1, \dots, e_n$. Иначе говоря, алгебра симметрических многочленов совпадает с алгеброй многочленов $\mathbb{Z}[e_1, \dots, e_n]$.

Пример 5.18 (дискриминант)
Дискриминантом приведённого многочлена $f(x) = t^n + a_1 t^{n-1} + \dots + a_n = \prod_{i=1}^{n}(x - \alpha_i)$ называется произведение $\Delta_f = \prod_{i<j}(\alpha_i - \alpha_j)^2$ квадратов разностей его корней, вычисленное в любом кольце, над которым f полностью раскладывается на линейные множители. Будучи симметрическим многочленом от корней, Δ_f является многочленом от $e_i(\alpha_1, \dots, \alpha_n) = (-1)^i a_i$, т. е. многочленом от коэффициентов уравнения. При этом $\Delta_f = 0$ если и только если f не сепарабелен. Так, дискриминант квадратного трёхчлена $f(x) = x^2 + px + q = (x - \alpha_1)(x - \alpha_2)$ равен $(\alpha_1 - a_2)^2 = (\alpha_1 + \alpha_2)^2 - 4\alpha_1\alpha_2 = p^2 - 4q$. Он зануляется если и только если f является полным квадратом линейного двучлена, и если $\Delta_f = \delta^2$ сам является квадратом, то корни f находятся из равенств $\alpha_1 + \alpha_2 = -p$, $\alpha_1 - \alpha_2 = \pm\delta$.

Упражнение 5.29. Вычислите дискриминант кубического трёхчлена $x^3 + px + q$.

5.3.3. Матрицы линейных отображений. Пусть K-модули N и M линейно порождаются наборами векторов $\boldsymbol{u} = (u_1, \dots, u_n)$ и $\boldsymbol{w} = (w_1, \dots, w_m)$ соответственно. Всякое K-линейное отображение $F\colon N \to M$ однозначно задаётся набором $F(\boldsymbol{u}) \stackrel{\text{def}}{=} \big(F(u_1), \dots, F(u_n)\big)$ своих значений на порождающих векторах и действует на произвольный вектор $v = \boldsymbol{u}\boldsymbol{x}$, где $\boldsymbol{x} \in K^n$ — столбец коэффициентов линейного выражения вектора v через образующие $\boldsymbol{u}$, по правилу

$$F(\boldsymbol{u}\boldsymbol{x}) = F\Big(\sum_{i=1}^{n} u_i x_i\Big) = \sum_{i=1}^{n} F(u_i)\, x_i = F(\boldsymbol{u})\boldsymbol{x}\,. \tag{5-22}$$

Матрица перехода от набора векторов $F(\boldsymbol{u})$ к образующим $\boldsymbol{w}$ модуля M обозначается

$$F_{\boldsymbol{w}\boldsymbol{u}} = C_{\boldsymbol{w}\,F(\boldsymbol{u})} \in \mathrm{Mat}_{m\times n}(K)$$

и называется *матрицей отображения*[1] F в образующих $\boldsymbol{w}$ и $\boldsymbol{u}$. Её j-й столбец состоит из коэффициентов линейного выражения вектора $F(u_j)$ через векторы $\boldsymbol{w}$. Согласно (5-22) произвольный вектор $v = \boldsymbol{u}\boldsymbol{x} \in N$, выражающийся через образующие $\boldsymbol{u}$ со столбцом коэффициентов $\boldsymbol{x}$, переводится отображением F в вектор $F(v) = \boldsymbol{w}F_{\boldsymbol{w}\boldsymbol{u}}\boldsymbol{x} \in M$, который выражается через образующие $\boldsymbol{w}$ со столбцом коэффициентов $F_{\boldsymbol{w}\boldsymbol{u}}\boldsymbol{x}$.

Вычисление (5-22) также показывает, что для любого набора векторов $\boldsymbol{v} = (v_1, \dots, v_k)$ в N, любой матрицы $A \in \mathrm{Mat}_{\ell\times k}(K)$ и любого K-линейного отображения $F\colon N \to M$ выполняется равенство $F(\boldsymbol{v}A) = F(\boldsymbol{v})A$.

Если K-модуль L порождается векторами $\boldsymbol{v} = (v_1, \dots, v_\ell)$ и K-линейные отображения

$$F\colon N \to L \quad \text{и} \quad G\colon L \to M$$

имеют матрицы $F_{\boldsymbol{v}\boldsymbol{u}}$ и $G_{\boldsymbol{w}\boldsymbol{v}}$, соответственно, в образующих $\boldsymbol{v}$, $\boldsymbol{u}$ и в образующих $\boldsymbol{w}$, $\boldsymbol{v}$, то композиция $H = GF\colon N \to M$ имеет в образующих $\boldsymbol{w}$, $\boldsymbol{u}$ матрицу $H_{\boldsymbol{w}\boldsymbol{u}} = G_{\boldsymbol{w}\boldsymbol{v}}F_{\boldsymbol{v}\boldsymbol{u}}$, поскольку

$$H(\boldsymbol{u}) = G\big(F(\boldsymbol{u})\big) = G\big(\boldsymbol{v}F_{\boldsymbol{v}\boldsymbol{u}}\big) = G(\boldsymbol{v})F_{\boldsymbol{v}\boldsymbol{u}} = \boldsymbol{w}G_{\boldsymbol{w}\boldsymbol{v}}F_{\boldsymbol{v}\boldsymbol{u}}\,.$$

[1] Ср. с n° 5.2.1 на стр. 90.

Предостережение 5.3. (некорректность обозначения $F_{\boldsymbol{wu}}$) Если образующие $\boldsymbol{w}$ линейно зависимы, то как и в n° 5.3.2, матрица $F_{\boldsymbol{wu}}$ линейного отображения F определяется образующими $\boldsymbol{w}$ и $\boldsymbol{u}$ не однозначно, поскольку набор векторов $F(\boldsymbol{u})$ имеет много разных линейных выражений через векторы $\boldsymbol{w}$. Предыдущие формулы означают при этом, что если задано какое-то выражение $v = \boldsymbol{ux}$ вектора v через образующие $\boldsymbol{u}$, то столбец коэффициентов $\boldsymbol{y} = F_{\boldsymbol{wu}}\boldsymbol{x}$ даёт одно из возможных линейных выражений $F(v) = \boldsymbol{wy}$ вектора $F(v)$ через образующие $\boldsymbol{w}$ и что получить одну из возможных матриц для композиции отображений можно перемножив какие-нибудь из матриц этих отображений в том же порядке, в каком берётся композиция.

Предостережение 5.4. (не все матрицы являются матрицами гомоморфизмов) Если образующие $\boldsymbol{u}$ линейно зависимы, то матрица $F_{\boldsymbol{wu}}$ не может быть произвольной: для любого линейного соотношения $\boldsymbol{ux} = 0$ между векторами $\boldsymbol{u}$ в N в модуле M должно выполняться соотношение

$$0 = F(0) = F(\boldsymbol{ux}) = \boldsymbol{w}F_{\boldsymbol{wu}}\boldsymbol{x}\,,$$

т. е. отображение $\boldsymbol{x} \mapsto F_{\boldsymbol{wu}}\boldsymbol{x}$ должно переводить коэффициенты любого линейного соотношения между образующими $\boldsymbol{u}$ в коэффициенты линейного соотношения между образующими $\boldsymbol{w}$. Наоборот, если матрица $F_{\boldsymbol{wu}}$ обладает этим свойством, то правило $\boldsymbol{ux} \mapsto \boldsymbol{w}\,F_{\boldsymbol{wu}}\boldsymbol{x}$ корректно задаёт K-линейное отображение $N \to M$, поскольку равенство $\boldsymbol{ux_1} = \boldsymbol{ux_2}$ означает, что $\boldsymbol{u}(\boldsymbol{x_1} - \boldsymbol{x_2}) = 0$, откуда $\boldsymbol{w}F_{\boldsymbol{wu}}(\boldsymbol{x_1} - \boldsymbol{x_2}) = 0$, и значит, $\boldsymbol{w}F_{\boldsymbol{wu}}\boldsymbol{x_1} = \boldsymbol{w}F_{\boldsymbol{wu}}\boldsymbol{x_2}$. Мы получаем

Предложение 5.7
Если модули $N = K^n/R_N$ и $M = K^m/R_M$ заданы при помощи образующих и соотношений, как в прим. 5.12 на стр. 88, то матрица $A \in \mathrm{Mat}_{m\times n}(K)$ тогда и только тогда является матрицей некоторого линейного отображения $F\colon N \to M$, когда для любого столбца $x \in R_N$ столбец $Ax \in R_M$. Две такие матрицы A и B задают одинаковые отображения $N \to M$ если и только если $(A - B)x \in R_M$ для всех $x \in K^n$. □

Пример 5.19 (гомоморфизмы между аддитивными группами вычетов)
Как мы уже отмечали в прим. 5.4 на стр. 82, любые две абелевы группы A и B могут рассматриваться как модули над кольцом $\mathbb{Z}$.

Упражнение 5.30. Убедитесь, что отображение $A \to B$ является гомоморфизмом абелевых групп[1] если и только если оно $\mathbb{Z}$-линейно.

В аддитивной группе вычетов $\mathbb{Z}/(m)$, рассматриваемой как $\mathbb{Z}$-модуль, результатом умножения класса $[k]_m \in \mathbb{Z}/(m)$ на число $z \in \mathbb{Z}$ является класс $[zk]_m$. Поэтому класс $[1]_m$ порождает $\mathbb{Z}/(m)$ над $\mathbb{Z}$ и отображение факторизации $\mathbb{Z} \twoheadrightarrow \mathbb{Z}/(m)$, $z \mapsto [z]_m$, является сюръективным гомоморфизмом $\mathbb{Z}$-модулей. Таким образом, $\mathbb{Z}/(m)$ является фактором свободного модуля $\mathbb{Z}$ по подмодулю соотношений $R = (m) \subset \mathbb{Z}$, который тоже свободен с базисом m. По предл. 5.7 каждое $\mathbb{Z}$-линейное отображение $\mathbb{Z}/(n) \to \mathbb{Z}/(m)$ получается из некоторого $\mathbb{Z}$-линейного отображения $\mathbb{Z} \to \mathbb{Z}$, отправляющего n в подмодуль $(m) \subset \mathbb{Z}$. Но $\mathrm{End}_{\mathbb{Z}}(\mathbb{Z}) \simeq \mathrm{Mat}_1(\mathbb{Z}) \simeq \mathbb{Z}$, и числу $a \in \mathbb{Z}$ отвечает при этом отождествлении эндоморфизм умножения на $a\colon z \mapsto az$. Так как $an \in (m)$ если и только если an является общим кратным m и n, мы заключаем, что $a = k\,\mathrm{нок}(m,n)/n$, где $k \in \mathbb{Z}$ — любое. Два таких числа $a_1 = k_1\,\mathrm{нок}(m,n)/n$ и $a_2 = k_2\,\mathrm{нок}(m,n)/n$ задают одинаковые гомоморфизмы $\mathbb{Z}/(n) \to \mathbb{Z}/(m)$ если и только если они одинаково действуют на образующую $[1]_n$, т. е. тогда и только тогда, когда $[a_1]_m = [a_2]_m$. Поскольку $(k_1 - k_2)\,\mathrm{нок}(m,n)/n$

[1] См. n° 1.5 на стр. 30.

делится на m если и только если $k_1 - k_2$ делится на $mn/\text{нок}(m,n) = \text{нод}(m,n)$, мы заключаем, что $\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}/(n), \mathbb{Z}/(m)) \simeq \mathbb{Z}/(\text{нод}(m,n))$. При этом изоморфизме классу $[k] \in \mathbb{Z}/(\text{нод}(m,n))$ отвечает гомоморфизм $\mathbb{Z}/(n) \to \mathbb{Z}/(m)$, $[z]_n \mapsto [kz\ \text{нок}(n,m)/n]_m$. В частности, для всех n, m

$$\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}/(n), \mathbb{Z}/(m)) \simeq \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}/(m), \mathbb{Z}/(n))\,,$$

и если m и n взаимно просты, то $\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}/(n), \mathbb{Z}/(m)) \simeq \mathbb{Z}/(1) = 0$.

Пример 5.20 (матрицы гомоморфизмов свободных модулей)
Если оба модуля N и M свободны и наборы векторов $\boldsymbol{u}$ и $\boldsymbol{w}$ являются их базисами, то, как мы видели в n° 5.2.1 на стр. 90, сопоставление K-линейному отображению $F : N \to M$ его матрицы $F_{\boldsymbol{wu}}$ в этих базисах задаёт K-линейный изоморфизм $\operatorname{Hom}_K(N,M) \xrightarrow{\sim} \operatorname{Mat}_{m\times n}(K)$, $F \mapsto F_{\boldsymbol{wu}}$. В других базисах $\boldsymbol{e} = \boldsymbol{w}\,C_{\boldsymbol{we}}$ и $\boldsymbol{f} = \boldsymbol{u}\,C_{\boldsymbol{uf}}$ матрица гомоморфизма F примет вид

$$F_{\boldsymbol{fe}} = C_{\boldsymbol{fu}} F_{\boldsymbol{uw}} C_{\boldsymbol{we}} = C^{-1}_{\boldsymbol{uf}} F_{\boldsymbol{u}} C_{\boldsymbol{we}} = C_{\boldsymbol{fu}} F_{\boldsymbol{u}} C^{-1}_{\boldsymbol{ew}}\,, \tag{5-23}$$

поскольку $F(\boldsymbol{e}) = F(\boldsymbol{w}\,C_{\boldsymbol{we}}) = F(\boldsymbol{w})\,C_{\boldsymbol{we}} = \boldsymbol{u}\,F_{\boldsymbol{uw}} C_{\boldsymbol{uw}} = \boldsymbol{f}\,C_{\boldsymbol{fu}} F_{\boldsymbol{uw}} C_{\boldsymbol{uw}}$.

Пример 5.21 (матрицы эндоморфизмов)
Пусть модуль M свободен и набор векторов $\boldsymbol{u}$ составляет его базис. Матрица $F_{\boldsymbol{uu}}$ линейного эндоморфизма $F : M \to M$ в базисах $\boldsymbol{u}$ и $\boldsymbol{u}$ обозначается просто $F_{\boldsymbol{u}}$ и называется *матрицей эндоморфизма* F в базисе $\boldsymbol{u}$. По формуле (5-23) любом другом базисе $\boldsymbol{w} = \boldsymbol{u}\,C_{\boldsymbol{uw}}$ матрица оператора F имеет вид

$$F_{\boldsymbol{w}} = C_{\boldsymbol{wu}} F_{\boldsymbol{u}} C_{\boldsymbol{uw}} = C^{-1}_{\boldsymbol{uw}} F_{\boldsymbol{u}} C_{\boldsymbol{uw}} = C_{\boldsymbol{wu}} F_{\boldsymbol{u}} C^{-1}_{\boldsymbol{wu}}\,. \tag{5-24}$$

§6. Конечно порождённые модули над областью главных идеалов

Всюду в этом параграфе K означает произвольную область главных идеалов. Все рассматриваемые нами K-модули по умолчанию предполагаются конечно порождёнными. Под свободным K-модулем ранга нуль понимается нулевой K-модуль.

6.1. Метод Гаусса. Будем называть *элементарным преобразованием строк* прямоугольной матрицы $A \in \mathrm{Mat}_{m\times n}(K)$ замену каких-нибудь двух строк r_i и r_j их линейными комбинациями

$$r_i' = \alpha r_i + \beta r_j \quad \text{и} \quad r_j' = \gamma r_i + \delta r_j$$

с обратимым определителем $\Delta = \alpha\delta - \beta\gamma \in K$. В этом случае матрица преобразования

$$\begin{pmatrix} r_i \\ r_j \end{pmatrix} \mapsto \begin{pmatrix} r_i' \\ r_j' \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} r_i \\ r_j \end{pmatrix}$$

обратима[1], и исходные строки r_i и r_j восстанавливаются из преобразованных строк r_i' и r_j' по формулам $r_i' = (\delta r_i - \beta r_j)/\Delta$ и $r_j' = (-\gamma r_i + \alpha r_j)/\Delta$.

Упражнение 6.1. Убедитесь в этом.

В частности, прибавление к одной строке другой строки, умноженной на произвольное число $x \in K$, а также перестановка двух строк местами и умножение строк на обратимые элементы $s_1, s_2 \in K$ тоже являются элементарными преобразованиями, задаваемыми 2×2 матрицами

$$\begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \text{и} \quad \begin{pmatrix} s_1 & 0 \\ 0 & s_2 \end{pmatrix}.$$

Элементарное преобразование не меняет линейной оболочки строк матрицы A и заключается в умножении A слева на обратимую $m \times m$ матрицу L, которая получается из единичной $m \times m$ матрицы тем же самым элементарным преобразованием строк, что происходит в матрице A.

Симметричным образом, *элементарным преобразованием столбцов* матрицы A мы называем замену каких-нибудь двух столбцов c_i и c_j их линейными комбинациями $c_i' = \alpha c_i + \beta c_j$ и $c_j' = \gamma c_i + \delta c_j$ с обратимым в K определителем $\alpha\delta - \beta\gamma$. Такое преобразование не меняет линейной оболочки столбцов матрицы A и достигается умножением A справа на обратимую $n \times n$ матрицу R, которая получается из единичной $n \times n$ матрицы тем же самым элементарным преобразованием столбцов, что производится в матрице A. Прибавление к одному из столбцов другого, умноженного на произвольное число $x \in K$, а также перестановка столбцов местами и умножение столбцов на обратимые элементы из K являются частными примерами элементарных преобразований.

Лемма 6.1
В области главных идеалов K любую пару ненулевых элементов (a, b), стоящих в одной строке (соотв. в одном столбце) матрицы $A \in \mathrm{Mat}_{m\times n}(K)$, можно подходящим элементарным преобразованием содержащих их столбцов (соотв. строк) заменить парой $(d, 0)$, где $d = \text{нод}(a, b)$.

Доказательство. Запишем $d = \text{нод}(a, b)$ как $d = ax + by$, и пусть $a = da'$, $b = db'$. Тогда $a'x + b'y = 1$ и $a'b - b'a = 0$. Поэтому

$$(a, b) \cdot \begin{pmatrix} x & -b' \\ y & a' \end{pmatrix} = (d, 0) \quad \text{и} \quad \begin{pmatrix} x & y \\ -b' & a' \end{pmatrix} \cdot \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} d \\ 0 \end{pmatrix},$$

[1] См. прим. 5.15 на стр. 92.

где $\det\begin{pmatrix} x & -b' \\ y & a' \end{pmatrix} = \det\begin{pmatrix} x & y \\ -b' & a' \end{pmatrix} = 1$. □

Теорема 6.1
В области главных идеалов K любая матрица $A \in \mathrm{Mat}_{m\times n}(K)$ конечным числом элементарных преобразований строк и столбцов преобразуется в матрицу $D_A = (d_{ij})$, у которой $d_{ij} = 0$ при $i \neq j$ и $d_{ii} \mid d_{jj}$ при $i < j$, где мы считаем, что $d \mid 0$ для всех $d \in K$, но $0 \nmid d$ при $d \neq 0$.

Доказательство. Если $A = 0$, то доказывать нечего. Если $A \neq 0$, то перестановками строк и столбцов добьёмся, чтобы $a_{11} \neq 0$. Если все элементы матрицы A делятся на a_{11}, то вычитая из всех строк подходящие кратности первой строки, а из всех столбцов — подходящие кратности первого столбца, добьёмся того, чтобы все элементы за исключением a_{11} в первом столбце и первой строке занулились. При этом все элементы матрицы останутся делящимися на a_{11}, и можно заменить A на матрицу размера $(m-1)\times(n-1)$, дополнительную к первой строке и первому столбцу матрицы A, после чего повторить процедуру.

Пусть в матрице A есть элемент a, не делящийся на a_{11}, и $d = \text{нод}(a, a_{11})$. Ниже мы покажем, что в этом случае можно элементарными преобразованиями перейти к новой матрице A' с $a'_{11} = d$. Так как $(a_{11}) \subsetneq (d)$, главный идеал, порождённый левым верхним угловым элементом матрицы, при таком переходе строго увеличится. Поскольку в области главных идеалов не существует бесконечно возрастающих цепочек строго вложенных друг в друга идеалов, после конечного числа таких переходов мы получим матрицу, все элементы которой делятся на a_{11}, и к этой матрице будут применимы предыдущие рассуждения.

Если не делящийся на a_{11} элемент a стоит в первой строке или первом столбце, достаточно заменить пару (a_{11}, a) на $(d, 0)$ по лем. 6.1. Если все элементы первой строки и первого столбца делятся на a_{11}, а не делящийся на a_{11} элемент a стоит строго ниже и правее a_{11}, то мы, как и выше, сначала занулим все элементы первой строки и первого столбца за исключением самого a_{11}, вычитая из всех строк подходящие кратности первой строки, а из всех столбцов — подходящие кратности первого столбца. К элементу a при этом будут добавляться числа, кратные a_{11}, и $\text{нод}(a, a_{11})$ не изменится. Далее, прибавим ту строку, где стоит a, к первой строке и получим в ней копию элемента a. Наконец, заменим пару (a_{11}, a) на $(d, 0)$ по лем. 6.1. □

6.1.1. Инвариантные множители и нормальная форма Смита. Ниже, в n° 6.3.4 на стр. 118 мы покажем, что «диагональная» матрица D_A, в которой $d_{ij} = 0$ при $i \neq j$ и $d_{ii} \mid d_{jj}$ при $i < j$, с точностью до умножения её элементов на обратимые элементы из K не зависит от выбора последовательности элементарных преобразований, приводящих матрицу A к такому виду. По этой причине диагональные элементы d_{ii} матрицы D_A называются *инвариантными множителями* матрицы A, а сама диагональная матрица D_A — *нормальной формой Смита* матрицы A.

Так как каждое элементарное преобразование строк (соотв. столбцов) матрицы A является результатом умножения матрицы A слева (соотв. справа) на квадратную обратимую матрицу, которая получается из единичной матрицы E ровно тем же преобразованием, что совершается в матрице A, мы заключаем, что $D_A = LAR$, где $L = L_\ell \dots L_2 L_1$ и $R = R_1 R_2 \dots R_r$ — обратимые матрицы размеров $m\times m$ и $n\times n$, являющиеся произведениями обратимых матриц L_i и R_j, осуществляющих последовательные элементарные преобразования строк и столбцов матрицы A. Мы будем называть L и R *матрицами перехода* от матрицы A к её нормальной форме Смита. Так как $L = L_\ell \dots L_1 E$ и $R = E R_1 \dots R_r$, матрицы L и R получаются из единичных матриц размеров $m\times m$ и $n\times n$ теми же цепочками элементарных преобразований строк и соответственно столбцов, которые производились с матрицей A. Поэтому для явного отыскания матриц L

и R следует приписать к матрице $A \in \mathrm{Mat}_{m\times n}(K)$ справа и снизу единичные матрицы размеров $m \times m$ и $n \times n$ так, что получится Г-образная таблица вида

$$\begin{array}{|c|c|}\hline A & E \\ \hline E & \\ \cline{1-1}\end{array},$$

и в процессе приведения матрицы A к диагональному виду осуществлять элементарные преобразования строк и столбцов сразу во всей Г-образной таблице. В результате на выходе получится Г-образная таблица

$$\begin{array}{|c|c|}\hline D_A & L \\ \hline R & \\ \cline{1-1}\end{array}.$$

Пример 6.1
Вычислим нормальную форму Смита и матрицы перехода к ней для целочисленной матрицы

$$A = \begin{pmatrix} -9 & -18 & 15 & -24 & 24 \\ 15 & 30 & -27 & 42 & -36 \\ -6 & -12 & 6 & -12 & 24 \\ 31 & 62 & -51 & 81 & -87 \end{pmatrix} \in \mathrm{Mat}_{4x5}(\mathbb{Z}).$$

Составляем Г-образную матрицу

$$\begin{array}{|c|c|}\hline A & E \\ \hline E & \\ \cline{1-1}\end{array} = \begin{array}{|rrrrr|cccc|}\hline -9 & -18 & 15 & -24 & 24 & 1 & 0 & 0 & 0 \\ 15 & 30 & -27 & 42 & -36 & 0 & 1 & 0 & 0 \\ -6 & -12 & 6 & -12 & 24 & 0 & 0 & 1 & 0 \\ 31 & 62 & -51 & 81 & -87 & 0 & 0 & 0 & 1 \\ \hline 1 & 0 & 0 & 0 & 0 & & & & \\ 0 & 1 & 0 & 0 & 0 & & & & \\ 0 & 0 & 1 & 0 & 0 & & & & \\ 0 & 0 & 0 & 1 & 0 & & & & \\ 0 & 0 & 0 & 0 & 1 & & & & \\ \cline{1-5}\end{array}.$$

Прибавим к 4-й строке третью, умноженную на 5 и переставим полученную строку наверх:

$$\begin{array}{|rrrrr|cccc|}\hline 1 & 2 & -21 & 21 & 33 & 0 & 0 & 5 & 1 \\ -9 & -18 & 15 & -24 & 24 & 1 & 0 & 0 & 0 \\ 15 & 30 & -27 & 42 & -36 & 0 & 1 & 0 & 0 \\ -6 & -12 & 6 & -12 & 24 & 0 & 0 & 1 & 0 \\ \hline 1 & 0 & 0 & 0 & 0 & & & & \\ 0 & 1 & 0 & 0 & 0 & & & & \\ 0 & 0 & 1 & 0 & 0 & & & & \\ 0 & 0 & 0 & 1 & 0 & & & & \\ 0 & 0 & 0 & 0 & 1 & & & & \\ \cline{1-5}\end{array}.$$

Теперь обнулим 1-ю строку и 1-й столбец левой матрицы вне левого верхнего угла, прибавив

ко всем строкам и столбцам надлежащие кратности 1-й строки и 1-го столбца:

$$\left(\begin{array}{ccccc|cccc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 5 & 1 \\ 0 & 0 & -174 & 165 & 321 & 1 & 0 & 45 & 9 \\ 0 & 0 & 288 & -273 & -531 & 0 & 1 & -75 & -15 \\ 0 & 0 & -120 & 114 & 222 & 0 & 0 & 31 & 6 \\ \hline 1 & -2 & 21 & -21 & -33 & & & & \\ 0 & 1 & 0 & 0 & 0 & & & & \\ 0 & 0 & 1 & 0 & 0 & & & & \\ 0 & 0 & 0 & 1 & 0 & & & & \\ 0 & 0 & 0 & 0 & 1 & & & & \end{array}\right).$$

Делаем второй столбец пятым, а к 3-му столбцу прибавляем 4-й:

$$\left(\begin{array}{ccccc|cccc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 5 & 1 \\ 0 & -9 & 165 & 321 & 0 & 1 & 0 & 45 & 9 \\ 0 & 15 & -273 & -531 & 0 & 0 & 1 & -75 & -15 \\ 0 & -6 & 114 & 222 & 0 & 0 & 0 & 31 & 6 \\ \hline 1 & 0 & -21 & -33 & -2 & & & & \\ 0 & 0 & 0 & 0 & 1 & & & & \\ 0 & 1 & 0 & 0 & 0 & & & & \\ 0 & 1 & 1 & 0 & 0 & & & & \\ 0 & 0 & 0 & 1 & 0 & & & & \end{array}\right).$$

Вычитаем из 2-й строки 4-ю:

$$\left(\begin{array}{ccccc|cccc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 5 & 1 \\ 0 & -3 & 51 & 99 & 0 & 1 & 0 & 14 & 3 \\ 0 & 15 & -273 & -531 & 0 & 0 & 1 & -75 & -15 \\ 0 & -6 & 114 & 222 & 0 & 0 & 0 & 31 & 6 \\ \hline 1 & 0 & -21 & -33 & -2 & & & & \\ 0 & 0 & 0 & 0 & 1 & & & & \\ 0 & 1 & 0 & 0 & 0 & & & & \\ 0 & 1 & 1 & 0 & 0 & & & & \\ 0 & 0 & 0 & 1 & 0 & & & & \end{array}\right).$$

Все элементы 3×4 матрицы, стоящей в строках со 2-й по 4-ю и столбцах со 2-го по 5-й, делятся на 3. Поэтому мы обнуляем в этой матрице верхнюю строку и левый столбец, вычитая из 3-й и 4-й строк подходящие кратности 2-й строки, а потом из 3-го и 4-го столбцов — подходящие кратности 2-го:

$$\left(\begin{array}{ccccc|cccc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 5 & 1 \\ 0 & -3 & 0 & 0 & 0 & 1 & 0 & 14 & 3 \\ 0 & 0 & -18 & -36 & 0 & 5 & 1 & -5 & 0 \\ 0 & 0 & 12 & 24 & 0 & -2 & 0 & 3 & 0 \\ \hline 1 & 0 & -21 & -33 & -2 & & & & \\ 0 & 0 & 0 & 0 & 1 & & & & \\ 0 & 1 & 17 & 33 & 0 & & & & \\ 0 & 1 & 18 & 33 & 0 & & & & \\ 0 & 0 & 0 & 1 & 0 & & & & \end{array}\right).$$

Теперь прибавляем к 3-й строке 4-ю:

$$\left(\begin{array}{rrrrr|rrrr} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 5 & 1 \\ 0 & -3 & 0 & 0 & 0 & 1 & 0 & 14 & 3 \\ 0 & 0 & -6 & -12 & 0 & 3 & 1 & -2 & 0 \\ 0 & 0 & 12 & 24 & 0 & -2 & 0 & 3 & 0 \\ \hline 1 & 0 & -21 & -33 & -2 & & & & \\ 0 & 0 & 0 & 0 & 1 & & & & \\ 0 & 1 & 17 & 33 & 0 & & & & \\ 0 & 1 & 18 & 33 & 0 & & & & \\ 0 & 0 & 0 & 1 & 0 & & & & \end{array}\right)$$

и видим, что можно занулить все недиагональные элементы исходной матрицы, прибавляя к 4-й строке удвоенную 3-ю и вычитая из 4-го столбца удвоенный 3-й:

$$\left(\begin{array}{rrrrr|rrrr} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 5 & 1 \\ 0 & -3 & 0 & 0 & 0 & 1 & 0 & 14 & 3 \\ 0 & 0 & -6 & 0 & 0 & 3 & 1 & -2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 4 & 2 & -1 & 0 \\ \hline 1 & 0 & -21 & 9 & -2 & & & & \\ 0 & 0 & 0 & 0 & 1 & & & & \\ 0 & 1 & 17 & -1 & 0 & & & & \\ 0 & 1 & 18 & -3 & 0 & & & & \\ 0 & 0 & 0 & 1 & 0 & & & & \end{array}\right).$$

Таким образом, инвариантные множители матрицы A суть $1, -3, -6, 0$ и

$$L = \begin{pmatrix} 0 & 0 & 5 & 1 \\ 1 & 0 & 14 & 3 \\ 3 & 1 & -2 & 0 \\ 4 & 2 & -1 & 0 \end{pmatrix}, \quad R = \begin{pmatrix} 1 & 0 & -21 & 9 & -2 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 17 & -1 & 0 \\ 0 & 1 & 18 & -3 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}, \quad D_A = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & -3 & 0 & 0 & 0 \\ 0 & 0 & -6 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Упражнение 6.2. Проверьте равенство $LAR = D_A$ прямым вычислением.

6.1.2. Отыскание обратной матрицы. Пусть квадратная матрица $A \in \mathrm{Mat}_n(K)$ обратима. Тогда и любая матрица вида $B = LAR$, где $L, R \in \mathrm{Mat}_n(K)$ обратимы, тоже обратима, ибо матрица $R^{-1}A^{-1}L^{-1}$ обратна к B. В частности, обратимы все матрицы, которые получаются из A элементарными преобразованиями строк и столбцов, включая нормальную форму Смита D_A.

Упражнение 6.3. Убедитесь, что диагональная матрица обратима если и только если обратимы все её диагональные элементы.

Таким образом, матрица A обратима если и только если обратимы все её инвариантные множители, и в этом случае существуют такие обратимые матрицы $L = L_\ell \dots L_1$ и $R = R_1 \dots R_r$,

что $LAR = E$, а каждая из матриц L_ν, R_μ имеет вид

$$\begin{pmatrix} \ddots & & & & & & & \\ & 1 & & & & & & \\ & & \alpha & & & & \beta & \\ & & & 1 & & & & \\ & & & & \ddots & & & \\ & & & & & 1 & & \\ & & \gamma & & & & \delta & \\ & & & & & & & 1 \\ & & & & & & & & \ddots \end{pmatrix},$$

где на обозначенных многоточиями местах главной диагонали стоят единицы, в остальных местах — нули, а определитель $\alpha\beta - \beta\gamma \in K$ обратим. В этом случае $A = L^{-1}ER^{-1} = L^{-1}R^{-1}$, откуда $A^{-1} = RL = RLE$, а $E = RLA$, т. е. умножение слева на матрицу $RL = R_1 \dots R_r L_\ell \dots L_1$ задаёт цепочку элементарных преобразований строк, превращающую матрицу A в матрицу E, а матрицу E — в матрицу A^{-1}.

Упражнение 6.4. Покажите, что элементарными преобразованиями строк матрицы A можно превратить любой её ненулевой столбец в столбец, единственным ненулевым элементом которого является нод элементов исходного столбца матрицы A, и если этот элемент необратим, то и матрица A необратима.

Таким образом, чтобы выяснить, обратима ли $n \times n$ матрица A, и найти A^{-1}, если A обратима, следует элементарными преобразованиями строк и столбцов $n \times 2n$ матрицы $\left[\begin{array}{c|c} A & E \end{array}\right]$ попытаться получить в левой половине матрицу E, последовательно слева направо обнуляя в каждом столбце все элементы, кроме одного. Если в ходе вычислений матрица A превратится в заведомо необратимую матрицу, то и сама матрица A необратима. Ну а если удастся превратить матрицу A в матрицу E, то на выходе получится матрица $\left[\begin{array}{c|c} E & B \end{array}\right]$, в которой $B = A^{-1}$.

Пример 6.2

Выясним, обратима ли в $\mathrm{Mat}_4(\mathbb{Z})$ матрица

$$A = \begin{pmatrix} 1 & -3 & 2 & 2 \\ -3 & 9 & -6 & -5 \\ -1 & 4 & 0 & 2 \\ 3 & -7 & 11 & 12 \end{pmatrix}.$$

Приписываем к ней справа единичную матрицу:

$$\left[\begin{array}{rrrr|cccc} 1 & -3 & 2 & 2 & 1 & 0 & 0 & 0 \\ -3 & 9 & -6 & -5 & 0 & 1 & 0 & 0 \\ -1 & 4 & 0 & 2 & 0 & 0 & 1 & 0 \\ 3 & -7 & 11 & 12 & 0 & 0 & 0 & 1 \end{array}\right].$$

Обнуляем 1-й столбец вне левого верхнего угла, прибавляя ко всем строкам надлежащие кратности 1-й строки:

$$\left[\begin{array}{cccc|cccc} 1 & -3 & 2 & 2 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 3 & 1 & 0 & 0 \\ 0 & 1 & 2 & 4 & 1 & 0 & 1 & 0 \\ 0 & 2 & 5 & 6 & -3 & 0 & 0 & 1 \end{array}\right].$$

Теперь обнуляем верхний и нижний элементы 2-го столбца, прибавляя к верхней и нижней строкам надлежащие кратности 3-й строки, после чего переставляем 2-ю строку вниз:

$$\left(\begin{array}{cccc|cccc} 1 & 0 & 8 & 14 & 4 & 0 & 3 & 0 \\ 0 & 1 & 2 & 4 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & -2 & -5 & 0 & -2 & 1 \\ 0 & 0 & 0 & 1 & 3 & 1 & 0 & 0 \end{array}\right).$$

Обнуляем верхние два элемента 3-го столбца, прибавляя к верхним двум строкам надлежащие кратности 3-й строки:

$$\left(\begin{array}{cccc|cccc} 1 & 0 & 0 & 30 & 44 & 0 & 19 & -8 \\ 0 & 1 & 0 & 8 & 11 & 0 & 5 & -2 \\ 0 & 0 & 1 & -2 & -5 & 0 & -2 & 1 \\ 0 & 0 & 0 & 1 & 3 & 1 & 0 & 0 \end{array}\right).$$

Наконец, обнуляем 4-й столбец над нижней единицей, прибавляя к верхним трём строкам надлежащие кратности 4-й строки:

$$\left(\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & -46 & -30 & 19 & -8 \\ 0 & 1 & 0 & 0 & -13 & -8 & 5 & -2 \\ 0 & 0 & 1 & 0 & 1 & 2 & -2 & 1 \\ 0 & 0 & 0 & 1 & 3 & 1 & 0 & 0 \end{array}\right).$$

Таким образом, матрица A обратима и

$$A^{-1} = \begin{pmatrix} -46 & -30 & 19 & -8 \\ -13 & -8 & 5 & -2 \\ 1 & 2 & -2 & 1 \\ 3 & 1 & 0 & 0 \end{pmatrix}.$$

Упражнение 6.5. Проверьте прямым умножением двух матриц, что $AA^{-1} = E$.

6.1.3. Решение систем линейных уравнений. Система линейных уравнений

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n = b_2 \\ a_{31}x_1 + a_{32}x_2 + \ldots + a_{3n}x_n = b_3 \\ \qquad \ldots\ldots\ldots\ldots\ldots \\ a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n = b_m \end{cases} \tag{6-1}$$

на неизвестные $x_1, \ldots, x_n$ в матричных обозначениях записывается одним равенством $Ax = b$, в котором $A = \left(a_{ij}\right) \in \mathrm{Mat}_{m\times n}(K)$, а x и b обозначают столбцы высоты n и m, состоящие из неизвестных и правых частей уравнений (6-1). Как и выше, обозначим через $D_A = LAR$ нормальную форму Смита матрицы A. Умножая равенство $Ax = b$ слева на L и полагая $x = Ry$, где $y = R^{-1}x$ — новые переменные, получаем систему уравнений $D_A y = c$ на неизвестные y, в которой $c = Lb$ и матрица коэффициентов D_A диагональна, и которая равносильна (6-1) в том смысле, что между решениями обеих систем имеется K-линейная биекция $x = Ry$. В частности, система $D_A y = c$ совместна если и только если совместна исходная система (6-1).

Уравнения системы $D_A y = c$ имеют вид $d_{ii} y_i = c_i$. Такое уравнение не имеет решений, если и только если $d_{ii} \nmid c_i$. Если же $d_{ii} \mid c_i$, то при $d_{ii} = c_i = 0$ решениями уравнения являются все числа $y_i \in K$, а при $d_{ii} \neq 0$ уравнение имеет единственное решение $y_i = c_i / d_{ii}$.

Пусть $d_{ii} \neq 0$ при $i \leqslant r$ и $d_{jj} = 0$ при $j > r$. Мы заключаем, что система $D_A y = c$ несовместна если и только если $d_{ii} \nmid c_i$ хотя бы при одном $i \leqslant r$ или $c_j \neq 0$ хотя бы при одном $j > r$, и в этом случае исходная система (6-1) тоже несовместна. Если же система $D_A y = c$ совместна, то её решения имеют вид $y = w_0 + w$, где $w_0 = (c_1 / d_{11}, \ldots, c_r / d_{rr}, 0, \ldots, 0)^t$, а вектор $w \in K^n$ пробегает свободный подмодуль ранга $\min(m, n) - r$ с базисом из векторов

$$w_k = (0, \ldots, 0, 1, 0, \ldots, 0)^t, \text{ где 1 стоит на } (r+k)\text{-м месте,}$$

и в этом случае все решения исходной системы (6-1) имеют вид $x = u_0 + u$, где $u_0 = Rw_0$, а $u \in K^n$ пробегает свободный подмодуль ранга $\min(m, n) - r$ с базисом из векторов $u_k = Rw_k$.

Отметим, что столбец $c = Lb$ правых частей системы $D_A y = c$ получается из столбца b правых частей исходной системы (6-1) теми же преобразованиями строк, что производятся с матрицей A в процессе её приведения к виду D_A, а матрица R получается из единичной матрицы E теми же преобразованиями столбцов, что производятся с матрицей A в том же процессе. Поэтому для отыскания c и R можно составить Г-образную матрицу вида

A	b
E	

,

приведести A к нормальной форме Смита и получить на выходе

D_A	c
R	

.

Пример 6.3
Найдём все целые решения системы уравнений

$$\begin{cases} -65x_1 - 156x_2 + 169x_3 + 104x_4 = 117 \\ -143x_1 - 351x_2 + 364x_3 + 221x_4 = 195 \\ 52x_1 + 117x_2 - 143x_3 - 91x_4 = -156 \end{cases} \tag{6-2}$$

Для этого составим Г-образную таблицу из матрицы коэффициентов при неизвестных, к которой справа приписана матрица правых частей уравнений, а снизу — единичная матрица:

−65	−156	169	104	117
−143	−351	364	221	195
52	117	−143	−91	−156
1	0	0	0	
0	1	0	0	
0	0	1	0	
0	0	0	1	

.

Вычтем из 2-й строки 1-ю, умноженную на 2, и поменяем две верхние строки местами:

$$\left(\begin{array}{rrrr|r} -13 & -39 & 26 & 13 & -39 \\ -65 & -156 & 169 & 104 & 117 \\ 52 & 117 & -143 & -91 & -156 \end{array}\right) \left(\begin{array}{rrrr} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{array}\right).$$

Поскольку все элементы матрицы коэффициентов делятся на 13, зануляем в ней верхнюю строку и левый столбец, за исключением верхнего левого углового элемента, прибавляя ко 2-й и 3-й строкам надлежащие кратности 1-й строки, а ко 2-му, 3-му и 4-му столбцам — надлежащие кратности 1-го столбца:

$$\left(\begin{array}{rrrr|r} -13 & 0 & 0 & 0 & -39 \\ 0 & 39 & 39 & 39 & 312 \\ 0 & -39 & -39 & -39 & -312 \end{array}\right) \left(\begin{array}{rrrr} 1 & -3 & 2 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{array}\right).$$

Прибавляем к 3-й строке 2-ю, после чего вычитаем 2-й столбец из 3-го и 4-го:

$$\left(\begin{array}{rrrr|r} -13 & 0 & 0 & 0 & -39 \\ 0 & 39 & 0 & 0 & 312 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right) \left(\begin{array}{rrrr} 1 & -3 & 5 & 4 \\ 0 & 1 & -1 & -1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{array}\right).$$

Мы заключаем, что система (6-2) равносильна системе

$$\begin{cases} -13y_1 = -39 \\ 39y_2 = 312 \end{cases} \tag{6-3}$$

на *четыре* неизвестные $y_1, \dots, y_4$, через которые исходные неизвестные $x_1, \dots, x_4$ выражаются по формуле:

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 1 & -3 & 5 & 4 \\ 0 & 1 & -1 & -1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{pmatrix}. \tag{6-4}$$

Все решения системы (6-3) описываются формулой:

$$(y_1, y_2, y_3, y_4) = (3, 8, z_1, z_2), \quad \text{где} \quad z_1, z_2 \in \mathbb{Z} \text{ — любые.}$$

Решения исходной системы получаются из них по формуле (6-4):

$$(x_1, x_2, x_3, x_4) = (5z_1 + 4z_2 - 21, 8 - z_1 - z_2, z_1, z_2), \quad \text{где} \quad z_1, z_2 \in \mathbb{Z} \text{ — любые.}$$

6.2. Инвариантные множители. Как мы видели в прим. 5.12 на стр. 88, произвольный K-модуль M, линейно порождённый над K конечным набором векторов

$$\boldsymbol{w} = (w_1, \dots, w_m),$$

представляет собою фактор $M \simeq K^m / R_{\boldsymbol{w}}$ свободного координатного модуля K^m по подмодулю $R_{\boldsymbol{w}} \subset K^m$ линейных соотношений между порождающими векторами $\boldsymbol{w}$. Подмодуль $R_{\boldsymbol{w}}$ состоит из всех таких строк $(x_1, \dots, x_m) \in K^m$, что $x_1 w_1 + \dots + x_m w_m = 0$ в M, и является ядром эпиморфизма

$$\pi_{\boldsymbol{w}} : K^m \twoheadrightarrow M, \quad (x_1, \dots, x_m) \mapsto x_1 w_1 + \dots + x_m w_m . \tag{6-5}$$

Теорема 6.2
Каждый подмодуль N в свободном модуле F конечного ранга над областью главных идеалов K тоже свободен, и $\operatorname{rk} N \leqslant \operatorname{rk} F$.

Доказательство. Индукция по $m = \operatorname{rk} F$. При $m = 1$ модуль $N \simeq K$, и каждый ненулевой подмодуль $N \subset K$ представляет собою главный идеал $(d) \subset K$, который является свободным K-модулем ранга 1 с базисом d. Пусть теперь $m > 1$. Зафиксируем в F базис $e_1, \dots, e_m$ и будем записывать векторы из N строками их координат в этом базисе. Первые координаты всевозможных векторов $v \in N$ образуют идеал $(d) \subset K$. Если $d = 0$, подмодуль N содержится в свободном модуле ранга $m-1$ с базисом $e_2, \dots, e_m$. По индукции, такой модуль N свободен и $\operatorname{rk} N \leqslant (m-1)$. Если $d \neq 0$, обозначим через $u \in N$ какой-нибудь вектор с первой координатой d. Порождённый вектором u модуль Ku свободен ранга 1, поскольку равенство $xu = 0$ влечёт равенство $xd = 0$, возможное в целостном кольце K только при $x = 0$. Покажем, что $N = Ku \oplus N'$, где $N' \subset N$ — подмодуль, состоящий из векторов с нулевой первой координатой. Очевидно, что $Ku \cap N' = 0$. Если первая координата вектора $v \in N$ равна xd, то $v = xu + w$, где $w = v - xu \in N'$. Поэтому $N = Ku + N'$, и $N = Ku \oplus N'$ по предл. 5.2 на стр. 85. Модуль N' содержится в свободном модуле ранга $m-1$ с базисом $e_2, \dots, e_m$. По индукции он свободен и $\operatorname{rk} N' \leqslant (m-1)$. Поэтому $N = Ku \oplus N'$ тоже свободен и $\operatorname{rk} N = 1 + \operatorname{rk} N' \leqslant m$. □

Пример 6.4 (качественный анализ систем линейных уравнений)
Каждая матрица $A \in \operatorname{Mat}_{m\times n}(K)$ задаёт K-линейное отображение $F_A : K^n \to K^m$, $x \mapsto Ax$, переводящее стандартные базисные векторы $e_1, \dots, e_n \in K^n$ в столбцы матрицы A. Множество решений системы линейных уравнений $Ax = b$ является полным прообразом $F^{-1}(b)$ данного вектора $b \in K^m$ при отображении F_A. Если $b \notin \operatorname{im} F_A$, то этот прообраз пуст и система $Ax = b$ несовместна. Если $b \in \operatorname{im} F_A$, то $F_A^{-1}(b) = w + \ker F_A$ представляет собою сдвиг свободного модуля $\ker F_A \subset K^n$ на такой вектор $w \in K^n$, что $F(w) = b$. На языке уравнений ядро $\ker F_A$ является множеством решений системы однородных линейных уравнений $Ax = 0$ с теми же самыми левыми частями, что и система $Ax = b$. Наличие у такой системы ненулевого решения означает, что $\ker F_A \neq 0$, и в этом случае любая система $Ax = b$ либо несовместна, либо множество её решений является сдвигом свободного модуля положительного ранга, что согласуется с n° 6.1.3 на стр. 108.

Теорема 6.3 (теорема о взаимном базисе)
Пусть F — свободный модуль ранга m над областью главных идеалов K, и $N \subset F$ — произвольный его подмодуль. Тогда в модуле F существует такой базис $\boldsymbol{e} = (e_1, \dots, e_m)$, что подходящие кратности $\lambda_1 e_1, \dots, \lambda_n e_n$ первых $n = \operatorname{rk} N$ его базисных векторов составляют базис в N и $\lambda_i \mid \lambda_j$ при $i < j$.

Доказательство. Зафиксируем произвольные базисы $\boldsymbol{w} = (w_1, \dots, w_m)$ в F и $\boldsymbol{u} = \boldsymbol{w}\,C_{\boldsymbol{wu}}$ в N. Последний существует по теор. 6.2 и состоит из $n \leqslant m$ векторов. Обозначим через $D = LC_{\boldsymbol{wu}}R$ нормальную форму Смита матрицы перехода $C_{\boldsymbol{wu}}$. Поскольку матрицы L и R обратимы, набор векторов $\boldsymbol{e} = \boldsymbol{w}\,L^{-1}$ является базисом в F, а набор векторов $\boldsymbol{v} = \boldsymbol{u}\,R$ — базисом в N. Так как

$$\boldsymbol{v} = \boldsymbol{u}\,R = \boldsymbol{w}\,C_{\boldsymbol{wu}}R = \boldsymbol{e}\,LC_{\boldsymbol{wu}}R = \boldsymbol{e}\,D$$

векторы $v_i = d_{ii}e_i$ базиса $\boldsymbol{v}$ имеют предписанный теоремой вид, в котором $\lambda_i = d_{ii}$ суть инвариантные множители матрицы $C_{\boldsymbol{wu}}$. □

Определение 6.1
Множители $\lambda_1, \dots, \lambda_n$ из теор. 6.3 называются *инвариантными множителями* подмодуля N в свободном модуле F, а построенные в теор. 6.3 базисы $e_1, \dots, e_m$ в F и $\lambda_1 e_1, \dots, \lambda_n e_n$ в N называются *взаимными базисами* свободного модуля F и его подмодуля N. В n° 6.3.4 на стр. 118 ниже мы покажем, что множители λ_i не зависят от выбора взаимных базисов, что оправдывает эпитет «инвариантные» в их названии.

Пример 6.5
Построим взаимные базисы целочисленной решётки $\mathbb{Z}^3$ и её подрешётки $L \subset \mathbb{Z}^3$, порождённой столбцами матрицы

$$A = \begin{pmatrix} 126 & 51 & 72 & 33 \\ 30 & 15 & 18 & 9 \\ 60 & 30 & 36 & 18 \end{pmatrix}. \tag{6-6}$$

Обозначим через $\boldsymbol{e} = (e_1, e_2, e_3)$ стандартный базис в $\mathbb{Z}^3$. По условию, столбцы матрицы A, т. е. векторы $\boldsymbol{a} = (a_1, a_2, a_3, a_4) = \boldsymbol{e}\,A$ порождают решётку L. Пусть $D_A = LAR$ — нормальная форма Смита матрицы A. Тогда векторы $\boldsymbol{w} = \boldsymbol{a}\,R = \boldsymbol{e}\,AR$ тоже порождают L, поскольку образующие $\boldsymbol{a} = \boldsymbol{w}\,R^{-1}$ линейно через них выражаются. По предл. 5.6 на стр. 97 векторы $\boldsymbol{u} = \boldsymbol{e}\,L^{-1}$ составляют базис в $\mathbb{Z}^3$, так как матрица перехода от них к стандартному базису обратима. При этом $\boldsymbol{e} = \boldsymbol{u}\,L$. В силу равенств $\boldsymbol{w} = \boldsymbol{e}\,AR = \boldsymbol{u}\,LAR = \boldsymbol{u}\,D_A$, образующие $w_i = d_{ii}u_i$ пропорциональны базисным векторам u_i. Поэтому взаимные базисы в $\mathbb{Z}^3$ и L состоят из векторов $\boldsymbol{u}$, т. е. столбцов матрицы L^{-1}, и векторов $w_i = d_{ii}u_i$ с ненулевыми d_{ii}. Для их отыскания приведём матрицу A к нормальной форме Смита. Так как матрица R нас сейчас не интересует, в вычислении из прим. 6.1 на стр. 104 можно ограничиться только верхней частью Г-образной таблицы:

$$\left[\begin{array}{c|c} A & E \end{array}\right] = \left[\begin{array}{cccc|ccc} 126 & 51 & 72 & 33 & 1 & 0 & 0 \\ 30 & 15 & 18 & 9 & 0 & 1 & 0 \\ 60 & 30 & 36 & 18 & 0 & 0 & 1 \end{array}\right].$$

Отнимаем из первой строки удвоенную третью:

$$\left[\begin{array}{cccc|ccc} 6 & -9 & 0 & -3 & 1 & 0 & -2 \\ 30 & 15 & 18 & 9 & 0 & 1 & 0 \\ 60 & 30 & 36 & 18 & 0 & 0 & 1 \end{array}\right]$$

и делаем четвёртый столбец первым:

$$\left[\begin{array}{cccc|ccc} -3 & 6 & -9 & 0 & 1 & 0 & -2 \\ 9 & 30 & 15 & 18 & 0 & 1 & 0 \\ 18 & 60 & 30 & 36 & 0 & 0 & 1 \end{array}\right].$$

Так как все элементы левой матрицы делятся на 3, зануляем в ней 1-ю строку и 1-й столбец вне левого верхнего угла:

$$\left(\begin{array}{cccc|ccc} -3 & 0 & 0 & 0 & 1 & 0 & -2 \\ 0 & 48 & -12 & 18 & 3 & 1 & -6 \\ 0 & 96 & -24 & 36 & 6 & 0 & -11 \end{array}\right).$$

Теперь зануляем 3-ю строку, отнимая из неё удвоенную 2-ю:

$$\left(\begin{array}{cccc|ccc} -3 & 0 & 0 & 0 & 1 & 0 & -2 \\ 0 & 48 & -12 & 18 & 3 & 1 & -6 \\ 0 & 0 & 0 & 0 & 0 & -2 & 1 \end{array}\right).$$

Прибавляем к 3-му столбцу 4-й и переставляем результат во 2-й столбец:

$$\left(\begin{array}{cccc|ccc} -3 & 0 & 0 & 0 & 1 & 0 & -2 \\ 0 & 6 & 48 & 18 & 3 & 1 & -6 \\ 0 & 0 & 0 & 0 & 0 & -2 & 1 \end{array}\right).$$

Отнимаем из 3-го и 4-го столбцов 2-й, умноженный на 8 и на 3, меняем знак в первой строке и получаем окончательно:

$$\left(\begin{array}{c|c} D_A & L \end{array}\right) = \left(\begin{array}{cccc|ccc} 3 & 0 & 0 & 0 & -1 & 0 & 2 \\ 0 & 6 & 0 & 0 & 3 & 1 & -6 \\ 0 & 0 & 0 & 0 & 0 & -2 & 1 \end{array}\right).$$

Из проделанного вычисления уже видно, что $L \simeq \mathbb{Z}^2$, а $\mathbb{Z}^3/L \simeq \mathbb{Z}/(3) \oplus \mathbb{Z}/(6) \oplus \mathbb{Z}$. Для отыскания матрицы L^{-1} действуем как в прим. 6.2 на стр. 107: приписываем к L единичную матрицу

$$L = \left(\begin{array}{ccc|ccc} -1 & 0 & 2 & 1 & 0 & 0 \\ 3 & 1 & -6 & 0 & 1 & 0 \\ 0 & -2 & 1 & 0 & 0 & 1 \end{array}\right),$$

прибавляем ко 2-й строке утроенную 1-ю:

$$\left(\begin{array}{ccc|ccc} -1 & 0 & 2 & 1 & 0 & 0 \\ 0 & 1 & 0 & 3 & 1 & 0 \\ 0 & -2 & 1 & 0 & 0 & 1 \end{array}\right),$$

затем прибавляем к 3-й строке удвоенную 2-ю:

$$\left(\begin{array}{ccc|ccc} -1 & 0 & 2 & 1 & 0 & 0 \\ 0 & 1 & 0 & 3 & 1 & 0 \\ 0 & 0 & 1 & 6 & 2 & 1 \end{array}\right),$$

наконец, отнимаем из 1-й строки удвоенную 3-ю, меняем в ней знак и получаем

$$L^{-1} = \begin{pmatrix} 11 & 4 & 2 \\ 3 & 1 & 0 \\ 6 & 2 & 1 \end{pmatrix}.$$

Таким образом, взаимные базисы решётки $\mathbb{Z}^3$ и её подрешётки L состоят из векторов

$$u_1 = (11, 3, 6), \quad u_2 = (4, 1, 2), \quad u_3 = (2, 0, 1)$$

и векторов $w_1 = 3u_1 = (33, 9, 18)$, $w_2 = 6u_2 = (24, 6, 12)$.

Упражнение 6.6. Выразите последние два вектора через столбцы матрицы (6-6).

6.3. Элементарные делители. Зафиксируем в каждом классе ассоциированных простых элементов кольца K какого-нибудь представителя и обозначим множество всех этих попарно неассоциированных представителей через $P(K)$. Как и ранее, будем обозначать через $\nu_p(m)$ показатель, с которым $p \in P(K)$ входит в разложение элемента $m \in K$ на простые множители. Сопоставим каждому упорядоченному набору необратимых чисел

$$\lambda_1, \dots, \lambda_n \in K\,, \text{ где } \lambda_i \mid \lambda_j \text{ при } i < j, \tag{6-7}$$

неупорядоченное дизъюнктное объединение по всем $i = 1, \dots, n$ степеней $p^{\nu_p(\lambda_i)}$ с ненулевыми показателями $\nu_p(\lambda_i)$. Иначе говоря, рассмотрим для каждого $i = 1, \dots, n$ разложение на простые множители $\lambda_i = \prod_{p \in P(K)} p^{\nu_p(\lambda_i)}$ и соберём все участвующие в этих разложениях сомножители p^ν с $\nu > 0$ в одно неупорядоченное множество, где каждая степень p^ν, присутствующая в разложении ровно k чисел λ_i, тоже присутствует ровно k раз. Получающееся таким образом неупорядоченное множество (возможно повторяющихся) степеней p^ν называется *набором элементарных делителей* упорядоченного набора (6-7).

Лемма 6.2
Описанная выше процедура устанавливает биекцию между рассматриваемыми с точностью до умножения каждого элемента на обратимое число из K упорядоченными наборами необратимых чисел $\lambda_1, \dots, \lambda_n \in K$, в которых $\lambda_i \mid \lambda_j$ при $i < j$, и всевозможными неупорядоченными наборами степеней p^ν, где $p \in P(K)$, $n \in \mathbb{N}$, элементы в которых могут повторяться.

Доказательство. Набор $\lambda_1, \dots, \lambda_n$ однозначно восстанавливается по своему набору элементарных делителей следующим образом. Расставим элементарные делители в клетки диаграммы Юнга так, чтобы в первой строке шли в порядке нестрого убывания степени того $p \in P(K)$, степеней которого в наборе элементарных делителей имеется больше всего. Во вторую строку поместим в порядке нестрого убывания степени простого числа, следующего за p по общему количеству вхождений его степеней в набор элементарных делителей и т. д. Поскольку λ_n делится на все остальные λ_i, в его разложение на простые множители входят все встречающиеся среди элементарных делителей простые основания, причём каждое из них — с максимально возможным показателем. Таким образом, λ_n является произведением всех элементарных делителей, стоящих в первом столбце построенной диаграммы Юнга. По индукции мы заключаем, что произведения элементарных делителей по столбцам диаграммы, перебираемым слева направо, суть $\lambda_n, \dots, \lambda_1$, т. е. прочитанный справа налево набор (6-7). □

Пример 6.6
Набор элементарных делителей

$$\begin{array}{ccccc} 3^2 & 3^2 & 3 & 3 & 3 \\ 2^3 & 2^3 & 2^2 & 2 & \\ 7^2 & 7 & 7 & & \\ 5 & 5 & & & \end{array}$$

возникает из множителей $\lambda_1 = 3, \lambda_2 = 3 \cdot 2, \lambda_3 = 3 \cdot 2^2 \cdot 7, \lambda_4 = 3^2 \cdot 2^3 \cdot 7 \cdot 5, \lambda_5 = 3^2 \cdot 2^3 \cdot 7^2 \cdot 5$.

Теорема 6.4 (теорема об элементарных делителях)
Всякий конечно порождённый модуль над областью главных идеалов K изоморфен

$$K^{n_0} \oplus \frac{K}{\left(p_1^{n_1}\right)} \oplus \dots \oplus \frac{K}{\left(p_\alpha^{n_\alpha}\right)} \tag{6-8}$$

где $n_\nu \in \mathbb{N}$, все $p_\nu \in K$ просты, и слагаемые в прямой сумме могут повторяться. Два модуля

$$K^{n_0} \oplus \frac{K}{\left(p_1^{n_1}\right)} \oplus \ldots \oplus \frac{K}{\left(p_\alpha^{n_\alpha}\right)} \quad \text{и} \quad K^{m_0} \oplus \frac{K}{\left(q_1^{m_1}\right)} \oplus \ldots \oplus \frac{K}{\left(q_\beta^{m_\beta}\right)}$$

изоморфны если и только если $n_0 = m_0$, $\alpha = \beta$ и слагаемые можно перенумеровать так, чтобы $n_\nu = m_\nu$ и $p_\nu = s_\nu q_\nu$, где все $s_\nu \in K$ обратимы.

Определение 6.2
Набор (возможно повторяющихся) степеней $p_i^{n_i}$, по которым происходит факторизация в (6-8), называется *набором элементарных делителей* модуля (6-8).

Доказательство существования разложения (6-8). Пусть K-модуль M порождается векторами

$$w_1, \ldots, w_m .$$

Тогда $M = K^m/R$, где R — ядро эпиморфизма $K^m \twoheadrightarrow M$, переводящего стандартные базисные векторы $e_i \in K^m$ в образующие $w_i \in M$, как в форм. (6-5) на стр. 111. По теор. 6.3 в K^m существует такой базис $u_1, \ldots, u_m$, что некоторые кратности $\lambda_1 u_1, \ldots, \lambda_k u_k$ первых K базисных векторов составляют базис в R. Таким образом, $M = K^m/R = K/(\lambda_1) \oplus \ldots \oplus K/(\lambda_k) \oplus K^{m-k}$. Если i-й инвариантный множитель λ_i обратим, то отвечающее ему слагаемое $K/(\lambda_i) = K/K$ нулевое. Если λ_i необратим, то $\lambda_i = p_1^{m_1} \ldots p_s^{m_s}$, где $p_j \in K$ — попарно не ассоциированные простые элементы, и по китайской теореме об остатках $K/(\lambda_i) = K/(p_1^{m_1}) \oplus \ldots \oplus K/(p_s^{m_s})$, что и даёт разложение (6-8). □

Чтобы установить единственность разложения (6-8) для заданного K-модуля M, мы дадим инвариантное описание его ингредиентов во внутренних терминах модуля M. Этому посвящены идущие ниже разделы n° 6.3.1 – n° 6.3.3. Далее, в n° 6.3.4 мы установим обещанные ранее независимость инвариантных множителей матрицы A от способа её приведения к нормальной форме Смита D_A и независимость инвариантных множителей подмодуля $N \subset F$ в свободном модуле F от выбора взаимных базисов в F и N.

6.3.1. Отщепление кручения. Вектор w из модуля M над целостным[1] кольцом K называется *элементом кручения*, если $xw = 0$ для какого-нибудь ненулевого $x \in K$. Например, любой класс $[k]_n \in \mathbb{Z}/(n)$ является элементом кручения в $\mathbb{Z}$-модуле $\mathbb{Z}/(n)$, так как $n[k]_n = [nk]_n = [0]_n$. В общем случае элементы кручения составляют подмодуль в M, который обозначается

$$\operatorname{Tors} M \stackrel{\text{def}}{=} \{ w \in M \mid \exists\, x \neq 0 :\ xm = 0 \} \tag{6-9}$$

и называется *подмодулем кручения* в M.

Упражнение 6.7. Убедитесь в том, что $\operatorname{Tors} M$ действительно является подмодулем в M.

Если $\operatorname{Tors} M = 0$, то говорят, что модуль M *не имеет кручения*. Например, любой идеал целостного кольца K и любой подмодуль в координатном модуле K^n над таким кольцом не имеют кручения. Если $\operatorname{Tors} M = M$, то M называется *модулем кручения*. Например, фактор K/I по любому ненулевому идеалу $I \subset K$ является K-модулем кручения, поскольку для любого класса $[a] \in K/I$ и любого ненулегого $x \in I$ класс $x[a] = [xa] = [0]$, так как $xa \in I$.

[1] См. n° 1.4.1 на стр. 28.

Предложение 6.1
Для любого модуля M над целостным кольцом K фактормодуль $M/\mathrm{Tors}(M)$ не имеет кручения. Если подмодуль $N \subset M$ таков, что $\mathrm{Tors}(M/N) = 0$, то $\mathrm{Tors}(M) \subset N$.

Доказательство. При ненулевом $x \in K$ равенство $x[w] = [xw] = [0]$ в $M/\mathrm{Tors}(M)$ означает, что $xw \in \mathrm{Tors}(M)$, т. е. $yxw = 0$ для некоторого ненулевого $y \in K$. Так как в K нет делителей нуля, $xy \neq 0$ и $w \in \mathrm{Tors}(M)$, т. е. $[w] = [0]$. Это доказывает первое утверждение. Для доказательства второго заметим, что если $w \in \mathrm{Tors}(M) \smallsetminus N$, то класс $[w] \in M/N$ является ненулевым элементом кручения. □

Теорема 6.5
Всякий конечно порождённый модуль M над областью главных идеалов K является прямой суммой свободного модуля и подмодуля кручения. В частности, любой модуль без кручения автоматически свободен.

Доказательство. По уже доказанному $M \simeq K^{n_0} \oplus K/\left(p_1^{n_1}\right) \oplus \ldots \oplus K/\left(p_\alpha^{n_\alpha}\right)$, где первое слагаемое свободно от кручения, а сумма остальных $N = K/(p_1^{n_1}) \oplus \ldots \oplus K/(p_\alpha^{n_\alpha})$ является модулем кручения, и тем самым содержится в $\mathrm{Tors}(M)$. Так как $M/N \simeq K^{n_0}$ не имеет кручения, $\mathrm{Tors}(M) \subset N$ по предл. 6.1. Тем самым, $\mathrm{Tors}(M) = N$, $M = K^{n_0} \oplus \mathrm{Tors}(M)$ и $M/\mathrm{Tors}(M) \simeq K^{n_0}$. □

Следствие 6.1 (из существования разложения из теор. 6.5)
В форм. (6-8) на стр. 114 сумма $K/\left(p_1^{n_1}\right) \oplus \ldots \oplus K/\left(p_\alpha^{n_\alpha}\right) = \mathrm{Tors}(M)$ и число n_0, равное рангу свободного модуля $M/\mathrm{Tors}(M)$, не зависят от выбора разложения (6-8). □

6.3.2. Отщепление p-кручения. Для каждого простого $p \in P(K)$ назовём подмодуль

$$\mathrm{Tors}_p(M) \stackrel{\text{def}}{=} \{w \in M \mid \exists\, k \in \mathbb{N} :\ p^k w = 0\}$$

подмодулем p-кручения в M, а его элементы — *элементами p-кручения*.

Упражнение 6.8. Убедитесь, что $\mathrm{Tors}_p(M)$ действительно является подмодулем в M и докажите для него аналог предл. 6.1: фактор $M/\mathrm{Tors}_p(M)$ не имеет p-кручения, и если подмодуль $N \subset M$ таков, что $\mathrm{Tors}_p(M/N) = 0$, то $\mathrm{Tors}_p(M) \subset N$.

Теорема 6.6
Всякий конечно порождённый модуль кручения $M = \mathrm{Tors}(M)$ над областью главных идеалов K является прямой суммой своих подмодулей p-кручения: $M = \bigoplus_p \mathrm{Tors}_p(M)$, где сумма берётся по всем таким $p \in P(K)$, что $\mathrm{Tors}_p(M) \neq 0$. При этом каждый конечно порождённый модуль p-кручения имеет вид $K/(p^{\nu_1}) \oplus \ldots \oplus K/(p^{\nu_k})$, где $\nu_1, \ldots, \nu_k \in \mathbb{N}$.

Доказательство. Если простое $q \in K$ не ассоциировано с p, то $\mathrm{нод}(p^k, q^m) = 1$ для всех k, m, и класс $[p^k]$ обратим в факторкольце $K/\left(q^m\right)$. Поэтому гомоморфизм умножения на p^k:

$$K/\left(q^m\right) \to K/\left(q^m\right), \quad x \mapsto p^k x,$$

биективен и, в частности, не имеет ядра. Напротив, модуль $K/\left(p^\nu\right)$ аннулируется умножением на p^ν. Тем самым, в разложении из форм. (6-8) на стр. 114

$$M = \mathrm{Tors}(M) = \left(\tfrac{K}{(p^{\nu_1})} \oplus \ldots \oplus \tfrac{K}{(p^{\nu_k})}\right) \oplus \left(\bigoplus\nolimits_{q \neq p} \left(\tfrac{K}{(q^{\mu_{q,1}})} \oplus \ldots \oplus \tfrac{K}{(q^{\mu_{q,m_q}})}\right)\right)$$

слагаемое в левых скобках содержится в $\mathrm{Tors}_p(M)$, а фактор по нему, изоморфный сумме в правых скобках, не имеет p-кручения. Поэтому $\mathrm{Tors}_p(M)$ совпадает с левым слагаемым, $M/\mathrm{Tors}_p(M)$ изоморфен правому слагаемому, и $M \simeq \mathrm{Tors}_p(M) \oplus \big(M/\mathrm{Tors}_p(M)\big)$. □

Следствие 6.2 (из существования разложения из теор. 6.6)
В форм. (6-8) на стр. 114 сумма всех подмодулей $K/(p^\nu)$ с заданным $p \in P(K)$ является подмодулем p-кручения в M и не зависит от выбора разложения (6-8). □

6.3.3. Инвариантность показателей p-кручения. Согласно теор. 6.6 каждый конечно порождённый модуль p-кручения M над областью главных идеалов K имеет вид

$$M = \frac{K}{(p^{\nu_1})} \oplus \ldots \oplus \frac{K}{(p^{\nu_n})}\,. \tag{6-10}$$

Упорядоченные по нестрогому убыванию натуральные числа $\nu_1 \geqslant \nu_2 \geqslant \ldots \geqslant \nu_n$ называются *показателями p-кручения* модуля M. Они образуют диаграмму Юнга $\nu = \nu(M) = (\nu_1, \ldots, \nu_n)$, которая называется *цикловым типом* модуля p-кручения M. Для завершения доказательства теор. 6.4 остаётся проверить, что цикловой тип зависит только от модуля M, а не от выбора конкретного разложения (6-10). Для этого рассмотрим гомоморфизм умножения на p

$$\varphi\colon M \to M\,, \quad w \mapsto pw$$

и обозначим через $\varphi^k = \varphi \circ \ldots \circ \varphi\colon w \mapsto p^k w$ его k-кратную итерацию, считая, что $\varphi^0 = \mathrm{Id}_M$. Очевидно, что $\ker \varphi^k \subseteq \ker \varphi^{k+1}$ при всех k, и $\ker \varphi^k = M$ при $k \geqslant \nu_1$, но $\ker \varphi^k \neq M$ при $k < \nu_1$. Таким образом, мы имеем конечную цепочку возрастающих подмодулей

$$0 = \ker \varphi^0 \subseteq \ker \varphi^1 \subseteq \ldots \subseteq \ker \varphi^{\nu_1 - 1} \subsetneq \ker \varphi^{\nu_1} = M\,, \tag{6-11}$$

которая зависит только от модуля M. В частности, ν_1 зависит только от M.

Лемма 6.3
Для каждого $k = 1, \ldots, \nu_1$ фактормодуль $\ker \varphi^k / \ker \varphi^{k-1}$ является векторным пространством над полем $\Bbbk = K/(p)$ размерности, равной высоте k-го столбца диаграммы Юнга $\nu(M)$.

Доказательство. Зададим умножение класса $[x] \in K/(p)$ на класс $[w] \in \ker \varphi^k / \ker \varphi^{k-1}$ правилом $[x][z] \stackrel{\text{def}}{=} [xz]$. Оно корректно, поскольку для $x' = x + py$ и $w' = w + u$, где $p^{k-1}u = 0$, имеем $x'w' = xw + (x + py)u + pyw$, где $p^{k-1}\big((x + py)\,u + pyw\big) = 0$, так как $p^{k-1}u = 0$ и $p^k w = 0$. Аксиомы дистрибутивности и ассоциативности очевидно выполняются. Это доказывает первое утверждение. Для доказательства второго рассмотрим произвольное разложение (6-10). Гомоморфизм φ переводит каждое слагаемое этого разложения в себя. Обозначим через $\varphi_i = \varphi|_{K/(p^{\nu_i})}$ ограничение φ на i-е слагаемое $K/(p^{\nu_i})$ разложения (6-10). Фактор модуль $\ker \varphi^k / \ker \varphi^{k-1}$ изоморфен прямой сумме фактормодулей $\ker \varphi_i^k / \ker \varphi_i^{k-1}$.

Упражнение 6.9. Убедитесь, что при каждом i для каждого $k = 1, \ldots, \nu_i$ отображение

$$K/(p) \to \ker \varphi_i^k / \ker \varphi_i^{k-1}\,, \quad x \,(\mathrm{mod}\, p) \mapsto p^{\nu_i - k} x \,(\mathrm{mod}\, \ker \varphi_i^{k-1})\,,$$

корректно определено, $\Bbbk$-линейно и биективно.

Таким образом, на каждом слагаемом разложения (6-10) цепочка ядер (6-11) имеет вид

$$0 = \ker \varphi_i^0 \subsetneq \ker \varphi_i^1 \subsetneq \ldots \subsetneq \ker \varphi_i^{\nu_i - 1} \subsetneq \ker \varphi^{\nu_i} = K/(p_i^{\nu_i})\,,$$

и каждый из её факторов $\ker \varphi_i^k/\ker \varphi_i^{k-1}$ при $k = 1, \dots, \nu_i$ является одномерным векторным пространством над полем $\Bbbk = K/(p)$, а во всём модуле (6-10) пространство $\ker \varphi^k/\ker \varphi^{k-1}$ является прямой суммой этих одномерных пространств в количестве, равном числу строк диаграммы ν, длина которых не меньше k, т. е. длине k-го столбца диаграммы ν. □

На этом доказательство теоремы об элементарных делителях заканчивается.

Следствие 6.3 (теорема об инвариантных множителях)
Всякий конечно порождённый модуль над областью главных идеалов K изоморфен

$$K^{n_0} \oplus \frac{K}{(\lambda_1)} \oplus \dots \oplus \frac{K}{(\lambda_g)} \tag{6-12}$$

где n_0, g — целые неотрицательные, а $\lambda_1, \dots, \lambda_g \in K$ — такие ненулевые необратимые элементы, что $\lambda_i \mid \lambda_j$ при $i < j$. Два таких модуля

$$K^{n_0} \oplus \frac{K}{(\lambda_1)} \oplus \dots \oplus \frac{K}{(\lambda_g)} \quad \text{и} \quad K^{m_0} \oplus \frac{K}{(\mu_1)} \oplus \dots \oplus \frac{K}{(\mu_h)}$$

изоморфны если и только если $n_0 = m_0$, $g = h$ и $\lambda_i = s_i\mu_i$, где все $s_i \in K$ обратимы. □

6.3.4. Единственность инвариантных множителей. Пусть F — свободный модуль конечного ранга m над областью главных идеалов K и $N \subset F$ — его подмодуль. Покажем, что множители $\lambda_1, \dots, \lambda_n$ из теоремы о взаимном базисе[1] не зависят от выбора взаимных базисов. В самом деле, фактормодуль $M = F/N$ ничего не знает о взаимных базисах, и по теореме об элементарных делителях[2] он имеет вид

$$M \simeq K^{m_0} \oplus \frac{K}{(p_1^{m_1})} \oplus \dots \oplus \frac{K}{(p_\alpha^{m_\alpha})}\,. \tag{6-13}$$

С другой стороны, если базис $e_1, \dots, e_m$ модуля F таков, что векторы $\lambda_1 e_1, \dots, \lambda_n e_n$ составляют базис в N и $\lambda_i \mid \lambda_j$ при $i < j$, то $M = F/N \simeq K^{m-n} \oplus K/(\lambda_1) \oplus \dots \oplus K/(\lambda_n)$, где каждый фактор $K/(\lambda)$ либо нулевой (если λ обратим), либо — когда λ необратим — распадается по китайской теореме об остатках в прямую сумму модулей вида $K/(p^{\nu_p(\lambda)})$, где $p^{\nu_p(\lambda)}$ берутся из разложения $\lambda = \prod_{p \in P(K)} p^{\nu_p(\lambda)}$ на простые множители. Мы заключаем, что $m_0 = m - n$, а набор степеней $p^{\nu_p(\lambda)}$ является набором элементарных делителей упорядоченного по отношению делимости набора всех необратимых множителей λ, который по лем. 6.2 на стр. 114 однозначно восстанавливается по набору своих элементарных делителей. Таким образом число $n = m - m_0$ и все ненулевые необратимые инвариантные множители подмодуля N однозначно считываются с разложения (6-13), что и доказывает независимость инвариантных множителей подмодуля N от выбора взаимного базиса.

Применительно к модулю $F = K^m$ со стандартным базисом $\boldsymbol{e} = (e_1, \dots, e_m)$ и его подмодулю $N \subset K^m$, порождённому столбцами $\boldsymbol{a} = (a_1, \dots, a_n)$ матрицы $A \in \mathrm{Mat}_{m\times n}(K)$, это утверждение означает, что элементы d_{ii} нормальной формы Смита матрицы A не зависят от способа её приведения к нормальной форме и даже собственно от матрицы, а зависят лишь от подмодуля N. В самом деле, если $D = LAR$ — это (какая-нибудь) нормальная форма Смита матрицы A, то из равенства $\boldsymbol{a} = \boldsymbol{e}A$ вытекает равенство $\boldsymbol{a}R = \boldsymbol{e}L^{-1}LAR = \boldsymbol{e}L^{-1}D$. В силу обратимости матриц R

[1] См. теор. 6.3 на стр. 111.
[2] См. теор. 6.4 на стр. 114.

и L векторы $\boldsymbol{u} = \boldsymbol{e}\,L^{-1}$ тоже составляют базис в K^m, а векторы $\boldsymbol{w} = \boldsymbol{a}R$ линейно порождают N. Так как $\boldsymbol{w} = \boldsymbol{u}\,D$, векторы $\boldsymbol{u} = (u_1, \ldots, u_m)$ и векторы $w_i = d_{ii}u_i$ с ненулевыми d_{ii} образуют взаимные базисы модуля K^m и его подмодуля N, а ненулевые диагональные элементы d_{ii} являются инвариантными множителями этого подмодуля.

§7. Конечно порождённые абелевы группы

7.1. Фробениусово и жорданово представления. При $K = \mathbb{Z}$ теорема об инвариантных множителях[1] и теорема об элементарных делителях[2] дают две альтернативных полных классификации конечно порождённых абелевых групп.

Теорема 7.1 (теорема об инвариантных множителях)
Всякая конечно порождённая абелева группа изоморфна прямой сумме аддитивных групп

$$\mathbb{Z}^r \oplus \frac{\mathbb{Z}}{(n_1)} \oplus \ldots \oplus \frac{\mathbb{Z}}{(n_g)}, \tag{7-1}$$

где r — целое неотрицательное, а натуральные $n_1, \ldots, n_g \geqslant 2$ таковы, что $n_i \mid n_j$ при $i < j$. Две такие группы

$$\mathbb{Z}^r \oplus \frac{\mathbb{Z}}{(n_1)} \oplus \ldots \oplus \frac{\mathbb{Z}}{(n_g)} \quad \text{и} \quad \mathbb{Z}^s \oplus \frac{\mathbb{Z}}{(m_1)} \oplus \ldots \oplus \frac{\mathbb{Z}}{(m_h)}$$

изоморфны если и только если $r = s$, $g = h$ и $n_i = m_i$ при всех i. □

Теорема 7.2 (теорема об элементарных делителях)
Всякая конечно порождённая абелева группа изоморфна прямой сумме аддитивных групп

$$\mathbb{Z}^r \oplus \frac{\mathbb{Z}}{(p_1^{n_1})} \oplus \ldots \oplus \frac{\mathbb{Z}}{(p_\alpha^{n_\alpha})}, \tag{7-2}$$

где $p_\nu \in \mathbb{N}$ — простые числа (не обязательно различные). Две такие группы

$$\mathbb{Z}^r \oplus \frac{\mathbb{Z}}{(p_1^{n_1})} \oplus \ldots \oplus \frac{\mathbb{Z}}{(p_\alpha^{n_\alpha})} \quad \text{и} \quad \mathbb{Z}^s \oplus \frac{\mathbb{Z}}{(q_1^{m_1})} \oplus \ldots \oplus \frac{\mathbb{Z}}{(q_\beta^{m_\beta})}$$

изоморфны если и только если $r = s$, $\alpha = \beta$ и после надлежащей перестановки слагаемых будут выполняться равенства $n_\nu = m_\nu$ и $p_\nu = q_\nu$ при всех ν. □

При этом в разложениях (7-1) и (7-2) данной абелевой группы A целые неотрицательные r одинаковы, а упорядоченный набор натуральных чисел $n_1 \mid \ldots \mid n_g$ из разложения (7-1) и неупорядоченное множество возможно повторяющихся степеней p^ν из разложения (7-2) однозначно определяют друг друга по лем. 6.2 на стр. 114: множество элементарных делителей является дизъюнктным объединением степеней $p^{\nu_p(n_i)}$ с $\nu_p(m_i) > 0$ по всем $1 \leqslant i \leqslant g$ и всем простым $p \in \mathbb{N}$, а набор инвариантных множителей $n_1, \ldots, n_g$ является прочитанным справа налево набором произведений, взятых по столбцам диаграммы Юнга, в первую строку которой выписаны в порядке нестрого убывания показателей все степени того числа p, степеней которого больше всего, во вторую — все степени следующего по общему количеству степеней числа p и т. д. Единственная с точностью до перестановки прямых слагаемых аддитивная группа (7-2), изоморфная заданной конечно порождённой абелевой группе A, называется *стандартным* (или *жордановым*) *представлением* группы A или разложением группы A в прямую сумму неразложимых циклических подгрупп, а прямая сумма (7-1) — *фробениусовым представлением* группы A.

[1] См. сл. 6.3 на стр. 118.
[2] См. теор. 6.4 на стр. 114.

Пример 7.1 (абелевы группы порядка $\leqslant 10$)
Абелевы группы из двух, трёх, пяти, шести, семи и десяти элементов с точностью до изоморфизма единственны и их стандартные представления (7-2) имеют, соответственно, вид:

$$\mathbb{Z}/(2)\,,\ \mathbb{Z}/(3)\,,\ \mathbb{Z}/(5)\,,\ \mathbb{Z}/(3)\oplus\mathbb{Z}/(2)\,,\ \mathbb{Z}/(7)\,,\ \mathbb{Z}/(5)\oplus\mathbb{Z}/(2)\,.$$

Групп из четырёх элементов с точностью до изоморфизма две: $\mathbb{Z}/(4)$ и $\mathbb{Z}/(2)\oplus\mathbb{Z}/(2)$.

Упражнение 7.1. Убедитесь явным образом, что эти две группы не изоморфны.

Групп из девяти элементов с точностью до изоморфизма тоже две: $\mathbb{Z}/(9)$ и $\mathbb{Z}/(3)\oplus\mathbb{Z}/(3)$. Группы из восьми элементов с точностью до изоморфизма исчерпываются тремя попарно не изоморфными группами $\mathbb{Z}/(8)$, $\mathbb{Z}/(4)\oplus\mathbb{Z}/(2)$ и $\mathbb{Z}/(2)\oplus\mathbb{Z}/(2)\oplus\mathbb{Z}/(2)$.

7.1.1. Канонические и не канонические слагаемые стандартного представления. Для каждого простого p, участвующего в стандартном представлении данной группы A, в A имеется единственная подгруппа, изоморфная прямой сумме всех прямых слагаемых вида $\mathbb{Z}/(p^m)$ в разложении (7-2) — это подгруппа p-кручения $\mathrm{Tors}_p(A)\subset A$. Прямая сумма этих подгрупп, т. е. подгруппа кручения $\mathrm{Tors}(A)=\bigoplus_p \mathrm{Tors}_p(A)$ — это единственная подгруппа в A, изоморфная сумме всех отличных от $\mathbb{Z}^r$ элементов разложения (7-2). В противоположность этому, дополнительная к $\mathrm{Tors}(A)$ свободная подгруппа $B\subset A$, изоморфная $\mathbb{Z}^r\simeq A/\mathrm{Tors}(A)$ может быть выбрана в A разными способами. Например, группа $A=\mathbb{Z}\oplus\mathbb{Z}/(3)$ иначе раскладывается как $B\oplus\mathbb{Z}/(3)$, где подгруппа $B\subset A$ порождена элементом $(1,[1]_3)\in A$.

Упражнение 7.2. Убедитесь в этом и перечислите для группы $A=\mathbb{Z}\oplus\mathbb{Z}/(3)$ все изоморфные $\mathbb{Z}$ подгруппы $B\subset A$, дополнительные к $\mathrm{Tors}(A)$.

Разложение подгруппы p-кручения в сумму неразложимых циклических подгрупп

$$\mathrm{Tors}_p(A)=\frac{\mathbb{Z}}{(p^{\nu_1})}\oplus\ldots\oplus\frac{\mathbb{Z}}{(p^{\nu_n})}$$

тоже не единственно: для каждого показателя ν_i изоморфная $\mathbb{Z}/(p^{\nu_i})$ подгруппа в A может выбираться разными способами. Например, группа $A=\mathbb{Z}/(4)\oplus\mathbb{Z}(2)$ иначе раскладывается в сумму $B\oplus C$ подгрупп $B\simeq\mathbb{Z}/(4)$ и $C\simeq\mathbb{Z}/(2)$, порождённых элементами $([1]_4,[1]_2)$ и $([2]_4,[1]_2)$ соответственно. Но цикловой тип группы A, т. е. набор $(\nu_1,\ldots,\nu_n)$ показателей p-кручения, от выбора разложения не зависит.

7.1.2. Циклические группы и минимальные наборы образующих. Пусть абелева группа A порождается как $\mathbb{Z}$-модуль элементами $a_1,\ldots,a_m$. Наборы образующих с наименьшим возможным m называется *минимальными*. Группа (7-1)

$$A=\mathbb{Z}^r\oplus\frac{\mathbb{Z}}{(n_1)}\oplus\ldots\oplus\frac{\mathbb{Z}}{(n_g)}\,,$$

где $n_i\mid n_j$ при $i<j$, порождается $r+g$ элементами вида $(0,\ldots,0,1,0,\ldots,0)$. Покажем, что это минимальный набор образующих. Пусть A порождается m элементами $a_1,\ldots,a_m$. Тогда

$$A\simeq\mathbb{Z}^m/R\,,$$

где $R\subset\mathbb{Z}^m$ — ядро сюръективного гомоморфизма $\mathbb{Z}\twoheadrightarrow A$, переводящего стандартные базисные векторы $e_1,\ldots,e_m\in\mathbb{Z}^m$ в $a_1,\ldots,a_m\in A$. Пусть векторы $f_1,\ldots,f_m$ и $\lambda_1f_1,\ldots,\lambda_kf_k$ образуют

взаимные базисы в $\mathbb{Z}^m$ и R, и пусть $\lambda_1 = \ldots = \lambda_s = 1$, а $\lambda_{s+1} \mid \ldots \mid \lambda_k$ строго больше 1. Тогда фробениусово представление группы $A = \mathbb{Z}^m / R$ имеет вид

$$\frac{\mathbb{Z}}{(\lambda_{s+1})} \oplus \ldots \oplus \frac{\mathbb{Z}}{(\lambda_k)} \oplus \mathbb{Z}^{m-k},$$

и в силу единственности фробениусова представления $r = (m-k)$, $g = k - s$ и $n_i = \lambda_{s+i}$ при всех $i = 1, \ldots, g$. В частности $r + g = m - s \leqslant m$, что и утверждалось.

В терминах разложения (7-2) в прямую сумму неразложимых циклических подгрупп число g конечных слагаемых фробениусова разложения абелевой группы A равно максимальному числу элементарных делителей с одним и тем же простым основанием, т. е. длине верхней строки диаграммы Юнга, составленной из элементарных делителей группы A.

Абелевы группы, которые можно породить одним элементом, называются *циклическими*. Фробениусово разложение такой группы имеет ровно одно слагаемое. Тем самым, циклические абелевы группы исчерпываются группами $\mathbb{Z}$ и $\mathbb{Z}/(n)$. В терминах элементарных делителей абелева группа A циклическая если и только если все простые числа в слагаемых $\mathbb{Z}/(p^m)$ её стандартного представления (7-2) попарно различны. Например, группа $\mathbb{Z}/(125) \oplus \mathbb{Z}/(9) \oplus \mathbb{Z}/(16)$ циклическая, а группа $\mathbb{Z}/(2) \oplus \mathbb{Z}/(3) \oplus \mathbb{Z}/(4) \simeq \mathbb{Z}/(2) \oplus \mathbb{Z}/(12)$ — нет.

7.1.3. Неразложимые группы. Абелева группа A называется *разложимой*, если она является прямой суммой $A = B \oplus C$ двух ненулевых собственных подгрупп $B, C \subsetneq A$. Из теор. 7.2 на стр. 120 вытекает, что каждая неразложимая абелева группа изоморфна $\mathbb{Z}$ или $\mathbb{Z}/(p^m)$, где $p \in \mathbb{N}$ — простое, причём эти неразложимые группы попарно не изоморфны, а произвольная конечно порождённая абелева группа является прямой суммой неразложимых.

7.1.4. Простые и полупростые группы. Абелева группа A называется *простой*[1], если в ней нет ненулевых собственных подгрупп. Каждая простая группа автоматически неразложима. Обратное неверно: группы $\mathbb{Z}$ и $\mathbb{Z}/(p^m)$, где $m \geqslant 2$ неразложимы, но не просты, поскольку содержат ненулевые собственные подгруппы.

Упражнение 7.3. Опишите все ненулевые собственные подгруппы в $\mathbb{Z}$ и в $\mathbb{Z}/(p^m)$, где $m \geqslant 2$.

Поскольку порядок любой подгруппы в конечной группе A делит порядок A, все конечные группы простого порядка просты. Мы заключаем, что конечно порождённые простые абелевы группы с точностью до изоморфизма исчерпываются группами $\mathbb{Z}/(p)$, где $p \in \mathbb{N}$ — простое, и при разных p такие группы не изоморфны.

Абелева группа называется *полупростой*, если она является прямой суммой простых подгрупп. Таким образом, конечно порождённые полупростые абелевы группы исчерпываются конечными прямыми суммами групп вида $\mathbb{Z}/(p)$, где $p \in \mathbb{N}$ — простое.

Предложение 7.1
Следующие свойства конечно порождённой абелевой группы A эквивалентны:

(1) A полупроста

(2) A порождается своими простыми подгруппами

(3) каждая ненулевая собственная подгруппа $B \subsetneq A$ отщепляется прямым слагаемым, т. е. найдётся такая подгруппа $C \subset A$, что $A = B \oplus C$.

[1] В другой терминологии — *неприводимой*.

Доказательство. Импликация (1) ⇒ (2) очевидна. Докажем импликацию (2) ⇒ (3). Так как все простые абелевы группы являются группами кручения, группа A, удовлетворяющая условию (2), тоже является группой кручения и по теор. 7.2 на стр. 120 конечна. Пересечение любой простой подгруппы $U \subset A$ с любой подгруппой $W \subsetneq A$, будучи подгруппой в U, либо нулевое, либо совпадает с U. Так как $\mathbb{Z}$-линейная оболочка простых подгрупп совпадает с A, для любой собственной подгруппы $B \subsetneq A$ найдётся простая подгруппа $U_1 \subsetneq B$. Сумма подгрупп B и U_1 прямая. Если $B \oplus U_1 \neq A$, заменяем B на $B \oplus U_1$ и повторяем рассуждение, до тех пор пока не получим равенство $A = B \oplus U_1 \oplus \ldots \oplus U_k$, где все U_k просты. Остаётся положить $C = U_1 \oplus \ldots \oplus U_k$.

Чтобы установить импликацию (3) ⇒ (1), докажем сначала, что если группа A обладает свойством (3), то им обладает и каждая подгруппа $B \subset A$. Пусть $V \subset B$ — любая подгруппа. Тогда в A существуют такие подгруппы C, U, что $A = B \oplus C = V \oplus C \oplus U$. Обозначим через

$$\pi : A \twoheadrightarrow B\,, \quad b + c \mapsto b\,,$$

проекцию A на B вдоль C и положим $W = \pi(U)$.

Упражнение 7.4. Проверьте, что $B = V \oplus W$.

Поскольку группы $\mathbb{Z}^n$ и $\mathbb{Z}/(p^m)$ с $m \geqslant 2$ не просты и неразложимы, они не обладают свойством (3) и по доказанному не могут входить в стандартное представление группы, которая обладает свойством (3). Тем самым, каждая группа, обладающая свойством (3) является прямой суммой простых групп. □

Упражнение 7.5. Убедитесь непосредственно, что группы $\mathbb{Z}$ и $\mathbb{Z}/(p^m)$ с $m \geqslant 2$ не порождаются своими простыми подгруппами.

7.2. Группы, заданные образующими и соотношениями. На практике конечно порождённые абелевы группы часто задаются образующими и соотношениями. Это описание обычно звучит так: «рассмотрим абелеву группу A, порождённую элементами $a_1, \ldots, a_m$, которые связаны соотношениями

$$\begin{cases} a_1 r_{11} + a_2 r_{21} + \ldots + a_m r_{m1} = 0 \\ a_1 r_{12} + a_2 r_{22} + \ldots + a_m r_{m2} = 0 \\ \qquad \ldots\ldots\ldots\ldots\ldots \\ a_1 r_{1n} + a_2 r_{2n} + \ldots + a_m r_{mn} = 0\,, \end{cases} \tag{7-3}$$

где $R = (r_{ij}) \in \mathrm{Mat}_{m\times n}(\mathbb{Z})$». Оно означает, что $A = \mathbb{Z}^m / M$, где подмодуль $M \subset \mathbb{Z}^m$ порождается над $\mathbb{Z}$ строками $r_1, \ldots, r_m$ матрицы R, а образующие $a_j = [e_j]_M \in A$ суть классы стандартных базисных векторов $e_j \in \mathbb{Z}^m$ по модулю подрешётки $M \subset \mathbb{Z}^m$.

7.2.1. Стандартное представление. Рассмотрим векторное пространство $\mathbb{Q}^m \supset \mathbb{Z}^m$, в которое координатный модуль $\mathbb{Z}^m$ естественным образом вложен, и обозначим через

$$\mathbb{Q} \otimes M \stackrel{\text{def}}{=} \mathrm{span}_{\mathbb{Q}}(M) \subset \mathbb{Q}^m$$

$\mathbb{Q}$-линейную оболочку строк матрицы R в $\mathbb{Q}^m$. Её размерность $\dim_{\mathbb{Q}}(\mathbb{Q} \otimes M) = \mathrm{rk}\, R = \mathrm{rk}\, M$ совпадает как с рангом матрицы R над полем $\mathbb{Q}$, так и с рангом свободного $\mathbb{Z}$-модуля $M \subset \mathbb{Z}^n$, поскольку любой базис решётки M над $\mathbb{Z}$ одновременно является базисом пространства $\mathbb{Q} \otimes M$ над $\mathbb{Q}$.

Упражнение 7.6. Докажите, что набор векторов $v_1, \ldots, v_k \in \mathbb{Z}^m \subset \mathbb{Q}^m$ линейно независим над $\mathbb{Z}$ если и только если он линейно независим над $\mathbb{Q}$.

Мы заключаем, что ранг свободного слагаемого $A/\mathrm{Tors}(A)$ в стандартном представлении [1] группы $A = \mathbb{Z}^m / M$ равен $m - \operatorname{rk} R$, причём ранг матрицы R можно вычислять над полем $\mathbb{Q}$. Для вычисления остальных слагаемых стандартного представления необходимо найти все ненулевые инвариантные множители $\lambda_1, \dots, \lambda_r$ матрицы R. Тогда фробениусово представление группы $A = \mathbb{Z}^m / M$ будет иметь вид $\mathbb{Z}^{m-r} \oplus \mathbb{Z}/(\lambda_1) \oplus \dots \oplus \mathbb{Z}/(\lambda_r)$, а стандартное представление получится из него разложением каждого фактора $\mathbb{Z}/(\lambda_i)$ по китайской теореме об остатках.

Упражнение 7.7. Найдём стандартное представление абелевой группы, порождённой элементами a_1, a_2, a_3, которые связаны соотношениями

$$\begin{cases} -57a_1 + 58a_2 - 55a_3 = 0 \\ -34a_1 + 40a_2 - 22a_3 = 0 \\ 5a_1 - 10a_2 - 5a_3 = 0 \\ 9a_1 - 11a_2 + 5a_3 = 0\,. \end{cases}$$

Для этого методом Гаусса найдём инвариантные множители матрицы

$$R = \begin{pmatrix} -57 & -34 & 5 & 9 \\ 58 & 40 & -10 & -11 \\ -55 & -22 & -5 & 5 \end{pmatrix}$$

Прибавим к 1-й строке 2-ю:

$$\begin{pmatrix} 1 & 6 & -5 & -2 \\ 58 & 40 & -10 & -11 \\ -55 & -22 & -5 & 5 \end{pmatrix}$$

Зануляем верхнюю строку и левый столбец вне левого верхнего угла:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -308 & 280 & 105 \\ 0 & 308 & -280 & -105 \end{pmatrix}$$

Так как 3-я строка кратна 2-й, и наибольший общий делитель второй строки равен 7, ненулевые множители матрицы R суть 1 и 7, а её ранг равен 2. Мы заключаем, что

$$A = \mathbb{Z}^3 / M \simeq \mathbb{Z} \oplus \mathbb{Z}/(7)\,.$$

7.2.2. Порядки элементов. На практике часто бывает важно знать, отлична ли от нуля та или иная $\mathbb{Z}$-линейная комбинация $w = k_1a_1 + \dots + k_ma_m$ образующих a_i, и если да, то каков порядок[2] $\mathrm{ord}([w])$ элемента $[w]$ в группе A. Для ответа на эти вопросы необходимо выяснить, лежит или нет какое-нибудь целое кратное zw вектора $w = (k_1, \dots, k_m)$ в целочисленной линейной оболочке строк $r_1, \dots, r_n \in \mathbb{Z}^m$ матрицы соотношений R из формулы (7-3). Если строки матрицы R линейно независимы над $\mathbb{Q}$, т. е. образуют базис модуля $M \subset \mathbb{Z}^m$ соотношений между образующими $a_1, \dots, a_m$ над $\mathbb{Z}$, то достаточно решить над полем $\mathbb{Q}$ систему уравнений

$$r_1x_1 + \dots + r_mx_m = w \tag{7-4}$$

[1] См. теор. 7.2 на стр. 120.

[2] Напомню, что *порядком* $\mathrm{ord}(w)$ элемента w в аддитивной абелевой группе называется наименьшее такое $n \in \mathbb{N}$, что $nw = 0$, а если такого n нет, то $\mathrm{ord}(w) = \infty$, см. n° 2.5.1 на стр. 51.

которая в матричных обозначениях имеет вид $R^t x = w^t$, и в силу линейной независимости векторов $r_1, \dots, r_n$ либо несовместна, либо имеет единственное рациональное решение. В первом случае никакое целое кратное zw не лежит в M. Поэтому класс $[w]_M$ отличен от нуля в группе $A = \mathbb{Z}^m / M$ и имеет в ней бесконечный порядок. Если же система (7-4) имеет рациональное решение $x_i = p_i / q_i \in \mathbb{Q}$, где нод$(p_i, q_i) = 1$ при всех i, то

$$w = \frac{p_1}{q_1} r_1 + \dots + \frac{p_n}{q_n} r_n$$

и $\operatorname{ord}([w]_M) = \text{нок}(q_1, \dots, q_n)$. В частности, $[w]_M = 0$ если и только если все $q_i = 1$, т. е. когда система (7-4) решается в целых числах.

7.2.3. Подрешётки в $\mathbb{Z}^m$. Абелевы подгруппы $L \subset \mathbb{Z}^m$ обычно называют *подрешётками* в $\mathbb{Z}^m$. Согласно теор. 6.2 на стр. 111 каждая подрешётка $L \subset \mathbb{Z}^m$ является свободным $\mathbb{Z}$-модулем ранга $\operatorname{rk} L \leqslant m$. Если $\operatorname{rk} L = m$, подрешётка L называется *соизмеримой* с $\mathbb{Z}^m$. Из сказанного выше вытекает

Предложение 7.2 (соизмеримые подрешётки)
Следующие свойства подрешётки $L_A \subset \mathbb{Z}^m$, порождённой столбцами матрицы $A \in \operatorname{Mat}_{m\times n}(\mathbb{Z})$, эквивалентны друг другу:

(1) $\operatorname{rk} L = m$

(2) факторгруппа $\mathbb{Z}^m / L$ конечна

(3) ранг матрицы A над полем $\mathbb{Q}$ равен m. □

Решётка $L \subset \mathbb{Z}^m$ называются *отщепимой*, если она удовлетворят следующему предложению.

Предложение 7.3 (отщепимые подрешётки)
Следующие свойства подрешётки $L \subset \mathbb{Z}^m$ эквивалентны друг другу:

(1) все ненулевые инвариантные множители подрешётки L равны единице

(2) факторгруппа $\mathbb{Z}^m / L$ не имеет кручения

(3) существует такая подрешётка $N \subset \mathbb{Z}^m$, что $\mathbb{Z}^m = L \oplus N$

(4) решётка L является множеством всех целых решений системы однородных линейных уравнений $Ax = 0$ с целочисленной матрицей A высоты m.

Доказательство. Равносильность условий (1), (2) и импликации (1) ⇒ (3), (4) вытекают из теоремы о взаимном базисе: если первые r базисных векторов базиса $u_1, \dots, u_m$ в $\mathbb{Z}^m$ образуют базис в L, то дополнительная к L подрешётка N является линейной оболочкой последних $m - r$ базисных векторов, а решётка L задаётся линейными однородными уравнениями, констатирующими обнуление последних $m - r$ координат вектора в базисе $u_1, \dots, u_m$.

Импликация (3) ⇒ (2) очевидна, так как $(L \oplus N)/L \simeq N$.

Докажем импликацию (4) ⇒ (2). Пусть $A \in \operatorname{Mat}_{k\times m}(\mathbb{Z})$ и подрешётка $L \subset \mathbb{Z}^m$ является ядром линейного отображения $\alpha\colon \mathbb{Z}^m \to \mathbb{Z}^k$, $x \mapsto Ax$. Тогда отображение $\overline{\alpha}\colon \mathbb{Z}^m / L \hookrightarrow \mathbb{Z}^k$, $[x] \mapsto Ax$, корректно определено и инъективно.

Упражнение 7.8. Убедитесь в этом.

Тем самым, $\mathbb{Z}^m / L$ изоморфен подмодулю модуля без кручения. □

7.3. Общие замечания о полупростоте. Пусть K — произвольное *ассоциативное кольцо*, т. е. абелева группа с операцией умножения $K \times K \to K$, которая дистрибутивна по отношению к сложению: $(x+y)z = xy + xz$, $x(y+z) = xz + yz$, и ассоциативна: $(xy)z = x(yz)$, где $x, y, z \in K$. Абелева группа V называется *левым K-модулем*, если задано умножение (или *действие*)

$$K \times V \to V\,,$$

которое тоже дистрибутивно и ассоциативно:

$$\forall\, z \in K,\ \forall\, u, w \in V\ z(u+w) = zu + zw \quad \text{и} \quad \forall\, x, y \in K,\ \forall\, v \in V\ (x+y)v = xv + yv\,,$$
$$\forall\, x, y \in K,\ \forall\, v \in V\ (xy)v = x(yv)\,.$$

Подмодуль в V — это абелева подгруппа, выдерживающая умножение на все элементы из K. Модуль U называется *простым*, если в нём нет ненулевых собственных подмодулей, и *полупростым*, если он является прямой суммой простых (не обязательно конечной).

Лемма 7.1
Пусть K-модуль W линейно порождается над K некоторым множеством $\mathcal{S}$ своих простых K-подмодулей. Тогда у любого собственного подмодуля $U \subsetneq W$ имеется дополнительный[1] подмодуль V, являющийся прямой суммой подходящих подмодулей из множества $\mathcal{S}$. Для нулевого подмодуля $U = 0$ это означает, что весь модуль W является прямой суммой подходящих подмодулей из множества $\mathcal{S}$. В частности, такой модуль W автоматически полупрост.

Доказательство. Так как $U \neq W$ и W линейно порождается подмодулями $S \in \mathcal{S}$, в множестве $\mathcal{S}$ найдётся подмодуль $S \not\subset U$. Сумма $U + S$ является прямой, поскольку пересечение $S \cap U \subsetneq S$ и S прост. Обозначим через $\mathcal{S}'$ множество всех полупростых подмодулей $M \subset W$, которые являются прямыми суммами модулей из $\mathcal{S}$ и имеют нулевое пересечение с U. По предыдущему, множество $\mathcal{S}'$ непусто. Введём на нём частичный порядок, полагая $M_1 < M_2$, когда $M_2 = M_1 \oplus M$ для ненулевого $M \in \mathcal{S}'$.

Упражнение 7.9. Убедитесь, что $\mathcal{S}'$ является полным чумом[2].

По лемме Цорна[3] в множестве $\mathcal{S}'$ имеется максимальный элемент V. По построению $U \cap V = 0$. Покажем, что $U + V = W$. Если $U + V \neq W$, то повторяя проведённое в начале доказательства рассуждение для подмодуля $U' = U + V$ в роли подмодуля U, мы найдём в $\mathcal{S}$ такой подмодуль $S \subset W$, что сумма $U' + S$ прямая. Это означает, что $V \oplus S \in \mathcal{S}'$ строго больше, чем V. Всё сказанное работает и для $U = 0$. □

Теорема 7.3
Модуль W полупрост если и только если каждый ненулевой подмодуль в W содержит простой ненулевой подмодуль и для каждого ненулевого собственного подмодуля $U \subset W$ найдётся такой подмодуль $V \subset W$, что $W = U \oplus V$.

Доказательство. Если модуль W полупрост, т. е. является прямой суммой простых подмодулей, подмодуль $V \subset W$, дополнительный к произвольно заданному подмодулю $U \subset W$, существует по лем. 7.1, применённой к множеству $\mathcal{S}$ всех простых подмодулей в W.

[1] Т. е. такой подмодуль $V \subset W$, что $W = U \oplus V$, см. прим. 5.10 на стр. 86.
[2] См. опр. 0.3 на стр. 20.
[3] См. сл. 0.1 на стр. 20.

Упражнение 7.10. Убедитесь, что проекция $\pi : W = U \oplus V \twoheadrightarrow U$, $u + v \mapsto u$, K-линейна, т. е. $\pi(xw) = x\pi(w)$ для всех $x \in K$ и $w \in W$.

Так как W линейно порождается простыми подмодулями, проекция π переводит хотя бы один из них в ненулевой подмодуль в U.

Упражнение 7.11. Убедитесь, что этот ненулевой подмодуль прост.

Это доказывает прямую импликацию «только если». Чтобы доказать обратную импликацию, обозначим через $\mathcal{S}$ множество всех полупростых ненулевых подмодулей $S \subseteq W$. Это множество непусто, поскольку содержит ненулевой простой подмодуль, имеющийся в W по условию. Зададим на $\mathcal{S}$ частичный порядок, полагая $S_1 < S_2$ когда $S_2 = S_1 \oplus S$ для некоторого $S \in \mathcal{S}$.

Упражнение 7.12. Убедитесь, что чум $\mathcal{S}$ полон.

По лемме Цорна, в $\mathcal{S}$ есть максимальный элемент M. Если он не совпадает с W, то найдётся такой нетривиальный подмодуль $V \subset W$, что $W = M \oplus V$. Поскольку в V есть нетривиальный простой подмодуль $S \subset V$, сумма $M \oplus S \in \mathcal{S}$ будет строго больше, чем M. Тем самым, $M = W$. □

Следствие 7.1 (критерии полупростоты)
Пусть каждый ненулевой подмодуль K-модуля W содержит ненулевой простой K-подмодуль. Тогда следующие свойства модуля W эквивалентны:

1) W полупрост
2) W линейно порождается простыми подмодулями
3) для каждого ненулевого собственного подмодуля $U \subset W$ существует такой ненулевой собственный подмодуль $V \subset W$, что $W = U \oplus V$. □

Упражнение 7.13. Пусть модуль V таков, что для любого ненулевого собственного подмодуля $U \subset V$ найдётся такой подмодуль $W \subset V$, что $V = U \oplus W$. Докажите, что любой подмодуль $V' \subset V$ тоже обладает этим свойством.

§8. Грассмановы многочлены и определители

8.1. Длина, знак и чётность перестановки. Биективные отображения

$$g\colon \{1,\dots,n\} \to \{1,\dots,n\}, \quad i \mapsto g_i,$$

называются *перестановками n элементов*. Перестановки образуют группу преобразований множества $\{1,\dots,n\}$ в смысле n° 0.6 на стр. 16. Эта группа обозначается $S_n = \mathrm{Aut}\big(\{1,\dots,n\}\big)$ и называется *n-той симметрической группой*. Перестановку $g \in S_n$ принято записывать словом

$$g = (g_1,\dots,g_n),$$

i-тая буква которого равна значению $g_i = g(i)$ отображения g на элементе i. Например, слово

$$(2,4,3,5,1) \in S_5$$

задаёт отображение $1 \mapsto 2$, $2 \mapsto 4$, $3 \mapsto 3$, $4 \mapsto 5$, $5 \mapsto 1$. Композиция fg перестановок f, g действует по правилу $fg\colon i \mapsto f\big(g(i)\big)$. Например, в группе S_5 две возможных композиции перестановок $f = (2,4,3,5,1)$ и $g = (3,2,1,5,4)$ суть $fg = (3,4,2,1,5)$ и $gf = (2,5,1,4,3)$.

Назовём пару возрастающих чисел $i < j$ *инверсной* для перестановки g, если $g_i > g_j$. Таким образом, каждая перестановка $g \in S_n$ разбивает множество всех $n(n-1)/2$ возрастающих пар $1 \leqslant i < j \leqslant n$ на два непересекающихся подмножества — инверсные пары и неинверсные пары. Количество инверсных пар перестановки g называется *числом инверсий* или *длиной* перестановки g и обозначается $\ell(g)$.

Упражнение 8.1. Найдите $\max \ell(g)$ по всем $g \in S_n$ и укажите все перестановки на которых он достигается.

Число $\mathrm{sgn}(g) \stackrel{\text{def}}{=} (-1)^{\ell(g)}$ называется *знаком* перестановки g. Перестановка g называется *чётной*, если $\mathrm{sgn}(g) = 1$ и *нечётной*, если $\mathrm{sgn}(g) = -1$.

Перестановка, меняющая местами какие-либо два элемента i, j и оставляющая все остальные элементы на месте, обозначается σ_{ij} и называется *транспозицией* i-го и j-го элементов.

Упражнение 8.2. Убедитесь, что каждая перестановка $g \in S_n$ является композицией транспозиций.

Разложение перестановки в композицию транспозиций не единственно: например, транспозицию $\sigma_{13} = (3,2,1) \in S_3$ иначе можно записать как $\sigma_{12}\sigma_{23}\sigma_{12}$ или как $\sigma_{23}\sigma_{12}\sigma_{23}$. Тем не менее чётность количества транспозиций, в композицию которых раскладывается данная перестановка g, не зависит от способа разложения и совпадает с чётностью числа инверсных пар перестановки g, т. е. все чётные перестановки являются композициями чётного числа транспозиций, а нечётные — нечётного. Это вытекает из следующей леммы.

Лемма 8.1
$\mathrm{sgn}(g\sigma_{ij}) = -\mathrm{sgn}(g)$ для любой перестановки $g \in S_n$ и любой транспозиции $\sigma_{ij} \in S_n$.

Доказательство. Перестановки

$$\begin{aligned} g &= \big(g_1,\dots,g_{i-1},\, \boldsymbol{g_i},\, g_{i+1},\dots,g_{i-1},\, \boldsymbol{g_j},\, g_{j+1},\dots,g_n\big) \\ g\sigma_{ij} &= \big(g_1,\dots,g_{i-1},\, \boldsymbol{g_j},\, g_{i+1},\dots,g_{i-1},\, \boldsymbol{g_i},\, g_{j+1},\dots,g_n\big) \end{aligned} \tag{8-1}$$

отличаются друг от друга транспозицией элементов g_i и g_j, стоящих на i-том и j-том местах перестановки g. В этих двух перестановках пара (i, j), а также $2(j - i - 1)$ пар вида (i, m) и (m, j) с произвольным m из промежутка $i < m < j$ имеют противоположную инверсность, а инверсность всех остальных пар одинакова. □

Следствие 8.1
Если перестановка g является композицией m транспозиций, то $\operatorname{sgn}(g) = (-1)^m$ и чётность перестановки совпадает с чётностью числа m.

Доказательство. Тождественная перестановка не имеет инверсных пар и, стало быть, чётна. В силу леммы, перестановка получающаяся из тождественной умножением на m транспозиций, имеет чётность $(-1)^m$. □

Следствие 8.2 (знаковый гомоморфизм)
Отображение $\operatorname{sgn}\colon S_n \twoheadrightarrow \{+1, -1\}$, $g \mapsto (-1)^{\ell(g)}$, является мультипликативным гомоморфизмом, т. е. $\operatorname{sgn}(gh) = \operatorname{sgn}(g)\operatorname{sgn}(h)$ для всех $g, h \in S_n$, и множества чётных и нечётных перестановок суть полные прообразы элементов 1 и -1 при этом гомоморфизме. □

Пример 8.1 (правило ниточек)
Интерпретация чётности перестановки как чётности числа инверсных пар даёт практический способ отыскания чётности перестановки — не самый быстрый[1], но полезный в ряде ситуаций, с которыми мы далее столкнёмся. Напишем исходные числа и их перестановку друг под другом, как на рис. 8◇1, и соединим одинаковые числа нитями так, чтобы ни одна из нитей не вылезала за пределы прямоугольника, образованного четырьмя угловыми числами, и чтобы все точки пересечения нитей были простыми двойными[2]. Тогда чётность числа инверсных пар будет равна чётности числа точек пересечения нитей.

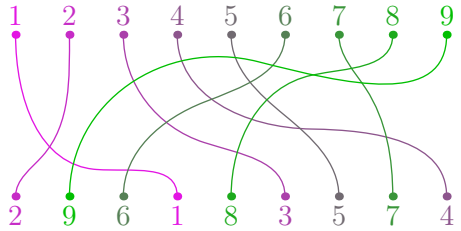


Рис. 8◇1. $\operatorname{sgn}(2, 9, 6, 1, 8, 3, 5, 7, 4) = +1$ (всего 18 пересечений).

Упражнение 8.3. Докажите это и убедитесь при помощи правила ниточек, что знак *тасующей перестановки* $(i_1, \dots, i_k, j_1, \dots, j_m)$, где оба набора номеров $i_1, \dots, i_k$ и $j_1, \dots, j_m$ возрастают слева направо, равен $\operatorname{sgn}(i_1, \dots, i_k, j_1, \dots, j_m) = (-1)^{|I|+k(k+1)/2}$, где $|I| \stackrel{\text{def}}{=} i_1 + \dots + i_k$.

[1] Обычно быстрее бывает разложить перестановку в композицию непересекающихся циклов и воспользоваться тем, что циклы чётной длины нечётны, а циклы нечётной длины чётны.

[2] Это означает, что в каждой точке пересечения встречается ровно две нити, причём пересечение происходит трансверсально:), а не по касательной:).

8.2. Определитель. Рассмотрим произвольное коммутативное кольцо K с единицей, произвольную квадратную матрицу $C = (c_{ij}) \in \mathrm{Mat}_n(K)$ и обозначим через $v_1, \dots, v_n \in K^n$ её столбцы. Многочлен

$$\det C = \det(v_1, \dots, v_n) \stackrel{\text{def}}{=} \sum\nolimits_{g \in S_n} \operatorname{sgn}(g) \cdot c_{g_1 1} c_{g_2 2} \dots c_{g_n n} \tag{8-2}$$

называется *определителем* матрицы C или набора векторов $v_1, \dots, v_n$. Формула (8-2) предписывает всеми возможными способами выбирать в матрице n элементов так, чтобы в каждой строке и в каждом столбце выбирался ровно один элемент. Каждые такие n элементов надо перемножить, а полученные $n!$ произведений сложить с надлежащими знаками, определяемыми так: множество клеток, где стоят выбранные n элементов, представляет собою график биективного отображения $j \mapsto g_j$ из множества номеров столбцов в множество номеров строк, т. е. перестановки n номеров $\{1, \dots, n\}$, и знак равен знаку этой перестановки. Например, определители матриц размеров 2×2 и 3×3 имеют вид

$$\det \begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix} = c_{11}c_{22} - c_{12}c_{21} \tag{8-3}$$

$$\det \begin{pmatrix} c_{11} & c_{12} & c_{13} \\ c_{21} & c_{22} & c_{23} \\ c_{31} & c_{32} & c_{33} \end{pmatrix} = \begin{aligned} &c_{11}c_{22}c_{33} + c_{13}c_{21}c_{32} + c_{12}c_{23}c_{31} - \\ &- c_{11}c_{23}c_{32} - c_{13}c_{22}c_{31} - c_{12}c_{21}c_{33} \end{aligned} \tag{8-4}$$

(во втором равенстве сначала выписаны тождественная и две циклических перестановки, потом — три транспозиции).

Предложение 8.1
Определитель $\det C = \det(v_1, \dots, v_n)$ линеен по каждому столбцу v_i матрицы C, кососимметричен (т. е. $\det(v_1, \dots, v_n) = 0$ если $v_i = v_j$ для некоторых $i \neq j$) и не меняется при транспонировании матрицы[1] (т. е. $\det C^t = \det C$, где $C^t = \left(c^t_{ij}\right)$ имеет $c^t_{ij} = c_{ji}$).

Доказательство. Так как каждое из $n!$ произведений, которые складываются в формуле (8-2), содержит ровно по одному сомножителю из каждого столбца, оно линейно по каждому столбцу, а значит линейна и их сумма. Если i-тый столбец матрицы C совпадает с j-тым, то $c_{g_i i} = c_{g_i j}$ и $c_{g_j j} = c_{g_j i}$ для любой перестановки $g \in S_n$. Множество всех перестановок разбивается в объединение не пересекающихся пар вида $(g, g\sigma_{ij})$, поскольку композиция с транспозицией $\sigma_{ij} \colon S_n \xrightarrow{\sim} S_n$, $g \mapsto g\sigma_{ij}$, является инволютивной[2] биекцией без неподвижных точек[3]. В сумме (8-2) слагаемые, отвечающие каждой паре g и $g\sigma_{ij}$ имеют вид

$$\operatorname{sgn}(g) \cdot c_{g_1 1} \dots c_{g_i i} \dots c_{g_j j} \dots c_{g_n n} \quad \text{и} \quad \operatorname{sgn}(g\sigma_{ij}) \cdot c_{g_1 1} \dots c_{g_j i} \dots c_{g_i j} \dots c_{g_n n}$$

и различаются только знаком, сокращая друг друга. Поэтому сумма получится нулевая. Наконец, равенство $\det C^t = \det C$ вытекает из того, что набор произведений n-ок матричных элементов в разложениях $\det C$ и $\det C^t$ одинаков, а знаки, с которыми каждое произведение входит в $\det C$ и $\det C^t$, суть знаки обратных друг другу перестановок.

Упражнение 8.4. Покажите, что знаки обратных друг другу перестановок совпадают.

Тем самым, разложения (8-2) для $\det C$ и $\det C^t$ состоят из одних и тех же слагаемых с одними и теми же знаками. □

[1] См. обсуждение перед предл. 5.4 на стр. 95.

[2] Т. е. обратной самой себе.

[3] Равенство $g = g\sigma_{ij}$ невозможно, так как умножая на g^{-1} слева, получаем $\mathrm{Id} = \sigma_{ij}$, что не так.

Следствие 8.3
Определитель является полилинейной кососимметричной функцией от строк матрицы. □

Следствие 8.4
Определитель меняет знак при любой транспозиции строк или столбцов матрицы[1].

Доказательство. В силу кососимметричности и полилинейности

$$0 = \det(\dots, (v_i + v_j), \dots, (v_i + v_j), \dots) = \det(\dots, v_i, \dots, v_j, \dots) + \det(\dots, v_j, \dots, v_i, \dots),$$

что и утверждается. □

Упражнение 8.5. Убедитесь, что если $1 + 1 \neq 0$ в K, то каждая знакопеременная функция от n векторов кососимметрична.

Пример 8.2 (знакопеременные многочлены, определитель Вандермонда и базис Шура)
Многочлен $f \in \mathbb{Z}[x_1, \dots, x_n]$ называется *знакопеременным* если для всех перестановок $g \in S^n$

$$f(x_{g_1}, \dots, x_{g_n}) = \operatorname{sgn}(g) \cdot f(x_1, \dots, x_n).$$

Так как при транспозиции любой пары переменных знакопеременный многочлен f меняет знак, в каждом мономе $x_1^{\nu_1} \dots x_n^{\nu_n}$ многочлена f все степени ν_i попарно различны, и вместе с таким мономом в f входят $n!$ мономов $x_{g_1}^{\nu_1} \dots x_{g_n}^{\nu_n}$, где $g \in S_n$, причём коэффициенты при мономах $x_1^{\nu_1} \dots x_n^{\nu_n}$ и $x_{g_1}^{\nu_1} \dots x_{g_n}^{\nu_n}$ получаются друг из друга умножением на знак $\operatorname{sgn}(g)$. Мы заключаем, что знакопеременные многочлены образуют свободный $\mathbb{Z}$ модуль с базисом из многочленов

$$\Delta_\nu \stackrel{\text{def}}{=} \sum_{g \in S_n} \operatorname{sgn}(g)\, x_{g_1}^{\nu_1} \dots x_{g_n}^{\nu_n} = \det(x_j^{\nu_i}) = \det \begin{pmatrix} x_1^{\nu_1} & x_2^{\nu_1} & \cdots & x_n^{\nu_1} \\ x_1^{\nu_2} & x_2^{\nu_2} & \cdots & x_n^{\nu_2} \\ \vdots & \vdots & \ddots & \vdots \\ x_1^{\nu_n} & x_2^{\nu_n} & \cdots & x_n^{\nu_n} \end{pmatrix}, \tag{8-5}$$

которые нумеруются диаграммами Юнга ν из n строк попарно разных длин $\nu_1 > \dots > \nu_n \geqslant 0$. Минимальной такой диаграмме $\delta = \big((n-1), \dots, 0\big)$ отвечает *определитель Вандермонда*

$$\Delta_\delta = \det(x_j^{n-i}) = \det \begin{pmatrix} x_1^{n-1} & \dots & x_n^{n-1} \\ \vdots & \vdots & \vdots \\ x_1 & \dots & x_n \\ 1 & \dots & 1 \end{pmatrix} = \prod_{i<j} (x_i - x_j). \tag{8-6}$$

Последнее равенство вытекает из того, что при подстановке $x_i = x_j$ с $j \neq i$ определитель Вандермонда, как и всякий знакопеременный многочлен, обращается в нуль, и поэтому делится в $\mathbb{Z}[x_1, \dots, x_n]$ на $x_i - x_j$. Так все такие разности неприводимы, а кольцо $\mathbb{Z}[x_1, \dots, x_n]$ факториально, определитель Вандермонда делится на $\prod_{i<j}(x_i - x_j)$, а поскольку лексикографически старшие мономы определителя и произведения равны $x_1^{n-1} x_2^{n-2} \dots x_{n-1}$ и имеют коэффициент 1, частное от деления равно 1. Это рассуждение показывает, что любой знакопеременный многочлен f делится в $\mathbb{Z}[x_1, \dots, x_n]$ на определитель Вандермонда, и частное является симметрическим многочленом. Мы заключаем, что знакопеременные многочлены образуют свободный модуль ранга 1 с базисом Δ_δ над кольцом симметрических многочленов, а симметрические *многочлены Шура* $\sigma_\lambda = \Delta_{\lambda+\delta}/\Delta_\delta$, где $\lambda = (\lambda_1, \dots, \lambda_n)$ пробегает произвольные диаграммы Юнга из n строк, а $\lambda + \delta = (\lambda_1 + (n-1), \lambda_2 + (n-2), \dots, \lambda_n)$, образуют базис $\mathbb{Z}$-модуля симметрических многочленов.

[1] Функции с таким свойством называются *знакопеременными*.

8.3. Грассмановы многочлены. Алгебра *грассмановых многочленов* $K\langle\xi_1,\dots,\xi_n\rangle$ от переменных $\xi_1,\dots,\xi_n$ с коэффициентами в произвольном коммутативном кольце K с единицей определяется точно также, как алгебра обычных многочленов, но только грассмановы переменные ξ_i, в отличие от обычных, не коммутируют, а *антикоммутируют* друг с другом, т. е. подчиняются соотношениям[1]

$$\forall\, i,j \quad \xi_i\wedge\xi_j = -\xi_j\wedge\xi_i \quad \text{и} \quad \forall\, i \quad \xi_i\wedge\xi_i = 0\,. \tag{8-7}$$

Символ «$\wedge$» здесь и далее используется для обозначения грассманова (антикоммутативного) умножения, чтобы отличать его от обычного (коммутативного). Константы из K по определению перестановочны с грассмановыми переменными, и умножение переменных на константы записывается обычным образом: $a\xi_i = \xi_i a$, для всех i и всех $a\in K$. Для каждой строго возрастающей слева направо последовательности номеров $I=(i_1,\dots,i_m)$, где $i_1<\dots<i_m$, положим

$$\xi_I \stackrel{\text{def}}{=} \xi_{i_1}\wedge\dots\wedge\xi_{i_m}\,. \tag{8-8}$$

Каждая перестановка $g=(g_1,\dots,g_m)\in S_m$ переменных в этом мономе меняет его знак по правилу

$$\xi_{i_{g(1)}}\wedge\dots\wedge\xi_{i_{g(m)}} = \operatorname{sgn}(g)\cdot\xi_{i_1}\wedge\dots\wedge\xi_{i_m}\,. \tag{8-9}$$

Поскольку квадраты грассмановых переменных равны нулю, мономы (8-9) исчерпывают всё множество грассмановых мономов, т. е. однородные грассмановы многочлены степени m от n переменных $\xi_1,\dots,\xi_n$ по-определению образуют свободный K-модуль ранга $\binom{n}{m}$ с базисом из мономов (8-8). Этот модуль обозначается Λ^m. Вся грассманова алгебра как модуль над K является конечной прямой суммой $K\langle\xi_1,\dots,\xi_n\rangle = \Lambda^0\oplus\Lambda^1\oplus\Lambda^2\oplus\dots\oplus\Lambda^n$, где младшее слагаемое $\Lambda^n\simeq K$ состоит из констант и имеет в качестве базиса моном $\xi_\varnothing\stackrel{\text{def}}{=}1$, отвечающий пустому набору $I=\varnothing$ и служащий единицей грассмановой алгебры, а старшее слагаемое $\Lambda^n\simeq K$ имеет в качестве базиса $\xi_{(1,\dots,n)}=\xi_1\wedge\dots\wedge\xi_n$ — единственный моном степени n, отвечающий набору $I=(1,\dots,n)$. Обратите внимание, что этот моном аннулируется умножением на любой грассманов многочлен с нулевым свободным членом. Умножение базисных мономов $\xi_I=\xi_{i_1}\wedge\dots\wedge\xi_{i_k}$ и $\xi_J=\xi_{j_1}\wedge\dots\wedge\xi_{j_m}$ происходит по правилу

$$\xi_I\wedge\xi_J = \begin{cases}\operatorname{sgn}(I,J)\,\xi_{I\sqcup J} & \text{если } I\cap J=\varnothing\\ 0 & \text{если } I\cap J\neq\varnothing\,,\end{cases} \tag{8-10}$$

где $\operatorname{sgn}(I,J)$ — знак тасующей перестановки, упорядочивающей набор $(i_1,\dots,i_k,\,j_1,\dots,j_m)$ по возрастанию[2]. Так как для базисных грассмановых мономов выполняется равенство[3]

$$(\xi_{i_1}\wedge\dots\wedge\xi_{i_k})\wedge(\xi_{j_1}\wedge\dots\wedge\xi_{j_m}) = (-1)^{km}(\xi_{j_1}\wedge\dots\wedge\xi_{j_m})\wedge(\xi_{i_1}\wedge\dots\wedge\xi_{i_k})\,,$$

однородные грассмановы многочлены коммутируют друг с другом по правилу

$$\omega\wedge\eta = (-1)^{\deg\omega\deg\eta}\eta\wedge\omega\,, \tag{8-11}$$

[1] Если $1+1$ не делит нуль в K, то соотношения $\xi_i\wedge\xi_i=0$ могут быть опущены, поскольку они вытекают из соотношений $\xi_i\wedge\xi_j=-\xi_j\wedge\xi_i$, если положить в них $i=j$. Если же $-1=1$, то антикоммутирование $\xi_i\wedge\xi_j=-\xi_j\wedge\xi_i$ не отличается от коммутирования $\xi_i\wedge\xi_j=\xi_j\wedge\xi_i$, и в этой ситуации именно соотношение $\xi_i\wedge\xi_i=0$ отличает грассмановы переменные от обычных.

[2] Если $I\sqcup J=\{1,\dots,n\}$, то $\operatorname{sgn}(i_1,\dots,i_k,\,j_1,\dots,j_m)=(-1)^{|I|+k(k+1)/2}$ по упр. 8.3 на стр. 129.

[3] Для проноса каждой из m переменных ξ_j влево через k переменных ξ_i нужно совершить k транспозиций.

которое называется *кошулевым правилом знаков*. В частности, любой однородный многочлен чётной степени коммутирует со всеми грассмановыми многочленами.

Упражнение 8.6. Опишите *центр* грассмановой алгебры

$$Z(K\langle\xi_1,\dots,\xi_n\rangle) \stackrel{\text{def}}{=} \{\tau\in K\langle\xi_1,\dots,\xi_n\rangle \mid \forall\,\omega\in K\langle\xi_1,\dots,\xi_n\rangle\ \ \tau\wedge\omega=\omega\wedge\tau\}\,.$$

8.3.1. Грассманова алгебра свободного модуля. Обозначим через V свободный K-модуль ранга r. Если векторы $e_1,\dots,e_r\in V$ образуют базис модуля V, то алгебра грассмановых многочленов $K\langle e_1,\dots,e_r\rangle$ от переменных $e_1,\dots,e_r$ обозначается ΛV и называется *грассмановой* (или *внешней*) алгеброй свободного модуля V, а подмодуль однородных грассмановых многочленов степени d обозначается $\Lambda^d V\subset\Lambda V$ и называется d-й *внешней степенью* свободного модуля V. Эти не апеллирующие к выбору базиса названия и обозначения связаны с тем, что при каждом $d=0,1,\dots,n$ подмодуль $\Lambda^d=\Lambda^d V\subset K\langle e_1,\dots,e_r\rangle$ однородных многочленов степени d не зависит от выбора базиса в V. В самом деле, подмодуль констант $\Lambda^0 V\simeq K$ порождается единицей грассмановой алгебры, подмодуль $\Lambda^1 V$ однородных грассмановых многочленов степени 1, т. е. множество всевозможных K-линейных комбинаций базисных векторов $e_1,\dots,e_r$, канонически отождествляется с модулем V и тоже не зависит от выбора базиса, а для прочих d подмодуль $\Lambda^d V\subset K\langle e_1,\dots,e_r\rangle$ является линейной оболочкой всевозможных произведений $v_1\wedge\ldots\wedge v_d$, составленных из d произвольных векторов $v_i\in V$ и опять таки не зависит от выбора базиса. Таким образом, вся алгебра $\Lambda V=\bigoplus_{d=0}^n\Lambda^d V$ является прямой суммой модулей, не зависящих от выбора базиса в V.

Упражнение 8.7. Убедитесь, что $v\wedge v=0$ и $u\wedge w=-w\wedge u$ для всех $u,v,w\in V$.

8.3.2. Линейные замены переменных и миноры. Пусть в обозначениях их предыдущего раздела n однородных грассмановых линейных форм $\eta_1,\dots,\eta_n\in\Lambda^1 V$ линейно выражается через m однородных грассмановых форм $\xi_1,\dots,\xi_m\in\Lambda^1 V$ по формуле

$$(\eta_1,\dots,\eta_n)=(\xi_1,\dots,\xi_m)\cdot C\,,$$

где $C\in\mathrm{Mat}_{n\times k}(K)$. Тогда при каждом $d=1,\dots,\min(m,n)$ набор мономов $\eta_J=\eta_{j_1}\wedge\ldots\wedge\eta_{j_d}$ степени d линейно выражается через набор мономов $\xi_I=\xi_{i_1}\wedge\ldots\wedge\xi_{i_d}$ степени d по формуле

$$\begin{aligned}\eta_J=\eta_{j_1}\wedge\ldots\wedge\eta_{j_d}&=\Big(\sum_{i_1}\xi_{i_1}c_{i_1j_1}\Big)\wedge\Big(\sum_{i_2}\xi_{i_2}c_{i_2j_2}\Big)\wedge\ldots\wedge\Big(\sum_{i_d}\xi_{i_d}c_{i_dj_d}\Big)=\\&=\sum_{1\leqslant i_1<\ldots<i_d\leqslant m}\xi_{i_1}\wedge\ldots\wedge\xi_{i_d}\cdot\sum_{g\in S_d}\operatorname{sgn}(g)\,c_{i_{g(1)}j_1}\ldots c_{i_{g(d)}j_d}=\sum_I\xi_I\cdot c_{IJ}\,,\end{aligned}\tag{8-12}$$

где $I=(i_1,\dots,i_d)$ пробегает наборы из d возрастающих номеров, а $c_{IJ}=\det C_{IJ}$ обозначает определитель $d\times d$-подматрицы $C_{IJ}\subset C$, сосредоточенной в пересечениях столбцов с номерами из J и строк с номерами из I. Определитель $c_{IJ}\stackrel{\text{def}}{=}\det C_{IJ}$ называется IJ-тым *минором* d-того порядка в матрице C. Таким образом, IJ-тый элемент матрицы, выражающей грассманов моном η_J через грассмановы мономы ξ_I равен IJ-тому минору d-того порядка в матрицы выражающей переменные η через переменные ξ. Матрица размера $\binom{n}{d}\times\binom{n}{d}$, клетки которой нумеруются лексикографически упорядоченными наборами I из d возрастающих номеров и которая имеет в клетке (IJ) минор c_{IJ} матрицы C, обозначается $\Lambda^d C$ и называется d-*й внешней степенью* матрицы C.

Предложение 8.2 (мультипликативность внешних степеней)
Для любых матриц $A \in \mathrm{Mat}_{m\times k}(K)$, $B \in \mathrm{Mat}_{k\times n}(K)$ над произвольным коммутативным кольцом K при всех $1 \leqslant d \leqslant \min(m,n,k)$ выполняется равенство $\Lambda^d(A\cdot B) = \Lambda^d A \cdot \Lambda^d B$. В частности, для квадратных матриц A и B одинакового размера $\det(AB) = \det(A)\det(B)$.

Доказательство. Рассмотрим в свободном K-модуле V с базисом $\boldsymbol{e} = (e_1,\dots,e_m)$ наборы векторов $\boldsymbol{a} = (a_1,\dots,a_k) = \boldsymbol{e}\,A$ и $\boldsymbol{b} = (b_1,\dots,b_n) = \boldsymbol{a}\,B = \boldsymbol{e}\,AB$. Обозначим через $\boldsymbol{e_d} \subset \Lambda^d V$ набор из $\binom{m}{d}$ грассмановых мономов $e_I = e_{i_1}\wedge\ldots\wedge e_{i_d}$, а через $\boldsymbol{b_d}, \boldsymbol{a_d} \subset \Lambda^d V$ — наборы из $\binom{n}{d}$ и $\binom{k}{d}$ грассмановых многочленов $b_J = b_{j_1}\wedge\ldots\wedge b_{j_d}$ и $a_L = a_{\ell_1}\wedge\ldots\wedge a_{\ell_d}$ соответственно. Набор мономов $\boldsymbol{e_d}$ является базисом в $\Lambda^d V$, а набор многочленов $\boldsymbol{b_d}$ выражается через него, с одной стороны, как $\boldsymbol{b_d} = \boldsymbol{e_d}\,\Lambda^d(AB)$, а с другой стороны — как $\boldsymbol{b_d} = \boldsymbol{a_d}\,\Lambda^d B = \boldsymbol{e_d}\,\Lambda^d A\,\Lambda^d B$. Поскольку матрица перехода от произвольного набора векторов к базису однозначно определяется этим набором, мы заключаем, что $\Lambda^d(A\cdot B) = \Lambda^d A\cdot\Lambda^d B$. □

Пример 8.3 (детерминантная формула для инвариантных множителей)
Из предл. 8.2 вытекает, что столбцы матрицы $\Lambda^k(AB)$ являются линейными комбинациями столбцов матрицы $\Lambda^k A$. Поэтому любое число $x \in K$, делящее все $k\times k$ миноры матрицы A, делит и все $k\times k$ миноры матрицы AB для любой матрицы B, на которую A можно умножить справа. Если матрица B обратима, то $A = (AB)B^{-1}$ получается из матрицы AB правым умножением на матрицу B^{-1}, и значит, число $x \in K$, делящее все $k\times k$ миноры матрицы AB, делит и все $k\times k$ миноры матрицы A. Мы заключаем, что наибольший общий делитель $k\times k$ миноров любой матрицы A не меняется при умножении матрицы A справа на обратимые матрицы. Аналогично проверяется, что наибольший общий делитель $k\times k$ миноров матрицы A не меняется при умножении матрицы A на обратимые матрицы слева. Обозначим наибольший общий делитель всех $k\times k$ миноров матрицы A через $\Delta_k(A)$.

Если кольцо K является областью главных идеалов, то по теор. 6.1 на стр. 103 для любой матрицы A найдутся такие обратимые матрицы L и R, что у матрицы $D_A = LAR$ все элементы d_{ij} с $i \neq j$ нулевые, и $d_{ii} \mid d_{jj}$ при $i < j$. Поскольку $\Delta_k(D_A) = d_{11}\ldots d_{kk}$ и $\Delta_k(A) = \Delta_k(D_A)$, мы заключаем, что $d_{ii} = \Delta_i(A)/\Delta_{i-1}(A)$, если $\Delta_{i-1}(A) \neq 0$, а если $\Delta_k(A) = 0$ при каком-то k, то $d_{jj} = 0$ при всех $j \geqslant k$. Это даёт новое доказательство независимости нормальной формы Смита[1] D_A и инвариантных множителей d_{ii} матрицы A от способа её приведения к нормальной форме Смита.

Пример 8.4 (дискриминант соизмеримой подрешётки и формула Пика)
Пусть $\mathbb{Z}$-подмодуль $U \subset \mathbb{Z}^n$ таков, что фактор $\mathbb{Z}^n/U$ конечен. Обозначим через $\boldsymbol{e}$ какой-нибудь базис в $\mathbb{Z}^n$, а через $\boldsymbol{u} = \boldsymbol{e}\,C_{\boldsymbol{eu}}$ — какой-нибудь базис в U. Абсолютная величина определителя матрицы $C_{\boldsymbol{eu}}$ называется *дискриминантом* соизмеримой[2] с $\mathbb{Z}^n$ подрешётки U и обозначается

$$D_U \stackrel{\text{def}}{=} |\det C_{\boldsymbol{eu}}|\,.$$

Упражнение 8.8. Покажите, что если матрица $C \in \mathrm{Mat}_n(K)$ обратима, то $\det C$ обратим в K.

Из упражнения вытекает, что дискриминант не зависит от выбора базисов $\boldsymbol{e}$ и $\boldsymbol{u}$, так как для любых других базисов $\boldsymbol{v} = \boldsymbol{e}\,C_{\boldsymbol{ev}}$ в $\mathbb{Z}^n$ и $\boldsymbol{w} = \boldsymbol{u}\,C_{\boldsymbol{uw}}$ в L матрицы переходов $C_{\boldsymbol{ve}} = C_{\boldsymbol{ev}}^{-1}$ и $C_{\boldsymbol{uw}}$, будучи обратимыми над $\mathbb{Z}$, имеют определители ±1, откуда

$$|\det C_{\boldsymbol{vw}}| = |\det(C_{\boldsymbol{ve}}C_{\boldsymbol{eu}}C_{\boldsymbol{uw}})| = |\det(C_{\boldsymbol{ve}})\,\det(C_{\boldsymbol{eu}})\,\det(C_{\boldsymbol{uw}})| = |\det C_{\boldsymbol{eu}}|\,.$$

[1] См. n° 6.1.1 на стр. 103.
[2] См. предл. 7.2 на стр. 125.

Беря качестве $\boldsymbol{e}$ и $\boldsymbol{u}$ взаимные базисы $v_1, \dots, v_n$ и $\lambda_1 e_1, \dots, \lambda_n e_n$, заключаем, что дискриминант $D_U = \lambda_1 \dots \lambda_n$ равен числу элементов в факторе $\mathbb{Z}^n / U \simeq \mathbb{Z}/(\lambda_1) \oplus \dots \oplus \mathbb{Z}/(\lambda_n)$.

На геометрическом языке[1] дискриминант D_U решётки $L \subset \mathbb{Z}^n \subset \mathbb{R}^n$ равен евклидову объёму[2] параллелепипеда Π, натянутого в пространстве $\mathbb{R}^n$ на какой-нибудь базис решётки U. Такой параллелепипед называется *фундаментальным параллелепипедом* решётки U. Его сдвиги на векторы решётки покрывают всё пространство $\mathbb{R}^n$, не имея при этом общих внутренних точек. Каждый элемент фактора $\mathbb{Z}^n / U$ представляется точкой, лежащей в Π. При этом каждая внутренняя точка Π не сравнима по модулю U ни с какими другими точками из Π, каждая внутренняя точка любой $(n-1)$-мерной гиперграни Π сравнима ещё ровно с одной точкой из Π, лежащей на параллельной гиперграни, каждая внутренняя точка любой $(n-2)$-мерной грани Π сравнима ровно с тремя точками из Π, лежащими на трёх параллельных $(n-2)$-мерных гранях, и т. д. Каждая вершина Π сравнима с остальными $2^n - 1$ вершинами. Мы заключаем, что объём Π, равный числу элементов в факторе $\mathbb{Z}^n/U$, может быть вычислен по *формуле Пика*:

$$\operatorname{Vol}\Pi = \sum\nolimits_{d=0}^{n} p_d / 2^{n-d},$$

где p_d при $d < n$ обозначает число точек, лежащих внутри d-мерных граней Π, а p_n — число внутренних точек самого Π.

8.3.3. Соотношения Лапласа. Для каждого набора из m возрастающих индексов

$$J = (j_1, \dots, j_m) \subset \{1, \dots, n\}$$

положим $\deg J \stackrel{\text{def}}{=} m$, $|J| \stackrel{\text{def}}{=} j_1 + \dots + j_m$ и обозначим через $\bar{J} = (\bar{j}_1, \dots, \bar{j}_{n-m}) = \{1, \dots, n\} \smallsetminus J$ дополнительный к J набор из $n-m$ возрастающих индексов. Для произвольной квадратной матрицы $A = (a_{ij}) \in \operatorname{Mat}_n(K)$ рассмотрим в грассмановой алгебре $K\langle \xi_1, \dots, \xi_n \rangle$ набор из n линейных форм

$$\alpha_j = \xi_1 a_{1j} + \xi_2 a_{2j} + \dots + \xi_n a_{nj}, \quad \text{где} \quad 1 \leqslant j \leqslant r, \tag{8-13}$$

или, в матричных обозначениях, $(\alpha_1, \dots, \alpha_n) = (\xi_1, \dots, \xi_n) A$. Для двух наборов индексов I, J одинаковой длины $\deg I = \deg J = m$ произведения

$$\alpha_J = \alpha_{j_1} \wedge \dots \wedge \alpha_{j_m} \quad \text{и} \quad \alpha_{\bar{I}} = \alpha_{\bar{i}_1} \wedge \dots \wedge \alpha_{\bar{i}_{n-m}}$$

имеют дополнительные степени m и $n-m$. Перемножая их по формуле (8-10), получим[3]

$$\alpha_J \wedge \alpha_{\bar{I}} = \begin{cases} (-1)^{|J| + \frac{m(m+1)}{2}} \alpha_1 \wedge \dots \wedge \alpha_n & \text{при } I = J \\ 0 & \text{при } I \neq J \end{cases} \tag{8-14}$$

Подставляя в равенство (8-14) разложения (8-13) и пользуясь формулами (8-12), в левой части равенства получим

$$\Big(\sum_M \xi_M a_{MJ}\Big) \wedge \Big(\sum_L \xi_L a_{L\bar{I}}\Big) = (-1)^{\frac{m(m+1)}{2}} \xi_1 \wedge \dots \wedge \xi_n \sum_M (-1)^{|M|} a_{MJ} a_{\overline{MI}},$$

[1] См. лекцию http://video.bogomolov-lab.ru/gorod/ps/stud/geom_ru/2122/lec_08.pdf.

[2] См. раздел 1.2.1 на стр. 133 лекции
http://video.bogomolov-lab.ru/gorod/ps/stud/geom_ru/2122/lec_10.pdf.

[3] Знак соответствующей тасующей перестановки был вычислен в упр. 8.3 на стр. 129.

где M пробегает все индексы длины $\deg M = m$, а в правой части при $I \neq J$ по-прежнему будет 0, а при $I = J$ получится $(-1)^{\frac{m(m+1)}{2}+|J|} \det A \cdot \xi_1 \wedge \ldots \wedge \xi_n$. Мы заключаем, для любых двух наборов J, I из m столбцов произвольной квадратной матрицы $A \in \mathrm{Mat}_n(K)$ выполняются *соотношения Лапласа*

$$\sum_M (-1)^{|M|+|J|} a_{MJ} a_{\overline{MI}} = \begin{cases} \det A & \text{при } I = J, \\ 0 & \text{при } I \neq J, \end{cases} \tag{8-15}$$

где суммирование идёт по всем наборам M из m строк матрицы A.

При $I = J$ соотношение (8-15) даёт формулу для вычисления определителя $\det A$ через всевозможные миноры a_{MJ} порядка m, сосредоточенные в m фиксированных столбцах матрицы A с номерами J, и *дополнительные* к ним миноры $a_{\overline{JM}}$ порядка $n - m$, равные определителям матриц, получающихся из A вычёркиванием всех строк и столбцов, содержащих минор a_{MJ}:

$$\det A = \sum_M (-1)^{|M|+|J|} a_{MJ} a_{\overline{MJ}}\,. \tag{8-16}$$

Произведение $(-1)^{|M|+|J|} a_{\overline{MJ}}$ называется *алгебраическим дополнением* к минору a_{MJ}. При $I \neq J$ соотношение (8-15) с точностью до знака имеет вид

$$\sum_M (-1)^{|M|+|I|} a_{MJ} a_{\overline{MI}} = 0 \tag{8-17}$$

и называется *теоремой об умножении на чужие алгебраические дополнения*, поскольку левая часть в (8-17) отличается от (8-16) тем, что миноры a_{MJ} умножаются не на свои алгебраические дополнения, а на дополнения к сосредоточенным в другом наборе столбцов $I \neq J$ минорам a_{MI}.

Упражнение 8.9. Установите транспонированный вариант соотношений Лапласа

$$\sum_M (-1)^{|I|+|M|} a_{JM} a_{\overline{IM}} = \begin{cases} \det A & \text{при } I = J \\ 0 & \text{при } I \neq J. \end{cases} \tag{8-18}$$

Если обозначить через $\Lambda^m A^\vee$ матрицу размера $\binom{n}{m} \times \binom{n}{m}$, клетки которой, как и у матрицы $\Lambda^m A$, нумеруются m-элементными подмножествами $I, J \subset \{1, \ldots, n\}$, но в клетке (IJ) стоит *алгебраическое дополнение* к JI-минору[1] матрицы A, т. е. $(-1)^{|I|+|J|} a_{\overline{JI}}$, то все соотношения (8-15) и (8-18) можно свернуть в одно матричное равенство

$$\Lambda^m A \cdot \Lambda^m A^\vee = \Lambda^m A^\vee \cdot \Lambda^m A = \det(A) \cdot E\,, \tag{8-19}$$

где E — единичная матрицу размера $\binom{n}{d} \times \binom{n}{d}$. Матрица $\Lambda^m A^\vee$ называется *присоединённой* к матрице $\Lambda^m A$.

Пример 8.5 (соотношение Плюккера)
Рассмотрим 2×4 матрицу

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \end{pmatrix}$$

[1] Обратите внимание, что индексы I и J преставились!

с элементами из кольца $K = \mathbb{Z}[a_{11}, \dots, a_{22}]$ многочленов от восьми переменных a_{ij} и обозначим через $A_{ij} = a_{1i}a_{2j} - a_{1j}a_{2i}$, где $1 \leqslant i < j \leqslant 4$, её 2×2 минор, образованный i-м и j-м столбцами. Раскладывая нулевой определитель

$$0 = \det \begin{pmatrix} A \\ A \end{pmatrix} = \det \begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \end{pmatrix}$$

по первым двум строкам, заключаем, что шесть миноров A_{ij} связаны *соотношением Плюккера*

$$A_{12}A_{34} - A_{13}A_{24} + A_{14}A_{23} = 0\,. \tag{8-20}$$

Упражнение 8.10. Убедитесь, для любого поля $\Bbbk$ и любых шести чисел $A_{ij} \in \Bbbk$, удовлетворяющих соотношению (8-20), существует матрица $A \in \mathrm{Mat}_{2\times 4}(\Bbbk)$ с 2×2 минорами A_{ij}.

Мы заключаем, что шесть чисел A_{ij} из поля $\Bbbk$ являются минорами 2×4 матрицы с элементами из $\Bbbk$ если и только если они удовлетворяют соотношению Плюккера (8-20).

Пример 8.6 (определитель пучка матриц)
Рассмотрим квадратные матрицы $A, B \in \mathrm{Mat}_n(K)$ и пару коммутирующих переменных x, y. Матрица $x\,A + y\,B$ имеет элементы в $K[x, y]$, и её определитель $\det(x\,A + y\,B)$ является однородным многочленом степени n от x и y. Покажем, что его коэффициент при $x^m y^{n-m}$ равен

$$\mathrm{tr}(\Lambda^m A \cdot \Lambda^m B^\vee) = \sum\nolimits_{IJ} (-1)^{|I|+|J|} a_{IJ} b_{\overline{IJ}}\,, \tag{8-21}$$

где суммирование идёт по всем m-элементным подмножествам $I, J \subset \{1, \dots, n\}$. Для этого рассмотрим наборы линейных форм $(\alpha_1, \dots, \alpha_n) = (\xi_1, \dots, \xi_n)\,A$ и $(\beta_1, \dots, \beta_n) = (\xi_1, \dots, \xi_n)\,B$ от грассмановых переменных $\xi_1, \dots, \xi_n$. Тогда

$$\det(xA + yB) \cdot \xi_1 \wedge \ldots \wedge \xi_n = (x\alpha_1 + y\beta_1) \wedge (x\alpha_2 + y\beta_2) \wedge \ \ldots \ \wedge (x\alpha_n + y\beta_n)\,.$$

Моном $x^m y^{n-m}$ возникает при выборе первого слагаемого в каких-либо m скобках, скажем, с номерами $i_1, \dots, i_m$, и второго слагаемого во всех остальных скобках. Вклад такого произведения в коэффициент при $x^m y^{n-m}$ равен

$$\begin{aligned} \mathrm{sgn}(i_1, \dots, i_m, \bar{i}_1, \dots, \bar{i}_{n-m}) \cdot \alpha_{i_1} \wedge \ldots \wedge \alpha_{i_k} \wedge \beta_{\bar{i}_1} \wedge \ldots \wedge \beta_{\bar{i}_{n-m}} = \\ = (-1)^{\frac{m(m+1)}{2}+|I|} \alpha_I \wedge \beta_{\bar{I}} = (-1)^{\frac{m(m+1)}{2}+|I|} \Big(\sum_J \xi_J a_{JI}\Big) \wedge \Big(\sum_M \xi_M b_{M\bar{I}}\Big) = \\ = (-1)^{\frac{m(m+1)}{2}+|I|} \sum_{JM} a_{JI} \cdot b_{M\bar{I}} \cdot \xi_J \wedge \xi_M = \Big(\sum_J (-1)^{|I|+|J|} a_{JI} \cdot b_{\overline{JI}}\Big) \cdot \xi_1 \wedge \ldots \wedge \xi_n. \end{aligned}$$

Коэффициент при $x^m y^{n-m}$ в $\det(x\,A + y\,B)$ равен сумме этих вкладов по всем наборам I из m возрастающих номеров, что и даёт формулу (8-21).

8.4. Присоединённая матрица. При $m = 1$ в вычислениях из n° 8.3.3 на стр. 135 наборы $I = (i)$, $J = (j)$ содержат по одному индексу и миноры $a_{IJ} = a_{ij}$ превращаются в матричные элементы, так что $\Lambda^1 A = A$. Присоединённая матрица $\Lambda^1 A^\vee$ в этом случае обозначается просто $A^\vee = (a^\vee_{ij})$ и называется *присоединённой* к матрице A. Она имеет в клетке (i, j) определитель $(n-1)\times(n-1)$-подматрицы, получающейся из A выкидыванием креста с центром в клетке (j, i), т. е.

$$a^\vee_{ij} = (-1)^{i+j} a_{\overline{ji}}\,.$$

Соотношения Лапласа из форм. (8-19) на стр. 136 в этом случае превращаются в равенства

$$AA^\vee = A^\vee A = \det(A)\cdot E \tag{8-22}$$

в алгебре матриц $\mathrm{Mat}_n(K)$.

8.4.1. Формула для обратной матрицы. Если определитель матрицы $A \in \mathrm{Mat}_n(K)$ обратим в K, то по (8-22) матрица A тоже обратима, и $A^{-1} = A^\vee/\det A$. Наоборот, если матрица A обратима, то $1 = \det E = \det(AA^{-1}) = \det(A)\det(A^{-1})$, и $\det A$ обратим в K. Мы получаем

Предложение 8.3
Квадратная матрица $A \in \mathrm{Mat}_n(K)$ с элементами из произвольного коммутативного кольца K с единицей обратима если и только если $\det A$ обратим в K, и в этом случае $A^{-1} = A^\vee/\det A$. □

Пример 8.7
Для матриц размера 2×2 и 3×3 с определителем 1

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}^{-1} = \begin{pmatrix} (a_{22}a_{33} - a_{23}a_{32}) & -(a_{12}a_{33} - a_{13}a_{31}) & (a_{12}a_{23} - a_{13}a_{22}) \\ -(a_{21}a_{33} - a_{23}a_{31}) & (a_{11}a_{33} - a_{13}a_{31}) & -(a_{11}a_{23} - a_{13}a_{21}) \\ (a_{21}a_{32} - a_{22}a_{31}) & -(a_{11}a_{32} - a_{12}a_{32}) & (a_{11}a_{22} - a_{12}a_{21}) \end{pmatrix}.$$

В общем случае все элементы матриц в правых частях надо поделить на $\det A$.

8.4.2. Разложение определителя по строке или столбцу. Вычисляя элемент в позиции ii первого произведения в (8-22), получаем равенство

$$\det A = \sum\nolimits_{j=1}^{n} (-1)^{i+j} a_{ij} A_{ij} \tag{8-23}$$

которое называется *разложением определителя по i-той строке*. Симметричным образом, вычисление jj-того элемента второго произведения в (8-22) даёт *разложение по j-му столбцу*

$$\det A = \sum\nolimits_{i=1}^{n} (-1)^{i+j} a_{ij} A_{ij}\,. \tag{8-24}$$

Например, разложение определителя 3×3 по первому столбцу имеет вид:

$$\det \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} = \\ = a_{11}\left(a_{22}a_{33} - a_{23}a_{32}\right) - a_{21}\left(a_{12}a_{33} - a_{13}a_{32}\right) + a_{31}\left(a_{12}a_{23} - a_{13}a_{22}\right)\,.$$

8.4.3. Правило Крамера для систем однородных линейных уравнений. Рассмотрим систему n линейных однородных уравнений на $n+1$ неизвестных

$$\begin{cases} a_{10}x_0 + a_{11}x_1 + \ldots + a_{1n}x_n = 0 \\ a_{20}x_0 + a_{21}x_1 + \ldots + a_{2n}x_n = 0 \\ \ldots\ldots\ldots\ldots\ldots \\ a_{n0}x_1 + a_{n1}x_1 + \ldots + a_{nn}x_n = 0 \end{cases} \tag{8-25}$$

и построим по матрице $A = (a_{ij})$ её коэффициентов вектор $\alpha = (A_0, A_1, \ldots, A_n) \in K^{n+1}$, у которого i-я координата равна умноженному на $(-1)^i$ определителю квадратной $n\times n$-матрицы, получающейся из $n \times (n+1)$-матрицы A выкидыванием i-того столбца:

$$A_i = (-1)^i \det \begin{pmatrix} a_{1,0} & \ldots & a_{1,i-1} & a_{1,i+1} & \ldots & a_{1,n} \\ a_{2,0} & \ldots & a_{2,i-1} & a_{2,i+1} & \ldots & a_{2,n} \\ \vdots & \ldots & \vdots & \vdots & \ldots & \vdots \\ a_{n,0} & \ldots & a_{n,i-1} & a_{n,i+1} & \ldots & a_{n,n} \end{pmatrix} \tag{8-26}$$

Покажем, что вектор α является решением системы (8-25). Дописывая к матрице A сверху ещё один экземпляр её i-той строки, мы получим квадратную матрицу размера $(n+1)\times(n+1)$ с нулевым определителем. Раскладывая этот определитель по верхней строке, получаем равенство $a_{i0}A_0 + \ldots + a_{in}A_n = 0$, справедливое при каждом i.

Упражнение 8.11. Проверьте, что если кольцо $K = \Bbbk$ является полем, то уравнения (8-25) линейно независимы если и только если $\alpha \neq 0$, и в этом случае решения системы (8-25) образуют в $\Bbbk^{n+1}$ одномерное векторное подпространство, порождённое вектором α.

Например, в векторном пространстве $\Bbbk^3$ пересечение не совпадающих плоскостей

$$\begin{cases} a_1x + a_2y + a_3z = 0 \\ b_1x + b_2y + b_3z = 0 \end{cases}$$

является прямой с направляющим вектором $(a_2b_3 - a_3b_2,\ -a_1b_3 + a_3b_1,\ a_1b_2 - a_2b_1)$.

8.4.4. Правило Крамера для систем неоднородных уравнений. По предл. 5.6 на стр. 97 столбцы $v_1, \ldots, v_n$ квадратной матрицы $C \in \mathrm{Mat}_n(K)$ образуют базис модуля K^n если и только если матрица C обратима, что по предл. 8.3 равносильно обратимости в K её определителя $\det(v_1, \ldots, v_n) = \det C$. Если это так, то коэффициенты разложения

$$w = x_1v_1 + \ldots + x_nv_n$$

произвольного вектора $w \in K^n$ по базису $v_1, \ldots, v_n$ вычисляются по *правилу Крамера*

$$x_i = \frac{\det\left(v_1, \ldots, v_{i-1},\ w,\ v_{i+1}, \ldots, v_n\right)}{\det(v_1, \ldots, v_n)}, \tag{8-27}$$

так как

$$\begin{aligned} \det\left(v_1, \ldots, v_{i-1}, w, v_{i+1}, \ldots, v_n\right) &= \det\Big(v_1, \ldots, v_{i-1}, \sum\nolimits_\nu x_\nu v_\nu, v_{i+1}, \ldots, v_n\Big) = \\ &= \sum\nolimits_\nu x_\nu \det\left(v_1, \ldots, v_{i-1}, v_\nu, v_{i+1}, \ldots, v_n\right) = x_i \det\left(v_1, \ldots, v_{i-1}, v_i, v_{i+1}, \ldots, v_n\right). \end{aligned}$$

8.4.5. Тождество Гамильтона – Кэли. Для любого коммутативного кольца K с единицей кольцо квадратных матриц $\mathrm{Mat}_n(K[t])$ с элементами из кольца многочленов $K[t]$ совпадает с кольцом многочленов $\mathrm{Mat}_n(K)[t]$ от переменной t с коэффициентами в $\mathrm{Mat}_n(K)$, поскольку каждую матрицу, в клетках которой стоят многочлены от t, можно записать как многочлен от t с матричными коэффициентами и наоборот. Например,

$$\begin{pmatrix} 3t^2+2t & t^3-1 \\ 2t+3 & t^3+t-1 \end{pmatrix} = t^3\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} + t^2\begin{pmatrix} 3 & 0 \\ 0 & 0 \end{pmatrix} + t\begin{pmatrix} 2 & 0 \\ 2 & 1 \end{pmatrix} + \begin{pmatrix} 0 & -1 \\ 3 & -1 \end{pmatrix}.$$

Определение 8.1 (характеристический многочлен)
Для матрицы $A = (a_{ij}) \in \mathrm{Mat}_n(K)$ многочлен

$$\chi_A(t) \stackrel{\text{def}}{=} \det(tE - A) = t^n - \sigma_1(A)\cdot t^{n-1} + \ \ldots\ + (-1)^{n-1}\sigma_{n-1}(A)\cdot t + (-1)^n\sigma_n(A) \in K[t]$$

называется *характеристическим многочленом* матрицы A. Коэффициент при t^{n-k} в характеристическом многочлене обозначается через $(-1)^k\sigma_k(A)$.

Упражнение 8.12. Убедитесь, что число $\sigma_k(A) \in K$ равно сумме *главных* $k \times k$ миноров[1] матрицы A. В частности, $\sigma_1(A) = \mathrm{tr}(A)$ и $\sigma_n(A) = \det A$ суть *след* и *определитель* матрицы A.

Теорема 8.1 (тождество Гамильтона – Кэли)
Рассмотрим кольцо $K = \mathbb{Z}[a_{ij}]$ многочленов с целыми коэффициентами от n^2 переменных a_{ij}, где $1 \leqslant i, j \leqslant n$. Матрица $A = (a_{ij}) \in \mathrm{Mat}_n(K)$ удовлетворяет в $\mathrm{Mat}_n(K)$ соотношению $\chi_A(A) = 0$.

Доказательство. Согласно форм. (8-22) на стр. 138, в кольце $\mathrm{Mat}_n(K[t])$ выполняется соотношение $\det(tE - A)\cdot E = (tE - A)(tE - A)^\vee$, где $(tE - A)^\vee \in \mathrm{Mat}_n(K[t])$ — матрица, присоединённая[2] к $(tE - A)$. Перепишем это равенство в виде равенства между многочленами от t с коэффициентами в кольце матриц $\mathrm{Mat}_n(K)$:

$$t^nE - \sigma_1(A)\,t^{n-1}E + \ldots + (-1)^n\sigma_n(A)\,E = (tE - A)(t^mA_m + \ldots + t\,A_1 + A_0),$$

где $A_0, A_1, \ldots, A_m \in \mathrm{Mat}_n(K)$ — некоторые матрицы. Подставляя в него $t = A$, получаем в кольце $\mathrm{Mat}_n(K)$ равенство $\chi_A(A)\cdot E = 0$, откуда $\chi_A(A) = 0$. □

Упражнение 8.13. Пусть $f(t) = \sum_{i=0}^m t^iA_i$, $g(t) = \sum_{j=0}^n t^jB_j \in \mathrm{Mat}_r(K)[t]$ и

$$h(t) = f(t)g(t) = \sum\nolimits_{k=0}^{m+n} t^kH_k \in \mathrm{Mat}_r(K)[t]\,,\ \text{где } H_k = \sum_{i+j=k} A_iB_j\,,$$

а матрица $C \in \mathrm{Mat}_r(K)$ такова, что $CA_i = A_iC$ при всех i. Убедитесь, что $f(C)g(C) = h(C)$ в $\mathrm{Mat}_r(K)$.

[1] Т. е. определителей таких $k \times k$ подматриц в A, главная диагональ которых является подмножеством главной диагонали матрицы A.

[2] См. n° 8.4 на стр. 138.

8.5. Результант. Пусть многочлены $f(x) = a_0 + a_1x + \ldots + a_nx^n$ и $g(x) = b_0 + b_1x + \ldots + b_mx^m$ имеют коэффициенты в произвольном поле $\Bbbk$ и $a_nb_m \neq 0$. Обозначим через $V_k \subset \Bbbk[x]$ векторное пространство многочленов степени строго меньше k. Наличие у f и g общего корня в каком-нибудь поле $\mathbb{F} \supset \Bbbk$ равносильно тому, что $\deg \text{нод}(f, g) \geqslant 1$, а это в свою очередь эквивалентно существованию таких не равных одновременно нулю многочленов $h_1 \in V_m$ и $h_2 \in V_n$, что $fh_1 + gh_2 = 0$.

Упражнение 8.14. Убедитесь в этом.

Мы заключаем, что многочлены f и g тогда и только тогда имеют общий корень в каком-нибудь расширении $\mathbb{F} \supset \Bbbk$, когда $\Bbbk$-линейное отображение

$$V_m \oplus V_n \to V_{m+n}, \quad (h_1, h_2) \mapsto fh_1 + gh_2, \tag{8-28}$$

имеет ненулевое ядро. Поскольку $\dim(V_m \oplus V_n) = m + n = \dim V_{m+n}$, это условие выражается равенством нулю определителя матрицы отображения (8-28) в каких-нибудь базисах. В стандартных базисах $(1,0), (x,0), \ldots, (x^{m-1},0), (0,1), (0,x), \ldots, (0,x^{n-1})$ в $V_m \oplus V_n$ и $1, x, \ldots, x^{m+n-1}$ в V_{m+n} отображение (8-28) имеет матрицу

$$\underbrace{\left.\begin{pmatrix} a_0 & & & b_0 & & \\ a_1 & \ddots & & \vdots & \ddots & \\ \vdots & \ddots & a_0 & b_{m-1} & \ddots & b_0 \\ a_n & \ddots & a_1 & b_m & \ddots & \vdots \\ & \ddots & \vdots & & \ddots & b_{m-1} \\ & & a_n & & & b_m \end{pmatrix}\right\}}_{m+n} \begin{matrix} \\ \\ \\ \\ \\ \\ \end{matrix} \tag{8-29}$$
$$\underbrace{\qquad\qquad}_{m} \qquad \underbrace{\qquad\qquad\qquad}_{n}$$

(в столбцах записаны коэффициентов многочленов f и g, последовательно сдвигаемые на одну клетку вниз при движении слева направо, все остальные элементы матрицы нулевые). Определитель матрицы (8-29) называется *детерминантом Сильвестра* многочленов f, g. Таким образом, многочлены $f, g \in \Bbbk[x]$ имеют общий корень в некотором расширении $\mathbb{F} \supset \Bbbk$ поля $\Bbbk$, если и только если их детерминант Сильвестра обращается в нуль.

Рассмотрим теперь кольцо $K = \mathbb{Z}[a_n, b_m, \alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m]$ и многочлены

$$\begin{aligned} A(x) = a_0 + a_1x + \ldots + a_nx^n &\stackrel{\text{def}}{=} a_n \prod_{i=1}^{n} (x - \alpha_i) \\ B(x) = b_0 + b_1x + \ldots + b_mx^m &\stackrel{\text{def}}{=} b_m \prod_{j=1}^{n} (x - \beta_j), \end{aligned} \tag{8-30}$$

лежащие в кольце $K[x]$. Элемент $R_{A,B}$ кольца K, задаваемый равенствами

$$R_{A,B} \stackrel{\text{def}}{=} a_n^m b_m^n \prod_{ij} (\alpha_i - \beta_j) = a_n^m \prod_{i=1}^{n} B(\alpha_i) = (-1)^{mn} b_m^n \prod_{j=1}^{m} A(\beta_j) \tag{8-31}$$

называется *результантом* многочленов (8-30). Будучи симметрическим как по переменным α_i, так и по переменным β_j, результант лежит в подкольце кольца K, состоящем из многочленов от a_n, b_m и от элементарных симметрических многочленов $e_k(\alpha_1, \ldots, \alpha_n)$ и $e_\ell(\beta_1, \ldots, \beta_m)$.

Предложение 8.4
Результант $R_{A,B}$ равен в кольце K детерминанту Сильвестра многочленов (8-30). Кроме того, существуют такие многочлены $\varphi, \psi \in K[x]$, что $A(x)\cdot\varphi(x) + B(x)\cdot\psi(x) = R_{A,B}$.

Доказательство. Обозначим матрицу (8-29) через S. По предыдущему для любых многочленов $\varphi(x) = \varphi_0 + \varphi_1 x + \ldots + \varphi_{n-1}x^{n-1}$ и $\psi(x) = \psi_0 + \psi_1 x + \ldots + \psi_{m-1}x^{m-1}$ столбец коэффициентов многочлена $A\varphi + B\psi$ является результатом умножения столбца $(\varphi_0, \ldots, \varphi_{m-1}, \psi_0, \ldots, \psi_{n-1})^t$ слева на матрицу S. Из равенства $S\cdot S^\vee = \det(S)\cdot E$ вытекает, что в первом столбце матрицы $S^\vee$ выписаны друг под другом коэффициенты таких многочленов $\varphi, \psi \in K[x]$, что

$$A(x)\cdot\varphi(x) + B(x)\cdot\psi(x) = \det S \in K\,. \tag{8-32}$$

Рассмотрим $\det S \in \mathbb{Z}[a_n, b_m, \alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m]$ как многочлен от α_i с коэффициентами в кольце многочленов от всех остальных переменных. Полагая $\alpha_i = \beta_j$ и подставляя в равенство (8-32) $x = \alpha_i = \beta_j$ получаем в левой части нуль, поскольку при $\alpha_i = \beta_j$ оба многочлена $A(x)$ и $B(x)$ обращаются в нуль при $x = \alpha_i = \beta_j$. Поэтому $\det S$ делится в кольце K на все разности $a_i - \beta_j$. Так как кольцо $K = \mathbb{Z}[a_n, b_m, \alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m]$ факториально, а все эти разности неприводимы и попарно не ассоциированы, $\det S$ делится на $\prod_{ij}(\alpha_i - \beta_j)$. С другой стороны, по формулам Виета $a_k = (-1)^{n-k}a_n e_{n-k}(\alpha_1, \ldots, \alpha_n)$ и $b_k = (-1)^{m-k}b_m e_{m-k}(\beta_1, \ldots, \beta_m)$, где e_i — элементарные симметрические многочлены. Поэтому первые m столбцов матрицы S делятся на a_n, а последние n — на b_m. Тем самым $\det S$ делится на $a_n^m b_m^n \prod_{ij}(\alpha_i - \beta_j) = R_{A,B}$. Поскольку лексикографически старшие члены у $\det S$ и $R_{A,B}$ оба равны $a_n^m b_m^n(\alpha_1 \ldots \alpha_n)^m$, мы заключаем, что частное от деления равно 1. □

Пример 8.8 (исключение переменных)
Над алгебраически замкнутым полем $\Bbbk$ пара чисел $(x_0, y_0) \in \Bbbk^2$ тогда и только тогда является решением системы полиномиальных уравнений $f(x,y) = g(x,y) = 0$, где $f, g \in \Bbbk[x,y]$, когда многочлены $f(x,y) = f_x(y)$ и $g(x,y) = g_x(y)$, рассматриваемые как многочлены от y с коэффициентами в кольце $\Bbbk[x]$, имеют при $x = x_0$ общий корень $y = y_0$, что равносильно обращению в нуль при $x = x_0$ результанта $R_{f_x,g_x} \in \Bbbk[x]$ этих двух многочленов от y. Таким образом каждая система из двух полиномиальных уравнений на x, y сводится к одному полиномиальному уравнению на x — обращению в нуль детерминанта Сильвестра, составленного из лежащих в $\Bbbk[x]$ коэффициентов многочленов $f_x, g_x \in \Bbbk[x][y]$. Эта процедура называется *исключением переменной* y из уравнений $f(x,y) = g(x,y) = 0$.

§9. Пространство с оператором

9.1. Классификация пространств с оператором. Пусть $\Bbbk$ — произвольное поле, V — конечномерное векторное пространство над $\Bbbk$, а $F: V \to V$ — линейный эндоморфизм пространства V. Мы будем называть пару (F, V) *пространством с оператором* или просто *оператором* над $\Bbbk$. Линейное отображение $C: U_1 \to U_2$ между пространствами с операторами (F_1, U_1) и (F_2, U_2) называется *гомоморфизмом*, если $F_2 \circ C = C \circ F_1$. В этом случае говорят, что диаграмма

$$\begin{array}{ccc} U_1 & \xrightarrow{C} & U_2 \\ {\scriptstyle F_1}\uparrow & & \uparrow{\scriptstyle F_2} \\ U_1 & \xrightarrow[C]{} & U_2 \end{array}$$

коммутативна[1]. Если гомоморфизм C биективен, операторы $F_1: U_1 \to U_1$ и $F_2: U_2 \to U_2$ называются *изоморфными* или *подобными*. Поскольку в этом случае $F_2 = CF_1C^{-1}$, то говорят, что оператор F_2 получается из F_1 *сопряжением* посредством изоморфизма C.

Подпространство $U \subset V$ называется *F-инвариантным*, если $F(U) \subset U$. В этом случае пара $(F|_U, U)$ тоже является пространством с оператором и вложение $U \hookrightarrow V$ представляет собою гомоморфизмом пространств с операторами. Оператор, не имеющий инвариантных подпространств, отличных от нуля и всего пространства, называется *неприводимым* или *простым*.

Упражнение 9.1. Покажите, что оператор умножения на класс $[t]$ в факторкольце $\mathbb{R}[t]/(t^2+1)$ неприводим.

Оператор $F: V \to V$ называется *разложимым*, если V раскладывается в прямую сумму двух ненулевых F-инвариантных подпространств, и *неразложимым* — в противном случае. Все простые операторы неразложимы.

Упражнение 9.2. Покажите, что оператор умножения на класс $[t]$ в факторкольце $\Bbbk[t]/(t^n)$ при всех $n > 1$ приводим, но неразложим.

Таким образом, над любым полем $\Bbbk$ имеются неразложимые пространства с оператором любой размерности. Очевидно, что всякое пространство с оператором является прямой суммой неразложимых.

9.1.1. Пространство с оператором как $\Bbbk[t]$-модуль. Задание на пространстве V линейного оператора $F: V \to V$ эквивалентно заданию на V структуры модуля над кольцом многочленов $\Bbbk[t]$. В самом деле, структура $\Bbbk[t]$-модуля включает в себя операцию умножения векторов на переменную t: $v \mapsto tv$, которая является линейным отображением $V \to V$. Если обозначить его буквой F, то умножение векторов на произвольный многочлен $f(t) = a_0 + a_1 t + \ldots + a_m t^m$ происходит по правилу $f(t)\,v = a_0 v + a_1 Fv + \ldots + a_m F^m v = f(F)\,v$, где

$$f(F) = a_0 \mathrm{Id}_V + a_1 F + \ldots + a_m F^m$$

есть результат вычисления многочлена f на элементе F в $\Bbbk$-алгебре $\mathrm{End}(V)$. Наоборот, каждый линейный оператор $F: V \to V$ задаёт на V структуру $\Bbbk[t]$-модуля, в котором умножение вектора $v \in V$ на многочлен $f(t) \in \Bbbk[t]$ происходит по формуле $f(t)\,v \stackrel{\text{def}}{=} f(F)\,v$. Мы будем обозначать такой $\Bbbk[t]$-модуль через V_F.

[1] Произвольная диаграмма отображений называется *коммутативной*, если композиции отображений вдоль любых двух путей с общим началом и концом одинаковы.

Гомоморфизм $C : V_F \to W_G$ между $\Bbbk[t]$-модулями, которые задаются линейными операторами $F : V \to V$ и $G : W \to W$, представляет собою $\Bbbk$-линейное отображение $C : V \to W$, перестановочное с умножением векторов на t, т. е. такое что $C \circ F = G \circ C$. Мы заключаем, что гомоморфизмы пространств с операторами — это то же самое, что $\Bbbk[t]$-линейные отображения между задаваемыми этими операторами $\Bbbk[t]$-модулями. В частности, операторы $F : V \to V$ и $G : W \to W$ изоморфны, если и только если изоморфны $\Bbbk[t]$-модули V_F и W_G.

Векторное подпространство $U \subset V$ является $\Bbbk[t]$-подмодулем в модуле V_F, если и только если оператор умножения на t переводит U в себя, т. е. тогда и только тогда, когда это подпространство F-инвариантно. Аналогично, разложимость V в прямую сумму инвариантных подпространств означает разложимость $\Bbbk[t]$-модуля V_F в прямую сумму $\Bbbk[t]$-подмодулей.

Если векторное пространство V конечномерно над $\Bbbk$, то $\Bbbk[t]$-модуль V_F конечно порождён, поскольку любой набор векторов, линейно порождающих V над $\Bbbk$, порождает и модуль V_F над $\Bbbk[t]$. В каноническом разложении конечномерного над $\Bbbk$ модуля V_F в прямую сумму свободного модуля и подмодуля кручения[1] свободное слагаемое отсутствует, так как оно бесконечномерно над $\Bbbk$. Таким образом, из теоремы об элементарных делителях[2] и теоремы об инвариантных множителях[3] мы получаем следующие два эквивалентных друг другу описания пространств с оператором над произвольным полем $\Bbbk$.

Теорема 9.1 (жорданово описание в терминах элементарных делителей)
Любой линейный оператор в конечномерном векторном пространстве над произвольным полем $\Bbbk$ подобен оператору умножения на класс $[t]$ в прямой сумме факторколец

$$\Bbbk[t]/(p_1^{m_1}(t)) \oplus \ldots \oplus \Bbbk[t]/(p_k^{m_k}(t)), \tag{9-1}$$

где все многочлены $p_\nu(t) \in \Bbbk[t]$ приведены и неприводимы, и слагаемые могут повторяться. Операторы умножения на класс $[t]$, действующие в суммах

$$\Bbbk[t]/(p_1^{m_1}(t)) \oplus \ldots \oplus \Bbbk[t]/(p_k^{m_k}(t)) \quad \text{и} \quad \Bbbk[t]/(q_i^{n_1}(t)) \oplus \ldots \oplus \Bbbk[t]/(q_\ell^{n_\ell}(t))$$

изоморфны, если и только если $k = \ell$ и прямые слагаемые можно переставить так, что $p_\nu = q_\nu$ и $m_\nu = n_\nu$ при всех ν. □

Теорема 9.2 (фробениусово описание в терминах инвариантных множителей)
Любой линейный оператор в конечномерном векторном пространстве над произвольным полем $\Bbbk$ подобен оператору умножения на класс $[t]$ в прямой сумме факторколец

$$\Bbbk[t]/(f_1) \oplus \ldots \oplus \Bbbk[t]/(f_r), \tag{9-2}$$

где $r \in \mathbb{N}$, а $f_1, \ldots, f_r \in \Bbbk[t]$ — такие приведённые многочлены, что $f_i \mid f_j$ при $i < j$. Два таких оператора на пространствах $\Bbbk[t]/(f_1) \oplus \ldots \oplus \Bbbk[t]/(f_r)$ и $\Bbbk[t]/(g_1) \oplus \ldots \oplus \Bbbk[t]/(g_s)$ подобны, если и только если $r = s$ и $f_i = g_i$ при всех i. □

[1] См. теор. 6.5 на стр. 116.
[2] См. теор. 6.4 на стр. 114.
[3] См. 6-12 на стр. 118.

9.1.2. Элементарные делители и инвариантные множители. Многочлены $f_1, \dots, f_r \in \Bbbk[t]$ из теор. 9.2 называются *инвариантными множителями* оператора $F : V \to V$, а дизъюнктное объединение[1] всех многочленов $p_\nu^{m_\nu}$ из теор. 9.1 называется *набором элементарных делителей* и обозначается через $\mathcal{El}(F)$. Инвариантные множители и элементарные делители связаны китайской теоремой об остатках: $\Bbbk[t]/(f_1) \oplus \dots \oplus \Bbbk[t]/(f_r) \simeq \bigoplus_{p^m \in \mathcal{El}(F)} \Bbbk[t]/(p^m)$ и однозначно определяют друг друга, как это объяснялось в n° 6.3 на стр. 114.

Следствие 9.1
Линейные операторы F и G подобны тогда и только тогда, когда $\mathcal{El}(F) = \mathcal{El}(G)$. □

Следствие 9.2
Линейный оператор неразложим тогда и только тогда, когда он подобен оператору умножения на класс $[t]$ в факторкольце $\Bbbk[t]/(p^m)$, где $p \in \Bbbk[t]$ неприводим и приведён. Неразложимый оператор неприводим, если и только если $m = 1$. □

Следствие 9.3
Многочлен $f \in \Bbbk[t]$ тогда и только тогда аннулирует оператор $F : V \to V$, когда он делится на все элементарные делители оператора F. Аннулирующий оператор F приведённый многочлен наименьшей степени равен последнему инвариантному множителю f_r из разложения (9-2). □

Упражнение 9.3. Пусть пространство с оператором (F, V) разлагается в прямую сумму F-инвариантных подпространств U_i. Покажите, что $\mathcal{El}(F) = \bigsqcup_i \mathcal{El}(F|_{U_i})$.

9.1.3. Отыскание элементарных делителей. Фиксируем в пространстве V какой-либо базис $\boldsymbol{v} = (v_1, \dots, v_n)$ над полем $\Bbbk$ и обозначим через $F_{\boldsymbol{v}} \in \mathrm{Mat}_n(\Bbbk)$ матрицу оператора $F : V \to V$ в этом базисе. Напомню[2], что она однозначно определяется тем, что $F(\boldsymbol{v}) = \boldsymbol{v}\, F_{\boldsymbol{v}}$ или, подробнее,

$$(F(v_1), \dots, F(v_n)) = (v_1, \dots, v_n)\, F_{\boldsymbol{v}}\,.$$

Так как векторы v_i линейно порождают пространство V над $\Bbbk$, они тем более порождают модуль V_F над $\Bbbk[t]$, и $V_F = \Bbbk[t]^n/R_{\boldsymbol{v}}$, где подмодуль $R_{\boldsymbol{v}} = \ker \pi_{\boldsymbol{v}} \subset \Bbbk[t]^n$ является ядром эпиморфизма[3] $\pi_{\boldsymbol{v}} : \Bbbk[t]^n \to V_F$, переводящего стандартный базисный вектор $e_i \in \Bbbk[t]^n$ в вектор $v_i \in V$, и состоит из всех $\Bbbk[t]$-линейных соотношений между векторами $\boldsymbol{v}$ в V_F. Таким образом, инвариантные множители оператора F суть отличные от единицы инвариантные множители подмодуля $R_{\boldsymbol{v}} \subset \Bbbk[t]^n$.

Лемма 9.1
Если записывать элементы свободного модуля $\Bbbk[t]^n$ в виде координатных столбцов с элементами из $\Bbbk[t]$, то подмодуль соотношений $\ker \pi_{\boldsymbol{v}} \subset \Bbbk[t]^n$ линейно порождается над $\Bbbk[t]$ столбцами матрицы $tE - F_{\boldsymbol{v}}$.

Доказательство. Пусть $F_{\boldsymbol{v}} = \left(f_{ij}\right)$. Тогда j-й столбец матрицы $tE - F_{\boldsymbol{v}}$ выражается через стандартный базис $\boldsymbol{e}$ модуля $\Bbbk[t]^n$ как $te_j - \sum_{i=1}^n e_i f_{ij}$. Применяя к этому вектору гомоморфизм $\pi_{\boldsymbol{v}}$,

[1] Каждый элементарный делитель p^m входит в него ровно столько раз, сколько прямых слагаемых вида $\Bbbk[t]/(p^m)$ имеется в разложении (9-1).

[2] См. n° 5.3.3 на стр. 99.

[3] См. n° 6.2 на стр. 111.

получаем $\pi_v\Big(te_j - \sum_{i=1}^n e_i f_{ij}\Big) = tv_j - \sum_{i=1}^n v_i f_{ij} = Fv_j - \sum_{i=1}^n v_i f_{ij} = 0$. Тем самым все столбцы матрицы $tE - F_v$ лежат в $\ker \pi_v$. Рассмотрим теперь произвольный вектор $h(t) \in \Bbbk[t]^n$ и запишем его в виде многочлена от t с коэффициентами в $\Bbbk^n$ (ср. с n° 8.4.5 на стр. 140):

$$h(t) = t^m h_m + t^{m-1} h_{m-1} + \ldots + t h_1 + h_0\,, \text{ где } h_i \in \Bbbk^n\,.$$

Этот многочлен можно поделить слева с остатком на многочлен $tE - F_v$ точно также, как делят «уголком» обычные полиномы с постоянными коэффициентами[1]. В результате получим равенство вида $t^m h_m + \ldots + t h_1 + h_0 = (tE - F_v)\cdot(t^{m-1} g_{m-1} + \ldots + t g_1 + g_0) + r$, где $g_i, r \in \Bbbk^n$.

Упражнение 9.4. Убедитесь в этом и проверьте, что остаток от деления $h(t)$ на $tE - A$, где $A \in \mathrm{Mat}_n(\Bbbk)$, равен $A(\ldots A(Ah_m + h_{m-1}) + \ldots + h_1) + h_0 = A^m h_m + \ldots + Ah_1 + h_0 = h(A)$.

Иными словами, вычитая из любого столбца $h(t) \in \Bbbk[t]^n$ подходящую $\Bbbk[t]$-линейную комбинацию столбцов матрицы $tE - F_v$, можно получить вектор $r \in \Bbbk^n$, т. е. $\Bbbk$-линейную комбинацию $r = \sum \lambda_i e_i$ стандартных базисных векторов $e_i \in \Bbbk[t]^n$. Так как столбцы матрицы $tE - F_v$ лежат в $\ker \pi_v$, мы заключаем, что $\pi_v(h(t)) = \pi_v(r) = \sum \lambda_i v_i$. Если $h \in \ker \pi_v$, то $\sum \lambda_i v_i = 0$, что возможно только когда все $\lambda_i = 0$, ибо векторы $v_i \in V$ линейно независимы над $\Bbbk$. Тем самым $r = 0$ для всех $h \in \ker \pi_v$, т. е. $\ker \pi_v$ содержится в $\Bbbk[t]$-линейной оболочке столбцов матрицы $tE - F_v$. □

Следствие 9.4
Множество $\mathcal{E}\ell(F)$ является дизъюнктным объединением степеней p^m неприводимых приведённых многочленов из разложений инвариантных множителей $f_i(t)$ матрицы $tE - F_v$. Последние равны диагональным элементам $d_{ii}(t)$ нормальной формы Смита[2] матрицы $tE - F_v$ и могут быть вычислены по формулам[3] $f_i(t) = \Delta_i(tE - F_v)/\Delta_{i-1}(tE - F_v)$, где $\Delta_i(tE - F_v)$ означает нод всех $k \times k$ миноров матрицы $tE - F_v$. □

9.1.4. Характеристический многочлен. Произведение всех элементарных делителей линейного оператора $F : V \to V$, по сл. 9.4 равное определителю $\Delta_n = \det(tE - F_v)$, где F_v — матрица оператора F в каком-либо базисе $\boldsymbol{v}$ пространства V, называется *характеристическим многочленом* оператора F и обозначается

$$\chi_F(t) \stackrel{\text{def}}{=} \det(tE - F_v) = \prod_{p^m \in \mathcal{E}\ell(F)} p^m\,.$$

Из предыдущего вытекает, что характеристический многочлен не зависит от выбора базиса и что подобные операторы имеют одинаковые характеристические многочлены.

Упражнение 9.5. Убедитесь прямым вычислением, что для всех $A \in \mathrm{Mat}_n(\Bbbk)$, $C \in \mathrm{GL}_n(\Bbbk)$ выполняется равенство $\det(tE - CAC^{-1}) = \det(tE - A)$.

Пример 9.1 (характеристический многочлен разложимого оператора)
Если пространство с оператором (F, V) распадается в прямую сумму пространств с операторами (G, U) и (H, W), то в базисе пространства $V = U \oplus W$, который получен объединением базиса в U и базиса в W, матрица $tE - F$ имеет блочно диагональный вид

$$tE - F = \begin{pmatrix} tE - G & 0 \\ 0 & tE - H \end{pmatrix}.$$

[1] См. n° 2.2 на стр. 40.
[2] См. n° 6.1.1 на стр. 103.
[3] См. прим. 8.3 на стр. 134.

Раскладывая её определитель по первым $\dim U$ столбцам[1], заключаем, что $\chi_F(t) = \chi_G(t)\,\chi_H(t)$. Это вполне согласуется с упр. 9.3 на стр. 145.

Упражнение 9.6. Убедитесь, что для любого приведённого многочлена $f \in \Bbbk[t]$ характеристический многочлен оператора умножения на класс $[t]$ в факторкольце $\Bbbk[t]/(f)$ равен f.

9.1.5. Минимальный многочлен. Для каждого неприводимого приведённого многочлена $p \in \Bbbk[t]$ обозначим через $m_p(F)$ максимальный показатель m, с которым p^m присутствует в наборе $\mathcal{E}\ell(F)$ элементарных делителей оператора F, а для тех неприводимых приведённых многочленов $p \in \Bbbk[x]$, степени которых не представлены в $\mathcal{E}\ell\, F$, положим $m_p(F) = 0$. Таким образом, $m_p(F) = 0$ для всех неприводимых приведённых $p \in \Bbbk[x]$ кроме конечного числа. В этих обозначениях сл. 9.3 на стр. 145 можно переформулировать следующим образом: аннулирующий оператор F приведённый многочлен $\mu_F(t)$ наименьшей возможной степени совпадает с инвариантным множителем оператора F наибольшей степени и равен

$$\mu_F(t) = f_r = \prod_p p^{m_p(F)}, \tag{9-3}$$

где произведение берётся по всем приведённым неприводимым $p \in \Bbbk[t]$. Многочлен $\mu_F(t)$ называется *минимальным многочленом* оператора $F\colon V \to V$. Он порождает ядро гомоморфизма

$$\mathrm{ev}_F\colon \Bbbk[t] \to \mathrm{End}_{\Bbbk}(V), \quad f(t) \mapsto f(F),$$

вычисления многочленов на операторе F и делит в $\Bbbk[t]$ все аннулирующие оператор F многочлены, включая характеристический многочлен $\chi_F(t) = \det(tE - F)$. Согласно сл. 9.4 на стр. 146 инвариантный множитель наибольшей степени оператора F равен отношению $\det(tE-F)$ к нод всех миноров порядка $n-1$ матрицы $tE-F$, где $n = \dim V$. Таким образом, $\chi_F/\mu_F = \Delta_{n-1}(tE-F)$ для любого ненулевого линейного оператора F на n-мерном векторном пространстве.

Пример 9.2 (отыскание минимального многочлена)
Вычисление минимального многочлена оператора $F\colon V \to V$ по явной детерминантной формуле довольно трудоёмко, и на практике обычно используют следующие соображения. Для каждого вектора $v \in V$ существует такой приведённый многочлен $\mu_{v,F}(t)$ наименьшей степени, что $\mu_{v,F}(F)v = 0$. Чтобы написать его явно, надо найти наименьшее такое $k \in \mathbb{N}$, что вектор $F^k v$ линейно выражается через векторы $v, Fv, \dots, F^{k-1}v$. Если это выражение имеет вид $F^k v = \mu_1 F^{k-1}v + \dots + \mu_{k-1}Fv + \mu_k v$, то $\mu_{v,F}(t) = t^k - \mu_1 t^{k-1} - \dots - \mu_{k-1}t - \mu_k$.

Упражнение 9.7. Убедитесь, что любой аннулирующий оператор F многочлен делится на все многочлены $\mu_{v,F}$, где $v \in V$.

Мы заключаем, что минимальный многочлен μ_F оператора F равен нок многочленов $\mu_{v_i,F}$ каких-нибудь векторов $v = v_1, \dots, v_m$, линейно порождающих пространство V над $\Bbbk$.

Упражнение 9.8. Убедитесь в этом.

Вычислим, к примеру, минимальный многочлен оператора $F\colon \mathbb{Q}^4 \to \mathbb{Q}^4$, заданного в стандартном базисе $e_1, \dots, e_4$ матрицей

$$A = \begin{pmatrix} -2 & -3 & 3 & 3 \\ 4 & 6 & -4 & -4 \\ 1 & 2 & 0 & -1 \\ 3 & 3 & -3 & -2 \end{pmatrix}$$

[1] См. формулу (8-16) на стр. 136.

Векторы[1]

$$e_1 = \begin{pmatrix}1\\0\\0\\0\end{pmatrix}, \quad Fe_1 = \begin{pmatrix}-2\\4\\1\\3\end{pmatrix}, \quad F^2e_1 = \begin{pmatrix}4\\0\\3\\-3\end{pmatrix}$$

линейно независимы. Чтобы выяснить, выражается ли через них вектор[2]

$$F^3e_1 = \begin{pmatrix}-8\\16\\7\\9\end{pmatrix},$$

необходимо решить неоднородную систему с расширенной матрицей

$$\left(\begin{array}{ccc|c} 1 & -2 & 4 & -8 \\ 0 & 4 & 0 & 16 \\ 0 & 1 & 3 & 7 \\ 0 & 3 & -3 & 9 \end{array}\right).$$

Методом Гаусса преобразуем эту матрицу к приведённому ступенчатому виду

$$\left(\begin{array}{ccc|c} 1 & 0 & 0 & -4 \\ 0 & 1 & 0 & 4 \\ 0 & 0 & 1 & 1 \end{array}\right)$$

и получаем решение $(-4, 4, 1)$, т. е. $F^3e_1 = -4e_1 + 4Fe_1 + F^2e_1$. Таким образом, минимальный многочлен от оператора F, аннулирующий вектор e_1, равен $F^3 - F^2 - 4F + 4E$. Вычисляя

$$A^2 = \begin{pmatrix}4&3&-3&-3\\0&4&0&0\\3&6&-2&-3\\-3&-3&3&4\end{pmatrix} \quad \text{и} \quad A^3 = \begin{pmatrix}-8&-9&9&9\\16&24&-16&-16\\7&14&-6&-7\\9&9&-9&-8\end{pmatrix},$$

убеждаемся, что $A^3 - A^2 - 4A + 4E = 0$. Тем самым, $\mu_F = t^3 - t^2 - 4t + 4$.

Упражнение 9.9. Как действует умножение на класс $[t]$ в факторкольце $\Bbbk[t]/(t-\lambda)$ и в прямой сумме конечного множества таких факторколец?

9.1.6. Линейные операторы над алгебраически замкнутым полем. Если основное поле $\Bbbk$ алгебраически замкнуто, то неприводимые приведённые многочлены в $\Bbbk[t]$ исчерпываются линейными двучленами $(t-\lambda)$, где $\lambda \in \Bbbk$. Оператор умножения на класс $[t] = [\lambda] + [t-\lambda]$ в факторкольце $\Bbbk[t]/\big((t-\lambda)^m\big)$ является суммой скалярного оператора $\lambda\,\mathrm{Id}: [g] \mapsto \lambda[g]$, умножающего все векторы на λ, и оператора умножения на класс $[t-\lambda]$, который действует на состоящий из векторов $e_i = \big[(t-\lambda)^{m-i}\big]$, $1 \leqslant i \leqslant m$, базис пространства $\Bbbk[t]/\big((t-\lambda)^m\big)$ по правилу

$$0 \leftarrow e_1 \leftarrow e_2 \leftarrow e_3 \leftarrow \ \dots \ \leftarrow e_{m-1} \leftarrow e_m\,. \tag{9-4}$$

[1] Векторы Fe_1 и F^2e_1 суть первые столбцы матриц A и A^2.

[2] Это первый столбец матрицы A^3.

Таким образом, умножение на класс $[t]$ задаётся в базисе $e_1, \dots, e_n$ матрицей

$$J_m(\lambda) \stackrel{\text{def}}{=} \begin{pmatrix} \lambda & 1 & 0 & \dots & 0 \\ 0 & \lambda & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ 0 & & \ddots & \ddots & 1 \\ 0 & 0 & \dots & 0 & \lambda \end{pmatrix}, \tag{9-5}$$

которая называется *жордановой клеткой* размера m с *собственным числом* λ. По теор. 9.1 каждый линейный оператор F над алгебраически замкнутым полем подобен оператору умножения на класс $[t]$ в прямой сумме факторколец вида $\Bbbk[t]/\big((t-\lambda)^m\big)$, и два таких оператора подобны, если и только если прямые суммы отличаются друг от друга перестановкой слагаемых. На языке матриц сказанное означает, что любая квадратная матрица A над алгебраически замкнутым полем $\Bbbk$ сопряжена блочно диагональной матрице, по главной диагонали которой располагаются жордановы клетки (9-5), причём эта блочно диагональная матрица однозначно с точностью до перестановки клеток определяется матрицей A. Она называется *жордановой нормальной формой* матрицы A. Две матрицы сопряжены, если и только если у них одинаковые с точностью до перестановки клеток жордановы нормальные формы.

Объединение всех жордановых клеток оператора $F\colon V \to V$ с заданным собственным числом $\lambda \in \Bbbk$ представляет собою матрицу, описывающую действие оператора F на подмодуле $(t-\lambda)$-кручения, который обозначается $K_\lambda \stackrel{\text{def}}{=} \{v \in V \mid \exists m \in \mathbb{N}\colon (\lambda \operatorname{Id} - F)^m v = 0\}$ и называется *корневым подпространством* оператора F, отвечающим собственному числу λ. Как $\Bbbk[t]$-модуль он изоморфен прямой сумме $\Bbbk[t]/((t-l)^{m_1}) \oplus \dots \oplus \Bbbk[t]/((t-l)^{m_\ell})$, в которой собраны все элементарные делители оператора F вида $(t-\lambda)^m$. Упорядоченный по нестрогому убыванию $m_1 \geqslant \dots \geqslant m_\ell$ набор показателей $(m_1, \dots, m_\ell)$ называется *цикловым типом* корневого подпространства K_λ. Его удобно изображать диаграммой Юнга из строк длины $m_1, \dots, m_\ell$. Эти показатели в точности равны размерам жордановых клеток с оператора F с собственным числом λ. Наибольший из них m_1 равен кратности корня $t = \lambda$ в минимальном многочлене $\mu_F(t)$ оператора F и и обозначается m_λ. Сумма $m_1 + \dots + m_\ell$ всех показателей равна кратности того же корня $t = \lambda$ в характеристическом многочлене $\chi_F(t)$. Обратите внимание, что характеристический и минимальный многочлены имеют одинаковый набор корней. Он называется *спектром* оператора F и обозначается $\operatorname{Spec} F$, а сами корни $\lambda \in \operatorname{Spec} F$ называются *собственными числами* или *собственными значениями* оператора F.

По лем. 6.3 на стр. 117 высота $\Bbbk$-го столбца диаграммы $(m_1, \dots, m_\ell)$ равна размерности векторного пространства $\ker(F-\lambda E)^k / \ker(F-\lambda E)^{k-1}$ над полем $\Bbbk[t]/(t-\lambda) \simeq \Bbbk$, т. е. разности $\dim\ker(F-\lambda E)^k - \dim\ker(F-\lambda E)^{k-1}$. Таким образом, для отыскания жордановой нормальной формы оператора F над алгебраически замкнутым полем достаточно взять какой-нибудь аннулирующий оператор F многочлен[1] $f \in \Bbbk[t]$, разложить его на линейные множители:

$$f(t) = \prod_\lambda (t-\lambda)^{m(\lambda)}$$

и для каждого корня λ многочлена f вычислить размерности $d_k = \dim\ker(F-\lambda E)^k$ для всех таких $k \geqslant 1$, что $d_k > d_{k-1}$, где мы полагаем $d_0 = 0$. При наступлении равенства[2] $d_{k+1} = d_k$,

[1] Например, характеристический многочлен $\chi_F(t) = \det(tE - F)$.

[2] А оно заведомо наступит при некотором $k \leqslant m(\lambda)$.

вычисление прекращается. Размеры $m_1 \geqslant \ldots \geqslant m_\ell$ жордановых клеток оператора F с собственным числом λ равны длинам строк диаграммы Юнга, k-тый столбец которой имеет длину $d_k - d_{k-1}$.

Пример 9.3 (отыскание жордановой нормальной формы)
Найдём жордановы нормальные формы матриц

$$A = \begin{pmatrix} 2 & -1 & -3 & 1 \\ -9 & -1 & 8 & -1 \\ -1 & -1 & 0 & 1 \\ -1 & 2 & 2 & -2 \end{pmatrix}, \; B = \begin{pmatrix} 5 & 5 & 7 & 1 \\ 6 & 4 & 7 & 1 \\ -6 & -5 & -8 & -1 \\ 3 & 1 & 5 & 1 \end{pmatrix}, \; C = \begin{pmatrix} -2 & 3 & 5 & 1 \\ 3 & 1 & 7 & 2 \\ -6 & 3 & -1 & -1 \\ -9 & 5 & 2 & -3 \end{pmatrix}.$$

Вычисляя след, сумму главных 2×2-миноров, сумму главных 3×3-миноров и определитель каждой из матриц, находим характеристические многочлены, после чего раскладываем их на линейные множители:

$$\chi_A(t) = t^4 + t^3 - 7t^2 - 13t - 6 = (x+1)^2(x+2)(x-3),$$
$$\chi_B(t) = t^4 - 2t^3 - 3t^2 + 4t + 4 = (x+1)^2(x-2)^2,$$
$$\chi_C(t) = t^4 + 5t^3 + 6t^2 - 4t - 8 = (t-1)(t+2)^3.$$

Таким образом, матрица A имеет два одномерных корневых подпространства с собственными числами -2 и 3 и двумерное корневое подпространство с собственным числом -1, цикловой типа которого (2) или (1, 1). Первому случаю отвечает $\dim\ker(A+E) = 1$, или $\mathrm{rk}(A+E) = 3$, а второму — $\dim\ker(A+E) = 2$, или $\mathrm{rk}(A+E) = 2$. Так как левый верхний угловой 3×3 минор матрицы $A + E$ равен

$$\det\begin{pmatrix} 3 & -1 & -3 \\ -9 & 0 & 8 \\ -1 & -1 & 1 \end{pmatrix} = 8 - 3 - 9 = -4,$$

мы заключаем, что имеет место первое, т. е. у A одна жорданова клетка размера 2×2 с собственным числом -1, и жорданова нормальная форма матрицы A такова:

$$\begin{pmatrix} -1 & 1 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -2 & 0 \\ 0 & 0 & 0 & 3 \end{pmatrix}.$$

Матрица B имеет два двумерных корневых подпространства с собственными числами $\lambda = -1, 2$. Их цикловые типы, как и выше, определяются размерностями ядер матриц

$$(B+E) = \begin{pmatrix} 6 & 5 & 7 & 1 \\ 6 & 5 & 7 & 1 \\ -6 & -5 & -7 & -1 \\ 3 & 1 & 5 & 2 \end{pmatrix} \quad \text{и} \quad (B-2E) = \begin{pmatrix} 3 & 5 & 7 & 1 \\ 6 & 2 & 7 & 1 \\ -6 & -5 & -10 & -1 \\ 3 & 1 & 5 & -1 \end{pmatrix}.$$

Поскольку первая матрица имеет ранг 2, а вторая — 3, мы заключаем, что B имеет две клетки 1×1 с собственным числом -1 и одну клетку 2×2 с собственным числом 2, т. е. жорданова

нормальная форма матрицы B такова:

$$\begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 2 \end{pmatrix}.$$

Матрица C имеет одну жорданову клетку 1×1 с собственным числом 1 и трёхмерное корневое подпространство с собственным числом -2, цикловой тип которого может быть (3), или (2, 1), или (1, 1, 1). Эти случаи тоже отличаются друг от друга размерностью ядра оператора $C+2E$, которая равна для них соответственно 1, 2, или 3. Так как ранг матрицы

$$C+2E=\begin{pmatrix} 0 & 3 & 5 & 1 \\ 3 & 3 & 7 & 2 \\ -6 & 3 & 1 & -1 \\ -9 & 5 & 2 & -1 \end{pmatrix}$$

равен 3, мы заключаем, что имеет место первый случай, и жорданова нормальная форма матрицы C такова:

$$\begin{pmatrix} -2 & 1 & 0 & 0 \\ 0 & -2 & 1 & 0 \\ 0 & 0 & -2 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

9.1.7. Нормальные формы матриц над незамкнутыми полями. Так как матрица умножения на t в факторкольце $k[x]/(f)$, где $f=t^m+a_1t^{m-1}+\ldots+a_m$, имеет в базисе из классов многочленов $t^{m-1},\ldots,t,1$ вид

$$F(f)\stackrel{\text{def}}{=}\begin{pmatrix} -a_1 & 1 & & & \\ -a_2 & 0 & 1 & & \\ \vdots & \vdots & \ddots & \ddots & \\ -a_{d-1} & 0 & \ldots & 0 & 1 \\ -a_d & 0 & \ldots & 0 & 0 \end{pmatrix}, \tag{9-6}$$

из теор. 9.2 на стр. 144 вытекает, что каждая матрица над произвольным полем $\Bbbk$ подобна единственной блочно диагональной матрице, составленной из блоков $F(f_1),\ldots,F(f_r)$ вида (9-6), где $f_i\mid f_j$ при $i<j$. Такая блочно диагональная матрица называется *фробенцусовой нормальной формой*. Обратите внимание, что последний многочлен f_r в нормальной форме Фробениуса равен минимальному многочлену μ_F оператора F.

Аналогом жордановой клетки (9-5) над произвольным полем $\Bbbk$ является матрица умножения на класс $[t]$ в факторкольце $\Bbbk[t]/(p^m)$, где $p=t^d+a_1t^{d-1}+\ldots+a_d\in\Bbbk[t]$ — неприводимый приведённый многочлен, записанная в базисе

$$p^{m-1}t^{d-1},\ldots,p^{m-1}t,p^{m-1},\ p^{m-2}t^{d-1},\ldots,p^{m-2}t,p^{m-2},\ \ldots,\ldots,\ldots,\ t^{d-1},\ldots,t,1\,, \tag{9-7}$$

который состоит из m последовательных фрагментов вида $p^kt^{m-1},\ldots,p^kt,p^k$ длины d, получающихся из самого правого фрагмента $t^{d-1},\ldots,t,1$ умножением на p^k, где $k=0,1,\ldots,m-1$.

Упражнение 9.10. Убедитесь, что классы многочленов (9-7) действительно образуют базис в $\Bbbk[t]/(p^m)$.

Так как умножение на t переводит класс $p^k t^\ell$ в классы многочленов

$$\begin{aligned} p^k t^{\ell+1}, &\text{ при } 0 \leqslant \ell \leqslant d-2, \\ p^{k+1} - a_1 p^k t^{d-1} + \ldots + a_d p^k, &\text{ при } \ell = d-1,\ k \leqslant m-2, \\ -a_1 p^{m-1} t^{d-1} + \ldots + a_d p^{m-1}, &\text{ при } \ell = d-1,\ k = m-1, \end{aligned}$$

эта матрица имеет вид

$$J_m(p) \stackrel{\text{def}}{=} \begin{pmatrix} -a_1 & 1 & & & & & & & & & & \\ -a_2 & 0 & 1 & & & & & & & & & \\ \vdots & 0 & \ddots & 1 & & & & & & & & \\ -a_d & \vdots & \ddots & 0 & 1 & & & & & & & \\ & 0 & \ddots & 0 & -a_1 & 1 & & & & & & \\ & & \ddots & \vdots & -a_2 & 0 & \ddots & & & & & \\ & & & 0 & \vdots & 0 & \ddots & \ddots & & & & \\ & & & & -a_d & \vdots & \ddots & \ddots & 1 & & & \\ & & & & & 0 & \ddots & \ddots & 0 & 1 & & \\ & & & & & & \ddots & \ddots & 0 & -a_1 & 1 & \\ & & & & & & & \ddots & \vdots & -a_2 & 0 & \ddots \\ & & & & & & & & 0 & \vdots & \vdots & \ddots \\ & & & & & & & & & -a_d & 0 & \ldots \end{pmatrix} \begin{matrix} \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ 1 \\ 0 \end{matrix} \tag{9-8}$$

где расположенная над главной диагональ заполнена единицами, а на главной диагонали и $d-1$ диагоналях под нею стоят последовательности вида

$$-a_i, \underbrace{0, \ldots, 0}_{d-1}, -a_i, \underbrace{0, \ldots, 0}_{d-1}, \ \ldots\ , -a_i \underbrace{0, \ldots, 0}_{d-i},$$

где $i = 1, \ldots, d$, а все остальные клетки матрицы нулевые.

Упражнение 9.11. Убедитесь, что при $d = 1$ и $p = t - \lambda$ матрица (9-8) превращается в жорданову клетку (9-5).

Из теор. 9.1 на стр. 144 вытекает, что каждая матрица над произвольным полем $\Bbbk$ подобна блочно диагональной матрице, состоящей из обобщённых жордановых клеток (9-8), и две такие матрицы подобны, если и только если они получаются друг из друга перестановкой клеток.

Например, умножение на t в вещественном векторном пространстве

$$V = \mathbb{R}[t]/\left((t^2+1)^2\right) \oplus \mathbb{R}[t]/\left((t+1)^2\right) \oplus \mathbb{R}[t]/(t+1)$$

имеет над полем $\mathbb{R}$ жорданову нормальную форму из трёх клеток размеров 4, 2, 1:

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ -1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 \end{pmatrix}$$

а его фробениусова нормальна форма получается из разложения $V = \mathbb{R}[t]/(f_1) \oplus \mathbb{R}[t]/(f_2)$, где $f_1 = t+1$, $f_2 = (t^2+1)^2(t+1)^2 = t^6 + 2t^5 + 3t^4 + 4t^3 + 3t^2 + 2t + 1$, и содержит две клетки:

$$\begin{pmatrix} -2 & 1 & 0 & 0 & 0 & 0 & 0 \\ -3 & 0 & 1 & 0 & 0 & 0 & 0 \\ -4 & 0 & 0 & 1 & 0 & 0 & 0 \\ -3 & 0 & 0 & 0 & 1 & 0 & 0 \\ -2 & 0 & 0 & 0 & 0 & 1 & 0 \\ -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 \end{pmatrix}, \tag{9-9}$$

Умножение на t в аналогичном комплексном векторном пространстве

$$W = \mathbb{C}[t]/\left((t^2+1)^2\right) \oplus \mathbb{C}[t]/\left((t+1)^2\right) \oplus \mathbb{C}[t]/(t+1) \simeq$$
$$\simeq \mathbb{C}[t]/\left((t-i)^2\right) \oplus \mathbb{C}[t]/\left((t+i)^2\right) \oplus \mathbb{C}[t]/\left((t+1)^2\right) \oplus \mathbb{C}[t]/(t+1)$$

имеет над полем $\mathbb{C}$ жорданову нормальную форму из 4-х клеток размеров 2, 2, 2, 1:

$$\begin{pmatrix} -i & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & -i & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & i & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & i & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 \end{pmatrix}$$

а его фробениусова нормальная форма совпадает с (9-9).

В общем случае объединение всех жордановых клеток (9-8), отвечающих данному неприводимому приведённому многочлену $p \in \Bbbk[t]$, описывает действие оператора $F\colon V \to V$ на подмодуле $p(F)$-кручения

$$K_p \stackrel{\text{def}}{=} \{v \in V \mid \exists\, m \in \mathbb{N}\colon\ p(F)^m v = 0\} \simeq \Bbbk[t]/(p^{m_1}) \oplus \ldots \oplus \Bbbk[t]/(p^{m_\ell})$$

(в правой части собраны все элементарные делители оператора F вида p^m). Упорядоченный по нестрогому убыванию $m_1 \geqslant \ldots \geqslant m_\ell$ набор показателей $(m_1, \ldots, m_\ell)$ называется *цикловым типом* подпространства K_p. Наибольший из них m_1 равен степени, в которой p входит в разложение минимального многочлена $\mu_F(t)$ на неприводимые множители в кольце $\Bbbk[t]$ и обозначается m_p. Сумма $m_1 + \ldots + m_\ell$ всех показателей равна степени, в которой p входит в разложение характеристического многочлена $\chi_F(t)$. По лем. 6.3 на стр. 117 высота $\Bbbk$-го столбца диаграммы Юнга $(m_1, \ldots, m_\ell)$ равна размерности векторного пространства $\ker p(F)^k \,/\, \ker p(F)^{k-1}$ над полем $\Bbbk[t]/(p)$, которое в свою очередь является векторным пространством размерности $\deg p$ над полем $\Bbbk$. Поэтому высота k-того столбца диаграммы $(m_1, \ldots, m_\ell)$ равна отношению

$$(\dim_{\Bbbk} \ker p(F)^k - \dim_{\Bbbk} \ker p(F)^{k-1}) / \deg p\,.$$

Пример 9.4

Выясним, подобны ли друг другу над полем $\mathbb{F}_5$ матрицы

$$A = \begin{pmatrix} 2 & 4 & 0 & 2 \\ 4 & 1 & 4 & 3 \\ 4 & 0 & 4 & 2 \\ 2 & 4 & 3 & 1 \end{pmatrix} \quad \text{и} \quad B = \begin{pmatrix} 4 & 2 & 4 & 2 \\ 3 & 3 & 3 & 2 \\ 2 & 3 & 3 & 0 \\ 0 & 1 & 1 & 3 \end{pmatrix}.$$

Обе матрицы имеют один и тот же характеристический многочлен

$$\det(tE - A) = \det(tE - B) = t^4 + 2t^3 + 3t^2 + 2t + 1 = (t^2 + t + 1)^2\,,$$

где $p(t) = t^2 + t + 1 \in \mathbb{F}_5[t]$ неприводим над $\mathbb{F}_5$. Поэтому всё пространство $\mathbb{F}_5^4$ является модулем p-кручения и имеет цикловой тип (2) или (1, 1). В первом случае многочлен p не аннулирует матрицу, а во втором — аннулирует. Так как

$$A^2 = \begin{pmatrix} 4 & 0 & 2 & 3 \\ 4 & 4 & 4 & 2 \\ 3 & 4 & 2 & 3 \\ 4 & 1 & 1 & 3 \end{pmatrix}, \quad \text{а} \quad B^2 = \begin{pmatrix} 0 & 3 & 1 & 3 \\ 2 & 1 & 2 & 3 \\ 3 & 2 & 1 & 0 \\ 0 & 4 & 4 & 1 \end{pmatrix},$$

и тем самым $p(A) = A^2 + A + E \neq 0$, а $p(B) = B^2 + B + E = 0$, мы заключаем, что матрицы не подобны. Отметим, что из проделанных вычислений вытекает, что жорданова и фробениусова нормальные формы матрицы A имеют соответственно вид

$$\begin{pmatrix} -1 & 1 & 0 & 0 \\ -1 & 0 & 1 & 0 \\ 0 & 0 & -1 & 1 \\ 0 & 0 & -1 & 0 \end{pmatrix} \quad \text{и} \quad \begin{pmatrix} -2 & 1 & 0 & 0 \\ -3 & 0 & 1 & 0 \\ -2 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \end{pmatrix},$$

а жорданова нормальная форма матрицы B совпадает с фробениусовой и имеет вид

$$\begin{pmatrix} -1 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 1 \\ 0 & 0 & -1 & 0 \end{pmatrix}.$$

9.2. Специальные классы операторов. В этом разделе мы подробно остановимся на свойствах нескольких специальных классов операторов, играющих важную роль в различных задачах из разных областей математики.

9.2.1. Нильпотентные операторы. Линейный оператор $F : V \to V$ называется *нильпотентным*, если $F^m = 0$ для некоторого $m \in \mathbb{N}$. Так как нильпотентный оператор аннулируется многочленом t^m, все его элементарные делители являются степенями t. В частности, минимальный многочлен тоже является степенью t и, будучи делителем характеристического многочлена, имеет степень не выше $\dim V$. Поэтому в определении нильпотентного оператора можно без ограничения общности считать, что $m \leqslant \dim V$. По теор. 9.1 нильпотентный оператор изоморфен оператору умножения на класс $[t]$ в прямой сумме факторколец вида

$$\Bbbk[t]/(t^{\nu_1}) \oplus \ldots \oplus \Bbbk[t]/(t^{\nu_k})\,, \tag{9-10}$$

и два таких оператора изоморфны друг другу, если и только если выписанные в порядке нестрогого убывания наборы показателей $\nu_1 \geqslant \nu_2 \geqslant \ldots \geqslant \nu_k$ у них одинаковы. Таким образом, нильпотентные операторы над произвольным полем $\Bbbk$ взаимно однозначно соответствуют диаграммам Юнга ν. Диаграмма $\nu(F)$, характеризующая нильпотентный оператор F, называется его *цикловым типом*.

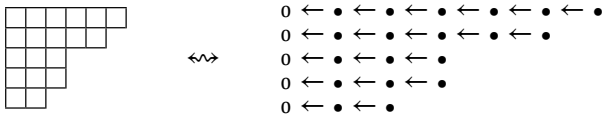
Умножение на t действует на состоящий из векторов $e_i = [t^{m-i}]$ базис в $\Bbbk[t]/(t^m)$ так[1]:

$$0 \leftarrow e_1 \leftarrow e_2 \leftarrow e_3 \leftarrow \ \dots \ \leftarrow e_{m-1} \leftarrow e_m$$

и имеет в этом базисе матрицу

$$J_m(0) \stackrel{\text{def}}{=} \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ 0 & & \ddots & \ddots & 1 \\ 0 & 0 & \dots & 0 & 0 \end{pmatrix},$$

которая называется *нильпотентной жордановой клеткой* размера m. Тем самым, для нильпотентного оператора F циклового типа $\nu(F)$ в пространстве V имеется базис, векторы которого размещаются по клеткам диаграммы $\nu(F)$ так, что F переводит каждый из них в левый соседний, а все векторы самого левого столбца — в нуль:



(9-11)

Базис такого вида называется *циклическим* или *жордановым* базисом нильпотентного оператора F, а наборы базисных векторов, стоящие по строкам диаграммы, называются *жордановыми цепочками*. Так как сумма длин первых m столбцов диаграммы $\nu(F)$ равна $\dim\ker F^m$, длина m-того столбца диаграммы $\nu(F)$ равна $\dim\ker F^m - \dim\ker F^{m-1}$.

9.2.2. Полупростые операторы. Прямая сумма простых[2] пространств с операторами называется *полупростым* или *вполне приводимым* пространством с оператором.

Предложение 9.1
Следующие свойства оператора $F : V \to V$ эквивалентны друг другу:

1) V является прямой суммой неприводимых F-инвариантных подпространств

2) V линейно порождается неприводимыми F-инвариантными подпространствами

3) для каждого ненулевого F-инвариантного подпространства $U \subsetneq V$ существует такое F-инвариантное подпространство $W \subset V$, что $V = U \oplus W$

4) оператор F подобен умножению на класс $[t]$ в прямой сумме факторколец

$$\Bbbk[t]/(p_1) \oplus \Bbbk[t]/(p_2) \oplus \dots \oplus \Bbbk[t]/(p_r),$$

где $p_i \in \Bbbk[t]$ приведены и неприводимы[3] (но не обязательно различны).

[1] См. формулу (9-4) на стр. 148.
[2] В другой терминологии — неприводимых, см. начало n° 9.1 на стр. 143.
[3] Иными словами, в прямой сумме (9-1) из теор. 9.1 все показатели степеней $m_i = 1$.

Доказательство. Импликация (1) ⇒ (2) очевидна. Импликация (2) ⇒ (3) вытекает из лем. 7.1 на стр. 126. Для лучшего понимания происходящего повторим её доказательство в нашем нынешнем контексте. Для каждого неприводимого F-инвариантного подпространства $L \subset V$ пересечение $L \cap U$, будучи F-инвариантным подпространством в L, либо нулевое, либо совпадает с L. Если все неприводимые инвариантные подпространства $L \subset V$ лежат в U, то $U = V$ в силу (2), и доказывать нечего. Если есть ненулевое неприводимое F-инвариантное подпространство $L_1 \subset V$ с $L_1 \cap U = 0$, заменим U на $U \oplus L_1$ и повторим рассуждение. Поскольку размерность подпространства U на каждом таком шагу строго увеличивается, через конечное число шагов получится равенство $U \oplus L_1 \oplus \ldots \oplus L_k = V$, и можно взять $W = L_1 \oplus \ldots \oplus L_k$.

Чтобы доказать импликацию (3) ⇒ (4), покажем сначала, что если свойство (3) выполнено для пространства V, то оно выполнено и для каждого F-инвариантного подпространства $H \subset V$. Рассмотрим любое инвариантное подпространство $U \subset H$ и отыщем в V такие инвариантные подпространства Q и R, что $V = H \oplus Q = U \oplus Q \oplus R$. Рассмотрим проекцию $\pi : V \twoheadrightarrow H$ с ядром Q и положим $W = \pi(R)$.

Упражнение 9.12. Проверьте, что $H = U \oplus W$.

Итак, если свойство (3) выполнено для прямой суммы факторколец (9-1) из теор. 9.1, то оно выполнено и для каждого слагаемого этой суммы. Однако по сл. 9.2 пространство $\Bbbk[t]/(p^m)$ при $m > 1$ приводимо, но неразложимо.

Импликация (4) ⇒ (1) также немедленно вытекает из сл. 9.2. □

Следствие 9.5 (из доказательства предл. 9.1)
Ограничение полупростого оператора на инвариантное подпространство также является полупростым оператором. □

9.2.3. Циклические векторы. Вектор $v \in V$ называется *циклическим вектором* линейного оператора $F : V \to V$, если его F-орбита v, Fv, F^2v, F^3v, , … линейно порождает пространство V над полем $\Bbbk$. Иначе можно сказать, что вектор v порождает модуль V_F над $\Bbbk[t]$.

Предложение 9.2
Следующие свойства оператора $F : V \to V$ эквивалентны друг другу:

1) F обладает циклическим вектором

2) F подобен умножению на класс $[t]$ в факторкольце $\Bbbk[t]/(f)$, где $f \in \Bbbk[t]$

3) простые основания всех элементарных делителей оператора F попарно различны

4) минимальный многочлен оператора F совпадает с характеристическим.

Доказательство. Условия (2), (3), (4) очевидно эквивалентны и означают, что оператор F подобен умножению на $[t]$ в прямой сумме факторколец $\Bbbk[t]/(p_1^{m_1}) \oplus \ldots \oplus \Bbbk[t]/(p_r^{m_r})$, где все неприводимые приведённые многочлены $p_1, \ldots, p_r$ попарно различны. Импликация (2) ⇒ (1) тоже очевидна: $\Bbbk[t]$-модуль $\Bbbk[t]/(f)$ порождается над $\Bbbk[t]$ классом $[1]$. Наоборот, если модуль V_F порождается над $\Bbbk[t]$ одним вектором v, то $V_F \simeq \Bbbk[t]/\ker\pi$, где эпиморфизм $\pi : \Bbbk[t] \twoheadrightarrow V_F$ переводит $h(t)$ в $h(F)\,v$. Поскольку $\Bbbk[t]$ — область главных идеалов, $\ker\pi = (f)$ для некоторого $f \in \Bbbk[t]$, откуда $V \simeq \Bbbk[t]/(f)$. □

9.2.4. Собственные подпространства и собственные числа. Максимальное по включению ненулевое подпространство в V, на котором оператор $F: V \to V$ действует как умножение на скаляр $\lambda \in \Bbbk$, называется *собственным подпространством* оператора F с *собственным числом* или *собственным значением* λ и обозначается $V_\lambda \stackrel{\text{def}}{=} \{v \in V \mid F(v) = \lambda v\} = \ker(\lambda \operatorname{Id}_V - F)$. Ненулевые векторы $v \in V_\lambda$ называются *собственными векторами* оператора F с собственным числом[1] λ.

Предложение 9.3
Любой набор собственных векторов с попарно различными собственными числами линейно независим.

Доказательство. Пусть собственные векторы $v_1, \ldots, v_m$ имеют попарно разные собственные числа $\lambda_1, \ldots, \lambda_m$ и линейно зависимы. Рассмотрим линейное соотношение между ними, в котором задействовано минимально возможное число векторов. Пусть это будут векторы $e_1, \ldots, e_k$. Тогда $k \geqslant 2$ и $e_k = x_1 e_1 + \ldots + x_{k-1} e_{k-1}$, где все $x_i \in \Bbbk$ отличны от нуля. При этом $\lambda_k e_k = F(e_k) = \sum x_i F(e_i) = \sum x_i \lambda_i e_i$. Вычитая из этого равенства предыдущее, умноженное на λ_k, получаем более короткую зависимость $x_1(\lambda_1 - \lambda_k)e_1 + \ldots + x_{k-1}(\lambda_{k-1} - \lambda_k)e_{k-1} = 0$ с ненулевыми коэффициентами. □

Следствие 9.6
Сумма ненулевых собственных подпространств с попарно разными собственными числами является прямой. □

9.2.5. Спектр. Множество собственных чисел линейного оператора $F: V \to V$, т. е. всех таких $\lambda \in \Bbbk$, что $V_\lambda = \ker(\lambda \operatorname{Id}_V - F) \neq 0$, называется *спектром*[2] оператора F и обозначается

$$\operatorname{Spec} F = \{\lambda \in \Bbbk \mid \ker(\lambda \operatorname{Id}_V - F) \neq 0\} = \{\lambda \in \Bbbk \mid \det(tE - F) = 0\},$$

или $\operatorname{Spec}_\Bbbk F$, если важно явно указать основное поле. Так как $\ker(\lambda \operatorname{Id}_V - F) \neq 0$, если и только если $\det(tE - F) = 0$, спектр представляет собою множество корней характеристического многочлена $\chi_F(t) = \det(tE - F)$ в поле $\Bbbk$. Над алгебраически замкнутым полем спектр любого оператора не пуст и совпадает с множеством собственных чисел жордановых клеток оператора F, о котором шла речь в n° 9.1.6 на стр. 148 выше. Над произвольным полем количество различных собственных чисел в спектре не превосходит $\deg \chi_F = \dim V$, что согласуется со сл. 9.6, согласно которому

$$\sum_{\lambda \in \operatorname{Spec} F} \dim V_\lambda \leqslant \dim V. \tag{9-12}$$

Упражнение 9.13. Покажите, что $\operatorname{Spec} F$ содержится в множестве корней любого многочлена, аннулирующего F.

Если известен спектр F, отыскание собственных подпространств сводится к решению систем линейных однородных уравнений $(\lambda \operatorname{Id}_V - F)\, v = 0$, которые гарантированно имеют ненулевые решения при $\lambda \in \operatorname{Spec} F$.

Следствие 9.7
Над алгебраически замкнутым полем $\Bbbk$ любой оператор обладает хотя бы одним ненулевым собственным подпространством. □

[1] Или собственным значением.
[2] Ср. с n° 9.1.6 на стр. 148.

Упражнение 9.14. Покажите, что над алгебраически замкнутым полем $\Bbbk$ оператор F нильпотентен, если и только если $\operatorname{Spec} F = \{0\}$, и приведите пример оператора, для которого неравенство (9-12) строгое.

9.2.6. Диагонализуемые операторы. Оператор $F : V \to V$ называется *диагонализуемым*, если в V имеется базис, в котором F записывается диагональной матрицей. Такой базис состоит из собственных векторов оператора F, а элементы диагональной матрицы суть собственные числа F, причём каждое собственное число $\lambda \in \operatorname{Spec} F$ встречается на диагонали ровно столько раз, какова кратность корня $t = \lambda$ в характеристическом многочлене $\chi_F(t)$ и какова размерность собственного подпространства V_λ. Иначе можно сказать, что диагонализуемый оператор F подобен оператору умножения на класс $[t]$ в прямой сумме факторколец[1] $\Bbbk[t]/(t-\lambda) \simeq \Bbbk$, где λ пробегает $\operatorname{Spec} F$, и каждое такое прямое слагаемое представлено в сумме ровно $\dim V_\lambda$ раз.

Предложение 9.4
Следующие свойства линейного оператора $F : V \to V$ эквивалентны:

1) F диагонализуем

2) пространство V линейно порождается собственными векторами оператора F

3) все элементарные делители F имеют вид $(t-\lambda)$, $\lambda \in \Bbbk$

4) характеристический многочлен $\chi_F(t) = \det(tE - F)$ полностью раскладывается в $\Bbbk[t]$ на линейные множители, и кратность каждого его корня λ равна размерности собственного подпространства V_λ

5) оператор F можно аннулировать многочленом, который раскладывается в $\Bbbk[t]$ в произведение попарно различных линейных множителей.

Доказательство. Эквивалентность свойств (3) и (5) очевидна. Эквивалентность свойств (1), (2), (3) и импликация (1) $\Rightarrow$ (4) были установлены перед формулировкой предл. 9.4. Из (4) вытекает, что $\sum \dim V_\lambda = \deg \chi_F = \dim V$. Поэтому прямая по сл. 9.6 сумма всех различных собственных подпространств V_λ совпадает с V, что даёт импликацию (4) $\Rightarrow$ (1). □

Следствие 9.8
Если оператор $F : V \to V$ диагонализуем, то его ограничение на любое инвариантное подпространство тоже диагонализуемо на этом подпространстве.

Доказательство. Это вытекает из свойства (5) предл. 9.4. □

Упражнение 9.15. Убедитесь, что над алгебраически замкнутым полем диагонализуемость равносильна полупростоте.

[1] Ср. с упр. 9.9 на стр. 148.

9.2.7. Что стоит за аннулирующим многочленом? Если известно разложение на простые множители того или иного многочлена, аннулирующего линейный оператор[1] $F\colon V \to V$, то это, во-первых, оставляет лишь конечное число возможностей для набора элементарных делителей $\mathcal{El}(F)$ оператора F, а во-вторых, позволяет явно строить F-инвариантные подпространства в V и/или раскладывать V в прямую сумму таких подпространств в терминах действия F непосредственно на пространстве V.

Пример 9.5 (инвариантные подпространства вещественного оператора)
Покажем, что над полем вещественных чисел $\mathbb{R}$ любой конечномерный линейный оператор F обладает одномерным или двумерным инвариантным подпространством. Пусть $\chi_F = q_1 \dots q_m$, где $q_i \in \mathbb{R}[t]$ — неприводимые приведённые линейные или квадратичные многочлены, не обязательно различные. Применим нулевой оператор $0 = \chi_F(F) = q_1(F) \circ q_2(F) \circ \dots \circ q_m(F)$ к какому-нибудь ненулевому вектору $v \in V$. При некотором $i \geqslant 0$ получится такой ненулевой вектор $w = q_{i+1}(F) \circ \dots \circ q_m(F)\, v$, что $q_i(F)\, w = 0$. Если $q_i(t) = t - \lambda$ линеен, то $F(w) = \lambda w$ и вектор w порождает одномерное F-инвариантное подпространство. Если $q_i(t) = t^2 - \alpha t - \beta$ квадратичен, то $F(Fw) = \alpha F(w) + \beta w$ лежит в линейной оболочке векторов w и Fw, которая тем самым является F-инвариантным подпространством размерности не больше 2.

Пример 9.6 (инволюции)
Линейный оператор $\sigma\colon V \to V$ называется *инволюцией*, если он удовлетворяет соотношению $\sigma^2 = \mathrm{Id}_V$, т. е. аннулируется многочленом $t^2 - 1$. Тождественная инволюция $\sigma = \mathrm{Id}_V$ называется *тривиальной*. Так как $t^2 - 1 = (t+1)(t-1)$ является произведением различных линейных множителей, все инволюции диагонализуемы, причём спектр любой инволюции исчерпывается числами ± 1. Таким образом, любое пространство V с инволюцией $\sigma \neq \pm\mathrm{Id}_V$ распадается в прямую сумму $V = V_+ \oplus V_-$ собственных подпространств $V_+ = \ker(\sigma - \mathrm{Id}_V) = \mathrm{im}(\sigma + \mathrm{Id}_V)$ и $V_- = \ker(\sigma + \mathrm{Id}_V) = \mathrm{im}(\sigma - \mathrm{Id}_V)$ с собственными числами ± 1, и любой вектор $v \in V$ однозначно записывается как $v = v_+ + v_-$, где $v_\pm \in V_\pm$ находятся по формулам $v_+ = (v+Fv)/2$, $v_- = (v-Fv)/2$.

Теорема 9.3 (теорема о разложении)
Пусть линейный оператор $F\colon V \to V$ на произвольном[2] векторном пространстве V над произвольным полем $\Bbbk$ аннулируется произведением $q = q_1 \dots q_r$ попарно взаимно простых многочленов $q_i \in \Bbbk[t]$. Положим $Q_j = q/q_j$. Тогда $\ker q_j(F) = \mathrm{im}\, Q_j(F)$ при всех j, эти подпространства F-инвариантны, и V является прямой суммой тех из них, что отличны от нуля.

Доказательство. Так как $q(F) = q_i(F) \circ Q_j(F) = 0$, имеем включение $\mathrm{im}\, Q_i(F) \subset \ker q_i(F)$. Поэтому достаточно показать, что V линейно порождается образами операторов $Q_i(F)$, а сумма ядер $\ker q_i(F)$ прямая[3], т. е. $\ker q_i(F) \cap \sum_{j\neq i} \ker q_j(F) = 0$ для всех i. Первое вытекает из того, что $\dots(Q_1, \dots, Q_r) = 1$, а значит, существуют такие $h_1, \dots, h_r \in \Bbbk[t]$, что $1 = \sum Q_j(t) h_j(t)$. Подставляя в это равенство $t = F$ и применяя обе части к произвольному вектору $v \in V$, получаем разложение $v = Ev = \sum Q_j(F) h_j(F) v \in \sum \mathrm{im}\, Q_j(F)$. Второе вытекает из взаимной простоты q_i и Q_i, в силу которой существуют такие $g, h \in \Bbbk[t]$, что $1 = g(t) \cdot q_i(t) + h(t) \cdot Q_i(t)$. Подставим сюда $t = F$ и применим обе части полученного равенства $E = g(F)\, q_i(F) + h(F) \circ Q_i(F)$ к произвольному вектору $v \in \ker q_i(F) \cap \sum_{j\neq i} \ker q_j$. Так как $\ker q_j(F) \subset \ker Q_i(F)$ при всех $j \neq i$, получим $v = Ev = g(F)\, q_i(F)\, v + h(F)\, Q_i(F)\, v = 0$, что и требовалось. □

[1] Например, характеристического многочлена $\chi_F(t) = \det(tE - F)$.

[2] Возможно даже бесконечномерном.

[3] См. предл. 5.2 на стр. 85.

Пример 9.7 (проекторы)
Линейный оператор $\pi : V \to V$ называется *идемпотентом* или *проектором*, если он аннулируется многочленом $t^2 - t = t(t-1)$, т. е. удовлетворяет соотношению $\pi^2 = \pi$. По теор. 9.3 образ любого идемпотента $\pi : V \to V$ совпадает с подпространством его неподвижных векторов: $\operatorname{im}\pi = \ker(\pi - \mathrm{Id}_V) = \{v \mid \pi(v) = v\}$, и всё пространство распадается в прямую сумму $V = \ker\pi \oplus \operatorname{im}\pi$. Тем самым, оператор π проектирует V на $\operatorname{im}\pi$ вдоль $\ker\pi$. Отметим, что оператор $\mathrm{Id}_V - \pi$ тоже является идемпотентом и проектирует V на $\ker\pi$ вдоль $\operatorname{im}\pi$. Таким образом, задание прямого разложения $V = U \oplus W$ равносильно заданию пары идемпотентных эндоморфизмов $\pi_1 = \pi_1^2$ и $\pi_2 = \pi_2^2$ пространства V, связанных соотношениями $\pi_1 + \pi_2 = 1$ и $\pi_1\pi_2 = \pi_2\pi_1 = 0$.

Упражнение 9.16. Выведите из этих соотношений, что $\ker\pi_1 = \operatorname{im}\pi_2$ и $\operatorname{im}\pi_1 = \ker\pi_2$.

9.3. Функции от операторов. Всюду в этом разделе мы предполагаем, что линейный оператор $F : V \to V$ действует на конечномерном векторном пространстве V над полем $\mathbb{R}$ или $\mathbb{C}$, которое мы будем обозначать через $\mathbb{K}$, и аннулируется многочленом

$$\alpha(t) = (t-\lambda_1)^{m_1} \dots (t-\lambda_r)^{m_r}, \text{ где } \lambda_i \neq \lambda_j \text{ при } i \neq j, \tag{9-13}$$

который полностью разлагается на линейные множители в $\mathbb{K}[t]$. Последнее означает, что минимальный и характеристический многочлены оператора F тоже полностью разлагался на линейные множители в $\mathbb{K}[t]$, и в практических вычислениях в качестве $\alpha(t)$ обычно берётся характеристический многочлен $\chi_F(t)$ оператора F. Однако, чем меньше степень многочлена $\alpha(t)$, тем проще будут все предстоящие нам вычисления.

Сделанные нами предположения на оператор F равносильны тому, что $\mathcal{E}\ell(F)$ исчерпывается степенями линейных двучленов $(t-\lambda)^m$, $\lambda \in \operatorname{Spec} F$. В этой ситуации $\mathbb{K}[t]$-модуль V_F является прямой суммой $V = \bigoplus_{\lambda\in\operatorname{Spec} F} K_\lambda$ *корневых подпространств*[1]

$$K_\lambda \stackrel{\text{def}}{=} \{v \in V \mid \exists\, m \in \mathbb{N} : (\lambda\,\mathrm{Id} - F)^m v = 0\} = \ker(\lambda\,\mathrm{Id} - F)^{m_\lambda}, \tag{9-14}$$

биективно соответствующих собственным числам $\lambda \in \operatorname{Spec} F$. Показатель m_λ в правой части формулы (9-14) равен кратности корня $t = \lambda$ минимального многочлена $\mu_F(t)$ оператора[2] F. Множество корней $\lambda_1, \dots, \lambda_r$ многочлена (9-13) содержит $\operatorname{Spec}(F)$ и для каждого $\lambda \in \operatorname{Spec} F$ показатель m_λ не больше кратности корня $t = \lambda$ многочлена (9-13).

Упражнение 9.17. Не прибегая к теор. 9.1 на стр. 144, выведите существование *корневого разложения* $V = \bigoplus_{\lambda\in\operatorname{Spec} F} K_\lambda$ из тождества Гамильтона – Кэли и теор. 9.3 на стр. 159.

9.3.1. Гомоморфизм вычисления. Алгебра $\mathcal{A}$, состоящая из функций $U \to \mathbb{K}$, заданных на каком-нибудь подмножестве $U \subset \mathbb{K}$, содержащем все корни многочлена (9-13), называется *алгебраически вычислимой* на операторе F, если $\mathbb{K}[t] \subset \mathcal{A}$ и для каждого корня λ кратности k многочлена (9-13) все функции $f \in \mathcal{A}$ определены в точке $\lambda \in \mathbb{K}$ вместе с первыми $k-1$ производными $f^{(\nu)} = \frac{d^\nu f}{dt^\nu}$ и допускают тейлоровское разложение вида

$$f(t) = f(\lambda) + \frac{f'(\lambda)}{1!}(t-\lambda) + \dots + \frac{f^{(k-1)}(\lambda)}{(k-1)!}(t-\lambda)^{k-1} + g_\lambda(t)\cdot(t-\lambda)^k, \tag{9-15}$$

[1] Т. е. подмодулей $(t-\lambda)$-кручения, см. n° 9.1.6 на стр. 148.

[2] Т. е. максимальному из показателей степеней элементарных делителей вида $(t-\lambda)^m$ оператора F.

где функция $g_\lambda(t)$ тоже лежит в алгебре $\mathcal{A}$.

Например, алгебра $\mathcal{A}$ всех функций, определённых в ε-окрестности каждого собственного числа $\lambda \in \operatorname{Spec} F$ и представимых в ней суммой абсолютно сходящегося степенного ряда от $(t-\lambda)$, алгебраически вычислима на операторе F. Подалгебра в $\mathcal{A}$, состоящая из всех аналитических функций[1] $\mathbb{K} \to \mathbb{K}$, алгебраически вычислима на всех операторах $F \in \operatorname{End}_{\mathbb{K}}(V)$, характеристические многочлены которых полностью разлагаются на линейные множители в $\mathbb{K}[t]$.

Теорема 9.4
В сделанных выше предположениях каждая алгебраически вычислимая на операторе $F: V \to V$ алгебра функций $\mathcal{A}$ допускает единственный такой гомоморфизм $\mathbb{K}$-алгебр $\operatorname{ev}_F: \mathcal{A} \to \operatorname{End} V$, что $\operatorname{ev}_F(p) = p(F)$ для всех многочленов $p \in \mathbb{K}[t] \subset \mathcal{A}$.

Доказательство теор. 9.4. Пусть оператор F аннулируется многочленом (9-13), и пусть искомый гомоморфизм $\operatorname{ev}_F: \mathcal{A} \to \mathbb{K}$ существует. Пространство V является прямой суммой F-инвариантных корневых подпространств $K_\lambda = \ker(F-\lambda\mathrm{Id})^{m_\lambda}$. Согласно формуле (9-15) оператор

$$f(F) = f(\lambda)\cdot E + f'(\lambda)\cdot(F-\lambda E) + \ldots + \frac{f^{(m_\lambda-1)}(\lambda)}{(m_\lambda-1)!}(F-\lambda E)^{m_\lambda-1} + g_\lambda(F)(F-\lambda E)^{m_\lambda} \tag{9-16}$$

действует на каждом подпространстве K_λ точно так же, как результат подстановки оператора F в многочлен $j_\lambda^{m_\lambda-1}f(t) \stackrel{\text{def}}{=} f(\lambda) + f'(\lambda)\cdot(t-\lambda) + \ldots + f^{(m_\lambda-1)}(\lambda)\cdot(t-\lambda)^{m_\lambda-1}/(m_\lambda-1)!$. Класс этого многочлена в факторкольце $\mathbb{K}[t]/\big((t-\lambda)^{m_\lambda}\big)$ называется $(m_\lambda-1)$-*струёй* функции $f \in \mathcal{A}$ в точке $\lambda \in \mathbb{K}$. По китайской теореме об остатках существует единственный такой многочлен $p_{f(F)}(t) \in \mathbb{K}[t]$ степени, строго меньшей $\deg\alpha(t)$, что $p_{f(F)}(t) \equiv j_\lambda^{m_\lambda-1}f(t) \pmod{\alpha(t)}$ сразу для всех корней λ многочлена α. Поскольку операторы $p_{f(F)}(F)$ и $f(F)$ одинаково действуют на каждом подпространстве K_λ, имеется равенство $f(F) = p_{f(F)}(F)$. Таким образом, гомоморфизм вычисления единствен. Остаётся убедиться, что отображение $f \mapsto p_{f(F)}(F)$ действительно является гомоморфизмом $\mathbb{K}$-алгебр. Проверим сначала, что отображение

$$\begin{gathered} J: \mathcal{A} \to \frac{\mathbb{K}[t]}{\big((t-\lambda_1)^{m_1}\big)} \times \ldots \times \frac{\mathbb{K}[t]}{\big((t-\lambda_r)^{m_r}\big)} \simeq \frac{\mathbb{K}[t]}{(\alpha)}, \\ f \mapsto \left(j_{\lambda_1}^{m_1-1}f, \ldots, j_{\lambda_s}^{m_r-1}f\right), \end{gathered} \tag{9-17}$$

сопоставляющее функции $f \in \mathcal{A}$ набор её струй[2] во всех корнях многочлена α, является гомоморфизмом $\mathbb{K}$-алгебр, т. е. $\mathbb{K}$-линейно и удовлетворяет равенству $J(fg) = J(f)J(g)$. Первое очевидно, второе достаточно установить для каждой струи j_λ^{m-1} отдельно. Используя правило Лейбница: $(fg)^{(k)} = \sum_{\nu=0}^{k}\binom{k}{\nu}f^{(\nu)}g^{(k-\nu)}$, получаем следующие равенства по модулю $(t-\lambda)^m$:

$$\begin{aligned} j_\lambda^{m-1}(fg) &= \sum_{k=0}^{m-1}\frac{(t-\lambda)^k}{k!}\sum_{\nu+\mu=k}\frac{k!}{\nu!\mu!}f^{(\nu)}(\lambda)g^{(\mu)}(\lambda) = \\ &= \sum_{k=0}^{m-1}\sum_{\nu+\mu=k}\frac{f^{(\nu)}(\lambda)}{\nu!}(t-\lambda)^\nu\cdot\frac{g^{(\mu)}(\lambda)}{\mu!}(t-\lambda)^\mu \equiv j_\lambda^{m-1}(f)j_\lambda^{m-1}(g). \end{aligned}$$

[1] Т. е. функций, задаваемых сходящимися всюду в $\mathbb{K}$ степенными рядами.

[2] Мы рассматриваем этот набор как элемент прямого произведения соответствующих колец вычетов, которое по китайской теореме об остатках изоморфно факторкольцу $\mathbb{K}[t]/(\alpha)$.

Отображение $f \mapsto p_{f(F)}(F)$ является композицией гомоморфизма (9-17) с гомоморфизмом вычисления многочленов $\mathrm{ev}_F : \mathbb{K}[t] \to \operatorname{End} V$, $p \mapsto p(F)$, который корректно пропускается через фактор $\mathbb{K}[t]/(\alpha)$, так как $\alpha(F) = 0$. □

Определение 9.1 (гомоморфизм вычисления)
Гомоморфизм $\mathrm{ev}_F : \mathcal{A} \to \operatorname{End} V$ из теор. 9.4 называется *вычислением* функций $f \in \mathcal{A}$ на операторе F. Линейный оператор $\mathrm{ev}_F(f) : V \to V$, в который переходит функция $f \in \mathcal{A}$ при гомоморфизме вычисления, обозначается $f(F)$ и называется *функцией f от оператора F*.

Замечание 9.1. (как относиться к функциям от операторов) Из теор. 9.4 вытекает, что если характеристический многочлен линейного оператора $F : V \to V$ полностью разлагается на линейные множители в $\mathbb{K}[t]$, то на пространстве V определены такие линейные операторы, как e^F или $\sin F$, а если $F \in \mathrm{GL}(V)$, то и такие задаваемые аналитическими вне нуля функциями операторы, как $\ln F$ или $\sqrt{F}$, причём алгебраические свойства всех этих операторов точно такие же, как у числовых функций e^t, $\sin t$, $\ln t$ и $\sqrt{t}$. В частности, все эти функции от оператора F коммутируют друг с другом и с F, а также удовлетворяют соотношениям вроде $\ln F^2 = 2 \ln F$ и $\sqrt{F}\sqrt{F} = F$. Таким образом, функции от операторов можно использовать для отыскания операторов с предписанными свойствами, например, удовлетворяющих заданному алгебраическому или дифференциальному уравнению, в частности, для извлечения корней из невырожденных операторов.

Предложение 9.5
В условиях теор. 9.4 на стр. 161 для любой функции f из алгебраически вычислимой на операторе F алгебры функций $\mathcal{A}$ спектр оператора $f(F)$ состоит из чисел $f(\lambda)$, где $\lambda \in \operatorname{Spec} F$. Если $f'(\lambda) \neq 0$, то элементарные делители $(t-\lambda)^m \in \mathcal{E}\ell(F)$ биективно соответствуют элементарным делителям $\big(t-f(\lambda)\big)^m \in \mathcal{E}\ell\big(f(F)\big)$. Если $f'(\lambda) = 0$, то каждому элементарному делителю $(t-\lambda)^m$ с $m > 1$ из $\mathcal{E}\ell(F)$ в множестве $\mathcal{E}\ell\big(f(F)\big)$ соответствует объединение нескольких элементарных делителей вида $\big(t-f(\lambda)\big)^{\ell_i}$ с $\ell_i \in \mathbb{N}$ и $\sum_i \ell_i = m$.

Доказательство. Реализуем F как оператор умножения на класс $[t]$ в прямой сумме факторколец $V = \mathbb{K}[t]/\big((t-\lambda_1)^{s_1}\big) \oplus \ldots \oplus \mathbb{K}[t]/\big((t-\lambda_r)^{s_r}\big)$. Как мы видели в доказательстве теор. 9.4 ограничение оператора $f(F)$ на корневое подпространство K_λ раскладывается в сумму скалярного оператора $f(\lambda)\,E$ и нильпотентного оператора $N = f'(\lambda)\cdot\eta + \frac{1}{2}f''(\lambda)\cdot\eta^2 + \ldots$, где $\eta : K_\lambda \to K_\lambda$ обозначает оператор умножения на класс $[t-\lambda]$. На каждом слагаемом $\mathbb{K}[t]/\big((t-\lambda)^m\big)$ оператор η имеет ровно одну жорданову цепочку максимальной длины m. Если $f'(\lambda) \neq 0$, то

$$N^{m-1} = f'(\lambda)^{m-1}\cdot\eta^{m-1} \neq 0\,.$$

Поэтому N тоже имеет ровно одну жорданову цепочку длины m. При $f'(\lambda) = 0$ и $m > 1$ равенство $N^k = 0$ наступит при $k < m$. Поэтому цикловой тип ограничения оператора N на каждое слагаемое вида $\mathbb{K}[t]/\big((t-\lambda)^m\big)$ состоит из нескольких цепочек суммарной длины m. □

Упражнение 9.18. Покажите, что матрица $J_n^{-1}(\lambda)$, обратная к жордановой клетке размера $n\times n$ с собственным числом λ, подобна матрице $J_n(\lambda^{-1})$.

9.3.2. Интерполяционный многочлен. Многочлен $p_{f(F)}(t) \in \mathbb{K}[t]$, принимающий на операторе F то же самое значение, что и функция $f \in \mathcal{A}$, называется *интерполяционным многочленом* для вычисления $f(F)$. Он однозначно определяется тем, что его степень строго меньше степени аннулирующего оператор f многочлена α и в каждом корне кратности m многочлена α сам многочлен $p_{f(F)}$ и первые его $m-1$ производные принимают те же значения, что функция f и её первые $m-1$ производные. Таким образом, при $\deg \alpha = d$ отыскание коэффициентов интерполяционного многочлена $p_{f(F)}$ сводится к решению системы из d линейных уравнений на d неизвестных.

Лемма 9.2 (об интерполяции с кратными узлами[1])
Для любых различных чисел $a_1, \ldots, a_n$ из любого поля $\Bbbk$ и произвольно заданного для каждого a_i набора из m_i значений $b_{i,0}, b_{i,1}, \ldots, b_{i,m_i-1} \in \Bbbk$ существует единственный такой многочлен $g \in \Bbbk[x]$ степени строго меньше $m = m_1 + \ldots + m_n$, что при каждом $i = 1, \ldots, n$ сам этот многочлен и первые его $m_i - 1$ производные принимают в точке a_i заданные значения

$$g(a_i) = b_{i,0},\ g'(a_i) = b_{i,1},\ \ldots\ ,\ g^{(m_i-1)}(a_i) = b_{i,m_i-1}\,,$$

где $g^{(k)}(x) = d^k g(x)/dx^k$ означает k-тую производную многочлена g.

Доказательство. Введём на m парах чисел (i,j), где $1 \leqslant i \leqslant n$, $0 \leqslant j < m_j$, какой-нибудь линейный порядок и рассмотрим отображение $F : \Bbbk[x]_{<m} \to \Bbbk^m$, переводящее каждый многочлен g степени меньше m в набор значений[2] $g^{(j)}(a_i)$, записанных в одну строку в выбранном на парах (i,j) порядке.

Упражнение 9.19. Убедитесь, что отображение F линейно.

Если $g \in \ker F$, то по предл. 2.6 на стр. 45 каждое число $a_i \in \Bbbk$ является как минимум m_i-кратным корнем многочлена g, т. е. g делится на $\prod_i (x-a_i)_i^m$, откуда $g = 0$, ибо степень произведения равна $m > \deg g$. Мы заключаем, что $\ker F = 0$. Поскольку $\dim \Bbbk[x]_{<m} = \dim \Bbbk^m$, отображение F биективно. □

Пример 9.8 (степенная функция и рекуррентные уравнения, ср. с прим. 3.6 на стр. 59)
Задача отыскания n-того члена a_n числовой последовательности $z : \mathbb{Z} \to \mathbb{K}$, $n \mapsto z_n$, решающей рекуррентное уравнение $z_n = \alpha_1 z_{n-1} + \alpha_2 z_{n-2} + \ldots + \alpha_m z_{n-m}$ с начальным условием $(z_0, \ldots, z_{n-1}) = (a_0, \ldots, a_{n-1}) \in \mathbb{K}^n$, сводится вычислению n-той степени *матрицы сдвига*

$$S = \begin{pmatrix} 0 & 0 & \ldots & 0 & \alpha_m \\ 1 & 0 & \ddots & \vdots & \alpha_{m-1} \\ 0 & 1 & \ddots & 0 & \vdots \\ \vdots & \ddots & \ddots & 0 & \alpha_2 \\ 0 & \ldots & 0 & 1 & \alpha_1 \end{pmatrix}$$

смещающей каждый фрагмент из m последовательных элементов на один шаг вправо:

$$(z_{k+1},\ z_{k+2},\ \ldots\ ,\ z_{k+m}) \cdot S = (z_{k+2},\ z_{k+3},\ \ldots\ ,\ z_{k+m+1})\,.$$

[1] Это утверждение обобщает прим. 2.5 на стр. 43.
[2] Где для единообразия обозначений мы полагаем $g^{(0)} \stackrel{\text{def}}{=} g$.

Искомый элемент a_n при этом равен первой координате вектора

$$(a_n,\ a_{n+1},\ \dots\ ,\ a_{n+m-1}) = (a_0, a_1, \dots, a_{m-1}) \cdot S^n\,.$$

Матрица $S^n = p_{S^n}(S)$ является результатом подстановки матрицы S в интерполяционный многочлен $p_{S^n}(t) \in \mathbb{K}[t]$ для вычисления на матрице S *степенной функции* $f(t) = t^n$. Обратите внимание, что $\deg p_{S^n} < m$, и коэффициенты многочлена p_{S^n} находятся решением системы из m линейных уравнений на m неизвестных.

Например, для *уравнения Фибоначчи* $a_n = a_{n-1} + a_{n-2}$ матрица сдвига имеет вид

$$S = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}.$$

Интерполяционный многочлен для вычисления степенной функции t^n на этой матрице линеен. Записывая его в виде $p_{S^n}(t) = at + b$ с неопределёнными коэффициентами a и b, получаем

$$S^n = a\,S + b\,E = \begin{pmatrix} b & a \\ a & a+b \end{pmatrix}.$$

Таким образом, n-тое *число Фибоначчи*, решающее уравнение Фибоначчи с начальным условием $(a_0, a_1) = (0, 1)$, равно первой координате вектора $\bigl(a_n, a_{n+1}\bigr) = (0,1) \cdot S^n = (a, a+b)$. Матрица S аннулируется своим характеристическим многочленом

$$\chi_S(t) = t^2 - t\ \operatorname{tr} S + \det S = t^2 - t - 1 = (t - \lambda_+)(t - \lambda_-)$$

с однократными корнями $\lambda_\pm = (1 \pm \sqrt{5})/2$. Функция t^n принимает на них значения $\lambda_\pm^n$. Коэффициенты a и b находятся из системы

$$\begin{cases} a\,\lambda_+ + b = \lambda_+^n \\ a\,\lambda_- + b = \lambda_-^n\,, \end{cases}$$

и по правилу Крамера $a = \bigl(\lambda_+^n - \lambda_-^n\bigr) / \bigl(\lambda_+ - \lambda_-\bigr)$. Тем самым,

$$a_n = a = \frac{(1+\sqrt{5})^n - (1-\sqrt{5})^n}{2^n \cdot \sqrt{5}}\,,$$

что согласуется с прим. 3.6 на стр. 59.

Пример 9.9 (квадратный корень из оператора)
Покажем, что если поле $\Bbbk$ алгебраически замкнуто и $\operatorname{char}\Bbbk \neq 2$, то из любого биективного линейного оператора F на конечномерном векторном пространстве V над полем $\Bbbk$ можно извлечь квадратный корень, являющийся многочленом от оператора F. В прим. 3.8 на стр. 63 мы видели, что при всех целых $k \geqslant 0$ биномиальный коэффициент $\binom{2k}{k}$ нацело делится на $(k+1)$, и если $\operatorname{char}\Bbbk \neq 2$, то корректно определён биномиальный степенной ряд[1]

$$\sqrt{1+x} = \sum_{k\geqslant 0} \binom{1/2}{k} x^k = 1 + \frac{1}{2} \sum_{k\geqslant 1} \frac{(-1)^{k-1}}{4^{k-1}} \binom{2k-2}{k-1} \frac{x^k}{k}\,. \tag{9-18}$$

[1] См. формулу (3-19) на стр. 63.

Упражнение 9.20. Убедитесь в том, что квадрат многочлена, равного сумме первых $n+1$ членов этого ряда, равен $1+x$ в $\Bbbk[x]/(x^{n+1})$.

Если поле $\Bbbk$ алгебраически замкнуто, характеристический многочлен $\chi_F(t)$ оператора F разлагается на взаимно простые множители $(t-\lambda)^{m_\lambda}$, где $\lambda \in \operatorname{Spec}(F)$, и пространство V является прямой суммой F-инвариантных корневых подпространств $K_\lambda = \ker(F-\lambda\mathrm{Id})^{m_\lambda}$. Так как F биективен, все числа λ в этом разложении отличны от нуля. Для каждого $\lambda \in \operatorname{Spec}(F)$ обозначим через $p_\lambda(t) \in \Bbbk[t]$ сумму первых m_λ членов формального разложения Тэйлора функции $\sqrt{t}$ в точке λ, которое получается из (9-18) заменой переменных:

$$\sqrt{t} = \sqrt{\lambda+(t-\lambda)} = \sqrt{\lambda}\cdot\bigl(1+(t-\lambda)/\lambda\bigr)^{1/2} = \lambda^{1/2} + \frac{t-\lambda}{2\lambda^{1/2}} - \frac{(t-\lambda)^2}{8\lambda^{3/2}} + \frac{(t-\lambda)^3}{16\lambda^{5/2}} - \dots .$$

Тогда $p_\lambda^2(t) \equiv t \bmod (t-\lambda)^{m_\lambda}$ в силу упр. 9.20. По китайской теореме об остатках существует многочлен $p(t)$, сравнимый с $p_\lambda(t)$ по модулю $(t-\lambda)^{m_\lambda}$ сразу для всех $\lambda \in \operatorname{Spec}(F)$. Он имеет $p^2(t) \equiv t \bmod (t-\lambda)^{m_\lambda}$ для всех $\lambda \in \operatorname{Spec}(F)$. Поскольку квадрат оператора $p(F)$ действует на каждом корневом подпространстве K_λ точно также, как F, мы заключаем, что $p^2(F) = F$.

Замечание 9.2. (аналитически определённые функции от оператора) Гомоморфизм вычисления значений многочленов на матрице $F \in \operatorname{Mat}_n(\mathbb{C})$ можно продолжать на бóльшие алгебры функций $\mathcal{C} \supset \mathbb{C}[z]$ средствами анализа: наделим пространства $\mathcal{C}$ и $\operatorname{Mat}_n(\mathbb{C})$ той или иной топологией, представим функцию $f \in \mathcal{C}$ в виде предела $f = \lim_{k\to\infty} f_k$ какой-нибудь последовательности многочленов f_k и положим матрицу $f(F)$ равной пределу последовательности матриц $f_k(F) \in \operatorname{Mat}_n(\mathbb{C})$. Разумеется, при этом необходимо проверять, что предел $\lim_{k\to\infty} f_k(F)$ существует и зависит только от функции f, а не от выбора сходящейся к f последовательности многочленов, и отдельно следует убедиться в том, что полученное таким образом отображение $\mathrm{ev}_F : \mathcal{C} \to \operatorname{Mat}_n(\mathbb{C})$, $f \mapsto f(F)$, является гомоморфизмом алгебр[1]. Но если это так, и если переход к пределу в пространстве матриц перестановочен со сложением и умножением на константы[2], то как бы ни определялась сходимость в пространстве функций и какой бы ни была сходящаяся к функции f последовательность многочленов f_k, последовательность матриц $f_k(F)$ будет лежать в конечномерном векторном пространстве, порождённом над $\mathbb{C}$ степенями F^m с $0 \leqslant m < n$, т. е. её предел *a priori* будет многочленом от F степени, строго меньшей n, а значит, может быть вычислен при помощи подходящего интерполяционного многочлена. Если матрицы F и G подобны, т. е. $G = CFC^{-1}$ для некоторой матрицы $C \in \mathrm{GL}_k(\mathbb{C})$, то аналитически определённые функции от этих матриц тоже будут подобны: так как равенство $f_k(G) = Cf_k(F)C^{-1}$ справедливо для всех многочленов, приближающих функцию f, оно выполняется и для предельной функции в силу непрерывности линейного отображения $\operatorname{Mat}_n(\mathbb{C}) \to \operatorname{Mat}_n(\mathbb{C})$, $X \mapsto CXC^{-1}$.

9.4. Перестановочные операторы и разложение Жордана. Если линейные операторы F и G на векторном пространстве V над произвольным полем $\Bbbk$ коммутируют друг с другом, то ядро

[1] Иначе не вполне понятно, зачем оно нужно. В качестве упражнения по анализу читателю настоятельно рекомендуется попробовать самостоятельно реализовать намеченную программу, используя на пространстве функций топологию, в которой сходимость последовательности функций означает равномерную сходимость в каждом круге в $\mathbb{C}$, а на пространстве $\operatorname{Mat}_n(\mathbb{C})$ — стандартную топологию пространства $\mathbb{C}^{n^2}$, где сходимость определяется покоординатно.

[2] Т. е. $\lim\limits_{k\to\infty}(\lambda F_k + \mu G_k) = \lambda \lim\limits_{k\to\infty} F_k + \mu \lim\limits_{k\to\infty} G_k$. Это означает, в частности, что все $\mathbb{C}$-линейные отображения $\operatorname{Mat}_n(\mathbb{C}) \to \operatorname{Mat}_n(\mathbb{C})$ непрерывны.

и образ любого многочлена от оператора F переводятся оператором G в себя:

$$f(F)\,v = 0 \quad \Rightarrow \quad f(F)\,Gv = Gf(F)\,v = 0$$
$$v = f(F)\,w \quad \Rightarrow \quad Gv = Gf(F)\,w = f(F)\,Gw\,.$$

В частности, все собственные подпространства $V_\lambda = \ker(F - \lambda E)$ инвариантны относительно любого перестановочного с F оператора G.

Предложение 9.6
В конечномерном векторном пространстве V над алгебраически замкнутым полем $\Bbbk$ любое множество коммутирующих друг с другом операторов обладает общим для всех операторов собственным вектором. Над произвольным полем $\Bbbk$ любое множество коммутирующих друг с другом диагонализуемых операторов на V можно одновременно диагонализовать в некотором общем для всех операторов базисе.

Доказательство. Индукция по $\dim V$. Если все операторы скалярны (что так при $\dim V = 1$), то доказывать нечего — подойдут, соответственно, любой ненулевой вектор и любой базис. Если среди операторов есть хоть один нескалярный оператор F, то над замкнутым полем у него есть собственное подпространство строго меньшей размерности, чем V, а в диагонализуемом случае V является прямой суммой таких собственных подпространств. Каждое собственное подпространство оператора F инвариантно для всех операторов, причём если операторы диагонализуемы на всём пространстве, то их ограничения на собственные подпространства оператора F тоже диагонализуемы по сл. 9.8. Применяя к собственному подпространству (соответственно ко всем собственным подпространствам) оператора F предположение индукции, получаем требуемое. □

Пример 9.10 (конечные группы операторов)
Если m линейных операторов на конечномерном пространстве V над алгебраически замкнутым полем $\Bbbk$ характеристики $\operatorname{char}\Bbbk \nmid m$ образуют группу G, то каждый из этих операторов аннулируется многочленом $t^m - 1$, который раскладывается в произведение m попарно различных линейных множителей[1]. Поэтому каждый оператор в группе G диагонализуем. Все операторы из группы G одновременно диагонализуются в одном общем базисе, если и только если группа G абелева.

Теорема 9.5 (разложение Жордана)
Для каждого оператора F на конечномерном векторном пространстве V над алгебраически замкнутым полем $\Bbbk$ существует единственная пара таких операторов F_d и F_n, что F_n нильпотентен, F_d диагонализуем, $F_dF_n = F_nF_d$ и $F = F_d + F_n$. Эти единственные операторы F_d и F_n являются многочленами без свободных членов от оператора F.

Доказательство. Пусть $\operatorname{Spec} F = \{\lambda_1, \dots, \lambda_r\}$. В силу алгебраической замкнутости поля $\Bbbk$, характеристический многочлен $\chi_F(t) = \prod_{\lambda\in\operatorname{Spec} F}(t-\lambda)^{m_\lambda}$ полностью разлагается на линейные множители, и пространство $V = \bigoplus_{\lambda\in\operatorname{Spec} F} K_\lambda$ является прямой суммой корневых подпространств $K_\lambda = \ker(F - \lambda\operatorname{Id})^{m_\lambda}$. В качестве диагонализуемого оператора F_d можно взять оператор, действующий на каждом корневом подпространстве K_λ умножением на λ, а в качестве нильпотентного

[1] Поскольку производная mt^{m-1} многочлена $t^m - 1$ отлична от нуля и взаимно проста с ним.

оператора F_n — разность $F_n = F - F_d$, которая действует на каждом корневом подпространстве K_λ нильпотентным оператором $F - \lambda\,\mathrm{Id}$.

Покажем, что оба эти оператора являются многочленами без свободного члена от F. Для этого достаточно представить в таком виде оператор F_d. Для каждого ненулевого $\lambda \in \operatorname{Spec} F$ обозначим через $g_\lambda \in \Bbbk[x]$ многочлен, представляющий класс λ/t в $\Bbbk[x]/\big((t-\lambda)^{m_\lambda}\big)$, а для $\lambda = 0$ положим $g_\lambda(t) = 0$. По китайской теореме об остатках существует многочлен $g \in \Bbbk[x]$, сравнимый с g_λ по модулю $(t-\lambda)^{m_\lambda}$ сразу для всех $\lambda \in \operatorname{Spec} F$. Многочлен tg_λ не имеет свободного члена, и его класс в $\Bbbk[x]/\big((t-\lambda)^{m_\lambda}\big)$ равен классу λ для всех $\lambda \in \operatorname{Spec} F$. Поэтому оператор $g(F)$ действует на каждом корневом подпространстве K_λ как умножение на λ, т. е. совпадает с F_d.

Будучи многочленами от F, операторы F_d и $F_n = F - F_d$ перестановочны между собою и с F. Это доказывает существование операторов F_d и F_n с требуемыми свойствами, включающими в себя и последнее утверждение предложения. Докажем их единственность.

Пусть есть ещё одно разложение $F = F'_d + F'_n$, в котором F'_d диагонализуем, F'_n нильпотентен и $F'_d F'_n = F'_n F'_d$. Из последнего равенства вытекает, что F'_d и F'_n перестановочны с любым многочленом от $F = F'_d + F'_n$, в частности, с построенными выше F_d и F_n. Поэтому каждое собственное подпространство V_λ оператора F_d переводится оператором F'_d в себя[1], причём F'_d диагонализуем[2] на каждом V_λ. Если бы оператор F'_d имел на V_λ собственный вектор с собственным значением $\mu \neq \lambda$, то этот вектор был бы собственным для оператора $F_n - F'_n = F_d - F'_d$ с собственным значением $\lambda - \mu \neq 0$, что невозможно, так как оператор $F_n - F'_n$ нильпотентен.

Упражнение 9.21. Докажите, что разность двух перестановочных нильпотентных операторов нильпотентна.

Следовательно, оператор F'_d действует на каждом собственном подпространстве V_λ оператора F_d как умножение на λ, откуда $F'_d = F_d$. Тогда и $F'_n = F - F'_d = F - F_d = F_n$. □

Определение 9.2
Операторы F_d и F_n из теор. 9.5 называются, соответственно, *диагонализуемой* и *нильпотентной* составляющими оператора F.

Замечание 9.3. Поскольку операторы F_d и F_n являются многочленами от F, каждое F-инвариантное подпространство $U \subset V$ является инвариантным для F_d и F_n.

[1] См. n° 9.4 на стр. 165.
[2] См. сл. 9.8 на стр. 158.

§10. Группы

10.1. Группы, подгруппы, циклы. Множество G называется *группой*, если на нём задана операция *композиции* $G \times G \to G$, $(g_1, g_2) \mapsto g_1 g_2$ со свойствами

$$\text{ассоциативность}: \quad \forall\, f, g, h \in G \quad (fg)h = f(gh) \tag{10-1}$$

$$\text{наличие единицы}: \quad \exists\, e \in G : \forall\, g \in G \quad eg = g \tag{10-2}$$

$$\text{наличие обратных}: \quad \forall\, g \in G \quad \exists\, g^{-1} \in G : g^{-1} g = e \tag{10-3}$$

Группа называется *коммутативной* или *абелевой*, если дополнительно имеет место

$$\text{коммутативность}: \quad \forall\, f, g \in G \quad fg = gf\,. \tag{10-4}$$

Левый обратный к g элемент g^{-1} из (10-3) является также и правым обратным, т. е. $gg^{-1} = e$, что устанавливается умножением правой и левой части в $g^{-1}gg^{-1} = eg^{-1} = g^{-1}$ слева на левый обратный к g^{-1} элемент.

Упражнение 10.1. Убедитесь, что обратный к g элемент g^{-1} однозначно определяется элементом g и что $\big(g_1 \dots g_k\big)^{-1} = g_k^{-1} \dots g_1^{-1}$.

Для единицы e из (10-2) при любом $g \in G$ выполнятся также и равенство $ge = g$, поскольку $ge = g(g^{-1}g) = (gg^{-1})g = eg = g$.

Упражнение 10.2. Убедитесь, что единичный элемент $e \in G$ единствен.

Если группа G конечна, число элементов в ней обозначается $|G|$ и называется *порядком* группы G. Подмножество $H \subset G$ называется *подгруппой*, если оно образует группу относительно имеющейся в G композиции. Для этого достаточно, чтобы вместе с каждым элементом $h \in H$ в H лежал и обратный к нему элемент h^{-1}, а вместе с каждой парой элементов $h_1, h_2 \in H$ — их произведение $h_1 h_2$. Единичный элемент $e \in G$ автоматически окажется в H, т. к. $e = hh^{-1}$ для произвольного $h \in H$.

Упражнение 10.3. Проверьте, что пересечение любого множества подгрупп является подгруппой.

Пример 10.1 (группы преобразований)
Модельными примерами групп являются *группы преобразований*, обсуждавшиеся нами в n° 0.6. Все взаимно однозначные отображения произвольного множества X в себя очевидно образуют группу. Она обозначается $\operatorname{Aut} X$ и называется *группой автоморфизмов* множества X. Подгруппы $G \subset \operatorname{Aut} X$ называются *группами преобразований* множества X. Для $g \in G$ и $x \in X$ мы часто будем сокращать обозначение $g(x)$ до gx. Группа всех автоморфизмов n-элементного множества $X = \{1, \dots, n\}$ называется n-той *симметрической группой* и обозначается S_n. Порядок $|S_n| = n!$. Чётные перестановки образуют в S_n подгруппу, обозначаемую A_n и часто называемую *знакопеременной группой*. Порядок $|A_n| = n!/2$.

10.1.1. Циклические группы и подгруппы. Наименьшая по включению подгруппа в G, содержащая заданный элемент $g \in G$, состоит из всевозможных целых степеней g^m элемента g, где мы, как обычно, полагаем $g^0 \stackrel{\text{def}}{=} e$ и $g^{-n} \stackrel{\text{def}}{=} \big(g^{-1}\big)^n$. Она называется *циклической подгруппой*, порождённой g, и обозначается $\langle g \rangle$. Группа $\langle g \rangle$ абелева и является образом сюръективного гомоморфизма абелевых групп $\varphi_g : \mathbb{Z} \twoheadrightarrow \langle g \rangle$, $m \mapsto g^m$, который переводит сложение в композицию. Если $\ker \varphi_g \neq 0$, то $\ker \varphi_g = (n)$ и $\langle g \rangle \simeq \mathbb{Z}/(n)$, где $n \in \mathbb{N}$ — наименьшая степень, для которой $g^n = e$. Она называется *порядком* элемента g и обозначается $\operatorname{ord}(g)$. В этом случае

группа $\langle g\rangle$ имеет порядок[1] $n = \operatorname{ord} g$ и состоит из элементов $e = g^0$, $g = g^1$, g^2, … , g^{n-1}. Если $\ker \varphi_g = 0$, то $\varphi_g : \mathbb{Z} \xrightarrow{\sim} \langle g\rangle$ является изоморфизмом и все степени g^m попарно различны. В этом случае говорят, что g имеет *бесконечный порядок* и пишут $\operatorname{ord} g = \infty$.

Напомним[2], что группа G называется *циклической*, если в ней есть такой элемент $g \in G$, 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 $\mathbb{Z}$ циклическая, и её образующей является любой из элементов ± 1. Согласно сл. 2.3 на стр. 52, всякая конечная подгруппа мультипликативной группы любого поля циклическая. Аддитивная группа вычетов $\mathbb{Z}/(10)$ тоже циклическая, и её образующей является любой из четырёх классов[3] $[\pm 1]_6$, $[\pm 3]_6$.

Упражнение 10.4. Укажите необходимые и достаточные условия для того, чтобы конечно порождённая абелева группа[4] $G = \mathbb{Z}^r \oplus \mathbb{Z}/(p_1^{n_1}) \oplus \ldots \oplus \mathbb{Z}/(p_\alpha^{n_\alpha})$ была циклической.

Лемма 10.1
Элемент $h = g^k$ тогда и только тогда является образующей циклической группы $\langle g\rangle$ порядка n, когда $\text{нод}(k, n) = 1$.

Доказательство. Так как $\langle h\rangle \subset \langle g\rangle$, равенство $\langle h\rangle = \langle g\rangle$ равносильно неравенству $\operatorname{ord} h \geqslant n$. Если $h^m = g^{mk} = e$, то $n \mid mk$. При $\text{нод}(n, k) = 1$ мы заключаем, что $n \mid m$, откуда $m \geqslant n$ и, в частности, $\operatorname{ord} h \geqslant n$. Если же $n = n_1 d$ и $k = k_1 d$, где $d > 1$, то $h^{n_1} = g^{kn_1} = g^{nk_1} = e$ и $\operatorname{ord} h \leqslant n_1 < n$. □

10.1.2. Разложение перестановок в композиции циклов. Перестановка $\tau \in S_n$ по кругу переводящая друг в друга какие-нибудь m различных элементов[5]

$$i_1 \mapsto i_2 \mapsto \ldots \mapsto i_{m-1} \mapsto i_m \mapsto i_1 \tag{10-5}$$

и оставляющая на месте все остальные элементы, называется *циклом* длины m.

Упражнение 10.5. Покажите, что k-тая степень цикла длины m является циклом тогда и только тогда, когда $\text{нод}(k, m) = 1$.

Цикл (10-5) часто бывает удобно обозначать $\tau = \big|i_1, \ldots, i_m\rangle$, не смотря на то, что один и тот же цикл (10-5) допускает m *различных* таких записей, получающихся друг из друга циклическими перестановками элементов.

Упражнение 10.6. Сколько имеется в S_n различных циклов длины k?

Теорема 10.1
Каждая перестановка $g \in S_n$ является композицией $g = \tau_1 \ldots \tau_k$ непересекающихся и, стало быть, попарно коммутирующих друг с другом циклов, причём такое разложение единственно с точностью до перестановки циклов.

[1] Таким образом, порядок элемента равен порядку порождённой им циклической подгруппы.
[2] См. n° 2.5.1 на стр. 51.
[3] Обратите внимание, что никакой из шести оставшихся классов образующей не являются.
[4] См. теор. 7.1 на стр. 120.
[5] Числа $i_1, \ldots, i_m$ могут быть любыми, не обязательно соседними или возрастающими.

Доказательство. Поскольку множество $X = \{1, \dots, n\}$ конечно, в последовательности

$$x \overset{g}{\longmapsto} g(x) \overset{g}{\longmapsto} g^2(x) \overset{g}{\longmapsto} g^3(x) \overset{g}{\longmapsto} \dots, \tag{10-6}$$

возникающей при применении g к произвольной точке $x \in X$, случится повтор. Так как преобразование $g : X \xrightarrow{\sim} X$ биективно, первым повторившимся элементом будет стартовый элемент x. Таким образом, каждая точка $x \in X$ под действием g движется по циклу. В силу биективности g два таких цикла, проходящие через различные точки x и y, либо не пересекаются, либо совпадают. Таким образом, перестановка g является произведением непересекающихся циклов, очевидно, перестановочных друг с другом. □

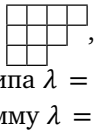
Упражнение 10.7. Покажите, что два цикла $\tau_1, \tau_2 \in S_n$ перестановочны ровно в двух случаях: когда они не пересекаются или когда $\tau_2 = \tau_1^s$ и оба цикла имеют одинаковую длину, взаимно простую с s.

Определение 10.1 (цикловой тип перестановки)
Написанный в порядке нестрогого убывания набор длин непересекающихся циклов[1], в которые раскладывается перестановка $g \in S_n$, называется *цикловым типом* перестановки g и обозначается $\lambda(g)$.

Цикловой тип перестановки $g \in S_n$ удобно изображать n-клеточной диаграммой Юнга, а сами циклы записывать по строкам этой диаграммы. Например, перестановка

$$g = (6,\ 5,\ 4,\ 1,\ 8,\ 3,\ 9,\ 2,\ 7) = |1, 6, 3, 4\rangle\, |2, 5, 8\rangle\, |7, 9\rangle =$$

1	6	3	4
2	5	8	
7	9		

имеет цикловой тип  , т. е. $\lambda(6,\ 5,\ 4,\ 1,\ 8,\ 3,\ 9,\ 2,\ 7) = (4, 3, 2)$. Единственной перестановкой циклового типа $\lambda = (1, \dots, 1)$ (один столбец высоты n) является тождественная перестановка Id. Диаграмму $\lambda = (n)$ (одна строка длины n) имеют $(n-1)!$ циклов максимальной длины n.

Упражнение 10.8. Сколько перестановок в симметрической группе S_n имеют заданный цикловой тип, содержащий для каждого $i = 1, \dots, n$ ровно m_i циклов длины i?

Пример 10.2 (вычисление порядка и знака 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 $5 \cdot 4 \cdot 3 = 60$. По правилу ниточек из прим. 8.1 на стр. 129 знак цикла длины ℓ равен $(-1)^{\ell-1}$. Поэтому перестановка чётна тогда и только тогда, когда у неё чётное число циклов чётной длины.

Упражнение 10.9. Найдите чётность $g = (6,\ 5,\ 4,\ 1,\ 8,\ 3,\ 9,\ 2,\ 7) \in S_9$ и вычислите g^{15}.

[1] Включая циклы длины один, отвечающие элементам, которые перестановка оставляет на месте.

10.2. Группы фигур. Для любой фигуры Φ в евклидовом[1] пространстве $\mathbb{R}^n$ биективные отображения $\Phi \to \Phi$ индуцированные ортогональными[2] линейными преобразованиями пространства $\mathbb{R}^n$, переводящими фигуру Φ в себя, образуют группу преобразований фигуры Φ. Эта группа называется *полной группой фигуры* Φ и обозначается O_Φ. Подгруппу $\mathrm{SO}_\Phi \subset \mathrm{O}_\Phi$, состоящую из биекций, индуцированных собственными[3] ортогональными операторами $\mathbb{R}^n \to \mathbb{R}^n$, мы будем называть *собственной группой фигуры* Φ. Если фигура $\Phi \subset \mathbb{R}^n$ содержится в некоторой гиперплоскости $\Pi \subset \mathbb{R}^n$, 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 10.10. Изготовьте модели пяти *платоновых тел* — тетраэдра, октаэдра, куба, додекаэдра и икосаэдра, см. рис. 10⋄5 – рис. 10⋄8 на стр. 173 – 174.

Пример 10.3 (группы диэдров D_n)
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 $n = 2$. Его можно представлять себе как вытянутую симметричную луночку с двумя сторонами, изображённую на рис. 10⋄1. Группа D_2 такой луночки совпадает с группами описанного вокруг неё прямоугольника и вписанного в неё ромба[4]. Она 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.

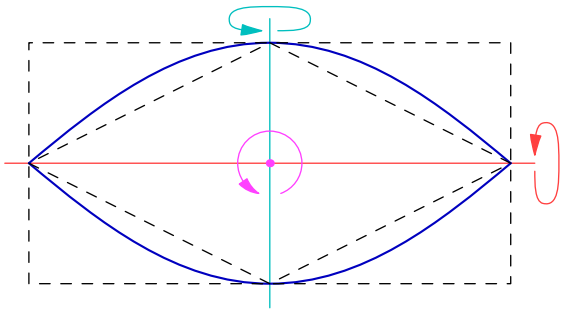


Рис. 10⋄1. Двуугольник D_2.

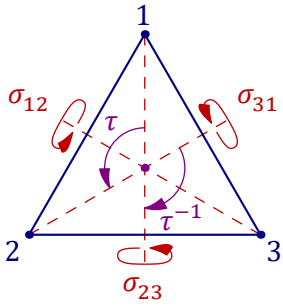


Рис. 10⋄2. Группа треугольника.

Упражнение 10.11. Убедитесь, что $D_2 \simeq \mathbb{Z}/(2) \oplus \mathbb{Z}/(2)$.

[1] Напомню, что *евклидовость* означает фиксацию в векторном пространстве $\mathbb{R}^n$ симметричного билинейного положительного скалярного произведения $V \times V \to \mathbb{R}$, обозначаемого (v, w), см. лекцию http://http://gorod.bogomolov-lab.ru//ps/stud/geom_ru/2122/lec_03.pdf.

[2] Линейный оператор $F : \mathbb{R}^n \to \mathbb{R}^n$ на евклидовом пространстве $\mathbb{R}^n$ называется *ортогональным*, если он сохраняет скалярное произведение, т. е. $\forall v, w \in \mathbb{R}^n \ (Fv, Fw) = (v, w)$ (достаточно, чтобы это равенство выполнялось при $v = w$), см. лекцию http://http://gorod.bogomolov-lab.ru//ps/stud/geom_ru/2122/lec_11.pdf.

[3] Т. е. сохраняющими ориентацию или, что то же самое, с определителем 1, см. раздел 10.2.1 на стр. 133 лекции http://gorod.bogomolov-lab.ru/ps/stud/geom_ru/2122/lec_10.pdf.

[4] Мы предполагаем, что луночка такова, что оба они не квадраты.

Следующая диэдральная группа — *группа треугольника* D_3 — состоит из шести движений: тождественного, двух поворотов τ, τ^{-1} на $\pm 120^\circ$ вокруг центра треугольника и трёх осевых симметрий σ_{ij} относительно его медиан (см. рис. 10⋄2). Так как движение плоскости однозначно задаётся своим действием на вершины треугольника, группа треугольника D_3 изоморфна группе перестановок S_3 его вершин. При этом повороты на $\pm 120^\circ$ отождествляются с циклическими перестановками $(2,\ 3,\ 1)$, $(3,\ 1,\ 2)$, а осевые симметрии — с транспозициями $\sigma_{23} = (1,\ 3,\ 2)$, $\sigma_{13} = (3,\ 2,\ 1)$, $\sigma_{12} = (2,\ 1,\ 3)$. Поскольку движение плоскости, переводящее в себя правильный n-угольник, однозначно определяется своим действием на аффинный репер, образованный какой-нибудь вершиной и примыкающей к ней парой сторон, группа диэдра D_n при каждом $n \geqslant 2$ состоит из $2n$ движений: выбранную вершину можно перевести в любую из n вершин, после чего одним из двух возможных способов совместить рёбра. Эти $2n$ движений суть n поворотов вокруг центра многоугольника на углы[1] $2\pi k/n$ с $k = 0, 1, \ldots, (n-1)$ и n осевых симметрий[2] 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. 10⋄3).

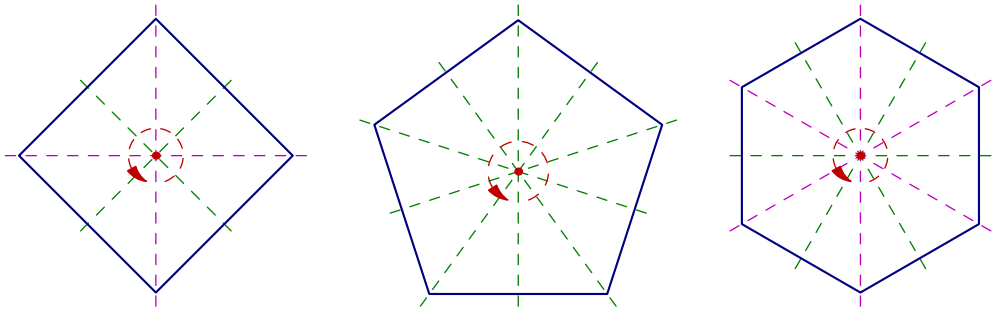


Рис. 10⋄3. Оси диэдров D_4, D_5 и D_6.

Упражнение 10.12. Составьте таблицы умножения в группах D_3, D_4 и D_5, аналогичные таблице из форм. (0-23) на стр. 13.

Пример 10.4 (группа тетраэдра)

Поскольку каждое движение трёхмерного евклидова пространства $\mathbb{R}^3$ однозначно задаётся своим действием на вершины правильного тетраэдра и это действие может быть произвольным, полная группа правильного тетраэдра с центром в нуле изоморфна группе S_4 перестановок его вершин и состоит из 24 движений. Собственная группа состоит из $12 = 4 \cdot 3$ движений: поворот тетраэдра однозначно задаётся своим действием на аффинный репер, образованный какой-нибудь вершиной и тремя выходящими из неё рёбрами, и может переводить эту вершину в любую из четырёх вершин, после чего остаются ровно три возможности для совмещения рёбер, сохраняющего ориентацию пространства. Полный список всех собственных движений тетраэдра таков: тождественное, $4 \cdot 2 = 8$ поворотов на углы $\pm 120^\circ$ вокруг прямых, проходящих через вершину и центр противоположной грани, а также 3 поворота на 180° вокруг прямых, проходящих через середины противоположных рёбер. В несобственной группе, помимо перечисленных поворотов, имеется 6 отражений σ_{ij} в плоскостях, проходящих через середину ребра $[i, j]$ и противоположное ребро, см. рис. 10⋄4.

[1] При $k = 0$ получается тождественное преобразование.

[2] Или, что то же самое, поворотов на 180° в пространстве.

При изоморфизме с S_4 отражение σ_{ij} переходит в транспозицию букв i и j, повороты на $\pm 120^\circ$, представляющие собой всевозможные композиции $\sigma_{ij}\sigma_{jk}$ с попарно разными i, j, k, переходят в циклические перестановки букв i, j, k, три вращения на 180° относительно осей, соединяющих середины противоположных рёбер, — в одновременные транспозиции непересекающихся пар букв: $\sigma_{12}\sigma_{34} = (2, 1, 4, 3)$, $\sigma_{13}\sigma_{24} = (3, 4, 1, 2)$, $\sigma_{14}\sigma_{23} = (4, 3, 2, 1)$.

Упражнение 10.13. Убедитесь, что вместе с тождественным преобразованием эти три поворота образуют группу двуугольника D_2.

Оставшиеся шесть несобственных преобразований тетраэдра отвечают шести циклическим перестановкам вершин $|1234\rangle$, $|1243\rangle$, $|1324\rangle$, $|1342\rangle$, $|1423\rangle$, $|1432\rangle$ и реализуются поворотами на $\pm 90^\circ$ относительно прямых, проходящих через середины противоположных рёбер с последующим отражением в плоскости, проходящей через центр тетраэдра и перпендикулярной оси поворота.

Упражнение 10.14. Выразите эти 6 движений через отражения σ_{ij}.

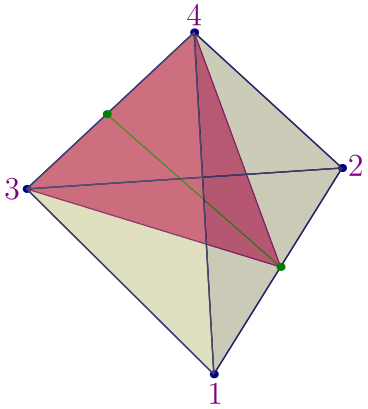


Рис. 10⋄4. Зеркало отражения σ_{12} и ось поворота на 180°.

Пример 10.5 (группа додекаэдра)
Как и для тетраэдра, всякое вращение додекаэдра однозначно задаётся своим действием на аффинный репер, образованный вершиной и тремя выходящими из неё рёбрами, и может переводить эту вершину в любую из 20 вершин, а затем тремя способами совмещать рёбра с сохранением ориентации. Поэтому собственная группа додекаэдра (см. рис. 10⋄5) состоит из $20 \cdot 3 = 60$ движений: $6 \cdot 4 = 24$ поворотов на углы $2\pi k/5$, $1 \leqslant k \leqslant 4$, 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, и тождественного преобразования. Полная группа додекаэдра состоит из $20 \cdot 6 = 120$ движений и помимо перечисленных 60 поворотов содержит их композиции с центральной симметрией относительно центра додекаэдра.

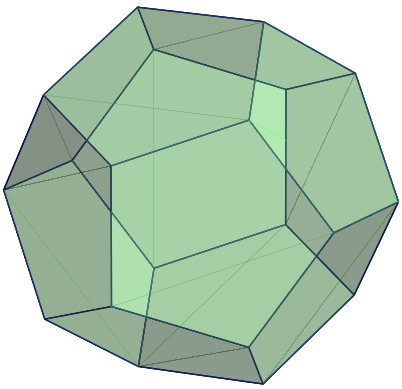


Рис. 10⋄5. Додекаэдр.

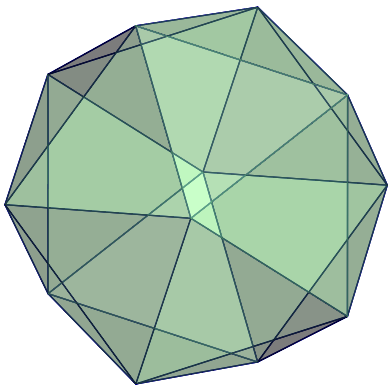


Рис. 10⋄6. Икосаэдр.

Упражнение 10.15. Покажите что полные группы куба, октаэдра и икосаэдра состоят, соответственно из 48, 48 и 120 движений, а собственные — из 24, 24 и 60 поворотов.

10.3. Гомоморфизмы групп. Отображение групп $\varphi\colon G_1 \to G_2$ называется *гомоморфизмом*, если оно переводит композицию в композицию, т. е. для любых $g, h \in G_1$ в группе G_2 выполняется соотношение $\varphi(gh) = \varphi(g)\varphi(h)$. Термины *эпиморфизм*, *мономорфизм* и *изоморфизм* применительно к отображению групп всегда подразумевают по умолчанию, что это отображение является *гомоморфизмом* групп.

Упражнение 10.16. Убедитесь, что композиция гомоморфизмов тоже является гомоморфизмом.

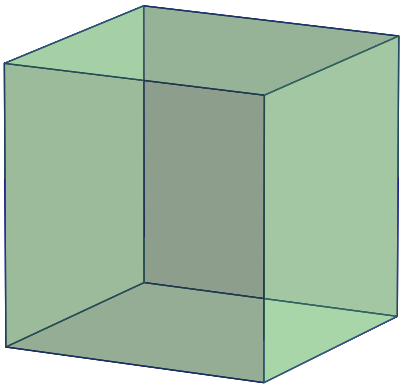


Рис. 10◇7. Куб.

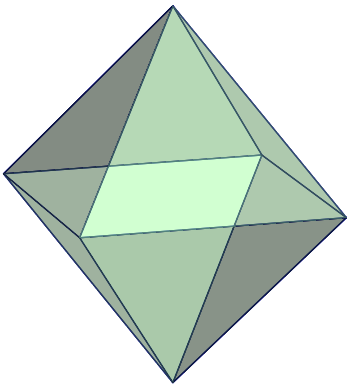


Рис. 10◇8. Октаэдр.

Каждый гомоморфизм групп $\varphi\colon G_1 \to G_2$ переводит единицу e_1 группы G_1 в единицу e_2 группы G_2: равенство $\varphi(e_1) = e_2$ получается из равенств $\varphi(e_1)\varphi(e_1) = \varphi(e_1e_1) = \varphi(e_1)$ умножением правой и левой части на $\varphi(e_1)^{-1}$. Кроме того, для любого $g \in G$ выполняется равенство $\varphi(g^{-1}) = \varphi(g)^{-1}$, так как $\varphi(g^{-1})\varphi(g) = \varphi(g^{-1}g) = \varphi(e_1) = e_2$. Поэтому образ

$$\operatorname{im}\varphi \stackrel{\text{def}}{=} \varphi(G_1) \subset G_2$$

гомоморфизма групп является *подгруппой* группы G_2. Полный прообраз единицы $e_2 \in G_2$ называется *ядром* гомоморфизма φ и обозначается

$$\ker\varphi \stackrel{\text{def}}{=} \varphi^{-1}\left(e_2\right) = \left\{ g \in G_1 \;\middle|\; \varphi(g_1) = e_2 \right\}.$$

Это подгруппа в G_1, поскольку равенства $\varphi(g) = \varphi(h) = e_2$ влекут равенства

$$\varphi(gh) = \varphi(g)\varphi(h) = e_2e_2 = e_2 \quad \text{и} \quad \varphi(g^{-1}) = \varphi(g)^{-1} = e_2^{-1} = e_2\,.$$

Предложение 10.1
Для любого гомоморфизма групп $\varphi\colon G_1 \to G_2$ и каждого $g \in G_1$ выполняются равенства

$$\varphi^{-1}\big(\varphi(g)\big) = g(\ker\varphi) = (\ker\varphi)g\,, \quad \text{где}$$
$$g(\ker\varphi) \stackrel{\text{def}}{=} \{gh \mid h \in \ker\varphi\} \quad \text{и} \quad (\ker\varphi)g \stackrel{\text{def}}{=} \{hg \mid h \in \ker\varphi\}\,.$$

В частности, все непустые слои φ находится в биекции с $\ker\varphi$.

Доказательство. Если $\varphi(t) = \varphi(g)$, то $\varphi(tg^{-1}) = \varphi(t)\varphi(g)^{-1} = e$ и $\varphi(g^{-1}t) = \varphi(g)^{-1}\varphi(t) = e$, т. е. $tg^{-1} \in \ker\varphi$ и $g^{-1}t \in \ker\varphi$. Поэтому $t \in (\ker\varphi)g$ и $t \in g(\ker\varphi)$. Наоборот, для всех $h \in \ker\varphi$ выполняются равенства $\varphi(hg) = \varphi(h)\varphi(g) = \varphi(g)$ и $\varphi(gh) = \varphi(g)\varphi(h) = \varphi(g)$. Тем

самым, полный прообраз $\varphi^{-1}\big(\varphi(g)\big)$ элемента $\varphi(g)$ совпадает и с $(\ker\varphi)g$, и с $g(\ker\varphi)$, а $(\ker\varphi)g$ и $g(\ker\varphi)$ совпадают друг с другом. Взаимно обратные биекции

$$(\ker\varphi)g \underset{hg\leftarrow h}{\overset{t\mapsto tg^{-1}}{\rightleftarrows}} \ker\varphi \underset{g^{-1}t\leftarrow t}{\overset{h\mapsto gh}{\rightleftarrows}} g(\ker\varphi)$$

между ядром и слоем $\varphi^{-1}\big(\varphi(g)\big) = (\ker\varphi)g = g(\ker\varphi)$ задаются правым и левым умножениями элементов ядра на g, а элементов слоя — на g^{-1}. □

Следствие 10.1
Для того, чтобы гомоморфизм групп $\varphi\colon G_1 \to G_2$ был инъективен, необходимо и достаточно, чтобы его ядро исчерпывалось единичным элементом. □

Следствие 10.2
Для любого гомоморфизма конечных групп $\varphi\colon G_1 \to G_2$ выполнено равенство

$$|\operatorname{im}(\varphi)| = |G_1|/|\ker(\varphi)|\,. \tag{10-7}$$

В частности, $|\ker\varphi|$ и $|\operatorname{im}\varphi|$ делят $|G_1|$. □

Пример 10.6 (знакопеременные группы)
Согласно сл. 8.2 на стр. 129 имеется мультипликативный гомоморфизм $\operatorname{sgn}\colon S_n \to \{\pm 1\}$, сопоставляющий перестановке её знак. Ядро этого гомоморфизма $\ker\operatorname{sgn} = A_n$ представляет собою группу чётных перестановок, имеющую порядок $|A_n| = n!/2$.

Пример 10.7 (линейные группы)
Все линейные автоморфизмы любого векторного пространства V над произвольным полем $\Bbbk$ образуют *полную линейную группу* $\mathrm{GL}(V)$. В силу мультипликативности определителя[1] отображение

$$\det\colon\ \mathrm{GL}(V) \to \Bbbk^\times\,,\quad F \mapsto \det F\,, \tag{10-8}$$

является гомоморфизмом полной линейной группы в мультипликативную группу $\Bbbk^\times$ поля $\Bbbk$. Его ядро называется *специальной линейной группой* и обозначается

$$\mathrm{SL}(V) = \ker\det = \{F\colon V \xrightarrow{\sim} V \ \ \det F = 1\}\,.$$

Если поле $\Bbbk = \mathbb{F}_q$ состоит из q элементов и $\dim V = n$, полная линейная группа конечна и

$$\big|\mathrm{GL}_n(\mathbb{F}_q)\big| = (q^n-1)(q^n-q)(q^n-q^2)\,\ldots\,(q^n-q^{n-1})\,,$$

Упражнение 10.17. Убедитесь в этом.

Так как гомоморфизм (10-8) сюръективен[2] порядок специальной линейной группы

$$\big|\mathrm{SL}_n(\mathbb{F}_q)\big| = \big|\mathrm{GL}_n(\mathbb{F}_q)\big|/|\Bbbk^\times| = \frac{(q^n-1)(q^n-q)\ldots(q^n-q^{n-1})}{q-1}\,.$$

[1] См. предл. 8.2 на стр. 134.
[2] Диагональный оператор F с собственными числами $(\lambda, 1, \ldots, 1)$ имеет $\det F = \lambda$.

Пример 10.8 (проективные группы)
Напомню[1], что с каждым векторным пространством V ассоциировано *проективное пространство* $\mathbb{P}(V)$, точками которого являются одномерные векторные подпространства в V или, что то же самое, классы пропорциональности ненулевых векторов в V. Каждый линейный оператор $F \in \mathrm{GL}(V)$ корректно задаёт биекцию $\overline{F}: \mathbb{P}(V) \to \mathbb{P}(V)$, переводящую класс вектора $v \neq 0$ в класс вектора $F(v)$. Таким образом возникает гомоморфизм $F \mapsto \overline{F}$ группы $\mathrm{GL}(V)$ в группу биективных преобразований проективного пространства $\mathbb{P}(V)$. Образ этого гомоморфизма обозначается $\mathrm{PGL}(V)$ и называется *проективной линейной группой* пространства V. Из курса геометрии известно, что два оператора $F, G \in \mathrm{GL}(V)$ тогда и только тогда задают одинаковые преобразования $\overline{F} = \overline{G}$ проективного пространства $\mathbb{P}(V)$, когда они пропорциональны, т. е. $F = \lambda G$ для некоторого $\lambda \in \Bbbk^\times$. Поэтому ядром эпиморфизма групп

$$\pi: \mathrm{GL}(V) \twoheadrightarrow \mathrm{PGL}(V), \quad F \mapsto \overline{F} \tag{10-9}$$

является *подгруппа гомотетий* $\Gamma \simeq \Bbbk^\times$, состоящая из скалярных диагональных операторов. Таким образом, группа $\mathrm{PGL}(V)$ образована классами пропорциональности линейных операторов. Классы пропорциональности операторов с единичным определителем образуют в ней подгруппу, обозначаемую $\mathrm{PSL}(V) \subset \mathrm{PGL}(V)$. Ограничивая эпиморфизм (10-9) на $\mathrm{SL}(V) \subset \mathrm{GL}(V)$ получаем эпиморфизм

$$\pi': \mathrm{SL}(V) \twoheadrightarrow \mathrm{PSL}(V), \quad F \mapsto \overline{F} \tag{10-10}$$

ядром которого является конечная мультипликативная подгруппа $\boldsymbol{\mu}_n(\Bbbk) \subset \Bbbk^\times$ содержащихся в поле $\Bbbk$ корней степени[2] $n = \dim V = \dim \mathbb{P}(V) + 1$ из единицы.

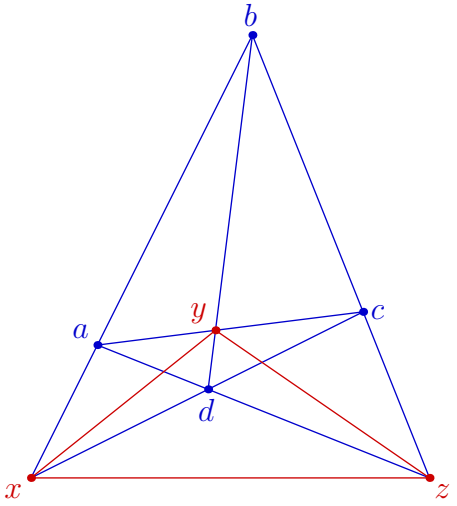


Рис. 10⋄9. Четырёхвешинник и ассоциированный треугольник.

Пример 10.9 (эпиморфизм $S_4 \twoheadrightarrow S_3$)
На проективной плоскости $\mathbb{P}_2$ над любым полем $\Bbbk$ с каждой четвёркой точек a, b, c, d, никакие три из которых не коллинеарны связана фигура, образованная тремя парами проходящих через эти точки прямых[3]

$$(ab) \text{ и } (cd), \quad (ac) \text{ и } (bd), \quad (ad) \text{ и } (bc) \tag{10-11}$$

и называемая *четырёхвершинником*, см. рис. 10⋄9. Пары прямых (10-11) называются *противоположными сторонами* четырёхвершинника. С четырёхвершинником $abcd$ ассоциирован треугольник xyz с вершинами в точках пересечения пар противоположных сторон

$$x = (ab) \cap (cd), \ y = (ac) \cap (bd), \ z = (ad) \cap (bc) \tag{10-12}$$

Каждая перестановка вершин a, b, c, d однозначно определяет линейное проективное преобразование[4] плоскости, что даёт вложение $S_4 \hookrightarrow \mathrm{PGL}_3(\Bbbk)$. Преобразования из S_4 переводят ассоци-

[1] Мы предполагаем, что читатель знаком с проективными пространствами и проективными преобразованиями по курсу геометрии, см. лекции http://gorod.bogomolov-lab.ru/ps/stud/geom_ru/2122/lec_16.pdf и http://gorod.bogomolov-lab.ru/ps/stud/geom_ru/2122/lec_17.pdf.

[2] Напомню, что по определению $\dim \mathbb{P}(V) \stackrel{\text{def}}{=} \dim V - 1$.

[3] Они отвечают трём возможным способам разбить точки a, b, c, d на две пары.

[4] Напомню, что каждое линейное проективное преобразование $\overline{F} \in \mathrm{PGL}(V)$ однозначно определяется своим действием на любые $\dim V + 1$ точек пространства $\mathbb{P}(V)$, никакие $\dim V$ из которых не лежат в одной гиперплоскости.

ированный треугольник xyz в себя, переставляя его вершины x, y, z согласно формулам (10-12). Например, 3-цикл $(b, c, a, d) \in S_4$ задаёт циклическую перестановку (y, z, x), а транспозиции (b, a, c, d), (a, c, b, d) и (c, b, a, d) дают транспозиции (x, z, y), (y, x, z) и (z, y, x) соответственно. Таким образом, мы получаем сюръективный гомоморфизм $S_4 \twoheadrightarrow S_3$. Его ядро имеет порядок $4!/3! = 4$ и состоит из тождественной перестановки и трёх пар независимых транспозиций (b, a, d, c), (c, d, a, b), (d, c, b, a).

Пример 10.10 (S_4 и собственная группа куба)
Линейные преобразования евклидова пространства $\mathbb{R}_3$, составляющие собственную группу куба с центром в нуле, действуют на четырёх прямых a, b, c, d, соединяющих противоположные вершины куба, а также на трёх прямых x, y, z, соединяющих центры его противоположных граней, см. рис. 10⋄10. На проективной плоскости $\mathbb{P}_2 = \mathbb{P}(\mathbb{R}^3)$ эти 7 прямых становятся вершинами четырёхвершинника $abcd$ и ассоциированного с ним треугольника xyz, как на рис. 10⋄9. Поворот на 180° вокруг оси, соединяющей середины противоположных рёбер куба, меняет местами примыкающие к этому ребру диагонали и переводит в себя каждую их двух оставшихся диагоналей. Тем самым, вращения куба осуществляют транспозиции любых двух соседних диагоналей, и мы имеем сюръективный гомоморфизм $\mathrm{SO}_{\text{куб}} \to S_4$. Так как обе группы имеют порядок 24, это изоморфизм. Он переводит 6 поворотов на $\pm 90°$ вокруг прямых x, y, z в 6 циклов длины 4 циклового типа $\square\square\square\square$, 3 поворота на 180° вокруг тех же прямых — в 3 пары независимых транспозиций циклового типа $\begin{smallmatrix}\square\square\\\square\square\end{smallmatrix}$, 8 поворотов на $\pm 120°$ вокруг прямых a, b, c, d — в 8 циклов длины 3 циклового типа $\begin{smallmatrix}\square\square\square\\\square\end{smallmatrix}$, а 6 поворотов на 180° вокруг осей, проходящих через середины противоположных рёбер — в 6 простых транспозиций циклового типа $\begin{smallmatrix}\square\square\\\square\\\square\end{smallmatrix}$. Гомоморфизм $\mathrm{SO}_{\text{куб}} \to S_3$, возникающий из действия группы куба на прямых x, y, z, согласован с изоморфизмом $\mathrm{SO}_{\text{куб}} \xrightarrow{\sim} S_4$ и эпиморфизмом $S_4 \twoheadrightarrow S_3$ из предыдущего прим. 10.9. Его ядро состоит из собственных ортогональных преобразований евклидова пространства $\mathbb{R}^3$, переводящих в себя каждую из декартовых координатных осей x, y, z в $\mathbb{R}^3$, и совпадает, таким образом, с группой двуугольника D_2 с осями x, y, z. В таком контексте эту группу иногда называют *четвертной группой Клейна* и обозначают V_4. Изоморфизм $\mathrm{SO}_{\text{куб}} \xrightarrow{\sim} S_4$ переводит её в ядро эпиморфизма $S_4 \twoheadrightarrow S_3$ из прим. 10.9.

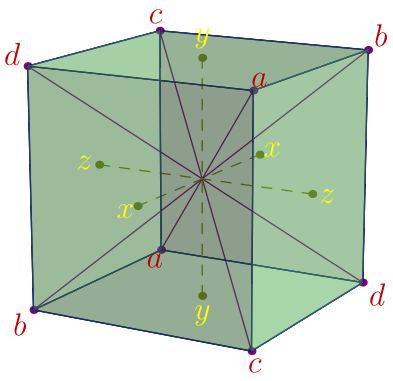


Рис. 10⋄10. От куба к четырёхвершиннику.

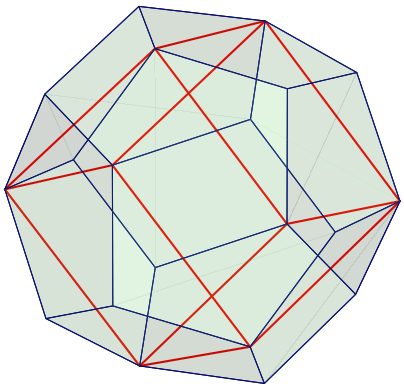


Рис. 10⋄11. Один из пяти кубов на додекаэдре.

Пример 10.11 (собственная группа додекаэдра и A_5)
Любая диагональ любой грани додекаэдра единственным образом достраивается до лежащего на поверхности додекаэдра куба, образованного диагоналями граней так, что в каждой грани

рисуется ровно одна диагональ[1], как на рис. 10⋄11. Всего таких кубов на поверхности додекаэдра имеется ровно пять, и они биективно соответствуют пяти диагоналям какой-нибудь фиксированной грани. Собственная группа додекаэдра переставляет эти кубы друг с другом, что даёт гомоморфизм собственной группы додекаэдра в симметрическую группу S_5

$$\psi_{\text{дод}} \colon \mathrm{SO}_{\text{дод}} \to S_5\,. \tag{10-13}$$

Глядя на модель додекаэдра, легко видеть, что образами $20\cdot 3 = 60$ поворотов, из которых состоит группа $\mathrm{SO}_{\text{дод}}$ являются 60 чётных перестановок: тождественное преобразование додекаэдра задаёт тождественную перестановку кубов; $6 \cdot 4 = 24$ поворота на углы $2\pi k/5$, $1 \leqslant k \leqslant 4$, вокруг осей, проходящих через центры противоположных граней, переходят во всевозможные циклы длины 5, т. е. в 24 перестановки циклового типа $\square\square\square\square\square$; $10 \cdot 2 = 20$ поворотов на углы $\pm 2\pi/3$ вокруг осей, проходящих через противоположные вершины додекаэдра, переходят во всевозможные циклы длины 3, т. е. в 20 перестановок циклового типа $\begin{smallmatrix}\square\square\square\\\square\\\square\end{smallmatrix}$; 15 поворотов на 180° вокруг осей, проходящих через середины противоположных рёбер додекаэдра, переходят во всевозможные пары независимых транспозиций, т. е. в 10 перестановок циклового типа $\begin{smallmatrix}\square\square\\\square\square\\\square\end{smallmatrix}$. Таким образом, гомоморфизм (10-13) является изоморфизмом собственной группы додекаэдра со знакопеременной подгруппой $A_5 \subset S_5$. В отличие от прим. 10.4 переход от собственной группы додекаэдра к полной не добавляет новых перестановок кубов, поскольку каждое несобственное движение является композицией собственного движения и центральной симметрии, которая переводит каждый из кубов в себя.

Упражнение 10.18. Покажите, что симметрическая группа S_5 не изоморфна полной группе додекаэдра.

10.4. 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

$$\varphi \colon G \to \mathrm{Aut}(X)$$

называется *действием* группы G на множестве X или *представлением* группы G автоморфизмами множества X. Отображение $\varphi(g) \colon X \to X$, отвечающее элементу $g \in G$ при действии φ часто бывает удобно обозначать через $\varphi_g \colon X \to X$. Тот факт, что сопоставление $g \mapsto \varphi_g$ является гомоморфизмом групп, означает, что $\varphi_{gh} = \varphi_g \circ \varphi_h$ для всех $g, h \in G$. Если понятно, о каком действии идёт речь, мы часто будем сокращать $\varphi_g(x)$ до gx. При наличии действия группы G на множестве X мы пишем $G : X$. Действие называется *транзитивным*, если любую точку множества X можно перевести в любую другую точку каким-нибудь преобразованием из группы G, т. е. $\forall x, y \in X\ \exists g \in G : gx = y$. Более общим образом, действие называется *m-транзитивным*, если любые два упорядоченных набора из m различных точек множества X можно перевести друг в друга подходящими преобразованиями из G. Действие называется *свободным*, если каждый отличный от единицы элемент группы действует на X без неподвижных точек, т. е. $\forall g \in G\ \forall x \in X\ gx = x \Rightarrow g = e$. Действие $\varphi \colon G \to \mathrm{Aut}\, X$ называется *точным* (или

[1]Проще всего это увидеть на модели додекаэдра, которую я ещё раз настоятельно рекомендую изготовить — см. упр. 10.10 на стр. 171.

эффективным), если каждый отличный от единицы элемент группы действует на X не тождественно, т. е. когда $\ker \varphi = e$. Точное представление отождествляет G с группой преобразований $\varphi(G) \subset \mathrm{Aut}(X)$ множества X. Отметим, что любое свободное действие точно.

Если группа G действует на множестве X, то она действует и на подмножествах множества X: элемент $g \in G$ переводит подмножество $M \subset X$ в подмножество $gM = \{gm \mid m \in M\}$. При этом отображение $g : M \to gM$, $x \mapsto gx$ биективно, и обратным к нему является отображение $g^{-1} : gM \to g$, $\mapsto g^{-1}y$, ибо $g^{-1}gx = ex = x$. Говорят, что элемент $g \in G$ *нормализует*[1] подмножество $M \subset X$, если $gM = M$, т. е. $gx \in M$ для каждого $x \in M$. Каждый такой элемент задаёт биекцию $g|_M : M \to M$. Если эта биекция тождественна, т. е. $gx = x$ для всех $x \in M$, то говорят, что элемент g *централизует* подмножество M. Множество всех элементов $g \in G$, нормализующих (соотв. централизующих) данное подмножество $M \subset X$ обозначается $N(M)$ (соотв. $Z(M)$) и называется *нормализатором* (соотв. *централизатором*) подмножества $M \subset X$ при заданном действии группы G на X.

Упражнение 10.19. Убедитесь, что $N(M)$ и $Z(M)$ являются подгруппами в G.

Пример 10.12 (регулярные действия)
Обозначим через X множество элементов группы G, а через $\mathrm{Aut}(X)$ — группу автоморфизмов этого *множества*[2]. Отображение $\lambda : G \to \mathrm{Aut}\, X$, переводящее элемент $g \in G$ в преобразование[3] $\lambda_g : x \mapsto gx$ левого умножения на g является гомоморфизмом групп, поскольку

$$\lambda_{gh}(x) = ghx = \lambda_g(hx) = \lambda_g\left(\lambda_h(x)\right) = \lambda_g \circ \lambda_h\,(x)\,.$$

Оно называется *левым регулярным действием* группы G на себе. Так как равенство $gh = h$ в группе G влечёт равенство $g = e$, левое регулярное действие свободно и, в частности, точно. Симметричным образом, *правое регулярное действие* $\varrho_g : G \to \mathrm{Aut}(X)$ сопоставляет элементу $g \in G$ преобразование $x \mapsto xg^{-1}$ правого умножения на обратный[4] к g элемент.

Упражнение 10.20. Убедитесь, что ϱ_g является свободным действием.

Тем самым, любая абстрактная группа G может быть реализована как группа преобразований некоторого множества. Например, левые регулярные представления числовых групп реализуют аддитивную группу $\mathbb{R}$ группой сдвигов $\lambda_v : x \mapsto x + v$ числовой прямой , а мультипликативную группу $\mathbb{R}^*$ — группой гомотетий $\lambda_c : x \mapsto cx$ проколотой прямой $\mathbb{R}^* = \mathbb{R} \smallsetminus \{0\}$.

Пример 10.13 (присоединённое действие)
Отображение $\mathrm{Ad} : G \to \mathrm{Aut}(G)$, сопоставляющее элементу $g \in G$ автоморфизм *сопряжения* этим элементом

$$\mathrm{Ad}_g : G \to G\,, \quad h \mapsto ghg^{-1}\,, \tag{10-14}$$

называется *присоединённым действием* группы G на себе.

[1] В этом случае также говорят, что подмножество $M \subset X$ является g-инвариантным.

[2] Возможно, не перестановочных с имеющейся в G композицией, т. е. не обязательно являющихся автоморфизмами *группы* G.

[3] Обратите внимание, что это преобразование множества X не является гомоморфизмом группы G, поскольку равенство $g(h_1h_2) = (gh_1)(gh_2)$, вообще говоря, не выполняется.

[4] 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).

Упражнение 10.21. Убедитесь, что $\forall\, g \in G$ сопряжение (10-14) является *гомоморфизмом* из G в G и что отображение $g \mapsto \mathrm{Ad}_g$ является гомоморфизмом из G в $\mathrm{Aut}\, G$.

Образ присоединённого действия $\mathrm{Ad}(G) \subset \mathrm{Aut}\, G$ обозначается $\mathrm{Int}(G)$ и называется группой *внутренних автоморфизмов* группы G. Не лежащие в $\mathrm{Int}(G)$ автоморфизмы группы G называются *внешними*. В отличие от левого и правого регулярных действий присоединённое действие, вообще говоря, не свободно и не точно. Например, если группа G абелева, все внутренние автоморфизмы (10-14) тождественные, и ядро присоединённого действия в этом случае совпадает со всей группой. 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

$$Z(G) = \ker(\mathrm{Ad}) = \{g \in G \mid \forall\, h \in G\ gh = hg\}\ .$$

Стабилизатор заданного элемента $g \in G$ в присоединённом действии состоит из всех элементов группы, коммутирующих с g. Он называется *централизатором* элемента g и обозначается

$$Z(g) = \{h \in G \mid hg = gh\}\ .$$

10.4.1. Орбиты. Со всякой группой преобразований G множества X связано бинарное отношение $y \sim x$ на X, означающее, что $y = gx$ для некоторого $g \in G$. Это отношение рефлексивно, ибо $x = ex$, симметрично, поскольку $y = gx \iff x = g^{-1}y$, и транзитивно, т. к. из равенств $y = gx$ и $z = hy$ вытекает равенство $z = (hg)x$. Таким образом, это отношение является эквивалентностью. Класс эквивалентности точки $x \in X$ состоит из всех точек, которые можно получить из x, применяя всевозможные преобразования из группы G. Он обозначается $Gx = \{gx \mid g \in G\}$ и называется *орбитой* x под действием G. Согласно n° 0.4 на стр. 10 множество X распадается в дизъюнктное объединение орбит. Множество всех орбит называется *фактором* множества X по действию группы G и обозначается X/G. С каждой орбитой Gx связано сюръективное отображение[1] множеств $\mathrm{ev}_x : G \twoheadrightarrow Gx$, $g \mapsto gx$, слой которого над точкой $y \in Gx$ состоит из всех преобразований группы G, переводящих x в y. Он называется *транспортёром* x в y и обозначается $G_{yx} = \{g \in G \mid gx = y\}$. Слой над самой точкой x состоит из всех преобразований, оставляющих x на месте. Он называется *стабилизатором* точки x в группе G и обозначается $\mathrm{Stab}_G(x) = G_{xx} = \{g \in G \mid gx = x\}$ или просто $\mathrm{Stab}(x)$, если понятно, о какой группе G идёт речь.

Упражнение 10.22. Убедитесь, что $\mathrm{Stab}_G(x)$ является подгруппой в группе G.

Если $y = gx$ и $z = hx$, то для любого $s \in \mathrm{Stab}(x)$ преобразование $hsg^{-1} \in G_{zy}$. Наоборот, если $fy = z$, то $h^{-1}fg \in \mathrm{Stab}(x)$. Таким образом, мы имеем обратные друг другу отображения множеств:

$$\mathrm{Stab}(x) \underset{h^{-1}fg \leftarrow f}{\overset{s \mapsto hsg^{-1}}{\rightleftarrows}} G_{zy}\,, \tag{10-15}$$

и стало быть, для любых трёх точек x, y, z из одной G-орбиты имеется биекция между G_{zy} и $\mathrm{Stab}(x)$.

[1] При желании его можно воспринимать как «некоммутативное» *отображения вычисления*.

Предложение 10.2 (формула для длины орбиты)
Длина орбиты произвольной точки x при действии на неё конечной группы преобразований G равна $|Gx| = |G| : |\mathrm{Stab}_G(x)|$. В частности, длины всех орбит и порядки стабилизаторов всех точек являются делителями порядка группы.

Доказательство. Группа G является дизъюнктным объединением множеств G_{yx} по всем $y \in Gx$ и согласно предыдущему все эти множества состоят из $|\mathrm{Stab}(x)|$ элементов. □

Предложение 10.3
Стабилизаторы всех точек, лежащих в одной орбите конечной группы, сопряжены:

$$y = gx \;\Rightarrow\; \mathrm{Stab}(y) = g\,\mathrm{Stab}(x)\,g^{-1} = \{ghg^{-1} \mid h \in \mathrm{Stab}(x)\}\,.$$

В частности, все они имеют одинаковый порядок.

Доказательство. Это сразу следует из диаграммы (10-15). □

Пример 10.14 (действие перестановок букв на словах)
Зафиксируем какой-нибудь k-буквенный алфавит $A = \{a_1, \dots, a_k\}$ и рассмотрим множество X всех n-буквенных слов w, которые можно написать с его помощью. Иначе X можно воспринимать как множество всех отображений $w : \{1, \dots, n\} \to A$. 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 $|\mathrm{Stab}(w)| = m_1! \dots m_k!$. Тем самым, длина орбиты такого слова равна мультиномиальному коэффициенту

$$|S_n w| = \frac{|S_n|}{|\mathrm{Stab}(w)|} = \frac{n!}{m_1! \dots m_k!} = \binom{n}{m_1 \dots m_k}.$$

Этот пример показывает, что разные орбиты могут иметь разную длину, и порядки стабилизаторов точек из разных орбит могут быть разными.

Упражнение 10.23. Для каждого из пяти платоновых тел рассмотрите действие группы этого тела на его гранях и по формуле для длины орбиты найдите порядок собственной и несобственной группы каждого из платоновых тел.

Пример 10.15 (классы сопряжённости в симметрической группе)
Перестановка $\mathrm{Ad}_g(\sigma) = g\sigma g^{-1}$, сопряжённая перестановке $\sigma = (\sigma_1, \dots, \sigma_n) \in S_n$, для каждого $i = 1, 2, \dots, n$ переводит элемент $g(i)$ в элемент $g(\sigma_i)$. Поэтому при сопряжении цикла $\tau = |i_1, \dots, i_k\rangle \in S_n$ перестановкой $g = (g_1, \dots, g_n)$ получится цикл $g\tau g^{-1} = \left|g_{i_1}, \dots, g_{i_k}\right\rangle$. Если перестановка $\sigma \in S_n$ имеет цикловой тип λ и является произведением независимых циклов, записанных по строкам диаграммы λ, то действие на такую перестановку внутреннего автоморфизма Ad_g заключается в применении отображения g к заполнению диаграммы λ, т. е. в замене каждого числа i числом g_i.

[1] Т. е. переводит слово $w = a_{\nu_1} \dots a_{\nu_n}$ 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.

Таким образом, орбиты присоединённого действия симметрической группы S_n на себе взаимно однозначно соответствуют n-клеточным диаграммам Юнга, и орбита, отвечающая диаграмме λ, состоит из всех перестановок циклового типа λ. Если диаграмма λ имеет m_i строк длины i для каждого $i = 1, \dots, n$, то централизатор любой перестановки σ циклового типа λ состоит из таких перестановок элементов заполнения диаграммы λ независимыми циклами перестановки σ, которые не меняют σ, т. е. циклически переставляют элементы вдоль строк или произвольным образом переставляют строки одинаковой длины между собой как единое целое. Тем самым, порядок стабилизатора перестановки циклового типа λ зависит только от λ и равен $z_\lambda = 1^{m_1} \cdot m_1! \cdot 2^{m_2} \cdot m_2! \cdot \ldots \cdot n^{m_n} \cdot m_n! = \prod_{i=1}^{n} m_i!\, i^{m_i}$. Количество перестановок циклового типа λ, т. е. длина соответствующей орбиты присоединённого действия, равна $n!/z_\lambda$.

10.4.2. 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 10.2 (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 $|X/G| = |G|^{-1} \sum_{g \in G} |X^g|$.

Доказательство. Обозначим через $F \subset G \times X$ множество всех таких пар (g, x), что $gx = x$. Иначе F можно описать как $F = \bigsqcup_{x \in X} \mathrm{Stab}(x) = \bigsqcup_{g \in G} X^g$. Первое из этих описаний получается из рассмотрения проекции $F \twoheadrightarrow X$, второе — из рассмотрения проекции $F \twoheadrightarrow G$. Согласно второму описанию, $|F| = \sum_{g \in G} |X^g|$. 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 $|X/G|$ орбитам, получаем требуемое. □

Пример 10.16 (ожерелья)
Пусть имеется неограниченный запас одинаковых по форме бусин n различных цветов. Сколько различных ожерелий 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 $\pm 60^\circ$, двух поворотов $\tau^{\pm 2}$ на $\pm 120^\circ$, 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. 10◇12 на стр. 183. Беря на этих рисунках все допустимые сочетания цветов, получаем, соответственно, n, n^2, n^3, n^4 и n^3 раскрасок. По теор. 10.2 число 6-бусинных ожерелий равно $(n^6 + 3n^4 + 4n^3 + 2n^2 + 2n)/12$.

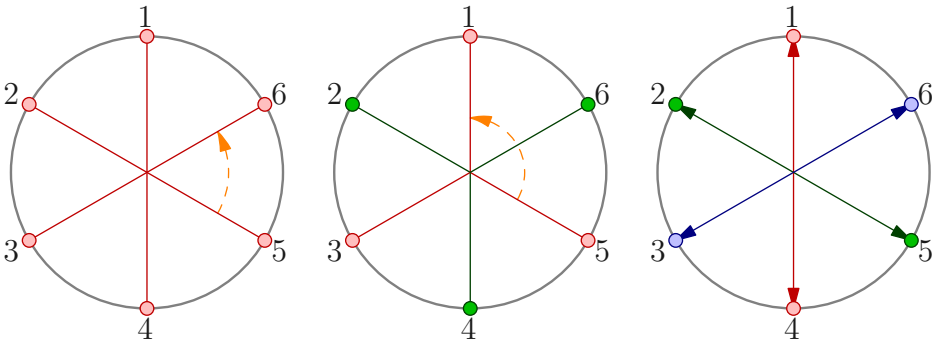
Упражнение 10.24. Подсчитайте количество ожерелий из 7, 8, 9, и 10 бусин.

10.5. Смежные классы и факторизация. Каждая подгруппа $H \subset G$ задаёт на группе G два отношения эквивалентности, происходящие из левого и правого регулярного действия подгруппы H на группе G. Левое действие $\lambda_h : g \mapsto hg$ приводит к эквивалентности

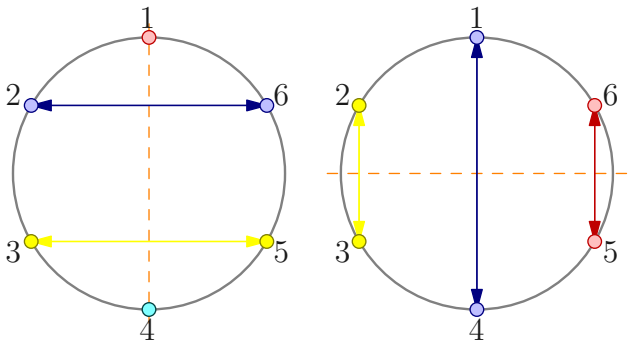
$$g_1 \underset{L}{\sim} g_2 \iff g_1 = hg_2 \text{ для некоторого } h \in H, \tag{10-16}$$

разбивающей группу G в дизъюнктное объединение орбит вида $Hg \stackrel{\text{def}}{=} \{hg \mid h \in H\}$, называемых *правыми смежными классами* (или *правыми сдвигами*) подгруппы H в группе G. Множество правых смежных классов обозначается $H\backslash G$.

Упражнение 10.25. Покажите, что равенство $Hg_1 = Hg_2$ равносильно любому из эквивалентных друг другу включений $g_2 g_1^{-1} \in H$, $g_1 g_2^{-1} \in H$.



τ-инваринтные бусы τ^2-инваринтные бусы τ^3-инваринтные бусы



σ_{14}-инваринтные бусы $\overline{\sigma}_{14}$-инваринтные бусы

Рис. 10◇12. Симметричные ожерелья из шести бусин.

С правым действием $\varrho_h : g \mapsto gh^{-1}$ связано отношение эквивалентности

$$g_1 \underset{R}{\sim} g_2 \iff g_1 = g_2 h \text{ для некоторого } h \in H, \tag{10-17}$$

разбивающее группу G в дизъюнктное объединение орбит $gH \stackrel{\text{def}}{=} \{gh \mid h \in H\}$, которые называются *левыми смежными классами* (или *левыми сдвигами*) подгруппы H в группе G. Множество левых смежных классов обозначается G/H.

Поскольку и левое и правое действия подгруппы H на группе G свободны, все орбиты каждого из них состоят из $|H|$ элементов. Тем самым, число орбит в обоих действиях одинаково и равно $|G| \,/\, |H|$. Это число называется *индексом* подгруппы H в группе G и обозначается $[G : H] \stackrel{\text{def}}{=} |G/H|$. Нами установлена

Теорема 10.3 (теорема Лагранжа об индексе подгруппы)
Порядок и индекс любой подгруппы H в произвольной конечной группе G нацело делят порядок G и $[G : H] = |G| : |H|$.

Следствие 10.3
Порядок любого элемента конечной группы нацело делит порядок группы.

Доказательство. Порядок элемента $g \in G$ равен порядку порождённой им циклической подгруппы $\langle g \rangle \subset G$. □

10.5.1. Нормальные погруппы. Подгруппа $H \subset G$ называется *нормальной* (или *инвариантной*), если для любого $g \in G$ выполняется равенство $gHg^{-1} = H$ или, что то же самое, $gH = Hg$. Иначе можно сказать, что подгруппа $H \subset G$ нормальна тогда и только тогда, когда левая и правая эквивалентности (10-16) и (10-17) совпадают друг с другом и, в частности, $H\backslash G = G/H$. Если подгруппа $H \subset G$ нормальна, мы пишем $H \lhd G$.

Пример 10.17 (ядра гомоморфизмов)
Ядро любого гомоморфизма групп $\varphi : G_1 \to G_2$ является нормальной подгруппой в G_1, поскольку при $\varphi(h) = e$ для любого $g \in G$ имеем равенство

$$\varphi(ghg^{-1}) = \varphi(g)\varphi(h)\varphi(g)^{-1} = \varphi(g)\varphi(g)^{-1} = e\,,$$

означающее, что $g\,(\ker\varphi)\,g^{-1} \subset \ker\varphi$. Это согласуется с равенством правых и левых смежных классов $g\,(\ker\varphi) = (\ker\varphi)\,g$, установленным нами в предл. 10.1.

Пример 10.18 ($V_4 \lhd S_4$)
Подгруппа Клейна $V_4 \subset S_4$ состоящая из перестановок циклового типа  и тождественной перестановки нормальна.

Пример 10.19 (внутренние автоморфизмы)
Подгруппа внутренних автоморфизмов $\mathrm{Int}(G) = \mathrm{Ad}(G)$ нормальна в группе $\mathrm{Aut}(G)$ всех автоморфизмов группы G, поскольку сопрягая внутренний автоморфизм $\mathrm{Ad}_g : h \mapsto ghg^{-1}$ произвольным автоморфизмом $\varphi : G \xrightarrow{\sim} G$, мы получаем внутренний автоморфизм $\varphi \circ \mathrm{Ad}_g \circ \varphi^{-1} = \mathrm{Ad}_{\varphi(g)}$.

Упражнение 10.26. Убедитесь в этом.

Пример 10.20 (параллельные переносы)
Подгруппа параллельных переносов нормальна в группе $\mathrm{Aff}(\mathbb{A}^n)$ всех биективных аффинных преобразований аффинного пространства $\mathbb{A}^n$, т. к. сопрягая параллельный перенос τ_v на вектор v любым аффинным преобразованием $\varphi : \mathbb{A}^n \to \mathbb{A}^n$, получаем перенос[1] $\tau_{D_\varphi(v)}$ на вектор $D_\varphi(v)$.

Упражнение 10.27. Убедитесь в этом.

[1] Напомню, что преобразование $\varphi : \mathbb{A}(V) \to \mathbb{A}(V)$ аффинного пространства $\mathbb{A}(V)$, ассоциированного с векторным пространством V, называется *аффинным*, если отображение $D_\varphi : \overrightarrow{pq} \mapsto \overrightarrow{\varphi(p)\varphi(q)}$ является корректно определённым линейным преобразованием векторного пространства V (оно называется *дифференциалом* отображения φ).

Пример 10.21 (нормализатор и централизатор, ср. с упр. 10.19 на стр. 179)
Пусть группа G действует на множестве X и $M \subset X$ — произвольное подмножество. Напомню[1], что подгруппы $N(M) \stackrel{\text{def}}{=} \{g \in G \mid \forall x \in M \ gx \in M\}$ и $Z(M) \stackrel{\text{def}}{=} \{g \in G \mid \forall x \in M \ gx = x\}$ называются соответственно *нормализатором* и *централизатором* подмножества M. Поскольку для любых $g \in N(M)$, $h \in Z(M)$ и $x \in M$ выполняется равенство $ghg^{-1}x = gg^{-1}x = x$, ибо $h(g^{-1}x) = g^{-1}x$, так как $g^{-1}x \in M$, централизатор является нормальной подгруппой в нормализаторе.

10.5.2. Фактор группы. Попытка определить умножение на множестве левых смежных классов G/H неабелевой группы G формулой

$$(g_1H)\cdot(g_2H) \stackrel{\text{def}}{=} (g_1g_2)H\,, \tag{10-18}$$

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 10.28. Убедитесь, что для группы $G = S_3$ и подгруппы второго порядка $H \subset G$, порождённой транспозицией σ_{12}, формула (10-18) некорректна.

Предложение 10.4
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. Если формула (10-18) корректна, то она задаёт на множестве смежных левых классов G/H групповую структуру: ассоциативность композиции наследуется из[2] G, единицей служит класс $eH = H$, обратным к классу gH — класс $g^{-1}H$. Факторизация $G \twoheadrightarrow G/H$, $g \mapsto gH$, является гомоморфизмом групп с ядром H. Поэтому подгруппа H нормальна в силу прим. 10.17. Наоборот, если H нормальна и $f_1H = g_1H$, $f_2H = g_2H$, то $f_1f_2H = f_1g_2H = f_1Hg_2 = g_1Hg_2 = g_1g_2H$ в силу равенства $g_2H = Hg_2$. □

Определение 10.2
Множество смежных классов G/H нормальной подгруппы $H \lhd G$ с операцией

$$g_1H \cdot g_2H \stackrel{\text{def}}{=} (g_1g_2)H$$

называется *фактором* (или *факторгруппой*) группы G по нормальной подгруппе H. Гомоморфизм групп $G \twoheadrightarrow G/H$, $g \mapsto gH$, называется *гомоморфизмом факторизации*.

Следствие 10.4
Каждый гомоморфизм групп $\varphi : G_1 \to G_2$ 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 $\varphi(g) \in G_2$. В частности, $\operatorname{im}\varphi \simeq G/\ker\varphi$.

Доказательство. Следствие утверждает, что слой $\varphi^{-1}\big(\varphi(g)\big)$ гомоморфизма φ над каждой точкой $\varphi(g) \in \operatorname{im}\varphi \subset G_2$ является левым сдвигом ядра $\ker\varphi$ на элемент g, что мы уже видели в предл. 10.1 на стр. 174. □

[1] См. n° 10.4 на стр. 178.
[2] $(g_1H\cdot g_2H)\cdot g_3H = (g_1g_2)H\cdot g_3H = \big((g_1g_2)g_3\big)H = \big(g_1(g_2g_3)\big)H = g_1H\cdot(g_2g_3)H = g_1H\cdot(g_2H\cdot g_3H)$.

Предложение 10.5
Если подгруппа $H \subset G$ нормализует[1] подгруппу $N \subset G$, то множества $HN = \{hn \mid h \in H,\ n \in N\}$ и $NH = \{nh \mid n \in N,\ h \in H\}$ совпадают друг с другом и являются подгруппой в G, причём $N \lhd HN$, $H \cap N \lhd H$ и $HN/N \simeq H/(H \cap N)$.

Доказательство. $NH = HN$ ибо $nh = h(h^{-1}nh) \in HN$ и $hn = (hnh^{-1})h \in NH$ для всех $n \in N$, $h \in H$. Это подгруппа, так как $(nh)^{-1} = h^{-1}n^{-1} \in HN = NH$ и

$$(n_1h_1)(n_2h_2) = n_1(h_1n_2)h_2 = n_1(n_3h_3)h_2 = (n_1n_3)(h_3h_2) \in NH$$

(существование таких $n_3 \in N$ и $h_3 \in H$, что $h_1n_2 = n_3h_3$, вытекает из равенства $HN = NH$). Подгруппы $H \cap N \lhd H$ и $N \lhd HN$ нормальны, так как по условию $hNh^{-1} \subset N$ для всех $h \in H$. Отображение $H/(H \cap N) \to HN/N$, $h(H \cap N) \mapsto hN$, очевидно корректно определено, биективно и является гомоморфизмом групп. □

Упражнение 10.29. Пусть $\varphi\colon G_1 \twoheadrightarrow G_2$ — сюръективный гомоморфизм групп. Покажите, что полный прообраз $N_1 = \varphi^{-1}(N_2)$ любой нормальной подгруппы $N_2 \lhd G_2$ является нормальной подгруппой в G_1 и $G_1/N_1 \simeq G_2/N_2$.

10.6. Коммутант. В группе G произведение $(g,h) \stackrel{\text{def}}{=} ghg^{-1}h^{-1}$ называется *коммутатором*[2] элементов g, h. Название связано с тем, что $(g,h)hg = gh$. В частности, $gh = hg$ если и только если $(g,h) = e$. Очевидно, что $(g,h)^{-1} = (h,g)$ и $\mathrm{Ad}_f(g,h) = (\mathrm{Ad}_f g, \mathrm{Ad}_f h)$, где

$$\mathrm{Ad}_f\colon G \to G, \quad x \mapsto fxf^{-1},$$

автоморфизм сопряжения. Поэтому всевозможные конечные произведения коммутаторов элементов группы G образуют нормальную подгруппу, которая обозначается $G' \lhd G$ и называется *коммутантом* группы G. Так как $(g,h) = \mathrm{Ad}_g(h)h^{-1}$, коммутаторы элементов $g \in G$ с элементами h из любой нормальной подгруппы $N \lhd G$ лежат в N, т. е. $(G,N) = (N,G) \subset N$. В частности, $(G,G') \subset G'$. Всякий гомоморфизм $\varphi\colon G \to H$ ограничивается в гомоморфизм $\varphi|_{G'}\colon G' \to H'$, и если φ сюръективен, то сюръективен и $\varphi|_{G'}$.

Предложение 10.6 (универсальное свойство фактора по коммутанту)
Всякий гомоморфизм $\varphi\colon G \to A$ в абелеву группу A единственным образом пропускается через гомоморфизм факторизации $\pi\colon G \twoheadrightarrow G/G'$, т. е. существует единственный такой гомоморфизм $\varphi'\colon G/G' \to A$, что $\varphi = \varphi'\pi$.

Доказательство. Гомоморфизм φ' обязан действовать по правилу $gG' \mapsto \varphi(g)$. Оно корректно, так как $G' \subset \ker\varphi$, поскольку в A все коммутаторы тривиальны. □

Следствие 10.5
Фактор группа G/N абелева если и только если $N \supseteq G'$.

Доказательство. Применяем предл. 10.6 к эпиморфизму $G \twoheadrightarrow G/N$. □

[1] Т. е. $hNh^{-1} = N$ для всех $h \in H$.

[2] Или *групповым коммутатором*, который не следует путать с коммутатором $[f,g] = fg - gf$ элементов ассоциативной алгебры.

Пример 10.22 (коммутанты симметрических и знакопеременных групп)
Поскольку каждый коммутатор в S_n является чётной перестановкой, $S_n' \lhd A_n$. Так как $|A_3| = 3$ и группа S_3 не абелева, $S_3' = A_3$. Тем самым, при любом n коммутант S_n' содержит все 3-циклы.

Упражнение 10.30. Убедитесь, что группа A_n порождается 3-циклами.

Мы заключаем, что $S_n' = A_n$. Поскольку $|A_4/V_4| = 3$, группа $A_4/V_4 \simeq \mathbb{Z}/(3)$ абелева, откуда $A_4' \subseteq V_4$ по сл. 10.5. Так как группа A_4 не абелева, A_4' содержит пару независимых транспозиций, а значит, и все сопряжённые ей пары, т. е. $A_4' = V_4$. Отсюда вытекает, что при любом n коммутатор A_n' содержит все пары независимых транспозиций.

Упражнение 10.31. Убедитесь, что при $n \geqslant 5$ группа A_n порождается парами независимых транспозиций.

Мы заключаем, что $A_n' = A_n$ при $n \geqslant 5$.

Пример 10.23 (коммутанты линейных групп)
Пусть $\Bbbk$ — произвольное поле. Так как $\det(f, g) = 1$ для всех $f, g \in \mathrm{GL}_n(\Bbbk)$, мы заключаем, что $\mathrm{GL}_n'(\Bbbk) \trianglelefteq \mathrm{SL}_n(\Bbbk)$. Покажем, что $\mathrm{SL}_n'(\Bbbk) = \mathrm{SL}_n(\Bbbk)$ за исключением $\mathrm{SL}_2(\mathbb{F}_2)$ и $\mathrm{SL}_2(\mathbb{F}_3)$.

Упражнение 10.32. Убедитесь, что $\mathrm{SL}_2(\mathbb{F}_2) = \mathrm{GL}_2(\mathbb{F}_2) \simeq S_3$ и $\mathrm{SL}_2(\mathbb{F}_3)/\{\pm E\} \simeq A_4$.

Легко видеть, что любую матрицу из $\mathrm{SL}_n(\Bbbk)$ можно превратить в единичную элементарными преобразованиями, заключающимися в прибавлении к одной из строк другой строки, умноженной на произвольное число, т. е. в умножении матрицы слева на матрицу вида[1]

$$T_{ij}(\alpha) \stackrel{\text{def}}{=} E + \alpha E_{ij}\,, \quad \text{где} \quad i \neq j\,. \tag{10-19}$$

Упражнение 10.33. Убедитесь в этом и покажите, что $(T_{ij}(\alpha), T_{jk}(\beta)) = T_{ik}(\alpha\beta)$ для любых трёх различных индексов i, j, k.

Из упражнения вытекает, что при $n \geqslant 3$ коммутант $\mathrm{SL}_n'(\Bbbk)$ содержит все трансвекции, и тем самым $\mathrm{GL}_n'(\Bbbk) = \mathrm{SL}_n'(\Bbbk) = \mathrm{SL}_n(\Bbbk)$ при $n \geqslant 3$.

Упражнение 10.34. Покажите, что при $n = 2$ и $\{i, j\} = \{1, 2\}$ коммутатор трансвекции $T_{ij}(\alpha)$ с диагональной матрицей $\beta E_{ii} + \beta^{-1} E_{jj} \in \mathrm{SL}_2(\Bbbk)$ равен $T_{ij}(\alpha(1 - \beta^2))$.

Мы заключаем, что при $\Bbbk \neq \mathbb{F}_2, \mathbb{F}_3$ коммутант $\mathrm{SL}_2'(\Bbbk)$ тоже содержит все трансвекции. Таким образом, $\mathrm{GL}_n'(\Bbbk) = \mathrm{SL}_n'(\Bbbk) = \mathrm{SL}_n(\Bbbk)$ за исключением групп GL_2 и SL_2 над полями $\mathbb{F}_2$ и $\mathbb{F}_3$.

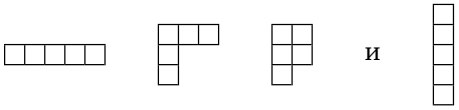
Упражнение 10.35. Вычислите коммутанты $\mathrm{GL}_2'(\mathbb{F}_2) = \mathrm{SL}_2'(\mathbb{F}_2)$, $\mathrm{GL}_2'(\mathbb{F}_3)$ и $\mathrm{SL}_2'(\mathbb{F}_3)$.

[1] Такие матрицы называются *трансвекциями*.

§11. Композиционные факторы, произведения и силовские подгруппы

11.1. 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[1] вообще не содержит никаких подгрупп кроме $\{e\}$ и G. Согласно сл. 10.1 на стр. 175 простота группы G равносильна тому, что всякий гомоморфизм $G \to H$ либо инъективен, либо тривиален[2]. Одним из выдающихся достижений математики XX века является перечисление всех конечных простых групп. Этот список состоит из нескольких бесконечных серий и 26 так называемых *спорадических групп*, не входящих в серии. Бесконечные серии делятся на три семейства: циклические группы $\mathbb{Z}/(p)$ простого порядка, знакопеременные группы A_n с $n \neq 4$ и простые линейные алгебраические группы над конечными полями[3], такие как $\mathrm{PSL}_n(\mathbb{F}_q)$, $\mathrm{PSO}_n(\mathbb{F}_q)$, $\mathrm{PSp}_n(\mathbb{F}_q)$ и т. п. Описание конечных простых групп стало итогом сотен работ десятков авторов по различным, напрямую не связанным друг с другом направлениям математики. Никакой универсальной концепции, позволяющей единообразно классифицировать все конечные простые группы не известно.

11.1.1. Простота знакопеременных групп. Покажем, что знакопеременная группа A_5 проста. Так как перестановки сопряжены если и только если у них одинаковый цикловой тип[4], классы сопряжённости чётных перестановок в S_5 состоят из перестановок цикловых типов



(11-1)

(5-циклы, 3-циклы, пары независимых транспозиций и тождественное преобразование), коих имеется[5] соответственно $24 = 5!/5$, $20 = 5!/(3 \cdot 2)$, $15 = 5!/(2^2 \cdot 2)$ и 1.

Упражнение 11.1. Покажите, что класс сопряжённости чётной перестановки g в S_n либо совпадает с её классом сопряжённости в A_n, либо является объединением двух классов сопряжённости в A_n, причём второе происходит если и только если все циклы перестановки g имеют разные нечётные длины.

Мы заключаем, что 3-циклы, пары независимых транспозиций и тождественная перестановка являются классами сопряжённости в A_5, а 5-циклы разбиваются на два класса сопряжённости в A_5, состоящие из 12 циклов, сопряжённых $|1,2,3,4,5\rangle$, и 12 циклов, сопряжённых $|2,1,3,4,5\rangle$. Поскольку нормальная подгруппа $H \trianglelefteq A_5$ вместе с каждой перестановкой содержит и все ей сопряжённые, её порядок $|H| = 12\varepsilon_1 + 12\varepsilon_2 + 20\varepsilon_3 + 15\varepsilon_4 + 1$, где каждый ε_i равен либо 1, либо 0, при этом по теореме Лагранжа $|H|$ делит $|A_5| = 60 = 3 \cdot 4 \cdot 5$.

Упражнение 11.2. Убедитесь, что такое возможно ровно в двух случаях: когда все $\varepsilon_i = 1$ или когда все $\varepsilon_i = 0$.

Тем самым, в A_5 нет нетривиальных собственных нормальных подгрупп.

---

[1] См. теор. 10.3 на стр. 184.

[2] Т. е. отображает всю группу G в единицу.

[3] Описанию таких групп посвящены спецкурсы по линейным алгебраическим и арифметическим группам, например, см. книгу *Дж. Хамфри*. *Линейные алгебраические группы*. М., «Наука», 1980.

[4] См. прим. 10.15 на стр. 181.

[5] См. упр. 10.8 на стр. 170.

Теорема 11.1
Все знакопеременные группы A_n с $n \geqslant 5$ просты.

Доказательство. Индукция по n. Случай $n = 5$ был разобран выше. Рассмотрим нормальную подгруппу $N \trianglelefteq A_n$. Так как стабилизатор элемента 1 в группе A_n изоморфен A_{n-1}, его пересечение с N, будучи нормальной подгруппой в A_{n-1}, либо совпадает с A_{n-1}, либо тривиально. Поскольку стабилизаторы всех элементов сопряжены, подгруппа N либо содержит стабилизаторы всех элементов, либо действует свободно[1]. В первом случае N содержит все 3-циклы и по упр. 10.30 на стр. 187 совпадает с A_n. Рассмотрим второй случай и допустим, что N содержит нетождественную перестановку g. Так как она действует без неподвижных точек, при $n \geqslant 6$ найдутся такие различные элементы $\{1, i, j, k, \ell, m\}$, что $g(1) = i$ и $g(j) = k$. Сопрягая g циклом $|k, \ell, m\rangle \in A_n$, получаем перестановку $h \in N$ с $h(1) = i$ и $h(j) = \ell \neq k$. Перестановка $gh^{-1} \in N$ не тождественна и оставляет 1 на месте. Противоречие. □

11.1.2. Простота групп $\mathrm{PSL}_n(\Bbbk)$. Фактор полной линейной группы координатного векторного пространства $\Bbbk^n$ по её центру, состоящему из скалярных матриц λE, где $\lambda \in \Bbbk^\times$, называется *проективной линейной группой* и обозначается $\mathrm{PGL}_n(\Bbbk) \stackrel{\text{def}}{=} \mathrm{GL}_n(\Bbbk) / \Bbbk^\times \cdot E$. Эта группа естественным образом действует на множестве одномерных векторных подпространств в $\Bbbk^n$, которое обозначается $\mathbb{P}_{n-1}(\Bbbk)$ и называется $(n-1)$-*мерным проективным пространством*[2] над полем $\Bbbk$. Состоящая из классов пропорциональных матриц определителя 1 подгруппа

$$\mathrm{PSL}_n(\Bbbk) = \mathrm{SL}_n(\Bbbk)/\boldsymbol{\mu}_n(\Bbbk) \cdot E \subset \mathrm{PGL}_n(\Bbbk),$$

где $\boldsymbol{\mu}_n(\Bbbk) \subset \Bbbk^\times$ — мультипликативная группа корней n-той степени из 1 в поле $\Bbbk$, называется *специальной* проективной линейной группой.

Упражнение 11.3. Убедитесь, что PSL_n действует 2-транзитивно[3] на $\mathbb{P}_{n-1}$.

Если $\Bbbk = \mathbb{F}_q$ состоит из q элементов, то мультипликативная группа $\mathbb{F}_q^\times$ циклическая порядка $q-1$ и корни уравнения $x^n = 1$ образуют в ней циклическую подгруппу порядка $\text{нод}(q-1, n)$.

Упражнение 11.4. Убедитесь, корни уравнения $nx = 0$ в $\mathbb{Z}/(m)$ составляют циклическую подгруппу порядка $\text{нод}(m, n)$.

Таким образом, $|\mathrm{PSL}_n(\mathbb{F}_q)| = |\mathrm{SL}_n(\mathbb{F}_q)|/\text{нод}(q-1, n) = \prod_{k=0}^{n}(q^n - q^k)/\big((q-1)\,\text{нод}(q-1, n)\big)$.

Теорема 11.2
Все группы $\mathrm{PSL}_n(\Bbbk)$ просты, за исключением[4] $\mathrm{PSL}_2(\mathbb{F}_2) = \mathrm{GL}_2(\mathbb{F}_2) \simeq S_3$ и $\mathrm{PSL}_2(\mathbb{F}_3) \simeq A_4$.

Доказательство. Обозначим через $P \subset \mathrm{PSL}_n$ стабилизатор одномерного подпространства, порождённого первым вектором стандартного базиса $e_1, \ldots, e_n$ в $\Bbbk^n$. Группа P состоит из классов пропорциональных матриц вида

$$\left(\begin{array}{c|ccc} * & * & \cdots & * \\ \hline 0 & & & \\ \vdots & & * & \\ 0 & & & \end{array}\right) \tag{11-2}$$

[1] Т. е. никакой отличный от единицы элемент не имеет неподвижных точек, см. n° 10.4 на стр. 178.
[2] См. стр. 204 и 222 курса http://gorod.bogomolov-lab.ru/ps/stud/geom_ru/2122/lec_total.pdf.
[3] Т. е. транзитивно действует на упорядоченных парах точек, см. n° 10.4 на стр. 178.
[4] См. упр. 10.32 на стр. 187.

с определителем 1 и содержит нормальную абелеву подгруппу $A \lhd P$ матриц, пропорциональных

$$\left(\begin{array}{c|ccc} 1 & \alpha_2 & \cdots & \alpha_n \\ \hline 0 & 1 & & 0 \\ \vdots & & \ddots & \\ 0 & 0 & & 1 \end{array}\right) = E + \alpha_2 E_{12} + \ldots + \alpha_n E_{1n}\,,$$

которая является ядром гомоморфизма $P \to \mathrm{PGL}_{n-1}$, переводящего матрицу (11-2) в её правую нижнюю угловую подматрицу размера $(n-1)\times(n-1)$.

Упражнение 11.5. Убедитесь, что это и в самом деле гомоморфизм групп.

Так как подгруппа A содержит все трансвекции вида $T_{1j}(\alpha)$, сопряжённые ей подгруппы gAg^{-1}, где $g \in \mathrm{PSL}_n$, содержат вообще все трансвекции и порождают[1] PSL_n.

Упражнение 11.6. Убедитесь, что $T_{ij}(\alpha) = gT_{1j}(\alpha)g^{-1}$, где $g \in \mathrm{SL}_n$ переводит e_1 в e_i, а e_i в $-e_1$, оставляя все остальные базисные векторы на месте.

Мы заключаем, что произведения элементов вида gag^{-1}, $a \in A$, $g \in \mathrm{PSL}_n$ исчерпывают PSL_n.

Рассмотрим теперь отличную от единичной нормальную подгруппу $N \trianglelefteq \mathrm{PSL}_n$. Пространство $\mathbb{P}_{n-1}$ является дизъюнктным объединением орбит подгруппы N, и в силу нормальности N каждый элемент $g \in \mathrm{PSL}_n$ переводит N-орбиту точки x в N-орбиту точки gx, ибо

$$y = hx \iff gy = (ghg^{-1})gx\,.$$

Таким образом, группа PSL_n, с одной стороны, не может перевести пару точек, лежащих в одной N-орбите, в пару точек, лежащих в разных N-орбитах, а с другой стороны, действует 2-транзитивно по упр. 11.3 на стр. 189. Такое возможно, только если N-орбита всего одна, т. е. для любого $g \in \mathrm{PSL}_n$ существует такое $h \in N$, что $ge_1 = he_1$, откуда $h^{-1}g \in P$ и $g \in hP$. Мы заключаем, что $\mathrm{PSL}_n = NP = PN$. Поскольку сопряжение элементами из P оставляет подгруппу $A \lhd P$ на месте, каждый элемент из PSL_n является произведением элементов вида hah^{-1} с $a \in A$, $h \in N$ и в силу равенства $AN = NA$ лежит в AN. В прим. 10.23 на стр. 187 мы видели, что все группы SL_n за исключением двух, указанных в условии теоремы, совпадают со своими коммутантами. Но коммутатор элементов вида ah с $a \in A$, $h \in N$ в силу абелевости A и нормальности N лежит в N.

Упражнение 11.7. Убедитесь в этом.

Поэтому $\mathrm{PSL}_n = \mathrm{PSL}_n' = N$ во всех случаях, кроме двух исключительных. □

11.2. Композиционные факторы. Конечная строго убывающая последовательность подгрупп

$$G = G_0 \supsetneq G_1 \supsetneq G_2 \supsetneq \ldots \supsetneq G_{n-1} \supsetneq G_n = \{e\} \tag{11-3}$$

называется *композиционным рядом* или *рядом Жордана–Гёльдера* группы G, если при каждом i подгруппа G_{i+1} нормальна в G_i и фактор G_i/G_{i+1} прост. В этой ситуации неупорядоченный набор простых групп G_i/G_{i+1} (в котором возможны повторения) называется набором *композиционных факторов* (или *факторов Жордана–Гёльдера*) группы G и обозначается $\mathrm{CF}(G)$, а число $n = |\mathrm{CF}(G)|$ называется *длиной* композиционного ряда (11-3) или группы G и обозначается $\mathrm{length}(G)$. В теор. 11.3 на стр. 191 ниже мы покажем, что набор композиционных факторов не зависит от выбора композиционного ряда, и тем самым $\mathrm{CF}(G)$ и $\mathrm{length}(G)$ корректно определены.

[1] См. упр. 10.33 на стр. 187.

Пример 11.1 (композиционные факторы S_4)
Выше мы видели, что симметрическая группа S_4 имеет композиционный ряд

$$S_4 \rhd A_4 \rhd V_4 \rhd \mathbb{Z}/(2) \rhd \{e\}\,,$$

в котором $A_4 \lhd S_4$ — подгруппа чётных перестановок, $V_4 \lhd A_4$ — подгруппа Клейна, состоящая из тождественной перестановки и трёх перестановок циклового типа  , а

$$\mathbb{Z}/(2) \lhd V_4 \simeq \mathbb{Z}/(2) \times \mathbb{Z}/(2)$$

любая из трёх циклических подгрупп второго порядка, порождённых неединичными элементами. Таким образом, симметрическая группа S_4 имеет композиционные факторы $\mathbb{Z}/(2) = S_4/A_4$, $\mathbb{Z}/(3) = A_4/V_4$, $\mathbb{Z}/(2) = V_4/\big(\mathbb{Z}/(2)\big)$ и $\mathbb{Z}/(2) = \mathbb{Z}/(2)/\{e\}$.

Упражнение 11.8. Убедитесь, что $A_4/V_4 \simeq \mathbb{Z}/(3)$.

Теорема 11.3 (теорема Жордана – Гёльдера)
Если группа G имеет конечный композиционный ряд, то неупорядоченный набор $\mathrm{CF}(G)$ его факторов не зависит от выбора композиционного ряда. В частности, все ряды Жордана – Гёльдера имеют одинаковую длину $\mathrm{length}(G)$.

Доказательство. Пусть у группы G есть два композиционных ряда

$$G = P_0 \supsetneq P_1 \supsetneq P_2 \supsetneq \ldots \supsetneq P_{n-1} \supsetneq P_n = \{e\} \tag{11-4}$$

$$G = Q_0 \supsetneq Q_1 \supsetneq Q_2 \supsetneq \ldots \supsetneq Q_{m-1} \supsetneq Q_m = \{e\}\,. \tag{11-5}$$

Мы собираемся вставить между последовательными членами этих рядов дополнительные цепочки нестрого убывающих подгрупп так, чтобы получившиеся удлинённые ряды стали равной длины, и установить между их последовательными факторами биекцию, при которой соответствующие друг другу факторы будут изоморфны. Для этого заменим каждое звено $P_i \rhd P_{i+1}$ верхней цепочки (11-4) цепочкой

$$P_i \supseteq (Q_1 \cap P_i)P_{i+1} \supseteq (Q_2 \cap P_i)P_{i+1} \supseteq \ldots \supseteq (Q_{m-1} \cap P_i)P_{i+1} \supseteq P_{i+1}\,, \tag{11-6}$$

которая получается пересечением нижней цепочки (11-5) с подгруппой P_i и умножением всех полученных групп на нормальную в P_i подгруппу P_{i+1}. В предл. 10.5 на стр. 186 мы видели, что если подгруппа H нормализует подгруппу N, то $NH = HN$ тоже является подгруппой, причём $NH \rhd N$, $H \rhd (H \cap N)$ и $HN/N \simeq H/(H \cap N)$. Применяя это к подгруппам

$$H = Q_k \cap P_i \quad \text{и} \quad N = (Q_{k+1} \cap P_i)P_{i+1}\,,$$

мы получаем $HN = (Q_k \cap P_i)P_{i+1}$ и $H \cap N = (Q_{k+1} \cap P_i)(Q_k \cap P_{i+1})$.

Упражнение 11.9. Убедитесь, что H нормализует N, и проверьте последние два равенства.

Таким образом, $(Q_k \cap P_i)P_{i+1} \trianglerighteq (Q_{k+1} \cap P_i)P_{i+1}$ и

$$\frac{(Q_k \cap P_i)P_{i+1}}{(Q_{k+1} \cap P_i)P_{i+1}} \simeq \frac{(Q_k \cap P_i)}{(Q_{k+1} \cap P_i)(Q_k \cap P_{i+1})}\,. \tag{11-7}$$

Группа P_{i+1} является нормальной подгруппой во всех группах цепочки (11-6). Факторизуя по ней, получаем цепочку фактор групп

$$\frac{P_i}{P_{i+1}} \trianglerighteq \frac{(Q_1 \cap P_i)P_{i+1}}{P_{i+1}} \trianglerighteq \frac{(Q_2 \cap P_i)P_{i+1}}{P_{i+1}} \trianglerighteq \ldots \trianglerighteq \frac{(Q_{m-1} \cap P_i)P_{i+1}}{P_{i+1}} \trianglerighteq \{e\}\,, \tag{11-8}$$

в которой каждая подгруппа нормальна в предыдущей, а последовательные факторы

$$\frac{(Q_k \cap P_i)P_{i+1}/P_{i+1}}{(Q_{k+1} \cap P_i)P_{i+1}/P_{i+1}} \simeq \frac{(Q_k \cap P_i)P_{i+1}}{(Q_{k+1} \cap P_i)P_{i+1}} \simeq \frac{(Q_k \cap P_i)}{(Q_{k+1} \cap P_i)(Q_k \cap P_{i+1})}$$

совпадают с (11-7). Так как группа P_i/P_{i+1} проста, мы заключаем, что в цепочке (11-8) имеется ровно одно нестрогое включение, а все остальные включения — равенства. Тем самым, ровно один из факторов (11-7) отличен от единицы и изоморфен P_i/P_{i+1}.

Те же самые рассуждения с заменой P на Q позволяют вставить между последовательными группами $Q_k \rhd Q_{k+1}$ композиционного ряда (11-5) убывающую цепочку подгрупп

$$Q_k \supseteq (P_1 \cap Q_k)Q_{k+1} \supseteq (P_2 \cap Q_k)Q_{k+1} \supseteq \ldots \supseteq (P_{n-1} \cap Q_k)Q_{k+1} \supseteq Q_{k+1}\,, \tag{11-9}$$

каждая из которых нормальна в предыдущей, а последовательные факторы имеют вид

$$\frac{(P_i \cap Q_k)Q_{k+1}}{(P_{i+1} \cap Q_k)Q_{k+1}} \simeq \frac{(P_i \cap Q_k)}{(P_{i+1} \cap Q_k)(P_i \cap Q_{k+1})} \tag{11-10}$$

и изоморфны соответствующим факторам (11-7), поскольку

$$(P_{i+1} \cap Q_k)(P_i \cap Q_{k+1}) = (Q_{k+1} \cap P_i)(Q_k \cap P_{i+1})\,,$$

так как заключённые в скобки пересечения нормализуют друг друга. Таким образом, вставляя между последовательными элементами композиционного ряда (11-4) цепочки (11-6), а между последовательными элементами ряда (11-5) — цепочки (11-9), мы получим ряды одинаковой длины, в которых не все включения строгие, но факторы находятся в биективном соответствии, сопоставляющем друг другу изоморфные факторы (11-10) и (11-7). Поскольку Q_{k+1} является нормальной подгруппой всех групп цепочки (11-9), те же аргументы, что применялись выше к подгруппе P_{i+1} и цепочке (11-6), показывают, что при фиксированном k среди факторов (11-10) имеется ровно один отличный от единицы, и он изоморфен Q_k/Q_{k+1}. □

Замечание 11.1. Непростая группа может иметь несколько разных композиционных рядов с одинаковым набором факторов, а группы с одинаковыми наборами факторов Жордана-Гёльдера не обязательно изоморфны.

Предложение 11.1
Если группа G обладает конечным композиционным рядом, то любая её нормальная подгруппа $N \lhd G$ и факторгруппа G/N тоже обладают конечными композиционными рядами, причём $\mathrm{CF}(G) = \mathrm{CF}(N) \sqcup \mathrm{CF}(G/N)$. В частности, $\mathrm{length}(G) = \mathrm{length}(N) + \mathrm{length}(G/N)$.

Доказательство. Пересечение композиционного ряда группы G с подгруппой $N \lhd G$ имеет вид

$$N \supseteq G_1 \cap N \supseteq \ldots \supseteq G_{n-1} \cap N \supseteq \{e\}\,, \tag{11-11}$$

где $(G_i \cap N) \rhd (G_{i+1} \cap N)$, так как $G_i \rhd G_{i+1}$. Согласно предл. 10.5 на стр. 186,

$$\frac{G_i \cap N}{G_{i+1} \cap N} = \frac{G_i \cap N}{(G_i \cap N) \cap G_{i+1}} \simeq \frac{(G_i \cap N)G_{i+1}}{G_{i+1}}\,.$$

Поскольку $G_i \trianglerighteq (G_i \cap N)G_{i+1} \trianglerighteq G_{i+1}$ и фактор G_i/G_{i+1} прост, одно включение строгое, другое — равенство. Если $(G_i \cap N)G_{i+1} = G_i$, то $(G_i \cap N)/(G_{i+1} \cap N) \simeq G_i/G_{i+1}$. Если $(G_i \cap N)G_{i+1} = G_{i+1}$, то $G_i \cap N = G_{i+1} \cap N$. Таким образом, убирая из цепочки (11-11) все равенства, получаем ряд Жордана – Гёльдера, факторы которого содержатся среди композиционных факторов группы G. Аналогично, применяя к композиционному ряду группы G эпиморфизм $\pi\colon\ G \twoheadrightarrow G/N$, получаем цепочку $G/N \trianglerighteq \pi(G_1) \trianglerighteq \ldots \trianglerighteq \pi(G_{n-1}) \trianglerighteq \{e\}$, в которой

$$\frac{\pi(G_i)}{\pi(G_{i+1})} \simeq \frac{\pi^{-1}(\pi(G_i))}{\pi^{-1}(\pi(G_{i+1}))} = \frac{G_iN}{G_{i+1}N} \simeq \frac{G_i}{G_i \cap (G_{i+1}N)} = \frac{G_i}{G_{i+1}(G_i \cap N)} = \frac{G_i}{(G_i \cap N)G_{i+1}}$$

и возникает противоположная альтернатива: если $(G_i \cap N)G_{i+1} = G_i$, то $\pi(G_i) = \pi(G_{i+1})$, а если $(G_i \cap N)G_{i+1} = G_{i+1}$, то $\pi(G_i)/\pi(G_{i+1}) \simeq G_i/G_{i+1}$. Поэтому, убирая из цепочки равенства, получаем композиционный ряд для группы G/N, факторы которого суть композиционные факторы группы G, не вошедшие в набор композиционных факторов подгруппы $N \lhd G$. □

Предложение 11.2
Если нормальная подгруппа $N \lhd G$ и факторгруппа $Q = G/N$ имеют конечные длины, то группа G тоже имеет конечную длину, и $\mathrm{length}(G) = \mathrm{length}(N) + \mathrm{length}(Q)$, $\mathrm{CF}(G) = \mathrm{CF}(N) \sqcup \mathrm{CF}(Q)$.

Доказательство. Пусть группы N и Q имеют композиционные ряды

$$N \rhd N_1 \rhd \ldots \rhd N_{n-1} \rhd \{e\}$$
$$Q \rhd Q_1 \rhd \ldots \rhd Q_{m-1} \rhd \{e\}\,.$$

Обозначим через $P_i = \pi^{-1}(Q_i)$ полный прообраз группы Q_i при гомоморфизме факторизации $\pi\colon\ G \twoheadrightarrow Q$ с ядром N. Цепочка подгрупп

$$G \rhd P_1 \rhd \ldots \rhd P_{m-1} \rhd N_1 \rhd \ldots \rhd N_{n-1} \rhd \{e\}$$

является рядом Жордана – Гёльдера с требуемыми свойствами. □

Следствие 11.1
Каждая конечная группа обладает конечным композиционным рядом. □

Упражнение 11.10. Постройте композиционный ряд аддитивной группы $\mathbb{Z}/(p^n)$, где p — простое.

11.3. Полупрямые произведения. Для пары подгрупп N, H группы G отображение

$$N \times H \to NH\,, \quad (x,h) \mapsto xh\,,$$

биективно если и только если $N \cap H = \{e\}$. В самом деле, при $x_1h_1 = x_2h_2$ элемент

$$x_2^{-1}x_1 = h_2h_1^{-1} \in N \cap H\,,$$

и если $N \cap H = \{e\}$, то $x_2 = x_1$ и $h_2 = h_1$, а если в $N \cap H$ есть элемент $z \neq e$, то разные пары (e,e), $(z,z^{-1}) \in N \times H$ перейдут в один и тот же элемент $e \in NH$. Будем называть подгруппы $N, H \subset G$ *дополнительными*, если $N \cap H = \{e\}$ и $NH = G$. В этом случае группа G как множество находится в биекции с прямым произведением $N \times H$. Если подгруппа $N \lhd G$ при этом нормальна, то композиция элементов $g_1 = x_1 h_1$ и $g_2 = x_2 h_2$ может быть выражена в терминах пар (x_1, h_1), $(x_2, h_2) \in N \times H$. А именно, так как

$$g_1 g_2 = x_1 h_1 x_2 h_2 = x_1 (h_1 x_2 h_1^{-1}) \cdot h_1 h_2 \quad \text{и} \quad h_1 x_2 h_1^{-1} \in N\,,$$

группу G можно *описать* как множество $N \times H$ с операцией

$$(x_1, h_1) \cdot (x_2, h_2) = (x_1 \operatorname{Ad}_{h_1}(x_2), h_1 h_2)\,, \tag{11-12}$$

где через $\operatorname{Ad}_h : N \xrightarrow{\sim} N$, $x \mapsto hxh^{-1}$, обозначено присоединённое действие элемента h на нормальной подгруппе N. В этой ситуации говорят, что группа G является *полупрямым произведением* нормальной подгруппы $N \lhd G$ и дополнительной к ней подгруппы $H \subset G$ и пишут $G = N \rtimes H$. Если сопряжение элементами из подгруппы H действует на подгруппе N тривиально, что равносильно перестановочности $xh = xh$ любых двух элементов $x \in N$ и $h \in H$, то полупрямое произведение называется *прямым*. В этом случае $(x_1, h_1) \cdot (x_2, h_2) = (x_1 x_2, h_1 h_2)$ для всех пар (x_1, h_1), $(x_2, h_2) \in N \times H$.

Пример 11.2 ($D_n = \mathbb{Z}/(n) \rtimes \mathbb{Z}/(2)$)
Группа диэдра D_n содержит нормальную подгруппу поворотов, изоморфную аддитивной группе $\mathbb{Z}/(n)$. Подгруппа второго порядка, порождённая любым отражением, дополнительна к группе поворотов и изоморфна аддитивной группе $\mathbb{Z}/(2)$. Присоединённое действие отражения на группе поворотов меняет знак у угла поворота. При отождествлении группы поворотов с $\mathbb{Z}/(n)$ это действие превращается в умножение на -1. Таким образом, $D_n = \mathbb{Z}/(n) \rtimes \mathbb{Z}/(2)$ и в терминах пар $(x,y) \in \mathbb{Z}/(n) \times \mathbb{Z}/(2)$ композиция на группе диэдра задаётся правилом

$$\big(x_1, y_1\big) \cdot \big(x_2, y_2\big) = \big(x_1 + (-1)^{y_1} x_2, y_1 + y_2\big)\,, \quad x_1, x_2 \in \mathbb{Z}/(n)\,, \quad y_1, y_2 \in \mathbb{Z}/(2)\,.$$

Пример 11.3 ($\operatorname{Aff}(V) = V \rtimes \operatorname{GL}(V)$, продолжение прим. 10.20 на стр. 184)
Аффинная группа[1] $\operatorname{Aff}(V)$ содержит нормальную подгруппу параллельных переносов, которая изоморфна аддитивной группе векторного пространства V и является ядром сюръективного гомоморфизма групп

$$D :\ \operatorname{Aff}(V) \twoheadrightarrow \operatorname{GL}(V)\,, \quad \varphi \mapsto D_\varphi\,, \tag{11-13}$$

сопоставляющего аффинному преобразованию $\varphi :\ \mathbb{A}(V) \to \mathbb{A}(V)$ его дифференциал

$$D_\varphi :\ V \to V\,, \quad \overrightarrow{pq} \mapsto \overrightarrow{\varphi(p)\varphi(q)}\,.$$

Если зафиксировать в $\mathbb{A}(V)$ какую-нибудь точку p, то ограничение гомоморфизма (11-13) на стабилизатор $\operatorname{Stab}_p \subset \operatorname{Aff}(V)$ задаст изоморфизм $D_p :\ \operatorname{Stab}_p \xrightarrow{\sim} \operatorname{GL}(V)$. Обратный изоморфизм сопоставляет линейному оператору $f :\ V \xrightarrow{\sim} V$ аффинное преобразование

$$\varphi_f :\ \mathbb{A}(V) \to \mathbb{A}(V)\,, \quad x \mapsto p + f(\overrightarrow{px})\,,$$

оставляющее на месте точку p. Поскольку каждое преобразование $\varphi \in \operatorname{Aff}(V)$ раскладывается в композицию $\varphi = \tau_v \circ (\tau_{-v} \circ \varphi)$ параллельного переноса τ_v на вектор $v = \overrightarrow{p\varphi(p)}$ и преобразования $\tau_{-v} \circ \varphi \in \operatorname{Stab}(p)$, группа $\operatorname{Aff}(V) = V \rtimes \operatorname{Stab}_p \simeq V \rtimes \operatorname{GL}(V)$. Согласно прим. 10.20 на стр. 184, композиция в группе $V \rtimes \operatorname{GL}(V)$ задаётся правилом $(u, f) \cdot (w, g) = (u + f(w),\ fg)$.

[1] См. прим. 10.20 на стр. 184.

11.3.1. Полупрямое произведение групп. Предыдущую конструкцию можно применить к двум абстрактным группам N и H как только задано действие группы H на группе N, т. е. гомоморфизм группы H в группу автоморфизмов группы N:

$$\psi\colon H \to \operatorname{Aut} N\,, \quad h \mapsto \psi_h\colon N \xrightarrow{\sim} N\,, \tag{11-14}$$

По аналогии с форм. (11-12) на стр. 194 зададим на множестве $N \times H$ операцию правилом

$$(x_1, h_1)\cdot(x_2, h_2) \stackrel{\text{def}}{=} (x_1\psi_{h_1}(x_2), h_1h_2)\,. \tag{11-15}$$

Упражнение 11.11. Проверьте, что формула (11-15) задаёт на $N \times H$ структуру группы с единицей (e, e) и обращением $(x, h)^{-1} = \left(\psi_h^{-1}(x^{-1}), h^{-1}\right)$, где $\psi_h^{-1} = \psi_{h^{-1}}$ — автоморфизм, обратный к $\psi_h : N \xrightarrow{\sim} N$.

Полученная таким образом группа называется *полупрямым произведением* групп N и H по действию $\psi\colon H \to \operatorname{Aut} N$ и обозначается $N \rtimes_\psi H$. Подчеркнём, что результат зависит от выбора действия ψ. Если действие тривиально, т. е. $\psi_h = \mathrm{Id}_N$ для всех $h \in H$, мы получаем прямое произведение $N \times H$ с покомпонентными операциями.

Упражнение 11.12. Убедитесь, что подмножество $N' \stackrel{\text{def}}{=} \{(x, e) \mid x \in N\}$ является изоморфной группе N нормальной подгруппой в $G = N \rtimes_\psi H$ и фактор $G/N' \simeq H$, а подмножество $H' \stackrel{\text{def}}{=} \{(e, h) \mid h \in H\}$ является изоморфной H и дополнительной к N' подгруппой в G, причём $G = N' \rtimes H'$ является полупрямым произведением своих подгрупп N' и H'.

Предложение 11.3
Для любых гомоморфизма $\psi\colon H \to \mathrm{Aut}(N)$, $h \mapsto \psi_h$, и автоморфизмов $\alpha\colon H \xrightarrow{\sim} H$ и $\beta\colon N \xrightarrow{\sim} N$ отображения $(n, h) \mapsto (n, \alpha^{-1}h)$ и $(n, h) \mapsto (\beta n, h)$ задают изоморфизмы полупрямых произведений $N \rtimes_\psi H \xrightarrow{\sim} N \rtimes_{\psi\circ\alpha} H$ и $N \rtimes_\psi H \xrightarrow{\sim} N \rtimes_{\mathrm{Ad}_\beta(\psi)} H$, где $\mathrm{Ad}_\beta(\psi)\colon H \to \mathrm{Aut}(N)$, $h \mapsto \beta\psi_h\beta^{-1}$.

Доказательство. Отображение $(n, h) \mapsto (n, \alpha^{-1}h)$ переводит сомножители из левой части равенства $(n_1, h_1)(n_2, h_2) = (n_1\psi_{h_1}n_2, h_1h_2)$ в $(n_1, \alpha^{-1}h_1)$ и $(n_2, \alpha^{-1}h_2)$, произведение которых в $N \rtimes_{\psi\circ\alpha} H$ равно $(n_1\psi_{h_1}n_2, \alpha^{-1}(h_1h_2))$. Отображение $(n, h) \mapsto (\beta n, h)$ переводит те же самые сомножители в $(\beta n_1, h_1)$ и $(\beta n_2, h_2)$. Их произведение в $N \rtimes_{\mathrm{Ad}_\beta(\psi)} H$ равно $(\beta(n_1\psi_{h_1}n_2), h_1h_2)$. □

Пример 11.4 (голоморф)
Группа автоморфизмов $\mathrm{Aut}\, G$ произвольной группы G тавтологически действует на G. Полупрямое произведение $\mathrm{Hol}\, G \stackrel{\text{def}}{=} G \rtimes \mathrm{Aut}\, G$ по этому действию называется *голоморфом* группы G. Вложение $G \hookrightarrow \mathrm{Hol}\, G$ замечательно тем, что любой автоморфизм группы G является сужением на G внутреннего автоморфизма объемлющей группы $\mathrm{Hol}\, G$.

Пример 11.5 (сплетение)
Для любых двух групп H, N множество N^H всех функций $f\colon H \to N$ имеет естественную структуры группы, в которой $f_1f_2\colon H \to N$, $x \mapsto f_1(x)f_2(x)$. Эту группу можно воспринимать как прямое произведение одинаковых копий группы N, занумерованных элементами[1] $x \in H$. Группа H действует на N^H по следующему правилу: элемент $h \in H$ переводит функцию $f\colon H \to N$ в функцию $hf\colon x \mapsto f(xh)$.

Упражнение 11.13. Убедитесь, что $h(f_1f_2) = (hf_1)(hf_2)$ и $(h_1h_2)f = h_1(h_2f)$.

[1] Ср. с n° 1.6 на стр. 34.

Полупрямое произведение $N \wr H \stackrel{\text{def}}{=} N^H \rtimes H$ по этому действию называется *сплетением*[1] группы N с группой H. Сплетение замечательно тем, что любая группа G с нормальной подгруппой $N \lhd G$ и фактор группой $H = G/N$ допускает гомоморфное *вложение Фробениуса* $\varphi : G \hookrightarrow N \wr H$. Чтобы задать его, зафиксируем какое-нибудь теоретико множественное сечение $\sigma : H \hookrightarrow G$ гомоморфизма факторизации $\pi : G \twoheadrightarrow H = G/N$, выбирающее в каждом классе $h \in G/N$ некоторый представитель $\sigma(h) \in G$. Тогда для любых $g \in G$ и $h \in H$ элемент $\sigma(h)g\sigma(h\pi(g))^{-1} \in N$, поскольку $\pi(\sigma(h)g\sigma(h\pi(g))^{-1}) = h\pi(g)(h\pi(g))^{-1} = e$. Рассмотрим функцию

$$\sigma_g : H \to N, \quad h \mapsto \sigma(h)g\sigma(h\pi(g))^{-1},$$

как элемент группы N^H и положим $\varphi_\sigma(g) = (\sigma_g, \pi(g)) \in N^H \rtimes H$.

Упражнение 11.14. Убедитесь, что $\varphi_\sigma(g_1g_2) = \varphi_\sigma(g_1)\varphi_\sigma(g_2)$ в $N^H \rtimes H$ и что образы двух вложений $\varphi_\sigma, \varphi_\tau : G \hookrightarrow N \wr H$, построенных при помощи разных сечений $\sigma, \tau : H \hookrightarrow G$, сопряжены в группе $N \wr H$.

11.4. p-группы и теоремы Силова. Группа порядка p^n, где $p \in \mathbb{N}$ — простое, называется *p-группой*. Поскольку все нетривиальные 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 11.4
Пусть p-группа G действует на конечном множестве X, число элементов в котором не делится на p. Тогда G имеет на X неподвижную точку. □

Предложение 11.5
Любая p-группа имеет нетривиальный центр.

Доказательство. Рассмотрим присоединённое действие группы на себе. Центр группы является множеством одноточечных орбит этого действия. Так как число элементов в группе и длины всех неодноточечных орбит делятся на p, одноточечные орбиты не могут исчерпываться одной орбитой элемента e. □

Упражнение 11.15. Покажите, что любая группа G порядка p^2, где p простое, абелева.

Определение 11.1 (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 $S \subset G$ порядка $|S| = p^n$ называется *силовской p-подгруппой* в G. Количество силовских p-подгрупп в G обозначается через $N_p(G)$.

Теорема 11.4 (теорема Силова)
Для любого простого $p \mid |G|$ силовские p-подгруппы в G существуют. Все они сопряжены друг другу, и любая p-подгруппа в G содержится в некоторой силовской p-подгруппе.

Доказательство (Ж.–П. Серр). Пусть $|G| = p^n m$ и $p \nmid m$. Обозначим через $\mathcal{E}$ множество p^n-элементных подмножеств в G и рассмотрим действие G на $\mathcal{E}$, индуцированное левым регулярным действием G на себе. Стабилизатор точки $F \in \mathcal{E}$ состоит из всех элементов $g \in G$, левое

[1] По английски *wreath product*.

умножение на которые переводит множество $F \subset G$ в себя: $\mathrm{Stab}(F) = \{g \in G \mid gF \subset F\}$. Так как $gx = x$ в группе G только при $g = e$, группа $\mathrm{Stab}(F)$ свободно действует на множестве F и все орбиты этого действия состоят из $|\mathrm{Stab}(F)|$ точек. Поэтому $|F| = p^n$ делится на $|\mathrm{Stab}(F)|$, откуда $|\mathrm{Stab}(F)| = p^k$, и имеется следующая альтернатива: либо $k < n$, и в этом случае длина G-орбиты элемента $F \in \mathcal{E}$ делится на p, либо $k = n$, и в этом случае подгруппа $\mathrm{Stab}(F) \subset G$ силовская, а G-орбита элемента $F \in \mathcal{E}$ состоит из m элементов. Во втором случае по предл. 11.4 каждая p-подгруппа $H \subset G$ (в частности, каждая силовская подгруппа), имеет на G-орбите элемента F неподвижную точку gF, а значит, содержится в силовской подгруппе $\mathrm{Stab}(gF) = g\,\mathrm{Stab}(F)\,g^{-1}$, сопряжённой к $\mathrm{Stab}(F)$, и совпадает с ней, если H силовская. Таким образом, для доказательства теоремы остаётся убедиться, что в множестве $\mathcal{E}$ есть G-орбита, длина которой не делится на p. Это следует из лем. 11.1 ниже. □

Лемма 11.1
$|\mathcal{E}| = \binom{p^n m}{p^n} \equiv m \pmod p$ не делится на p.

Доказательство. Класс вычетов $\binom{p^n m}{p^n} \pmod p$ равен коэффициенту при x^{p^n}, возникающему при раскрытии бинома $(1+x)^{p^n m}$ над полем $\mathbb{F}_p = \mathbb{Z}/(p)$. Так как над $\mathbb{F}_p$ возведение в p-тую степень является аддитивным гомоморфизмом, $(1+x)^{p^n} = 1 + x^{p^n}$, откуда $(1+x)^{p^n m} = \left(1 + x^{p^n}\right)^m = 1 + mx^{p^n} +$ старшие степени. □

Следствие 11.2 (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 $\mathcal{S}$ и рассмотрим действие G на $\mathcal{S}$, индуцированное присоединённым действием G на себе. По теореме Силова это действие транзитивно, откуда $|\mathcal{S}| = |G|/|\mathrm{Stab}(P)|$, где $P \in \mathcal{S}$ — произвольно взятая силовская p-подгруппа. Поскольку $P \subset \mathrm{Stab}(P)$, порядок $|\mathrm{Stab}(P)|$ делится на $|P| = p^n$, а значит $|\mathcal{S}|$ делит $|G|/p^n = m$, что доказывает первое утверждение.

Для доказательства второго утверждения достаточно проверить, что P, действуя сопряжениями на $\mathcal{S}$, имеет там ровно одну неподвижную точку, а именно, саму себя. Тогда порядки всех остальных P-орбит будут делиться на p, и мы получим $|\mathcal{S}| \equiv 1 \pmod p$.

Пусть силовская подгруппа $H \in \mathcal{S}$ неподвижна при сопряжении подгруппой P. Это означает, что $P \subset \mathrm{Stab}(H) = \{g \in G \mid gHg^{-1} \subset H\}$ и $|\mathrm{Stab}(H)| = p^n m'$, где $m' | m$ взаимно просто с p. Так как $H \subset \mathrm{Stab}(H)$, подгруппы P и H являются силовскими в $\mathrm{Stab}(H)$. Поскольку H нормальна в $\mathrm{Stab}(H)$, и все силовские подгруппы сопряжены, мы заключаем, что $H = P$. □

Пример 11.6 (группы порядка pq с простыми $p > q$)
Пусть $|G| = pq$, где $p > q$ простые. Тогда в G есть ровно одна, автоматически нормальная силовская p-подгруппа $H_p \simeq \mathbb{Z}/(p)$. Рассмотрим любую силовскую q-подгруппу $H_q \simeq \mathbb{Z}/(q)$. Поскольку H_p и H_q просты, $H_p \cap H_q = e$ и $G = H_p H_q$. Согласно n° 11.3 $G = \mathbb{Z}/(p) \rtimes_\psi \mathbb{Z}/(q)$ для некоторого гомоморфизма $\psi : \mathbb{Z}/(q) \to \mathrm{Aut}(\mathbb{Z}/(p))$.

Упражнение 11.16. Убедитесь, что $\mathrm{Aut}(\mathbb{Z}/(p)) \simeq \mathbb{F}_p^\times \simeq \mathbb{Z}/(p-1)$.

Гомоморфизм $\psi : \mathbb{Z}/(q) \to \mathrm{Aut}(\mathbb{Z}/(p)) \simeq \mathbb{F}_p^\times$ однозначно задаётся своим значением на образующей $[1]_q$, которая является элементом порядка q. Поэтому элемент $\eta = \psi([1]_q) \in \boldsymbol{\mu}_q(\mathbb{F}_p) \subset \mathbb{F}_p^\times$

является корнем q-й степени из 1 в поле $\mathbb{F}_p$. По упр. 11.4 на стр. 189 группа $\boldsymbol{\mu}_q(\mathbb{F}_p)$ циклическая порядка нод$(q, p-1)$. Мы заключаем, что если $q \nmid (p-1)$, то всякий гомоморфизм $\mathbb{Z}/(q) \to \mathrm{Aut}(\mathbb{Z}/(p))$ тривиален и, стало быть, единственной группой порядка pq в этом случае является $\mathbb{Z}/(p) \times \mathbb{Z}/(q)$. Если же $q \mid (p-1)$, то существует нетривиальный гомоморфизм

$$\psi : \ \to \mathrm{Aut}(\mathbb{Z}/(p)), \quad [1]_q \mapsto \eta, \tag{11-16}$$

где $\eta \in \mathbb{F}_p^\times$ порождает мультипликативную группу $\boldsymbol{\mu}_q(\mathbb{F}_p)$. Гомоморфизм (11-16) сопоставляет каждому элементу $[y]_q \in \mathbb{Z}/(q)$ автоморфизм $\psi_y : \mathbb{Z}/(p) \xrightarrow{\sim} \mathbb{Z}/(p)$, $[x]_p \mapsto [\eta^y x]_p$, и задаёт полупрямое произведение $\mathbb{Z}/(p) \rtimes_\psi \mathbb{Z}/(q)$ с операцией

$$\big([x_1]_p, [y_1]_q\big) \cdot \big([x_2]_p, [y_2]_q\big) = \big([x_1 + \eta^{y_1} x_2]_p, [y_1 + y_2]_q\big). \tag{11-17}$$

Любой другой нетривиальный гомоморфизм $\mathbb{Z}/(q) \to \mathrm{Aut}(\mathbb{Z}/(p))$ имеет вид $\psi^m : [1]_q \mapsto \eta^m$, где $1 \leqslant m \leqslant q-1$, и является композицией гомоморфизма (11-16) с автоморфизмом умножения на $m : \mathbb{Z}/(q) \xrightarrow{\sim} \mathbb{Z}/(q)$, $[y]_q \mapsto [my]_q$. По предл. 11.3 на стр. 195 задаваемое им полупрямое произведение $\mathbb{Z}/(p) \rtimes_{\psi\circ m} \mathbb{Z}/(q) \simeq \mathbb{Z}/(p) \rtimes_\psi \mathbb{Z}/(q)$. Мы заключаем, что при $q \mid (p-1)$ кроме абелевой группы $\mathbb{Z}/(p) \times \mathbb{Z}/(q)$ существует единственная с точностью до изоморфизма неабелева группа порядка pq. Она изоморфна $\mathbb{Z}/(p) \rtimes \mathbb{Z}/(q)$ с операцией (11-17). В частности, для простого $p > 2$ единственной с точностью до изоморфизма неабелевой группой порядка $2p$ является группа диэдра[1] D_p.

[1] См. прим. 11.2 на стр. 194.

§12. Задание групп образующими и соотношениями

12.1. Свободные группы и соотношения. С любым множеством M можно связать группу F_M, которая называется *свободной группой*, порождённой множеством M. Она состоит из классов эквивалентных слов, которые можно написать буквами x и x^{-1}, где $x \in M$, по наименьшему отношению эквивалентности, отождествляющему между собою слова, отличающиеся друг от друга вставкой или удалением[1] двубуквенного фрагмента xx^{-1} или $x^{-1}x$. Композиция определяется как приписывание одного слова к другому. Единицей служит класс пустого слова. Обратным к классу слова $w = x_1 \dots x_m$ является класс слова $w^{-1} = x_m^{-1} \dots x_1^{-1}$, где каждая из букв x_i равна x или x^{-1} для некоторого $x \in M$, и $\left(x^{-1}\right)^{-1} \stackrel{\text{def}}{=} x$.

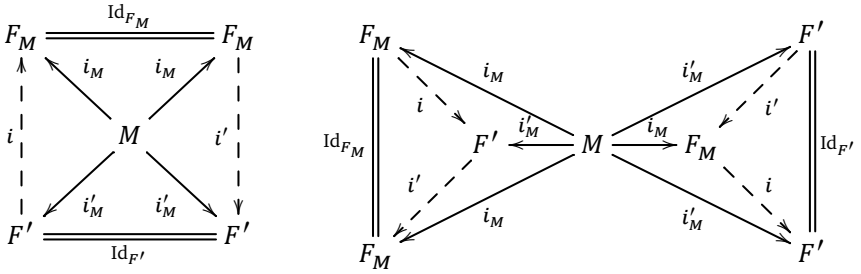
Упражнение 12.1. Убедитесь, что композиция корректно определена на классах эквивалентности слов и что в каждом классе содержится ровно одно *несократимое*[2] слово, которое одновременно является и самым коротким словом в своём классе.

Элементы множества M называются *образующими* свободной группы F_M. Свободная группа с k образующими обозначается F_k. Группа $F_1 \simeq \mathbb{Z}$ — это циклическая группа бесконечного порядка. Группа F_2 классов слов на четырёхбуквенном алфавите x, y, x^{-1}, y^{-1} уже трудно обозрима.

Упражнение 12.2. Постройте инъективный гомоморфизм групп $F_{\mathbb{N}} \hookrightarrow F_2$.

Предложение 12.1 (универсальное свойство свободных групп)
Отображение $i_M : M \to F_M$, переводящее элемент $x \in M$ в класс однобуквенного слова $x \in F_M$, обладает следующим универсальным свойством: для любых группы G и отображения множеств $\varphi_M : M \to G$ существует единственный такой гомоморфизм групп $\varphi : F_M \to G$, что $\varphi_M = \varphi \circ i_M$. Для любого обладающего этим свойством отображения $i'_M : M \to F'$ множества M в группу F' имеется единственный такой изоморфизм групп $i' : F_M \xrightarrow{\sim} F'$, что $i'_M = i' \circ i_M$.

Доказательство. Гомоморфизм φ единствен, так как обязан переводить слово $x_1^{\varepsilon_1} \dots x_m^{\varepsilon_m} \in F_M$, где $x_\nu \in M$, $\varepsilon_\nu = \pm 1$, в произведение $\varphi_M(x_1)^{\varepsilon_1} \dots \varphi_M(x_m)^{\varepsilon_m} \in G$. С другой стороны, это правило корректно задаёт гомоморфизм групп, что доказывает первое утверждение. Если отображение $i' : M \to F'$ множества M в группу F' обладает универсальным свойством из предл. 12.1, то существуют единственные гомоморфизмы $i' : F_M \to F'$ и $i : F' \to F_M$, встраивающиеся в коммутативные диаграммы



Разложения вида $i_M = \varphi \circ i_M$, $i'_M = \psi \circ i'_M$ в силу их единственности возможны только с $\varphi = \mathrm{Id}_{F_M}$, $\psi = \mathrm{Id}_{F'}$. Поэтому $i' \circ i = \mathrm{Id}_{F'}$, $i \circ i' = \mathrm{Id}_{F_M}$. □

[1] В начале, в конце, или же между произвольными двумя последовательными буквами слова.
[2] Т. е. не содержащее двубуквенных фрагментов xx^{-1} и $x^{-1}x$.

12.1.1. Задание групп образующими и соотношениями. Если гомоморфизм групп

$$\varphi : F_M \twoheadrightarrow G\,, \tag{12-1}$$

заданный отображением $\varphi_M : M \to G$ множества M в группу G, является *сюръективным*, то говорят, что группа G *порождается* элементами $g_m = \varphi_M(m)$, $m \in M$, а сами элементы g_m называются *образующими* группы G. В этом случае G исчерпывается всевозможными произведениями $g_1^{\varepsilon_1}\dots g_k^{\varepsilon_k}$, $\varepsilon = \pm 1$, образующих и обратных к ним элементов. Группа G называется *конечно порождённой*, если она допускает конечное множество образующих. Ядро $\ker\varphi \lhd F_M$ эпиморфизма (12-1) называется *группой соотношений* между образующими g_m. Набор слов $R \subset \ker\varphi$ называется набором *определяющих соотношений*, если $\ker\varphi$ — это наименьшая нормальная подгруппа в F_M, содержащая R. Это означает, что любое соотношение можно получить из слов множества R конечным числом умножений, обращений и сопряжений произвольными элементами из свободной группы F_M. Группа, допускающая конечное число образующих с конечным набором определяющих соотношений называется *конечно определённой*.

Всякую группу можно задать образующими и соотношениями, например, взяв в качестве M множество всех элементов группы. Удачный выбор образующих с простыми определяющими соотношениями может значительно прояснить устройство группы и её гомоморфизмов в другие группы. Однако в общем случае выяснить, изоморфны ли две группы, заданные своими образующими и определяющими соотношениями, или отлична ли группа, заданная образующими и соотношениями, от тривиальной группы $\{e\}$, может оказаться очень непросто. Более того, обе эти задачи являются *алгоритмически неразрешимыми*[1] даже в классе конечно определённых групп.

Предложение 12.2
Пусть группа G_1 задана множеством образующих M и набором определяющих соотношений R, а G_2 — произвольная группа. Отображение $\varphi : M \to G_2$ тогда и только тогда корректно задаёт гомоморфизм групп $G_1 \to G_2$ правилом $x_1^{\varepsilon_1}\dots x_m^{\varepsilon_m} \mapsto \varphi(x_1)^{\varepsilon_1}\dots\varphi(x_m)^{\varepsilon_m}$, когда для каждого слова $y_1^{\varepsilon_1}\dots y_m^{\varepsilon_m} \in R$ в группе G_2 выполняется соотношение $\varphi(y_1)^{\varepsilon_1}\dots\varphi(y_m)^{\varepsilon_m} = 1$.

Доказательство. Отображения множеств $\varphi_M : M \to G_2$ биективно соответствуют гомоморфизмам групп $\varphi : F_M \to G_2$. Такой гомоморфизм φ факторизуется до гомоморфизма из группы $G_1 = F_M/N_R$, где $N_R \lhd F_M$ — наименьшая нормальная подгруппа, содержащая R, тогда и только тогда, когда $N_R \subset \ker\psi$. Так как $\ker\psi \lhd F_M$, для этого необходимио и достаточно включения $R \subset \ker\psi$. □

Пример 12.1 (образующие и соотношения группы диэдра)
Покажем, что группа диэдра D_n задаётся двумя образующими x_1, x_2 и соотношениями

$$x_1^2 = x_2^2 = (x_1x_2)^n = e\,. \tag{12-2}$$

Оси симметрии правильного n-угольника разбивают его на $2n$ конгруэнтных прямоугольных треугольников как на рис. 12⋄1 ниже. Обозначим один из них через e. Поскольку любое движение плоскости однозначно задаётся своим действием на треугольник e, треугольники разбиения находятся в биекции с движениями $g \in D_n$, и каждый из них можно однозначно пометить

[1] В формальном смысле, принятом в математической логике.

тем единственным преобразованием g, которое переводит треугольник e в этот треугольник. При этом каждое преобразование $h \in D_n$ переводит каждый треугольник g в треугольник hg.

Упражнение 12.3. Для любого движения F евклидова пространства $\mathbb{R}^n$ и отражения σ_π в произвольной гиперплоскости $\pi \subset \mathbb{R}^n$ докажите соотношения

$$\sigma_{F(\pi)} = F \circ \sigma_\pi \circ F^{-1} \quad \text{и} \quad \sigma_{F(\pi)} \circ F = F \circ \sigma_\pi \,. \tag{12-3}$$

Обозначим через ℓ_1 и ℓ_2 боковые стороны треугольника e, а отражения плоскости в этих сторонах обозначим через $\sigma_1 = \sigma_{\ell_1}$ и $\sigma_2 = \sigma_{\ell_2}$. Тогда по второму из равенств (12-3) треугольники, получающиеся из e последовательными отражениями в направлении часовой стрелки пометятся элементами

$$\begin{aligned}
\sigma_{\ell_1} &= \sigma_1\,,\\
\sigma_{\sigma_1(\ell_2)}\sigma_1 &= \sigma_1\sigma_2\,,\\
\sigma_{\sigma_1\sigma_2(\ell_1)}\sigma_1\sigma_2 &= \sigma_1\sigma_2\sigma_1\,,\\
\sigma_{\sigma_1\sigma_2\sigma_1(\ell_2)}\sigma_1\sigma_2\sigma_1 &= \sigma_1\sigma_2\sigma_1\sigma_2\,,\ \ldots
\end{aligned}$$

а треугольники, получающиеся из e последовательными отражениями против часовой стрелки пометятся элементами

$$\begin{aligned}
\sigma_{\ell_2} &= \sigma_2\,,\\
\sigma_{\sigma_2(\ell_1)}\sigma_2 &= \sigma_2\sigma_1\,,\\
\sigma_{\sigma_2\sigma_1(\ell_2)}\sigma_2\sigma_1 &= \sigma_2\sigma_1\sigma_2\,,\\
\sigma_{\sigma_2\sigma_1\sigma_2(\ell_1)}\sigma_2\sigma_1\sigma_2 &= \sigma_2\sigma_1\sigma_2\sigma_1\,,\ \ldots
\end{aligned}$$

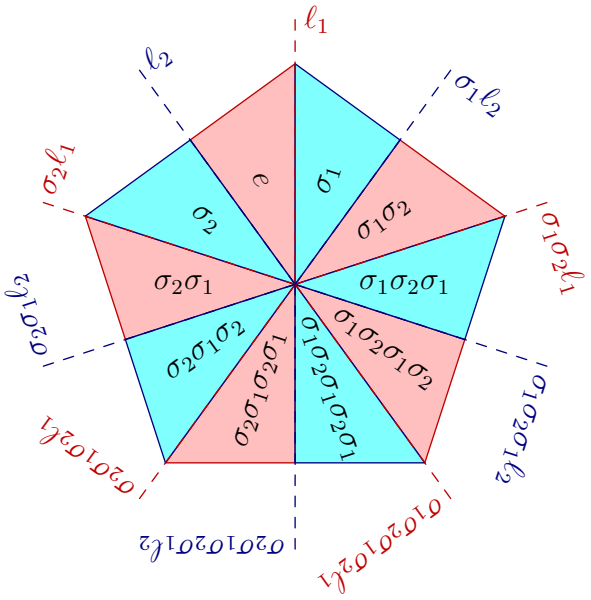


Рис. 12◇1. Образующие группы диэдра.

В результате каждый треугольник пометится словом вида $\sigma_1\sigma_2\sigma_1\sigma_2\ldots$ или $\sigma_2\sigma_1\sigma_2\sigma_1\ldots$ Так как композиция $\sigma_1 \circ \sigma_2$ является поворотом на угол $2\pi/n$, в группе D_n выполняются соотношения

$$\sigma_1^2 = \sigma_2^2 = (\sigma_1\sigma_2)^n = e\,, \tag{12-4}$$

и правило $x_1 \mapsto \sigma_1$, $x_2 \mapsto \sigma_2$ корректно задаёт сюръективный гомоморфизм $\varphi\colon F_2/H \twoheadrightarrow D_n$ из фактора свободной группы F_2 с образующими x_1, x_2 по наименьшей нормальной подгруппе $H \lhd F_2$, содержащей слова x_1^2, x_2^2 и $(x_1x_2)^n$. Покажем, что он инъективен. Поскольку последнее соотношение в (12-2) равносильно равенству

$$\underbrace{\sigma_1\sigma_2\sigma_1\ldots}_{k} = \underbrace{\sigma_2\sigma_1\sigma_2\ldots}_{2n-k}\,, \tag{12-5}$$

каждое слово в алфавите $\{x_1, x_2, x_1^{-1}, x_2^{-1}\}$ записывается по модулю соотношений (12-2) словом

$$x_1x_2x_1\ldots \quad \text{или} \quad x_2x_1x_2\ldots \tag{12-6}$$

из не более n букв, причём два n-буквенных слова равны друг другу в F_2/H. Согласно предыдущему, все эти слова переводятся гомоморфизмом φ в разные треугольники, т. е. в разные элементы $g \in D_n$. Мы заключаем, что гомоморфизм $\varphi : F_2/H \xrightarrow{\sim} D_n$ биективен, а все слова (12-6), за исключением двух равных n-буквенных слов, различны по модулю H и являются самими короткими выражениями элементов группы D_n через образующие σ_1, σ_2.

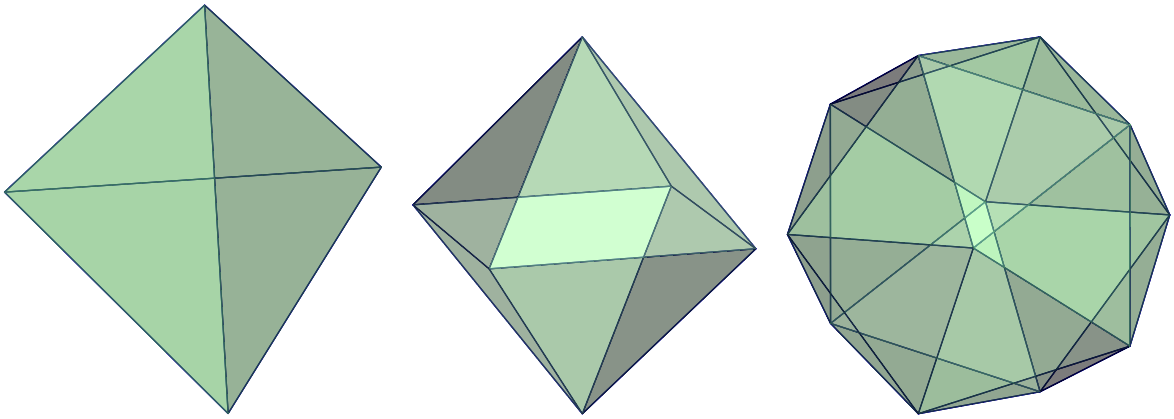


Рис. 12◇2. Тетраэдр, октаэдр и икосаэдр.

12.2. Пример: группы платоновых тел. Обозначим через M платоново тело с треугольными гранями, т. е. правильный *тетраэдр*, *октаэдр* или *икосаэдр*, см. рис. 12◇2. Плоскости симметрии многогранника M задают *барицентрическое разбиение* каждой грани на 6 конгруэнтных друг другу треугольников с вершинами в центре грани, в середине ребра этой грани и в одном из концов этого ребра, см. рис. 12◇3. Обозначим, соответственно, через π_1, π_2, π_3 плоскости симметрии, высекающие противолежащие этим вершинам стороны в одном из треугольников, который пометим единичным элементом e группы O_M многогранника M. Двугранный угол между плоскостями π_i и π_j обозначим через

$$\pi/m_k = \measuredangle(\pi_i, \pi_j), \quad \text{где} \quad k = \{1,2,3\} \smallsetminus \{i,j\}.$$

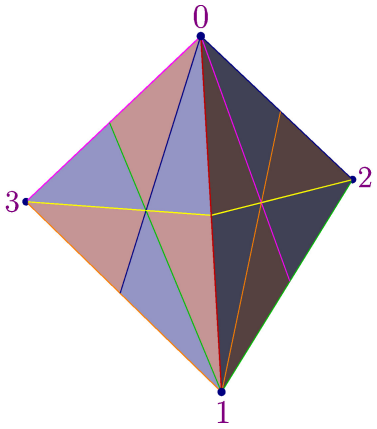


Рис. 12◇3. Барицентрическое разбиение тетраэдра плоскостями симметрии.

Числа m_i, а также число γ граней многогранника M и общее число треугольников $N = 6\gamma$ представлены в таблице[1]:

M	m_1	m_2	m_3	γ	N
тетраэдр	3	2	3	4	24
октаэдр	3	2	4	8	48
икосаэдр	3	2	5	20	120.

Обозначим через σ_i отражение в плоскости π_i. Так как каждое преобразование из группы O_M однозначно определяется своим действием на тройку векторов с концами в вершинах треугольника e, каждый треугольник триангуляции является образом треугольника e под действием единственного преобразования $g \in O_M$. Надпишем каждый треугольник этим преобразованием g,

[1] Обратите внимание, что помещённый в пространство n-угольный диэдр из прим. 12.1 тоже можно включить в этот список со значениями $m_1 = n$, $m_2 = 2$, $m_3 = 2$, $\gamma = 2$ и $N = 4n$, если условиться, что плоский диэдр имеет две двумерные грани: «верхнюю» и «нижнюю».

и пометим его стороны, высекаемые плоскостями $g(\pi_1)$, $g(\pi_2)$, $g(\pi_3)$ соответствующими номерами 1, 2, 3. Отметим, что каждое преобразование $h \in \mathrm{O}_M$ переводит каждый треугольник g в треугольник hg. На рис. 12⋄4 изображена стереографическая проекция картинки, которую 24 трёхгранных угла барицентрического разбиения тетраэдра с рис. 12⋄3 высекают на описанной около этого тетраэдра сфере. На каждом сферическом треугольнике написана композиция отражений $\sigma_1, \sigma_2, \sigma_3$, переводящая треугольник e в этот треугольник. Стороны треугольников, помеченные номерами 1, 2 и 3, изображены на рисунке в красным, зелёным и жёлтым цветом.

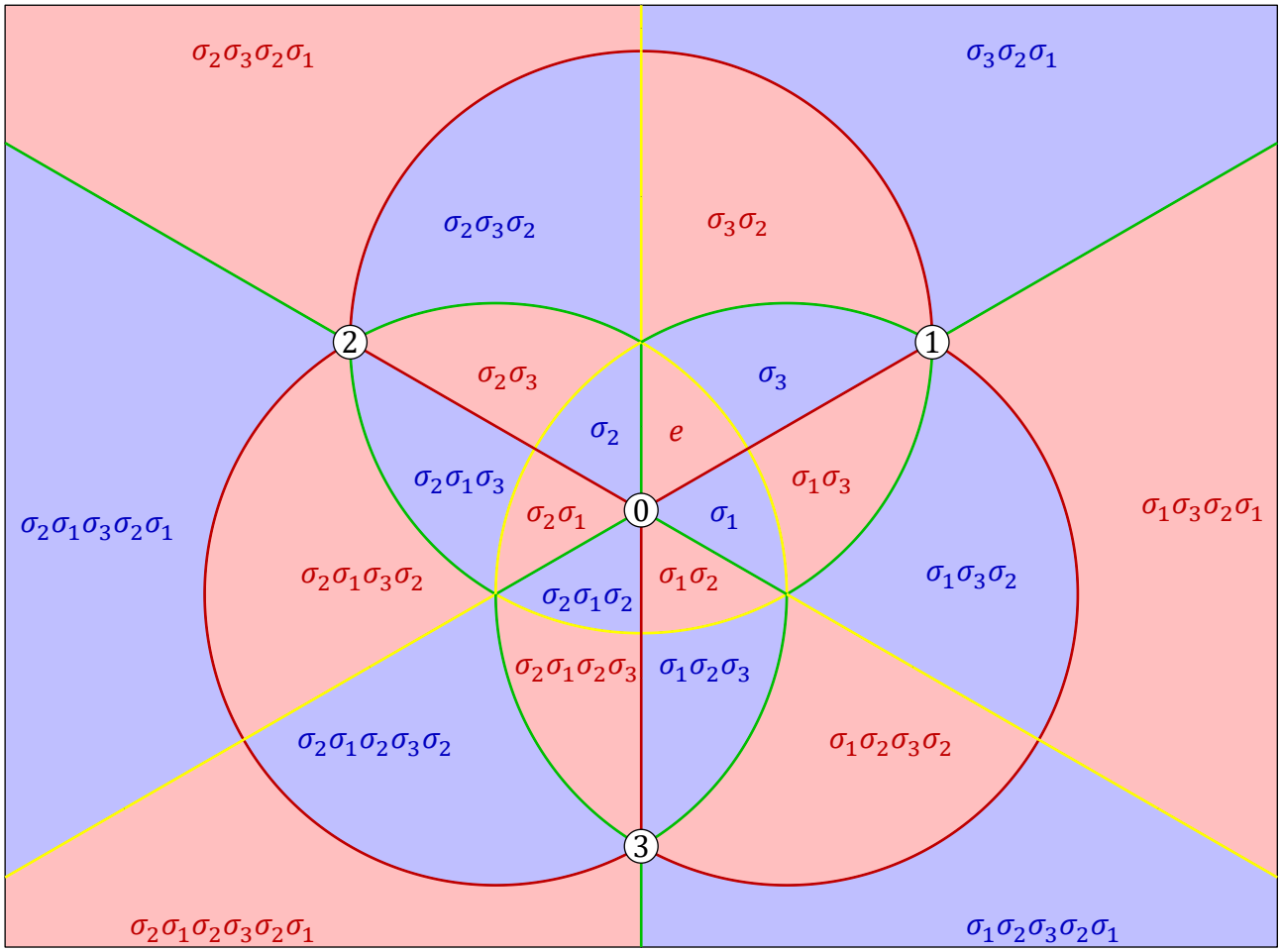


Рис. 12⋄4. Триангуляция описанной сферы плоскостями симметрии тетраэдра в стереографической проекции из диаметрально противоположного к вершине «0» полюса сферы на экваториальную плоскость, параллельную грани «123».

Чтобы явно написать композицию отражений $\sigma_1, \sigma_2, \sigma_3$, переводящую треугольник e в треугольник g, выберем внутри опирающихся на эти треугольники трёхгранных углов векторы u и w с концами на описанной около M сфере так, чтобы $w \neq -u$ и натянутая на них плоскость Π_{uw} не содержала линий пересечения плоскостей симметрии многогранника M. Пройдём из u в w по кратчайшей из двух дуг окружности, высекаемой плоскостью Π_{uw} на описанной около M сфере. Пусть мы при этом последовательно побываем в треугольниках

$$g_1 = e,\ g_2,\ g_3,\ \dots\ ,\ g_{m+1} = g\,.$$

Обозначим через $\nu_i \in \{1,2,3\}$ номер, надписанный на той стороне треугольника g_i, сквозь которую осуществляется проход из g_i в g_{i+1}. Это означает, что общая сторона треугольников g_i и g_{i+1} высекается плоскостью $g_i(\pi_{\nu_i})$, т. е. образом плоскости π_{ν_i} при отображении g_i. Тогда

$$g_2 = \sigma_{\nu_1}\,,\ g_3 = \sigma_{g_2(\pi_{\nu_2})}g_2 = \sigma_{\nu_1}\sigma_{\nu_2}\,,\ g_4 = \sigma_{g_3(\pi_{\nu_3})}g_3 = \sigma_{\nu_1}\sigma_{\nu_2}\sigma_{\nu_3}\,,\ \dots$$

по второму равенству из форм. (12-3) на стр. 201. Таким образом, последовательность индексов $\nu_i \in \{1,2,3\}$ в разложении $g = \sigma_{\nu_1}\dots\sigma_{\nu_m}$ состоит из выписанных по порядку номеров сторон, которые приходится пересекать по пути из $e = g_1$ в $g = g_{m+1}$ по дуге uw, как на рис. 12⋄5, где стороны с номерами 1, 2, 3 изображены соответственно красным, зелёным и жёлтым цветами. Отметим, что полученное нами разложение элемента $g \in \mathrm{O}_M$ в композицию отражений $\sigma_1, \sigma_2, \sigma_3$ не единственно и зависит от выбора векторов u и w внутри трёхгранных углов e и g. При изменении любого из этих векторов последовательность $\nu_1, \dots, \nu_m$ номеров зеркал, пересекаемых по дороге из u в w, не меняется до тех пор, пока натянутая на эти векторы плоскость Π_{uw} не натолкнётся на линию пересечения зеркал, а в момент пересечения такой линии в последовательности $\nu_1, \dots, \nu_m$ некоторый фрагмент вида $\sigma_i\sigma_j\sigma_i\sigma_j\dots$ длины m_k заменяется симметричным фрагментом $\sigma_j\sigma_i\sigma_j\sigma_i\dots$ той же самой длины m_k, как показано на рис. 12⋄5.

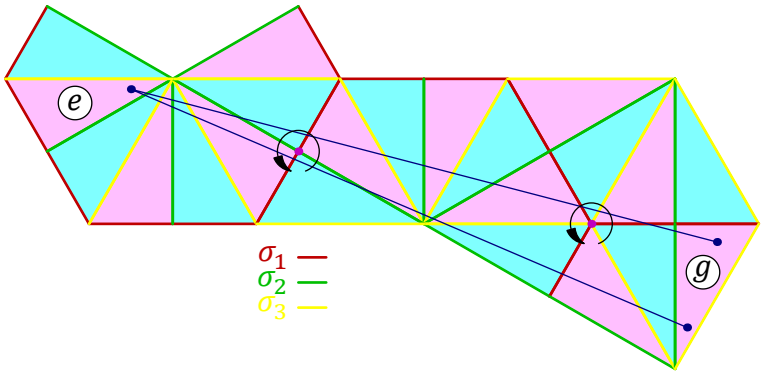


Рис. 12⋄5. $\sigma_2\sigma_3\sigma_2\sigma_3\boldsymbol{\sigma_1}\boldsymbol{\sigma_2}\sigma_3\sigma_2\sigma_3\sigma_2\boldsymbol{\sigma_3}\boldsymbol{\sigma_1}\boldsymbol{\sigma_3}\sigma_2 = g = \sigma_2\sigma_3\sigma_2\sigma_3\boldsymbol{\sigma_2}\boldsymbol{\sigma_1}\sigma_3\sigma_2\sigma_3\sigma_2\boldsymbol{\sigma_1}\boldsymbol{\sigma_3}\boldsymbol{\sigma_1}\sigma_2$.

Разложения, отвечающие верхней и нижней траекториям на рис. 12⋄5 отличаются друг от друга тем, что линии пересечения зеркал обходятся в противоположных направлениях. Композиции возникающих при этом отражений удовлетворяют соотношениям

$$\sigma_1\sigma_2 = \sigma_2\sigma_1 \quad \text{и} \quad \sigma_1\sigma_3\sigma_1 = \sigma_3\sigma_1\sigma_3$$

той же самой природы, что соотношения (12-4) в группе диэдра: так как композиция отражений $\sigma_i \circ \sigma_j$ является поворотом вокруг прямой $\pi_i \cap \pi_j$ на угол $2\pi/m_k$, равный удвоенному углу между плоскостями π_i и π_j, в группе O_M выполняются соотношения $\sigma_i^2 = e$ и $(\sigma_i\sigma_j)^{m_k} = e$, где тройка (i,j,k) пробегает три циклические перестановки номеров $(1,2,3)$.

Отсюда вытекает, во-первых, что длина представления $g = \sigma_{\nu_1}\dots\sigma_{\nu_m}$, считанного вдоль кратчайшей из двух дуг, соединяющих векторы u и w, не зависит от выбора этих векторов внутри трёхгранных углов, опирающихся на треугольники e и g, при условии, что плоскость Π_{uw} не проходит через линии пересечения зеркал, а во-вторых, что правило $x_i \mapsto \sigma_i$ задаёт сюръективный гомоморфизм $\varphi : F_3/H \twoheadrightarrow \mathrm{O}_M$ из фактора свободной группы F_3 с образующими x_1, x_2, x_3 по наименьшей нормальной подгруппе $H \lhd F_3$, содержащей шесть слов

$$x_i^2 \qquad \text{и} \qquad (x_ix_j)^{m_k}\,. \tag{12-7}$$

Докажем, что этот гомоморфизм инъективен. Для этого индукцией по $k \in \mathbb{N}$ установим, что каждый элемент $y \in F_3/H$, представимый в F_3 словом из $\leqslant k$ букв, — это единственный среди представимых словами из $\leqslant k$ букв элемент группы F_3/H, переводимый гомоморфизмом φ в треугольник $g = \varphi(y)$, причём представления $y = x_{\nu_1} \dots x_{\nu_m}$, считанные со всевозможных кратчайших дуг, соединяющих треугольник e с треугольником $g = \varphi(y)$ так, как это объяснялось выше, являются самыми короткими по модулю соотношений (12-7) представлениями элемента $y \in F_3/H$.

Для представимых однобуквенными словами элементов $y = x_1, x_2, x_3$ это очевидно. Пусть это так для всех $y \in F_3/H$, представимых словами из $\leqslant k$ букв. Рассмотрим в F_3/H элемент, представимый словом из $k+1$ букв и не представимый более коротким словом. Он имеет вид yx_j, где $j = 1, 2, 3$, а y представляется словом длины $\leqslant k$. Пусть $g = \varphi(y)$ и $h = \varphi(yx_j) = g\sigma_j$. Выберем в треугольниках e и g векторы $u \in e$ и $w \in g$ так, чтобы окружность, высекаемая из сферы плоскостью Π_{uw}, пересекала плоскость $H = g(\pi_j)$. Кратчайшая дуга этой окружности, ведущая из u в w, либо не пересекает плоскость H, как на рис. 12⋄6, либо пересекает, как на рис. 12⋄7.

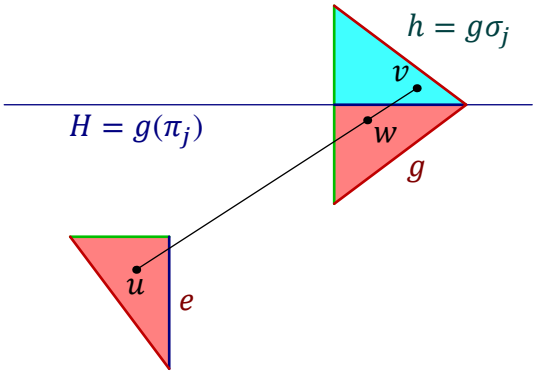


Рис. 12⋄6. H не разделяет e и g.

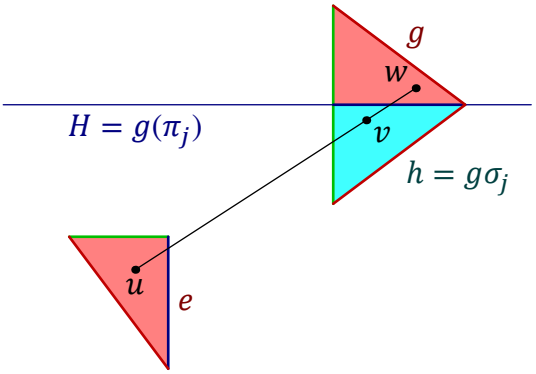


Рис. 12⋄7. H разделяет e и g.

Во втором случае обозначим через v какую-нибудь точку дуги $[u, w]$, лежащую в предыдущем треугольнике $\sigma_{g(\pi_j)}g = g\sigma_j g^{-1} g = g\sigma_j = h$. По предположению индукции, одно из минимальных по длине представлений $y = x_{\nu_1} \dots x_{\nu_m}$ имеет в качестве $\nu_1, \dots, \nu_m$ номера последовательных рёбер, которые приходится пересекать по пути из u в w по дуге $[u, w]$, и его длина $m \leqslant k$. В частности, последняя буква $x_{\nu_m} = x_j$. Поэтому элемент $yx_j = x_{\nu_1} \dots x_{\nu_{m-1}}$ записывается более коротким, чем y, словом из $< k$ букв, вопреки нашему предположению. Таким образом, имеет место первый случай, изображённый на рис. 12⋄6. Обозначим через $v \in h$ какой-нибудь вектор, лежащий на продолжении дуги $[u, w]$ за точку w. По предположению индукции, одно из минимальных по количеству букв представлений $y = x_{\nu_1} \dots x_{\nu_m}$ имеет в качестве $\nu_1, \dots, \nu_m$ номера последовательных рёбер, которые приходится пересекать по пути из u в w по дуге $[u, w]$, и его длина $m \leqslant k$. При этом $h = \varphi(yx_j) = g\sigma_j = \sigma_{i_1} \dots \sigma_{i_m}\sigma_j$, и представление $yx_j = x_{\nu_1} \dots x_{\nu_m} x_j$ по нашему предположению состоит, как минимум, из $k+1$ букв. Мы заключаем, что $m = k$, представление $yx_j = x_{\nu_1} \dots x_{\nu_k} x_j$ является одним из кратчайших для элемента yx_j и считывается с дуги $[u, v]$. В частности, элемент yx_j однозначно восстанавливается по треугольнику $h = \varphi(yx_j)$, что воспроизводит индуктивное предположение. Мы получили следующий результат.

Предложение 12.3
Полная группа O_M платонова тела M с треугольными гранями порождается тремя элементами x_1, x_2, x_3, связанными шестью определяющими соотношениями $x_i^2 = e$ и $(x_i x_j)^{m_k} = e$. □

12.3. Образующие и соотношения симметрической группы S_{n+1}. Обозначим числами от 0 до n концы стандартных базисных векторов $e_0, e_1, \dots, e_n$ в $\mathbb{R}^{n+1}$ и рассмотрим n-мерный правильный симплекс $\Delta \subset \mathbb{R}^{n+1}$ с вершинами в этих точках. Поскольку каждое аффинное преобразование n-мерной гиперплоскости $x_0+x_1+\dots+x_n = 1$, в которой лежит симплекс Δ, однозначно задаётся своим действием на вершины симплекса Δ, полная группа O_Δ симплекса Δ изоморфна симметрической группе S_{n+1} перестановок его вершин $0, 1, \dots, n$. Каждая k-мерная грань симплекса Δ является правильным k-мерным симплексом и представляет собою выпуклую оболочку каких-либо $k+1$ вершин симплекса Δ, и наоборот, выпуклая оболочка $[i_0, i_1, \dots, i_k]$ любых $k+1$ различных вершин $\{i_0, i_1, \dots, i_k\} \subset \{0, 1, \dots, n\}$ является k-мерной гранью симплекса Δ. Симплекс Δ симметричен относительно $n(n+1)/2$ гиперплоскостей π_{ij}, проходящих через середину ребра $[i, j]$ и противолежащую этому ребру грань коразмерности 2, содержащую вершины $\{0, 1, \dots, n\} \smallsetminus \{i, j\}$. Гиперплоскость π_{ij} перпендикулярна вектору $e_i - e_j$ и отражение $\sigma_{ij} \in \mathrm{O}_\Delta$ в этой гиперплоскости отвечает транспозиции элементов i и j в симметрической группе S_{n+1}.

Упражнение 12.4. Убедитесь, что гиперплоскости π_{ij} и π_{km} с $\{i, j\} \cap \{k, m\} = \varnothing$ ортогональны, а гиперплоскости π_{ij} и π_{jk} с различными i, j, k пересекаются под углом $\pi/3 = 60^\circ$.

Плоскости π_{ij} осуществляют *барицентрическое разбиение* симплекса Δ на $(n+1)!$ меньших симплексов с вершинами в центрах граней симплекса Δ и в центре самого симплекса. Если обозначить через $\langle i_0 i_1 \dots i_m \rangle$ центр m-мерной грани с вершинами в $i_0, i_1, \dots, i_m$, то каждый симплекс барицентрического разбиения будет иметь одну из вершин в какой-либо вершине $\langle i_0 \rangle$ симплекса Δ, следующую вершину — в центре $\langle i_0 i_1 \rangle$ какого-либо примыкающего к вершине i_0 ребра $[i_0, i_1]$, следующую вершину — в центре $\langle i_0 i_1 i_2 \rangle$ какой-либо примыкающей к ребру $[i_0, i_1]$ двумерной треугольной грани $[i_0, i_1, i_2]$ и т. д. вплоть до центра $\langle i_0 i_1 \dots i_n \rangle$ самого симплекса Δ. Эти симплексы находятся в естественной биекции с перестановками $g \in S_{n+1}$: симплекс

$$g = \big[\langle g_0 \rangle, \langle g_0, g_1 \rangle, \langle g_0, g_1, g_2 \rangle, \dots, \langle g_0 g_1 \dots g_{n-1} \rangle, \langle g_0 g_1 \dots g_n \rangle\big] \tag{12-8}$$

является образом начального симплекса

$$e = \big[\langle 0 \rangle, \langle 01 \rangle, \langle 012 \rangle, \dots, \langle 0, 1, \dots, n-1 \rangle, \langle 0, 1, \dots, n \rangle\big] \tag{12-9}$$

под действием единственной перестановки $g = (g_0, g_1, \dots, g_n) \in S_{n+1} = \mathrm{O}_M$. Спроектируем поверхность симплекса Δ из его центра на описанную сферу. Получим разбиение $(n-1)$-мерной сферы S^{n-1} на $(n+1)!$ конгруэнтных друг другу $(n-1)$-мерных симплексов, надписанных элементами $g \in S_{n+1}$. Грани этих симплексов высекаются из сферы гиперплоскостями π_{ij}. При $n = 3$ получится представленная на рис. 12⋄4 на стр. 203 триангуляция двумерной сферы S^2 двадцатью четырьмя сферическими треугольниками с углами $\pi/3$, $\pi/3$ и $\pi/2$. Помеченному тождественным преобразованием e начальному симплексу (12-9) отвечает сферический симплекс, высекаемый из сферы n гиперплоскостями $\pi_i \stackrel{\text{def}}{=} \pi_{i-1,i}$ с $1 \leqslant i \leqslant n$. Обозначим через $\sigma_i = \sigma_{i-1,i}$ отражения в этих гиперплоскостях. В симметрической группе S_{n+1} этим отражениям отвечают транспозиции $|i-1, i\rangle$ пар соседних элементов. По упр. 12.4 они удовлетворяют соотношениям[1]

$$\sigma_i^2 = e\,, \quad \sigma_i \sigma_{i+1} \sigma_i = \sigma_{i+1} \sigma_i \sigma_{i+1} \quad \text{и} \quad \sigma_i \sigma_j = \sigma_j \sigma_i\,, \quad \text{где} \quad |i-j| \geqslant 2\,. \tag{12-10}$$

[1] Соотношение $\sigma_i \sigma_{i+1} \sigma_i = \sigma_{i+1} \sigma_i \sigma_{i+1}$ является более употребительной в данном контексте записью циклического соотношения $(\sigma_i \sigma_{i+1})^3 = e$ на поворот $\sigma_i \sigma_{i+1}$ на 120° вокруг $(n-2)$-мерного подпространства $\pi_i \cap \pi_{i+1}$.

Упражнение 12.5. Убедитесь напрямую, что транспозиции $\sigma_i = |i-1, i\rangle \in S_{n+1}$ удовлетворяют соотношениям (12-10).

В силу этих соотношений, гомоморфизм свободой группы F_n с образующими $x_1, \dots, x_n$, переводящий x_i в σ_i, корректно факторизуется до гомоморфизма $\varphi : F_n / H \to S_{n+1}$, где $H \lhd F_n$ — наименьшая нормальная подгруппа, содержащая слова

$$x_i^2\,, \quad (x_i x_{i+1})^3 \quad \text{и} \quad (x_i x_j)^2\,, \quad \text{где} \quad |i-j| \geqslant 2\,. \tag{12-11}$$

Чтобы убедиться в его сюръективности, выберем в симплексах e и g точки a и b так, чтобы они не были диаметрально противоположны и соединяющая их геодезическая[1] не пересекала граней коразмерности[2] 2. Пройдя из a в b по этой геодезической, мы получим разложение

$$g = \sigma_{i_1} \dots \sigma_{i_m}\,, \tag{12-12}$$

в котором каждое $i_\nu \in \{1, \dots, n\}$ равно номеру такого зеркала π_{i_ν}, что переход из ν-того встреченного по дороге симплекса g_ν в следующий симплекс[3] $g_{\nu+1}$ осуществляется через грань, высекаемую гиперплоскостью $g_\nu(\pi_{i_\nu})$. Дословно также, как и в n° 12.2, проверяется, что длина представления (12-12), полученного с помощью дуги $[a, b]$ не зависит от выбора её концов $a \in e$ и $b \in g$ при условии, что они не диаметрально противоположны и плоскость π_{ab} не проходит через пересечения зеркал π_{ij}: если при перемещении точек a и b внутри симплексов e и g дуга $[a, b]$ пройдёт через пересечение $g_k(\pi_i \cap \pi_j)$ перпендикулярных гиперграней $g_k(\pi_i)$, $g_k(\pi_j)$ с $|i-j| \geqslant 2$, или через пересечение $g_k(\pi_i \cap \pi_{i+1})$ гиперграней $g_k(\pi_i)$, $g_k(\pi_{i+1})$, пересекающихся под углом 60°, то в представлении $g = \sigma_1 \dots \sigma_m$ стоящий на k-том месте фрагмент $\sigma_i\sigma_j$ или $\sigma_i\sigma_{i+1}\sigma_i$ заменится, соответственно, равным ему в группе O_Δ фрагментом $\sigma_j\sigma_i$ или $\sigma_{i+1}\sigma_i\sigma_{i+1}$. В ортогональной проекции вдоль $(n-2)$-мерного подпространства $g_k(\pi_i \cap \pi_j)$ или $g_k(\pi_i \cap \pi_{i+1})$ на ортогональную ему двумерную плоскость мы при этом увидим картину вроде показанной на рис. 12⋄5 на стр. 204. Точно такая же, как в n° 12.2, индукция по $k \in \mathbb{N}$ показывает, что каждый элемент $y \in F_n / H$, представимый по модулю соотношений (12-11) словом из $\leqslant k$ букв, является единственным среди представимых словами из $\leqslant k$ букв элементом, который переводится гомоморфизмом φ в симплекс $g = \varphi(y)$, и слова $x_{i_1} \dots x_{i_k} \in F_3$, считанные с соединяющих симплекс e с симплексом $g = \varphi(y)$ геодезических, являются кратчайшими по модулю соотношений (12-11) записями элемента $y \in F_n / H$. Таким образом, симметрическая группа S_{n+1} порождается n образующими x_i, $1 \leqslant i \leqslant n$, связанными определяющими соотношениями (12-11).

Эту геометрическую картину нетрудно выхолостить до сугубо комбинаторного рассуждения, представленного в следующем разделе.

12.4. Порядок Брюа на симметрической группе S_{n+1}. Напомню[4], что *длиной* $\ell(g)$ перестановки $g = (g_0, g_1, \dots, g_n) \in S_{n+1}$ называется количество всех её инверсных пар[5]. Правое умножение перестановки g на транспозицию $\sigma_i = |i-1, i\rangle$ приводит к перестановке $g\sigma_i$, отличающейся от g транспозицией $(i-1)$-того и i-го символов g_{i-1} и g_i:

$$\big(g_0,\ \dots\ , g_{i-2},\ \boldsymbol{g_{i-1}},\ \boldsymbol{g_i},\ g_{i+1},\ \dots\ , g_n\big) \circ \sigma_i = \big(g_0,\ \dots\ , g_{i-2},\ \boldsymbol{g_i},\ \boldsymbol{g_{i-1}},\ g_{i+1},\ \dots\ , g_n\big)\ ,$$

[1] Кратчайшая из двух дуг ab большой окружности, высекаемой из сферы двумерной плоскостью, проходящей через точки a, b и центр сферы.

[2] Т. е. пересечений всевозможных пар зеркал π_{ij}.

[3] Напомню, что при этом $g_\nu = \sigma_1 \dots \sigma_{\nu-1}$, f $g_{\nu+1} = \sigma_{g_\nu(\pi_{i_\nu})} g_\nu = g_\nu \sigma_{i_\nu}$.

[4] См. n° 8.1 на стр. 128.

[5] Т. е. таких пар $1 \leqslant i < j \leqslant n$, что $g_i > g_j$.

причём $\ell(g\sigma_i) = \ell(g) + 1$, если $g_{i-1} < g_i$, и $\ell(g\sigma_i) = \ell(g) - 1$, если $g_{i-1} > g_i$.

Упражнение 12.6. Убедитесь, что любая перестановка g длины $\ell(g) = m$ может быть записана таким словом $g = \sigma_{i_1} \dots \sigma_{i_m}$, что $\ell(\sigma_{i_1} \dots \sigma_{i_k}) = \ell(\sigma_{i_1} \dots \sigma_{i_{k-1}}) + 1$ при всех $2 \leqslant k \leqslant m$.

Частичный порядок на S_{n+1}, в котором $g < h$, если $h = g\sigma_{i_1} \dots \sigma_{i_s}$, где

$$\ell(g\sigma_{i_1} \dots \sigma_{i_k}) = \ell(g\sigma_{i_1} \dots \sigma_{i_{k-1}}) + 1 \text{ при всех } 1 \leqslant k \leqslant s\,,$$

называется *порядком Брюа*.

Слово $w = x_{i_1} \dots x_{i_m}$ в свободной группе F_n с образующими $x_1, \dots, x_n$ называется *минимальным словом* перестановки $g \in S_{n+1}$, если $m = \ell(g)$ и $g = \sigma_{i_1} \dots \sigma_{i_m}$. Начальные фрагменты минимального слова задают строго возрастающую в смысле порядка Брюа последовательность элементов $h_\nu = \sigma_{i_1} \dots \sigma_{i_\nu} \in S_{n+1}$. Перестановка g может иметь много разных минимальных слов, однако не может быть записана никаким более коротким словом.

Как и в предыдущем разделе, рассмотрим гомоморфизм $\varphi : F_n \to S_{n+1}$, $x_i \mapsto \sigma_i$.

Предложение 12.4
По модулю соотношений $x_i^2 = e$, $x_i x_{i+1} x_i = x_{i+1} x_i x_{i+1}$ и $x_i x_j = x_j x_i$, где $|i - j| \geqslant 2$, каждое слово $w \in F_n$ эквивалентно некоторому минимальному слову перестановки $\varphi(w) \in S_{n+1}$, а все минимальные слова перестановки $\varphi(w)$ эквивалентны между собой.

Доказательство. Индукция по количеству букв в слове $w \in F_{n-1}$. Для $w = \varnothing$ утверждение очевидно. Пусть оно справедливо для всех слов из $\leqslant m$ букв. Достаточно для каждого m-буквенного слова w и каждой буквы x_ν проверить предложение для слова wx_ν. Если слово w не является минимальным словом элемента $g = \varphi(w)$, то оно эквивалентно более короткому минимальному слову. Тогда и wx_ν эквивалентно более короткому слову, и предложение справедливо по индукции. Поэтому мы будем далее считать, что слово w является минимальным словом элемента $g = \varphi(w) = (g_0, g_1, \dots, g_n)$. Возможны два случая: либо $g_{\nu-1} > g_\nu$, либо $g_{\nu-1} < g_\nu$. В первом случае у перестановки g есть минимальное слово вида ux_ν, по предположению индукции эквивалентное слову w. Тогда $wx_\nu \sim ux_\nu x_\nu \sim u$ и элемент $\varphi(wx_\nu) = \varphi(u)$ является образом более короткого, чем w слова u, эквивалентного слову wx_ν. По индукции, слово u эквивалентно минимальному слову элемента $\varphi(wx_\nu)$ и все такие слова эквивалентны друг другу. Поэтому то же верно и для эквивалентного u слова wx_ν.

Остаётся рассмотреть случай $g_{\nu-1} < g_\nu$. Здесь $\ell(g\sigma_\nu) = \ell(g) + 1$ и слово wx_ν является минимальным словом для элемента $\varphi(wx_\nu)$. Мы должны показать, что любое другое минимальное слово w' этого элемента эквивалентно wx_ν. Для самой правой буквы слова w' есть 3 возможности: либо она равна x_ν, либо она равна $x_{\nu\pm1}$ либо она равна x_μ с $|\mu - \nu| \geqslant 2$. В пером случае $w' = ux_\nu$, где u, как и w, является минимальным словом элемента g. По индукции $u \sim w$, а значит, и $w' = ux_k \sim wx_k$.

Пусть теперь $w' = ux_{\nu+1}$. Поскольку оба слова wx_ν и $ux_{\nu+1}$ минимальны для перестановки $h = \varphi(wx_\nu) = \varphi(ux_{\nu+1})$, в перестановке h на местах с номерами $\nu - 1, \nu, \nu + 1$ стоят числа $g_\nu > g_{\nu-1} > g_{\nu+1}$, а в перестановке $g = (g_0, g_1, \dots, g_n) = \varphi(w)$ на этих же местах — числа $g_{\nu-1} < g_\nu > g_{\nu+1}$, где $g_{\nu-1} > g_{\nu+1}$. Поэтому у перестановки h имеется минимальное слово вида $sx_{\nu+1}x_\nu x_{\nu+1}$, а у перестановки g — минимальное слово вида $tx_\nu x_{\nu+1}$. Перестановка $h' = \varphi(s) = \varphi(t)$ отличается от h тем, что числа на местах с номерами $\nu-1, \nu, \nu+1$ в ней возрастают и равны $g_{\nu+1} < g_{\nu-1} < g_\nu$. Поскольку $\ell(h') = \ell(h) - 3 = \ell(g) - 2$, оба слова t и s минимальны для h' и по индукции эквивалентны. Кроме того, по индукции $w \sim tx_\nu x_{\nu+1}$. Поэтому

$$wx_\nu \sim tx_\nu x_{\nu+1} x_\nu \sim sx_\nu x_{\nu+1} x_\nu \sim sx_{\nu+1} x_\nu x_{\nu+1}\,.$$

Но $sx_{\nu+1}x_\nu \sim u$, поскольку оба слова минимальны для одной и той же перестановки[1] длины $m = \ell(h) - 1$. Таким образом, $wx_\nu \sim ux_{\nu+1}$. Случай $w' = ux_{\nu-1}$ полностью симметричен.

Наконец, пусть $h = \varphi(wx_\nu) = \varphi(ux_\mu)$, где $|\mu - \nu| \geqslant 2$. Тогда в h есть два непересекающихся фрагмента $g_{\nu-1} > g_\nu$ и $g_{\mu-1} > g_\mu$. Поэтому у h есть минимальные слова вида $tx_\mu x_\nu$ и вида $sx_\nu x_\mu$, где t и s являются минимальными словами для перестановки $\varphi(t) = \varphi(s)$, отличающейся от h тем, что расматриваемые 2 фрагмента в ней имеют вид $g_\nu < g_{\nu-1}$ и $g_\mu < g_{\mu-1}$. Так как длина этой перестановки равна $\ell(h) - 2 = m - 1$, по индукции $t \sim s$. Поскольку tx_μ — минимальное слово для g, по индукции $w \sim tx_\mu$. Аналогично, т. к. sx_ν и u — минимальные слова для перестановки $\varphi(sx_\nu) = \varphi(u)$, отличающейся от h' транспозицией первого из двух фрагментов и потому имеющей длину $\ell(h) - 1 = m$, по индукции $sx_\nu \sim u$. Таким образом, $wx_\nu \sim tx_\mu x_\nu \sim sx_\mu x_\nu \sim sx_\nu x_\mu \sim ux_\mu$, что и требовалось. □

Упражнение 12.7. Убедитесь, что $h \leqslant g$ в смысле порядка Брюа если и только если в симплексах e, h, g из n° 12.3 можно выбрать такие точки a, b, c, что длина геодезической дуги $[ac]$ меньше π и $b \in [ac]$.

[1] Она отличается от g, h и h' тем, что числа в позициях с номерами $\nu - 1, \nu, \nu + 1$ в ней упорядочены как $g_\nu > g_{\nu+1} < g_{\nu-1}$, где $g_\nu > g_{\nu-1}$.

Ответы и указания к некоторым упражнениям

Упр. 0.1. Ответ: 2^n.

Упр. 0.2. Ответ на второй вопрос — нет. Пусть $X = \{1, 2\}$, $Y = \{2\}$. Все их парные пересечения и объединения суть $X \cap Y = Y \cap Y = Y \cup Y = Y$ и $X \cup Y = X \cup X = X \cap X = X$, и любая формула, составленная из X, Y, $\cap$, $\cup$, даст на выходе или $X = \{1, 2\}$, или $Y = \{2\}$, тогда как $X \setminus Y = \{1\}$.

Упр. 0.3. В первом случае имеется 6 наложений и ни одного вложения, во втором — 6 вложений и ни одного наложения.

Упр. 0.5. Если X конечно, то инъективное или сюръективное отображение $X \to X$ автоматически биективно. Если X бесконечно, то в X есть подмножество, изоморфное $\mathbb{N}$. Инъекция $\mathbb{N} \hookrightarrow \mathbb{N}$, $n \mapsto (n + 1)$, и сюръекция $\mathbb{N} \twoheadrightarrow \mathbb{N}$, $n \mapsto \max(1, (n - 1))$, обе не биективны и продолжаются до точно таких же отображений $X \to X$ тождественным действием на $X \setminus \mathbb{N}$.

Упр. 0.6. Ответ: нет. Воспользуйтесь «диагональным трюком» Кантора: пусть все биекции $\mathbb{N} \to \mathbb{N}$ занумерованы натуральными числами; глядя на этот список, постройте биекцию, которая при каждом $k = 1, 2, 3, \ldots$ отображает некоторое число $n_k \in \mathbb{N}$ не туда, куда его отображает k-тая биекция из списка.

Упр. 0.7. Ответ: $\binom{n+m-1}{m-1} = \binom{n+m-1}{n} = \frac{(n+m-1)!}{n!(m-1)!}$. Указание: слагаемых столько же, сколько имеется упорядоченных наборов неотрицательных целых чисел $(k_1, \ldots, k_m)$ с суммой $\sum k_i = n$. Такой набор можно закодировать словом, составленным из $(m - 1)$ букв 0 и n букв 1: сначала пишем k_1 единиц, потом нуль, потом k_2 единиц, потом нуль, и т. д. (слово кончится k_m единицами, стоящими следом за последним, $(m - 1)$-м нулём) .

Упр. 0.8. Ответ: $\binom{n+k}{k}$. Каждая такая диаграмма представляет собою ломаную, ведущую из левого нижнего угла прямоугольника в правый верхний. В такой ломаной ровно n горизонтальных звеньев и ровно k вертикальных.

Упр. 0.9. Пусть $[x']_n = [x]_n$ и $[y']_n = [y]_n$, т. е. $x' = x + nk$, $y' = y + n\ell$ с некоторыми $k, \ell \in \mathbb{Z}$. 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 $[x'y']_n = [xy]_n$.

Упр. 0.10. Положим $x \sim y$, если существует конечная последовательность точек

$$x = z_0,\ z_1,\ z_2,\ \ldots\ ,\ z_n = y$$

как в условии задачи. Проверьте, что это отношение эквивалентности и что оно содержится в любой эквивалентности $S \subset X \times X$, содержащей R.

Упр. 0.11. 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. $(p, q) \sim (u, w)$.

Упр. 0.12. Если прямые ℓ_1 и ℓ_2 пересекаются в точке O под углом $0 < \alpha \leqslant \pi/2$, то отражение относительно ℓ_1, за которым следует отражение относительно ℓ_2, это поворот вокруг точки O на угол 2α в направлении от первой прямой ко второй. Таким образом, отражения относительно пересекающихся прямых коммутируют тогда и только тогда, когда прямые перпендикулярны.

Упр. 0.14. Таблица композиций gf в симметрической группе S_3:

$g \diagdown f$	$(1,2,3)$	$(1,3,2)$	$(3,2,1)$	$(2,1,3)$	$(2,3,1)$	$(3,1,2)$
$(1,2,3)$	$(1,2,3)$	$(1,3,2)$	$(3,2,1)$	$(2,1,3)$	$(2,3,1)$	$(3,1,2)$
$(1,3,2)$	$(1,3,2)$	$(1,2,3)$	$(3,1,2)$	$(2,3,1)$	$(2,1,3)$	$(3,2,1)$
$(3,2,1)$	$(3,2,1)$	$(2,3,1)$	$(1,2,3)$	$(3,1,2)$	$(1,3,2)$	$(2,1,3)$
$(2,1,3)$	$(2,1,3)$	$(3,1,2)$	$(2,3,1)$	$(1,2,3)$	$(3,2,1)$	$(1,3,2)$
$(2,3,1)$	$(2,3,1)$	$(3,2,1)$	$(2,1,3)$	$(1,3,2)$	$(3,1,2)$	$(1,2,3)$
$(3,1,2)$	$(3,1,2)$	$(2,1,3)$	$(1,3,2)$	$(3,2,1)$	$(1,2,3)$	$(2,3,1)$

Упр. 0.15. Отношение $n \mid m$ на множестве $\mathbb{Z}$ не кососимметрично: $n \mid m$ и $m \mid n$ если и только если $m = \pm n$. Фактор множества $\mathbb{Z}$ по этому отношению эквивалентности можно отождествить с множеством $\mathbb{Z}_{\geqslant 0}$ неотрицательных целых чисел, на котором отношение $n \mid m$ является частичным порядком (обратите внимание, что нуль является нижней гранью этого множества, т. е. делит все элементы.)

Упр. 0.16. Пусть множество $S \subset W$ состоит из всех таких элементов $z \in W$, что утверждение $\Phi(z)$ ложно. Если $S \neq \varnothing$, то в нём есть начальный элемент $s_* \in S$. Поскольку утверждение $\Phi(w)$ истинно для всех $w < s_*$, утверждение $\Psi(s_*)$ тоже истинно, т. е. $s_* \notin S$. Противоречие.

Упр. 0.17. Обозначим через x_I начальный элемент дополнения $W \smallsetminus I$. Начальный интервал $[x_I) \subset W$ является объединением начальных интервалов $[y) \subset W$ по всем $y < x_I$. Так как I содержит все интервалы $[y)$ с $y < x_I$, мы заключаем, что $I \supseteq [x_I)$, откуда $I = [x_I)$.

Упр. 0.18. Пусть соотношение $U \geqslant W$ не выполняется. Покажем, что любой начальный отрезок $[u) \subset U$ изоморфен некоторому начальному отрезку $[w) \subset W$, где $w = w(u)$ однозначно восстанавливается по u. Это верно для пустого начального отрезка $\varnothing = [u_*)$, где $u_* \in U$ — минимальный элемент. Пусть это верно для всех начальных отрезков $[y) \subset U$ с $y < u$.

Если в начальном интервале $[u)$ имеется максимальный элемент u', то $[u) = [u') \sqcup \{u'\}$, и $[u')$ изоморфен некоторому начальному интервалу $[w') \subset W$, отличному от W, поскольку равенство $[w') = W$ означает, что $U \geqslant W$. Тем самым, интервал $[u) = [u') \sqcup \{u'\}$ изоморфен вполне упорядоченному множеству $[w') \sqcup \{w'\}$, которое не совпадает с W по тем же причинам, что и выше, и является начальным интервалом вида $[w) \subset W$, где $w = w(u)$ — наименьший элемент в дополнении к подмножеству $[w') \sqcup \{w'\}$ в W.

Если в начальном интервале $[u)$ нет максимального элемента, то $[u) = \bigcup_{y<u}[y)$ изоморфен объединению вложенных начальных интервалов $\bigcup_{y<u}[w(y)) \subset W$. Это объединение не исчерпывает всё множество W, поскольку в противном случае $W \simeq [y)$ и $W \leqslant U$. Положим $w(u) \in W$ равным минимальному элементу, не содержащемуся в $\bigcup_{y<u}[w(y))$. Проверьте, что $\bigcup_{y<u}[w(y)) = [w(u))$ и что отображение $u \mapsto w(u)$ устанавливает изоморфизм множества U с некоторым начальным отрезком множества W.

Упр. 0.19. Пусть рекурсивные подмножества $W_1, W_2 \subset P$ имеют общий начальный элемент. Рассмотрим подмножество $Z \subseteq W_1$, состоящее из всех таких $z \in W_1$, что начальный интервал $[z)_1$ в множестве W_1 совпадает с начальным интервалом $[z)_2$ в множестве W_2. Множество Z не пусто, поскольку содержит общий начальный элемент множеств W_1 и W_2. В силу рекурсивности W_1 и W_2 множество Z содержится в $W_1 \cap W_2$, являясь, по упр. 0.17 на стр. 18, начальным интервалом как в W_1, так и в W_2. Если $Z \neq W_1$ и $Z \neq W_2$, то точные верхние грани Z в W_1 и W_2, с одной стороны, не лежат в Z и поэтому различны, а с другой стороны обе равны $\varrho(Z)$ в силу рекурсивности W_1 и W_2. Тем самым, $Z = W_1$ или $Z = W_2$.

Упр. 0.20. Каждое подмножество $S \subset U$ имеет непустое пересечение с каким-нибудь рекурсивным вполне упорядоченным подмножеством $W \subset P$ с начальным элементом $\varrho(\varnothing)$. По упр. 0.19 подмножество W является начальным интервалом всех содержащих W рекурсивных вполне упорядоченных подмножеств с начальным элементом $\varrho(\varnothing)$. Поэтому начальный элемент пересечения $S \cap W$ не зависит от выбора такого W, что $W \cap S \neq \varnothing$, и является начальным элементом подмножества S. Каждый начальный интервал $[u) \subset U$ является начальным интервалом любого содержащего u множества W из цепи. В силу рекурсивности W элемент $\varrho[u) = u$.

Упр. 0.21. Пользуясь аксиомой выбора, зафиксируем для каждого $W \in \mathcal{W}(P)$ какую-нибудь верхнюю грань $b(W) \in P$. Если $f(x) > x$ для всех $x \in P$, то отображение $\beta\colon\ \mathcal{W}(P) \to P, W \mapsto f(b(W))$ противоречит лем. 0.2 на стр. 19.

Упр. 0.22. Обозначим через $\mathcal{S}(X)$ множество всех непустых подмножеств данного множества X, включая само X. При помощи аксиомы выбора постройте такое отображение $\mu\colon\ \mathcal{S}(X) \to X$, что $\mu(Z) \in Z$ для всех $Z \in \mathcal{S}(X)$. Обозначим через $\mathcal{W}(X)$ множество всех $W \in \mathcal{S}(X)$, которые можно вполне упорядочить так, что $\mu(X \smallsetminus [w)) = w$ для всех $w \in W$. Вдохновляясь лем. 0.2 на стр. 19 покажите, что $\mathcal{W}(X) \neq \varnothing$, и убедитесь, что $X \in \mathcal{W}(X)$.

Упр. 0.23. Убедитесь, что множество всех цепей, содержащих данную цепь, является полным чумом относительно отношения включения, и примените лемму Цорна.

Упр. 1.2. Ответы: $1 + x$ и $xy + x + y$.

Упр. 1.3. Если умножить числитель и знаменатель любой дроби в левой части равенств (1-11) на c, числитель и знаменатель правой части также умножится на c. Отсюда следует корректность. Проверка аксиом бесхитростна.

Упр. 1.5. Пусть $ax_0 + by_0 = k$. Тогда $a(x_0 + n\beta) + b(y_0 - n\alpha) = ax_0 + by_0 + n(a\beta - b\alpha) = k$ при всех $n \in \mathbb{Z}$. Если $ax + by = k$, то $a(x - x_0) = -b(y - y_0)$ делится на нок$(ab) = \alpha\beta d$. Тем самым, число $n = (x - x_0)/\beta = -(y - y_0)/\alpha \in \mathbb{Z}$, и $x = x_0 + n\beta$, а $y = y_0 - n\alpha$.

Упр. 1.6. Пусть числа таблицы $\begin{pmatrix} m & x & y \\ n & s & t \end{pmatrix}$ удовлетворяют равенствам $m = xa + by$, $n = as + bt$ и $xt - ys = 1$. Прибавляя к 1-й строке 2-ю, умноженную на k, получаем таблицу $\begin{pmatrix} m' & x' & y' \\ n & s & t \end{pmatrix}$, в которой $m' = m + nk$, $x' = x + ks$, $y' = t + kt$. Тогда

$$m' = ax + by + k(as + bt) = ax' + by'$$
$$x't - y's = xt - ys + kst - kst = 1\,.$$

Упр. 1.7. Подставьте в это равенство $x = y = 0$.

Упр. 1.8. Существование разложения. 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, каждое из которых в свою очередь или просто или является произведением 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 разложения. Для любого простого числа p и любого целого z имеется альтернатива: либо нод$(z, p) = |p|$, и тогда z делится на p, либо нод$(z, p) = 1$, и тогда z взаимно прост с p. Пусть в равенстве $p_1 \ldots p_k = q_1 \ldots q_m$ все сомножители просты. Так как $\prod q_i$ делится на p_1, число p_1 не может быть взаимно просто с каждым q_i в силу лем. 1.3 на стр. 27. Согласно упомянутой альтернативе, хотя бы один из множителей q_i (будем считать, что q_1) делится на p_1. Поскольку q_1 прост, $q_1 = \pm p_1$. Сокращаем первые множители и повторяем рассуждение.

Упр. 1.9. При любом $k \in \mathbb{N}$ умножение на класс $[x]^{-1}[y]$ переводит класс $[a^k x]$ в класс $[a^k y]$, а умножение на класс $[x][y]^{-1}$ переводит класс $[a^k y]$ назад в $[a^k x]$.

Упр. 1.11. 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 форм. (1-24) на стр. 29, получаем

$$(1+x)^{p^n m} = \left((1+x)^p\right)^{p^{n-1}m} = \left(1+x^p\right)^{p^{n-1}m} = \left((1+x^p)^p\right)^{p^{n-2}m} = \left(1+x^{p^2}\right)^{p^{n-2}m} = \cdots$$
$$\cdots = \left(1+x^{p^n}\right)^m = 1 + mx^{p^n} + \text{ старшие степени}$$

Упр. 1.13. Если число $\alpha \in \Bbbk$ является корнем многочлена $f(x)$, то $f(x)$ делится на $(x-\alpha)$ (разделите $f(x)$ на $(x-\alpha)$ с остатком и подставьте $x=\alpha$).

Упр. 1.14. По малой теореме Ферма[1] каждый элемент $x \in \operatorname{im}\psi$ удовлетворяет уравнению $x^2 = 1$.

Упр. 1.16. Ненулевой гомоморфизм полей инъективен, переводит единицу в единицу и перестановочен со сложением, вычитанием, умножением и делением[2]. Простое подполе состоит из элементов вида $\pm(1+\cdots+1)/(1+\cdots+1)$, каждый из которых остаётся на месте. Если имеется ненулевой гомоморфизм $\Bbbk \to \mathbb{F}$, то равенство или неравенство нулю суммы некоторого количества единиц в поле $\Bbbk$ влечёт точно такое же равенство или неравенство в поле $\mathbb{F}$, откуда $\operatorname{char}\Bbbk = \operatorname{char}\mathbb{F}$.

Упр. 1.17. Воспользуйтесь тем, что $\mathbb{R}$ является множеством дедекиндовых сечений линейно упорядоченного множества $\mathbb{Q}$.

Упр. 2.3. Ответ: $(y^n - x^n)/(y-x) = y^{n-1} + y^{n-2}x + y^{n-3}x^2 + \ldots + yx^{n-2} + x^{n-1}$.

Упр. 2.5. $\left(a_0 + a_1x + a_2x^2 + \ldots\right)^p = a_0^p + a_1^p x^p + a_2^p x^{2p} + \ldots = a_0 + a_1x^p + a_2x^{2p} + \ldots$ (первое равенство справедливо, поскольку возведение в p-тую степень перестановочно со сложением, второе — по малой теореме Ферма).

Упр. 2.6. Если $f(x) = \sum a_k x^k$, 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

$$f_\nu(x) = \sum_{k\geqslant\nu} a_k \binom{k}{\nu} \cdot x^{k-\nu} = \frac{1}{\nu!}\frac{d^k}{dx^k}\sum_{k\geqslant 0} a_k x^k\,.$$

Упр. 2.7. Годятся дословно те же аргументы, что и в упр. 1.8.

Существование. Если f неприводим, то сам он и является своим разложением. Если f приводим, то он раскладывается в произведение 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, в конце концов получится требуемое разложение.

Единственность. Для неприводимого $p \in \Bbbk[x]$ и любого $g \in \Bbbk[x]$ имеется следующая альтернатива: либо $\operatorname{нод}(p,g) = \lambda p$, где $\lambda \in \Bbbk^\times$ — ненулевая константа, и в этом случае g делится на p, либо $\operatorname{нод}(p,g) = 1$, и тогда g взаимно прост с p. Пусть все сомножители в равенстве $p_1 \ldots p_k = q_1 \ldots q_m$ неприводимы. Поскольку $\prod q_i$ делится на p_1, многочлен p_1, не может быть

[1] См. сл. 1.1 на стр. 30.
[2] См. n° 1.5.4 на стр. 32.

взаимно прост с каждым q_i в силу лем. 1.3 на стр. 27. Поэтому найдётся q_i, делящийся на p_1. После надлежащей перенумерации можно считать, что это q_1. Так как q_1 неприводим, $q_1 = \lambda p_1$, где λ — ненулевая константа. Сокращаем первый множитель и повторяем рассуждение.

Упр. 2.8. При умножении любой из строк таблицы $\begin{pmatrix} p & r & s \\ q & u & w \end{pmatrix}$ на ненулевую константу равенства $p = rf + sg$, $q = uf + wg$ сохраняются, а многочлен $rw - us$ умножается на эту константу. Если заменить любую строку таблицы на её сумму с другой строкой, умноженной на любой многочлен, равенства $p = rf + sg$, $q = uf + wg$ сохранятся, а многочлен $rw - us$ вообще не поменяется (ср. с упр. 1.6 на стр. 26). Пусть в итоговой таблице

$$\begin{pmatrix} d' & h_1 & h_2 \\ 0 & m_1 & m_2 \end{pmatrix}$$

$h_1 m_2 - h_2 m_1 = \delta \in \Bbbk^\times$. Умножая это равенство на f и на g и пользуясь тем, что $d' = fh_1 + gh_2$, а $fm_1 = -gm_2$, получаем

$$\delta f = fh_1 m_2 - fh_2 m_1 = fh_1 m_2 + gh_2 m_2 = d' m_2$$
$$\delta g = gh_1 m_2 - gh_2 m_1 = -fh_1 m_1 - gh_2 m_1 = -d' m_1 .$$

Поэтому $f = d' m_2 \delta^{-1}$ и $g = -d' m_1 \delta^{-1}$ делятся на d'. Для любого $q = fs = gt$ из равенства

$$\delta q = qh_1 m_2 - qh_2 m_1 = gth_1 m_2 - fsh_2 m_1 = -c'(th_1 + sh_2),$$

где $c' = fm_1 = -gm_2$, заключаем, что $q = -c'(th_1 + sh_2)\delta^{-1}$ делится на c'.

Упр. 2.9. Если многочлен степени $\leqslant 3$ приводим, то у него есть делитель первой степени, корень которого будет корнем исходного многочлена.

Упр. 2.11. См. упр. 0.9 на стр. 11.

Упр. 2.12. Вложение $\varphi : \Bbbk \hookrightarrow \Bbbk[x]/(x-\alpha)$ в качестве констант сюръективно, 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. 2.13. 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. 2.14. Ответ: $(1+\vartheta)^{-1} = -\vartheta$.

Упр. 2.15. Решение этой задачи опирается на теор. 2.3 на стр. 51 и теор. 2.4 на стр. 52. Обозначим через $\mathbb{F}_q$ конечное поле из q элементов[1]. Пусть $f \in \mathbb{F}_q[x]$ неприводим. Из доказательства теор. 2.1 на стр. 45 вытекает, что существует такое конечное поле $\mathbb{F}_r \supset \mathbb{F}_q$, что f полностью раскладывается на линейные множители в $\mathbb{F}_r[x]$. Так как поле $\mathbb{F}_r$ состоит из корней многочлена $g = x^r - x$, этот многочлен имеет общие корни с f, откуда нод$(f, g) \neq 1$ в $\mathbb{F}_q[x]$. Так как f неприводим, $g \vdots f$ в $\mathbb{F}_q[x]$. А поскольку g сепарабелен, f тоже сепарабелен.

[1] Согласно теор. 2.3 и теор. 2.4 такое поле единственно с точностью до изоморфизма и состоит из корней многочлена $x^q - x$ в таком расширении простого подполя поля $\mathbb{F}_q$, над которым этот многочлен полностью раскладывается на линейные множители.

Упр. 2.17. Число $\zeta = \cos(2\pi/5) + i \cdot \sin(2\pi/5)$ является корнем многочлена

$$z^5 - 1 = (z-1)(z^4 + z^3 + z^2 + z + 1)\,.$$

Уравнение $z^4 + z^3 + z^2 + z + 1 = 0$ можно решить в радикалах, деля обе части на z^2 и вводя новую переменную $t = z + z^{-1}$.

Упр. 2.18. Пусть $\zeta = \cos(2\pi/n) + i\sin(2\pi/n)$ — первообразный корень с наименьшим положительным аргументом, и $\xi = \zeta^k$. Так как равенство $\zeta^m = \xi^x$ означает, что $m = kx + ny$ для некоторого $y \in \mathbb{Z}$, среди целых степеней корня ξ встречаются те и только те степени первообразного корня ζ, которые делятся на нод(k, n).

Упр. 2.19. См. листок $2\frac{1}{2}$.

Упр. 2.22. Конечное поле $\mathbb{F}$ характеристики p является векторным пространством над своим простым подполем $\mathbb{F}_p \subset \mathbb{F}$, и в нём имеются такие векторы $v_1, \ldots, v_m$, что любой вектор $w \in \mathbb{F}$ линейно выражается через них в виде $w = x_1 v_1 + \ldots + x_m v_m$, где все $x_i \in \mathbb{F}_p$. Удаляя из набора $v_1, \ldots, v_m$ все векторы, которые линейно выражаются через оставшиеся, мы получим такой набор векторов $\{e_1, \ldots, e_n\} \subset \{v_1, \ldots, v_m\}$, через который каждый вектор $w \in \mathbb{F}$ выражается единственным способом, так как равенство $x_1 e_1 + \ldots + x_n e_n = y_1 e_1 + \ldots + y_n e_n$, в котором $x_i \neq y_i$ для какого-нибудь i, позволяет выразить e_i через остальные векторы как $e_i = \sum_{\nu \neq i} e_\nu (y_\nu - x_\nu)/(x_i - y_i)$, что невозможно. Коль скоро каждый элемент поля $\mathbb{F}$ однозначно записывается в виде $x_1 e_1 + \ldots + x_n e_n$, где каждый коэффициент x_i независимо принимает p значений, мы заключаем, что $|\mathbb{F}| = p^n$.

Упр. 2.23. См. доказательство теоремы Эйлера из прим. 1.6 на стр. 29.

Упр. 2.24. Отображение $\mathrm{ev}_\zeta \colon \mathbb{F}_p[x] \to \mathbb{F}$, $f \mapsto f(\zeta)$, является гомоморфизмом колец. Поскольку поле $\mathbb{F}$ конечно, а кольцо многочленов $\mathbb{F}_p[x]$ бесконечно, у этого гомоморфизма ненулевое ядро. Многочлен g — это приведённый многочлен минимальной степени в $\ker \mathrm{ev}_\zeta$. Если $g(x) = h_1(x)\,h_2(x)$, то $h_1(\zeta) = 0$ или $h_2(\zeta) = 0$, что по выбору g невозможно при $\deg h_1, \deg h_2 < \deg g$. Пусть $f(\zeta) = 0$ для $f = gh + r$, где $\deg r < \deg g$ или $r = 0$. Подставляя $x = \zeta$, получаем $r(\zeta) = 0$, откуда $r = 0$.

Упр. 3.1. Воспользуйтесь лем. 3.1.

Упр. 3.2. По теор. 3.1 на стр. 55 эпиморфизм $\pi \colon K = \mathbb{Z}/(30) \twoheadrightarrow \mathbb{Z}/(15)$, $[n]_{30} \mapsto [n]_{15}$, раскладывается в композицию гомоморфизма $\iota_S \colon K \to KS^{-1}$ и гомоморфизма

$$\pi_S \colon KS^{-1} \twoheadrightarrow \mathbb{Z}/(15)\,, \quad [m]_{30}/[2^k]_{30} \mapsto [m]_{15}[2^k]_{15}^{-1}\,,$$

сюръективного в силу сюръективности π. Если $[m]_{30}/[2^k]_{30} \in \ker \pi_S$, то $[m]_{15} = 0$, а значит, $[m]_{30}/[2^k]_{30} = [2m]_{30}/[2^{k+1}]_{30} = 0$ в KS^{-1}. Тем самым, $\ker \pi_S = 0$ и π_S инъективен.

Упр. 3.4. По правилу дифференцирования композиции $\bigl(f^m\bigr)' = m f^{m-1} f'$, откуда

$$\frac{d}{dx}(1-x)^{-m} = \frac{d}{dx}\left(\frac{1}{1-x}\right)^m = m(1-x)^{-(m+1)}\,.$$

Нужная формула получается отсюда по индукции.

Упр. 3.5. Первое равенство вытекает и правила дифференцирования сложной функции[1], второе доказывается дифференцированием обеих частей.

[1] См. формулу (2-8) на стр. 39.

Упр. 3.9. Ответы: $a_1 = \frac{1}{2}$, $a_2 = \frac{1}{6}$, $a_3 = 0$, $a_4 = -\frac{1}{30}$, $a_5 = 0$, $a_6 = \frac{1}{42}$, $a_7 = 0$, $a_8 = -\frac{1}{30}$, $a_9 = 0$, $a_{10} = \frac{5}{66}$, $a_{11} = 0$, $a_{12} = -\frac{691}{2730}$,

$$S_4(n) = n(n+1)(2n+1)(3n^2+3n-1)/30$$
$$S_5(n) = n^2(n+1)^2(2n+1)(2n^2+2n-1)/12$$
$$S_{10}(1000) = 91\,409\,924\,241\,424\,243\,424\,241\,924\,242\,500\,.$$

Упр. 3.10. Подставьте $t = 1$ в $(m+1)\,S_m(t) = (a^{\downarrow} + t)^{m+1} - a_{m+1}$.

Упр. 4.1. Импликации (а)⇒(б)⇒(в) очевидны. Если I содержит обратимый элемент, то среди его кратных есть единица, кратные которой исчерпывают всё кольцо.

Упр. 4.2. Первое очевидно, второе вытекает из того, что суммы $b_1a_1 + \ldots + b_ma_m$, где $a_i \in M$, $b_i \in K$, лежат во всех идеалах, содержащих M.

Упр. 4.3. Если a и b являются старшими коэффициентами многочленов f и g из идеала I, и $\deg f = m$, а $\deg g = n$, где $m \geqslant n$, то $a + b$ либо нуль, т. е. является старшим коэффициентом нулевого многочлена, либо является старшим коэффициентом многочлена $f + x^{m-n}g \in I$ степени m. Аналогично, для любого $\alpha \in K$ произведение αa является старшим коэффициентом многочлена $\alpha f(x) \in I$ степени m.

Упр. 4.4. Повторите доказательство теор. 4.1, следя за младшими коэффициентами вместо старших.

Упр. 4.6. Обозначим через I_0 идеал, образованный всеми аналитическими функциями[1], обращающимися в нуль на множестве $\mathbb{Z} \subset \mathbb{C}$, а через I_k — идеал всех функций, обращающихся в нуль на множестве $\mathbb{Z} \smallsetminus \{1,\ 2,\ \ldots\ ,\ k\}$. Убедитесь, что $\sin(2\pi z)/\prod_{\alpha=1}^{k}(z-\alpha) \in I_k \smallsetminus I_{k-1}$, откуда $I_k \subsetneq I_{k+1}$.

Упр. 4.7. 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. 0.9: 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 идеал вместе с каждым элементом содержит и все его кратные); таким образом, $[a' + b']I = [a + b]_I$ и $[a'b']_I = [ab]_I$.

Упр. 4.8. Возьмите в качестве J^* объединение всех идеалов из M.

Упр. 4.9. В (а) всякий идеал в $\mathbb{C}[x]$ является главным. Если факторкольцо $\mathbb{C}[x]/(f)$ не имеет делителей нуля, то многочлен f неприводим. Над полем $\mathbb{C}$ неприводимые многочлены исчерпываются линейными, поэтому $f(x) = x - p$ для некоторого $p \in \mathbb{C}$ и $(f) = (x - p) = \ker \mathrm{ev}_p$. В (б) с помощью леммы о конечном покрытии докажите, что для любого идеала I в кольце непрерывных функций $[0, 1] \to \mathbb{R}$ найдётся точка $p \in [0, 1]$, в которой все функции из I обращаются в нуль, что даст включение $I \subset \ker \mathrm{ev}_p$. В (в) подойдёт главный идеал $\mathfrak{m} = (x^2 + 1)$.

Упр. 4.11. Если в каждом идеале I_k есть элемент $x_k \in I_k \smallsetminus \mathfrak{p}$, то произведение этих элементов $x_1 \ldots x_m \in \bigcap I_k \subset \mathfrak{p}$, что противоречит простоте $\mathfrak{p}$.

[1] Функция $\mathbb{C} \to \mathbb{C}$ называется *аналитической*, если она задаётся сходящимся всюду в $\mathbb{C}$ степенным рядом из $\mathbb{C}[\![z]\!]$.

Упр. 4.12. Рассмотрим эпиморфизм факторизации $\pi\colon K \twoheadrightarrow K/I$. 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. 4.13. В (в) и (г) для любого $z \in \mathbb{C}$ в рассматриваемом кольце существует такой элемент w, что $|z-w|<1$. Взяв такой w для $z=a/b$, заключаем, что $|a-bw|<|b|$.

Упр. 4.14. Если $\exists\ b^{-1}$, то $v(ab) \leqslant v(abb^{-1}) = v(a)$. Наоборот, если $v(ab)=v(a)$, то деля a на ab с остатком, получаем $a = abq + r$, где либо $v(r) < v(ab) = v(a)$, либо $r=0$. Из равенства $r = a(1-bq)$ вытекает, что либо $v(r) \geqslant v(a)$, 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. 4.15. Если $b=ax$ и $a=by=axy$, то $a(1-xy)=0$, откуда $xy=1$.

Упр. 4.16. 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. 4.17. По аналогии с комплексными числами, назовём *сопряжённым* к числу $\vartheta = a + b\sqrt{5}$ число $\overline{\vartheta} = a - b\sqrt{5}$, а целое число $\|\vartheta\| \stackrel{\text{def}}{=} \vartheta\cdot\overline{\vartheta} = a^2 - 5b^2$ назовём *нормой* числа ϑ. Легко видеть, что $\overline{\vartheta_1\vartheta_2} = \overline{\vartheta}_1\cdot\overline{\vartheta}_2$, откуда $\|\vartheta_1\vartheta_2\| = \vartheta_1\vartheta_2\overline{\vartheta}_1\overline{\vartheta}_2 = \|\vartheta_1\|\cdot\|\vartheta_2\|$. Поэтому $\vartheta \in \mathbb{Z}[\sqrt{5}]$ обратим тогда и только тогда, когда $\|\vartheta\| = \pm1$, 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 при $\|x\| = \|y\| = \pm2$. Но элементов нормы ±2 в $\mathbb{Z}[\sqrt{5}]$ нет, так как равенство $a^2 - 5b^2 = \pm2$ при редукции по модулю 5 превращается в равенство $a^2 = \pm2$ в поле $\mathbb{F}_5$, где числа ±2 не являются квадратами.

Упр. 4.18. Из равенства $z_1z_2 = 1$ вытекает равенство $|z_1|\cdot|z_2| = 1$. Так как $|z|^2 \in \mathbb{N}$ для всех $z\in\mathbb{Z}[i]$, гауссово число z может быть обратимо только если $|z|=1$.

Упр. 4.19. Пусть $n = p_1^{\alpha_1}\dots p_s^{\alpha_r}q_1^{\beta_1}\dots q_s^{\beta_s}$, где $p_i, q_j \in \mathbb{N}$ — попарно разные простые числа, причём p_i представляются в виде суммы двух квадратов, а q_j — нет, т. е. все $q_j \equiv 3 \pmod 4$, а все p_i — нет. Тогда разложение n на простые множители в области $\mathbb{Z}[i]$ имеет вид

$$n = \prod\nolimits_i (x_i+iy_i)^{\alpha_i}(x_i-iy_i)^{\alpha_i}\prod\nolimits_j q_j^{\beta_j},\ \text{где } q_j\in\mathbb{N}.$$

Если все β_j чётные, то $n=(a+ib)(a-ib)=a^2+b^2$ для $a+ib = \prod_i(x_i+iy_i)^{\alpha_i}\prod_j q_j^{\beta_j/2}$. Наоборот, пусть $n=a^2+b^2=(a+ib)(a-ib)$, и разложение гауссова числа $a+ib$ на простые множители в $\mathbb{Z}[i]$ имеет вид $a+bi=\prod_k \ell_k^{\gamma_k}$. Тогда разложение числа n на простые множители в $\mathbb{Z}[i]$ имеет вид $\prod_k \ell_k^{\gamma_k}\overline{\ell}_k^{\gamma_k}$, и все вещественные простые множители входят в него в чётных степенях.

Упр. 4.22. Это следует из равенства $a_0q^n + a_1q^{n-1}p + \ \dots\ + a_{n-1}qp^{n-1} + a_np^n = 0$

Упр. 4.23. Ответ: $(x^2-2x+2)(x^2+2x+2)$.

Упр. 5.1. 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 $x\cdot 0 = x(0\cdot v) = (x\cdot 0)\cdot v = 0\cdot v = 0$. 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. 5.2. Не вполне очевидно, разве что, самое первое равенство. Оно вытекает из коммутативности умножения в кольце K: $(vy)x = x(vy) = x(yv) = (xy)v = v(xy) = v(yx)$.

Упр. 5.4. $\varphi\psi(xu+yw) = \varphi(x\psi(u)+y\psi(w)) = x\varphi\psi(u) + y\varphi\psi(w)$.

Упр. 5.5. Сложите равенства $\varphi(\lambda u + \mu w) = \lambda\varphi(u) + \mu\varphi(w)$ и $\psi(\lambda u + \mu w) = \lambda\psi(u) + \mu\psi(w)$, а также умножьте первое из них на x.

Упр. 5.6. Ядро и образ любого гомоморфизма абелевых групп являются абелевыми подгруппами согласно n° 1.5 на стр. 30. Если гомоморфизм K-линеен, то обе эти подгруппы выдерживают умножение на элементы из K, поскольку $x\varphi(u) = \varphi(xu)$ и $\varphi(u) = 0 \Rightarrow \varphi(xu) = x\varphi(u) = 0$.

Упр. 5.7. Сопоставьте семейству гомоморфизмов $\varphi_\mu : N \to M_\mu$, в котором лишь конечное число ненулевых гомоморфизмов, отображение $\bigoplus_{\mu\in\mathcal{M}} \varphi_\mu : N \to \bigoplus_{\mu\in\mathcal{M}} M_\mu$, переводящее вектор $u \in N$ в семейство векторов $\bigl(\varphi_\mu(u)\bigr)_{\mu\in\mathcal{M}}$ с конечным числом ненулевых членов.

Упр. 5.8. Пусть $A \not\subseteq B$ — две подгруппы в абелевой группе. Выберем $a \in A \smallsetminus B$. Если $A \cup B$ является подгруппой, то $\forall\, b \in B\ a + b \in A \cup B$, но $a + b \notin B$, поскольку $a \notin B$. Следовательно, $a + b \in A$, откуда $b \in A$, т. е. $B \subseteq A$.

Упр. 5.9. Все проверки проводятся дословно также, как для классов вычетов по модулю идеала коммутативного кольца (ср. с упр. 4.7 на стр. 70).

Упр. 5.10. Так как каждый вектор $w \in M$ имеет единственное представление в виде $w = w_N + w_L$ с $w_N \in N$ и $w_L \in L$, корректно определены K-линейные сюръекции $\pi_N : M \twoheadrightarrow N$ и $\pi_L : M \twoheadrightarrow L$, переводящие $w_N + w_L$ соответственно в w_N и в w_L. Так как $\ker\pi_N = L$ и $\ker\pi_L = N$ отображения $\iota_{\pi_N} : M/L \xrightarrow{\sim} N$ и $\iota_{\pi_L} : M/N \xrightarrow{\sim} L$ из прим. 5.9 на стр. 86 являются искомыми изоморфизмами.

Упр. 5.13. Если $x' = x+y$ и $w' = w+u$, где $y \in I$, $u \in IM$, то $[x'w'] = [xw+(xu+yw+xu)] = [xw]$, так как сумма в круглых скобках лежит в IM.

Упр. 5.14. Поскольку подмодули N_i линейно порождают M, подмодули IN_i линейно порождают IM. Очевидно, что $IN_i \subset N_i \cap IM$, и при этом каждый подмодуль $N_i \cap IM$ имеет нулевое пересечение с суммой подмодулей $N_\nu \cap IM$ по всем $\nu \neq i$, ибо $N_i \cap \sum_{\nu\neq i} N_\nu = 0$.

Упр. 5.18. Ответ:

$$[E_{ij}, E_{k\ell}] \stackrel{\text{def}}{=} E_{ij}E_{k\ell} - E_{k\ell}E_{ij} = \begin{cases} E_{ii} - E_{jj} & \text{при } j = k \text{ и } i = \ell \\ E_{i\ell} & \text{при } j = k \text{ и } i \neq \ell \\ -E_{kj} & \text{при } j \neq k \text{ и } i = \ell \\ 0 & \text{в остальных случаях.} \end{cases}$$

Упр. 5.20. Прямая проверка:

$$(AB)^\vee = \left(\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}\begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}\right)^\vee = \begin{pmatrix} a_{11}b_{11} + a_{12}b_{21} & a_{11}b_{21} + a_{12}b_{22} \\ a_{21}b_{11} + a_{22}b_{21} & a_{21}b_{21} + a_{22}b_{22} \end{pmatrix}^\vee =$$
$$= \begin{pmatrix} a_{21}b_{21} + a_{22}b_{22} & -a_{11}b_{21} - a_{12}b_{22} \\ -a_{21}b_{11} - a_{22}b_{21} & a_{11}b_{11} + a_{12}b_{21} \end{pmatrix} = \begin{pmatrix} b_{22} & -b_{12} \\ -b_{21} & b_{11} \end{pmatrix}\begin{pmatrix} a_{22} & -a_{12} \\ -a_{21} & a_{11} \end{pmatrix} = B^\vee A^\vee$$

Упр. 5.25. Оба равенства проверяются прямым вычислением.

Упр. 6.1. $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}^{-1} = \frac{1}{\Delta}\begin{pmatrix} \delta & -\beta \\ -\gamma & \alpha \end{pmatrix}$ как мы видели в прим. 5.15 на стр. 92.

Упр. 6.3. Если матрица D диагональна, то матрица DA (соотв. AD) получается из матрицы A умножением её i-й строки (соотв. i-го столбца) на диагональный элемент d_{ii} матрицы D. Поэтому равенство $AD = DA = E$ равносильно тому, что $a_{ii}d_{ii} = 1$ и $a_{ij} = 0$ при всех $i \neq j$.

Упр. 6.4. Последовательно заменяя в данном столбце пары ненулевых элементов a, b по лем. 6.1 на стр. 102 парами нод$(a, b), 0$, получаем столбец в котором отличен от нуля ровно один элемент $d \in K$, равный нод элементов исходного столбца. Если матрица A обратима, то её столбцы $(a_1, \dots, a_n)$ образуют базис в K^n, причём $a_j = de_i$, где $(e_1, \dots, e_n)$ — стандартный базис в K^n. Пусть стандартный базисный вектор e_i выражается через столбцы матрицы A по формуле $e_i = \sum x_\nu a_\nu$. Тогда $a_j - \sum dx_\nu a_\nu = 0$, и вектор a_j входит в эту линейную комбинацию с коэффициентом $1 - dx_j$, откуда $dx_j = 1$.

Упр. 6.6. Векторы w_1, w_2 — это первые два вектора набора $\boldsymbol{w} = \boldsymbol{a}R$, где матрица $R = R_1R_2R_3R_4$ задаёт совершённые в прим. 6.5 на стр. 112 преобразования столбцов:

$$R_1 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

делает четвёртый столбец первым,

$$R_2 = \begin{pmatrix} 1 & 2 & -3 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

прибавляет ко 2-у и 3-у столбцам 1-й, умноженный на 2 и на -3,

$$R_3 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$$

записывает во 2-й столбец сумму к 3-го и 4-го, а в 3-й столбец — бывший 2-й,

$$R_4 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & -8 & -3 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

отнимает из 3-го и 4-го столбцов 2-й, умноженный на 8 и на 3. Вычисляя произведение[1], получаем

$$R = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & -8 & -3 \\ 0 & 1 & -8 & -2 \\ 1 & -3 & 26 & 9 \end{pmatrix},$$

откуда $w_1 = a_4$ и $w_2 = a_2 + a_3 - 3a_4$.

Упр. 6.7. Если $x_1w_1 = 0$ и $x_2w_2 = 0$ для ненулевых $x_1, x_2 \in K$, то $x_1x_2(w_1 \pm w_2) = 0$ и $x_1x_2 \neq 0$, так как в K нет делителей нуля, и $x_1(yw_1) = x_2(yw_2) = 0$ для всех $y \in K$.

[1] Или, что тоже самое, применяя указанные четыре преобразования к единичной матрице 4×4.

Упр. 6.8. Если $p^{k_1}w_1 = 0$ и $p^{k_2}w_2 = 0$, то $p^{k_1+k_2}(w_1 \pm w_2) = 0$ и $p^{k_1}yw_1 = 0$ для всех $y \in K$. Равенство $p^{k_1}[w] = [0]$ в $M/\mathrm{Tors}_p(M)$ означает, что $p^{k_1}w \in \mathrm{Tors}_p(M)$, т. е. $p^{k_2}p^{k_1}w = 0$ для некоторого $k_2 \in \mathbb{N}$, откуда $p^{k_1+k_2}w = 0$ и $w \in \mathrm{Tors}_p(M)$, т. е. $[w] = [0]$. Если $w \in \mathrm{Tors}_p(M) \setminus N$, то класс $[w] \in M/N$ является ненулевым элементом p-кручения.

Упр. 6.9. Класс $[p^{\nu_i-k}x] \in K/(p^{\nu_i})$ лежит в $\ker \varphi_i^k$, поскольку $p^k[p^{\nu_i-k}x] = [p^{\nu_i}x] = [0]$. Если $x' = x + py$, то $p^{\nu_i-k}x' = p^{\nu_i-k}x + p^{\nu_i-k+1}y$ и класс $[p^{\nu_i-k+1}y] \in K/(p^{\nu_i})$ лежит в $\ker \varphi_i^{k-1}$, так как $p^{k-1}[p^{\nu_i-k+1}y] = [p^{\nu_i}y] = [0]$. Линейность отображения очевидна. Оно сюрьективно, поскольку каждый класс $[y] \in K/(p^{\nu_i})$, такой что $[p^k y] = [0]$, имеет $y = p^{\nu_i-k}x$ для некоторого $x \in K$ в силу того, что $p^k x$ делится на p^{ν_i} в факториальном кольце K если и только если x делится на p^{ν_i-k}. Ядро отображения нулевое по той же причине: если класс $[p^{\nu_i-k}x] \in K/(p^{\nu_i})$ лежит в $\ker \varphi_i^{k-1}$, то $p^{k-1}p^{\nu_i-k}x = p^{\nu_i-1}x$ делится на p^{ν_i}, а значит $x \vdots p$ и класс $[x] \in K/(p)$ нулевой.

Упр. 7.1. В $\mathbb{Z}/(4)$ есть элемент порядка 4, а в $\mathbb{Z}/(2) \oplus \mathbb{Z}/(2)$ такого элемента нет.

Упр. 7.2. Имеется ровно три таких подгруппы. Они порождаются элементами $(1, [0]_3)$, $(1, [1]_3)$ и $(1, [-1]_3)$.

Упр. 7.3. Каждая ненулевая собственная подгруппа в $\mathbb{Z}$ имеет вид $(n) = \{x \in \mathbb{Z} \mid x \vdots n\}$, где $n \geqslant 2$, а каждая ненулевая собственная подгруппа в $\mathbb{Z}/(p^m)$ имеет вид $(p^k) = \{[x] \in \mathbb{Z}/(p^m) \mid x \vdots p^k\}$, где $1 \leqslant k \leqslant m$.

Упр. 7.4. Так как любой вектор $b \in B$ представляется в A как $b = v + c + u$, где $u \in U$, $c \in$, $u \in U$, выполняется равенство $b = \pi(b) = \pi(v + c + u) = v + \pi(u)$. Поэтому $B = V + W$. Если $b \in V \cap W$, то $b = \pi(u)$ для некоторого $u \in U$, и $\pi(b - u) = b - \pi(u) = 0$. Поэтому $b - u \in \ker \pi = C$, что возможно только при $b = u = 0$.

Упр. 7.6. Умножая $\mathbb{Q}$-линейную комбинацию векторов на общий знаменатель всех её коэффициентов, получаем $\mathbb{Z}$-линейную комбинацию тех же векторов.

Упр. 7.9. Верхней гранью цепи из $\mathcal{S}'$ является объединение всех модулей цепи.

Упр. 7.10. Пусть $w = u + v$. Тогда $fw = fu + fv$ и $fv \in V$. Поэтому $\pi(fw) = fu = f\pi(w)$.

Упр. 7.11. Пусть $S \subset W$ прост и $\pi(S) \neq 0$. Для любого K-подмодуля $M \subset \pi(S)$ пересечение

$$S \cap \pi^{-1}(M) = \{s \in S \mid \pi(s) \in M\}$$

является K-подмодулем в S: если $\pi(s) \in M$, то $\pi(fs) = f\pi(s) \in M$ для всех $f \in K$ и $s \in S$. Так как в S нет нетривиальных собственных подмодулей, их нет и в $\pi(S)$.

Упр. 7.12. Верхней гранью цепи из $\mathcal{S}$ является объединение или, что то же самое, прямая сумма всех модулей цепи.

Упр. 7.13. Воспользуйтесь рассуждением, которое использовалось при доказательстве импликации (3) ⇒ (1) в предл. 7.1 на стр. 122.

Упр. 8.1. $\max \ell(g) = n(n-1)/2$ достигается на единственной перестановке $(n, n-1, \ldots, 1)$.

Упр. 8.2. Индукция по n. Каждая перестановка $g = (g_1, \ldots, g_n)$ является композицией $g = \sigma \circ g'$ транспозиции σ, переставляющей между собою элементы n и g_n, и перестановки $g' = \sigma \circ g$, оставляющей элемент n на месте. По индукции, g' раскладывается в композицию транспозиций, не затрагивающих элемент n.

Упр. 8.3. Когда 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, если не ин-

версна[1]. Для тасующей перестановки $(i_1, \dots, i_k, j_1, \dots, j_m)$ нити, выходящие из $i_1, \dots, i_k$ верхней строки не пересекаются между собою и пересекают, соответственно, $i_1 - 1, i_2 - 2, \dots, i_k - k$ начинающихся левее нитей, выходящих из j-точек верхней строки, причём все эти нити не пересекаются между собою.

Упр. 8.4. Если g является композицией транспозиций $\sigma_k \sigma_{k-1} \dots \sigma_1$, то $g^{-1} = \sigma_1 \dots \sigma_k$ является произведением тех же транспозиций в противоположном порядке.

Упр. 8.6. При чётном n центр алгебры $K\langle \xi_1, \dots, \xi_n \rangle$ линейно порождается мономами чётных степеней, при нечётном n — мономами чётных степеней и старшим мономом $\xi_1 \wedge \dots \wedge \xi_n$, имеющим в этом случае нечётную степень.

Упр. 8.8. Беря определители в равенстве $C \cdot C^{-1} = E$, получаем $\det(C) \cdot \det(C^{-1}) = \det E = 1$.

Упр. 8.9. Это следует из равенств $\det A = \det A^t$ и $(AB)^t = B^t A^t$.

Упр. 8.10. Если все $A_{ij} = 0$, положим $A = 0$, если, скажем, $A_{12} \neq 0$, положим

$$A = \begin{pmatrix} 1 & 0 & -A_{23}/A_{12} & -A_{24}/A_{12} \\ 0 & A_{12} & A_{13} & A_{14} \end{pmatrix}.$$

Обратите внимание, что равенство

$$A_{34} = \det \begin{pmatrix} -A_{23}/A_{12} & -A_{24}/A_{12} \\ A_{13} & A_{14} \end{pmatrix}$$

эквивалентно соотношению Плюккера из форм. (8-20) на стр. 137.

Упр. 8.11. Если стоящие в левых частях уравнений (8-25) линейные формы

$$\alpha_i = \left(a_{i,0}, a_{i,1}, \dots, a_{i,n}\right) \in \mathbb{k}^{n+1*}$$

линейно независимы, то по лемме о замене[2] ими можно заменить подходящие n ковекторов стандартного базиса в $\mathbb{k}^{n+1*}$. Пусть это будут последние n базисных ковекторов. Коль скоро ковектор $(1, 0, \dots, 0)$ и ковекторы $\alpha_1, \dots, \alpha_n$ образуют базис, определитель, составленный из строк их координат, отличен от нуля. Раскладывая его по строке $(1, 0, \dots, 0)$, видим, что он равен A_0, откуда $A_0 \neq 0$. Если же строки матрицы A линейно зависимы, то все $A_i = 0$.

Упр. 8.12. Это вытекает из прим. 8.6 на стр. 137. Полагая в форм. (8-21) на стр. 137 $x = 1$, $y = t$ и $B = E$, получаем разложение

$$\det(tE + A) = t^n + \sum_{m=1}^{n} t^{n-m} \sum\nolimits_{\#I=m} a_{II} = \\ = t^n + t^{n-1} \sum\nolimits_i a_{ii} + t^{n-1} \sum\nolimits_{i<j} (a_{ii}a_{jj} - a_{ij}a_{ji}) + \dots + t \sum\nolimits_i a_{\overline{ii}} + \det A,$$

где коэффициент при t^{n-k} равен сумме определителей всех $k \times k$ подматриц в A с главной диагональю, содержащейся в главной диагонали матрицы A.

Упр. 8.13. $f(C)g(C) = \sum_{k=0}^{m+n} \sum_{i+j=k} C^i A_i C^j B_j = \sum_{k=0}^{m+n} \sum_{i+j=k} C^{i+j} A_i B_j = \sum_{k=0}^{m+n} C^k \sum_{i+j=k} A_i B_j =$
$= \sum_{k=0}^{m+n} C^k H_k = h(C)$.

[1] На самом деле картинку всегда можно нарисовать так, чтобы количества точек пересечения в этих двух случаях равнялись 1 и 0 соответственно

[2] См. лемму 4.2 на стр. 48 лекции http://gorod.bogomolov-lab.ru/ps/stud/geom_ru/2122/lec_04.pdf.

Упр. 8.14. Если $f = h\varphi$, $g = h\psi$, где $\deg h > 0$, то $\deg\varphi < n$, $\deg\psi < m$ и $f\psi - g\varphi = 0$. Если же f и g взаимно просты, то из равенства $fh_1 = -gh_2$ вытекает, что $g \mid h_1$, а $f \mid h_2$, что невозможно для ненулевых h_1, h_2 с $\deg h_1 < m$ и $\deg h_2 < n$.

Упр. 9.1. Если отождествить $\mathbb{R}[t]/(t^2+1)$ с полем $\mathbb{C}$, отправив классы $[1]$ и $[t]$ в 1 и i соответственно, умножение на класс $[t]$ превратится в умножение на i, т. е. в поворот на угол $\pi/2$, который не переводит никакое одномерное векторное подпространство в себя.

Упр. 9.2. Пусть $\Bbbk[t]/\left(t^n\right) = U \oplus W$, где U и W переводятся в себя умножением на $[t]$. Оба этих подпространства не могут целиком содержаться в образе оператора умножения на $[t]$, так как иначе их сумма тоже бы в нём содержалась. Поэтому в одном из них, пусть это будет U, имеется класс $[g]$ многочлена g с ненулевым свободным членом. Тогда классы $[t^{n-1}g], \ldots, [tg], [g] \in U$ выражаются через базис $[1], [t], \ldots, [t^{n-1}]$ пространства $\Bbbk[t]/(t^n)$ при помощи верхнетреугольной матрицы, на диагонаи которой всюду стоит ненулевой свободный член многочлена g. Следовательно, эти классы тоже образуют базис в $\Bbbk[t]/(t^n)$, и значит, содержащее их подпространство U совпадает со всем пространством $\Bbbk[t]/(t^n)$.

Упр. 9.3. Разложите каждое пространство $(F|_{U_i}, U_i)$ по форм. (9-1) на стр. 144. В силу единственности такого разложения прямая сумма полученных разложений является разложением исходного пространства (F, V).

Упр. 9.4. Коэффициенты $g_i \in \Bbbk^n$ неполного частного $g(t)$ от деления $h(t)$ на $tE - A$ вычисляются рекурсивно по формулам $g_{m-1} = h_m$, $g_{i-1} = h_i + Ag_i$ при $i \leqslant m-1$. Остаток $r = h(t) - (tE - A)\,g(t) \in \Bbbk^n$ не зависит от t. Подставляя $t = A$, что законно, ибо A коммутирует[1], заключаем, что $r = h(A)$.

Упр. 9.5. $\det(tE - C^{-1}AC) = \det(tC^{-1}EC - C^{-1}AC) = \det\left(C^{-1}(tE-A)C\right) = \det C^{-1}\cdot\det(tE-A)\cdot\det C = {} = \det(tE - A)$.

Упр. 9.6. Пусть $f = t^n + a_1 t^{n-1} + \ldots + a_n$. Напишите матрицу F оператора умножения на класс $[t]$ в факторкольце $\Bbbk[x]/(f)$ в базисе $[t^{n-1}], [t^{n-2}], \ldots, [t], [1]$ и разложите $\det(tE - F)$ по первому столбцу.

Упр. 9.7. Пусть $f(t) = \mu_{v,F}(t)g(t) + r(t)$, где либо $r = 0$, либо $\deg r < \deg\mu_{v,F}$. Если $f(F) = 0$, то $r(F)v = 0$, что невозможно для ненулевого r с $\deg r < \deg\mu_{v,F}$ по определению многочлена $\mu_{v,F}$. Поэтому $r = 0$.

Упр. 9.8. Если оператор $q(F)$ аннулирует все векторы из какого-нибудь линейного порождающего V множества, то он аннулирует любой вектор из V.

Упр. 9.12. Так как любой вектор $h \in H$ представляется в V как $h = u + q + r$ с $u \in U$, $q \in Q$, $r \in R$, в U выполняется равенство $h = \pi(h) = \pi(u) + \pi(r)$, в котором $\pi(u) = u \in U$ и $\pi(r) \in W$, т. е. $U + W = H$. Если $u \in U \cap W$, то $u = \pi(r)$ для некоторого $r \in R$, и $\pi(u - r) = \pi(u) - \pi(r) = u - u = 0$, откуда $u - r \in \ker\pi = Q$, что возможно только при $u = r = 0$. Поэтому $U \cap W = 0$.

Упр. 9.13. 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. 9.14. Над алгебраически замкнутым полем всякий многочлен имеющий только один корень 0 равен t^m. Поэтому $\chi_F(t) = t^m$ и по теореме Гамильтона – Кэли $F^m = 0$.

Упр. 9.17. Разложение характеристического многочлена оператора F в виде произведения степеней попарно разных линейных форм $\chi_F(t) = \prod\limits_{\lambda\in\operatorname{Spec} F} (t-\lambda)^{N_\lambda}$ удовлетворяет условиям теор. 9.3

[1] См. упр. 8.13 на стр. 140.

с $q_i = (t-\lambda)^{N_\lambda}$, а корневые подпространства $K_\lambda = \ker(\lambda\,\mathrm{Id} - F)^{N_\lambda}$.

Упр. 9.18. Над полем $\mathbb{C}$ можно применить предл. 9.5. Над произвольным полем $\Bbbk$ оператор F с матрицей $J_n(\lambda)$ имеет вид $\lambda\mathrm{Id} + N$, где $N^n = 0$, но $N^{n-1} \neq 0$. Обратный оператор

$$F^{-1} = (\lambda\mathrm{Id} + N)^{-1} = \lambda^{-1}(\mathrm{Id} + N/\lambda)^{-1} = \lambda^{-1} - \lambda^{-2}N + \lambda^{-3}N^2 - \ldots + (-1)^{n-1}\lambda^{-n}N^{n-1}$$

имеет вид $\lambda^{-1}\mathrm{Id} + M$, где оператор $M = -\lambda^{-2}N(1 - \lambda^{-1}N + \ldots)$ тоже имеет $M^n = 0$, а $M^{n-1} = \lambda^{2(1-n)}N^{n-1} \neq 0$. Таким образом, ЖНФ оператора F^{-1} это одна клетка $J_n\left(\lambda^{-1}\right)$.

Упр. 9.20. В $\Bbbk[\![x]\!]$ квадрат ряда $\sqrt{1+x}$ равен $1 + x$, а коэффициенты при x^k для $0 \leqslant k \leqslant n$ у квадрата ряда $\sqrt{1+x}$ такие же, как и у квадрата многочлена из условия.

Упр. 9.21. Если $a^n = 0$, $b^m = 0$ и $ab = ba$, то $(a-b)^{m+n-1} = 0$ по формуле Ньютона.

Упр. 10.1. Если $fg = e$ и $gh = e$, то $f = fe = f(gh) = (fg)h = eh = h$.

Упр. 10.2. Для двух единичных элементов e' и e'' выполнены равенства $e' = e'e'' = e''$.

Упр. 10.4. Ответ: либо $r = 1$ и $\mathrm{Tors}(G) = 0$ (т. е. $G \simeq \mathbb{Z}$), либо $r = 0$ (т. е. G конечна) и каждое простое число $p \in \mathbb{N}$ присутствует в каноническом разложении

$$G = \frac{\mathbb{Z}}{\left(p_1^{n_1}\right)} \oplus \ldots \oplus \frac{\mathbb{Z}}{\left(p_\alpha^{n_\alpha}\right)}$$

не более одного раза. Доказательство аналогично доказательству предл. 9.2 на стр. 156.

Упр. 10.5. Пусть $k = dr$, $m = \mathrm{ord}(\tau) = ds$, где $\mathrm{нод}(r,s) = 1$. 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 $\mathrm{нод}(k,m) = 1$ возможно только когда r делится на m. Поэтому $r \geqslant m$, т. е. длина содержащего a цикла перестановки τ^k не меньше m.

Упр. 10.6. Ответ: $n(n-1)\ldots(n-k+1)/k$ (в числителе дроби k сомножителей).

Упр. 10.7. 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. 10.5.

Упр. 10.8. Ответ: $n!\,/\prod_{i=1}^n i^{m_i}m_i!$ (ср. с форм. (0-11) на стр. 9). Решение: сопоставим каждому заполнению диаграммы циклов λ неповторяющимися числами от 1 до n произведение независимых циклов, циклически переставляющих элементы каждой строки слева направо; получаем сюръективное отображение множества заполнений на множество всех перестановок циклового типа λ; прообраз каждой перестановки состоит из $\prod_{i=1}^n i^{m_i}m_i!$ заполнений, получающихся друг из друга независимыми циклическими перестановками элементов в каждой строке и произвольными перестановками строк одинаковой длины между собою как единого целого.

Упр. 10.9. $|1,6,3,4\rangle^{15} \cdot |2,5,8\rangle^{15} \cdot |7,9\rangle^{15} = |1,6,3,4\rangle^{-1} \cdot |7,9\rangle = (4,\ 2,\ 6,\ 3,\ 5,\ 1,\ 9,\ 8,\ 7)$

Упр. 10.14. 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. 10.15. Подсчёт для группы куба дословно тот же, что и для группы додекаэдра. Группы октаэдра и икосаэдра изоморфны группам куба и додекадра с вершинами в центрах граней октаэдра и икосаэдра соответственно.

Упр. 10.17. Зафиксируем в V какой-либо базис и сопоставим оператору $F \in \mathrm{GL}(V)$ базис, состоящий из векторов $f_i = F(e_i)$. Для выбора первого базисного вектора f_1 имеется $|V| - 1 = q^n - 1$ возможностей, для выбора второго — $|V| - |\Bbbk \cdot f_1| = q^n - q$ возможностей, для выбора третьего — $|V| - |\Bbbk \cdot f_1 \oplus \Bbbk \cdot f_2| = q^n - q^2$ возможностей и т. д.

Упр. 10.18. 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. 10.23. Проиллюстрируем рассуждение на примере икосаэдра. И собственная и полная группы транзитивно действуют на 20 его треугольных гранях. Стабилизатор грани в собственной и полной группах представляет собой собственную и полную группу треугольника на плоскости, состоящую, соответственно из 3 и из 6 преобразований. По формуле для длины орбиты получаем $|\,\mathrm{SO}_{\text{ико}}\,| = 20 \cdot 3 = 60$ и $|\,\mathrm{O}_{\text{ико}}\,| = 20 \cdot 6 = 120$.

Упр. 10.25. Равенство $h_1 g_1 = h_2 g_2$ влечёт равенства $g_2 g_1^{-1} = h_2^{-1} h_1 \in H$ и $g_1 g_2^{-1} = h_1^{-1} h_2 \in H$. С другой стороны, если один из обратных друг другу элементов $g_2 g_1^{-1}$ и $g_1 g_2^{-1}$ лежит в H, то в H лежит и второй, и $Hg_1 = H(g_2 g_1^{-1})g_2 = Hg_2$.

Упр. 10.26. $\varphi \circ \mathrm{Ad}_g \circ \varphi^{-1} \colon\ h \mapsto \varphi\big(g\,\varphi^{-1}(h)\,g^{-1}\big) = \varphi(g)\,h\,\varphi(g)^{-1}$.

Упр. 10.27. Для любой точки $x \in \mathbb{R}^n$ положим $p = \varphi^{-1}(x)$. Так как $\varphi \colon\ \mathbb{R}^n \to \mathbb{R}^n$ аффинно, $\varphi(p + v) = x + D_\varphi(v)$. Поэтому $\varphi \circ \tau_v \circ \varphi^{-1} \colon\ x \mapsto \varphi(p + v) = x + D_\varphi(v)$.

Упр. 10.29. Если $\varphi(x) \in N_2$, то $\varphi(gxg^{-1}) = \varphi(g)\varphi(x)\varphi(g)^{-1} \in N_2$ в силу нормальности $N_2 \lhd G_2$. Поэтому $N_1 = \varphi^{-1}(N_2) \lhd G_1$. Композиция сюръективных гомоморфизмов $G_1 \twoheadrightarrow G_2 \twoheadrightarrow G_2/N_2$ является сюръективным гомоморфизмом с ядром N_1.

Упр. 10.30. Поскольку S_n порождается транспозициями, подгруппа A_n порождается парами транспозиций. Но $|ij\rangle|jk\rangle = |ijk\rangle$ и $|ij\rangle|k\ell\rangle = |ijk\rangle|jk\ell\rangle$ при различных i, j, k, ℓ.

Упр. 10.31. Воспользуйтесь равенством $|ij\rangle|jk\rangle = |ij\rangle|\ell m\rangle|jk\rangle|\ell m\rangle$ для различных i, j, k, ℓ, m.

Упр. 10.32. Первый изоморфизм задаётся действием группы $\mathrm{SL}_2(\mathbb{F}_2) \simeq \mathrm{GL}_2(\mathbb{F}_2)$ на трёх ненулевых векторах координатной плоскости $\mathbb{F}_2^2$, второй — действием группы $\mathrm{PSL}_2(\mathbb{F}_3) \stackrel{\text{def}}{=} \mathrm{SL}_2(\mathbb{F}_3)/\{\pm E\}$ на четырёх одномерных векторных подпространствах в $\mathbb{F}_3^2$ или, что то же самое, действием дробно линейных преобразований $t \mapsto (at+b)/(ct+d)$, где $a, b, c, d \in \mathbb{F}_3$ и $ad \neq bc$, на четырёх точках проективной прямой $\mathbb{P}_1(\mathbb{F}_3) = \{-1, 0, 1, \infty\}$.

Упр. 10.33. Модифицируйте метод Гаусса: используя только операцию прибавления к одной из строк матрицы некоторой кратности другой строки, сначала добейтесь того, чтобы в первом столбце было хотя бы два ненулевых элемента, причём один из них стоял в первой строке, затем добейтесь того, чтобы в левом верхнем углу матрицы оказалась единица, и наконец занулите первый столбец ниже первой строки, после чего повторите процедуру со вторым столбцом и второй строкой, и т. д. Для вычисления коммутатора воспользуйтесь равенствами

$$T_{ij}^{-1}(\alpha) = (E + \alpha E_{ij})^{-1} = E - \alpha E_{ij} = T_{ij}(-\alpha)$$
$$T_{ij}(\alpha)T_{jk}(\beta) = E + E_{ij}(\alpha) + E_{jk}(\beta) + E_{ik}(\alpha\beta)$$

Упр. 10.34. Прямое вычисление:

$$(E+\alpha E_{ij})(\beta E_{ii}+\beta^{-1}E_{jj})(E-\alpha E_{ij})(\beta^{-1}E_{ii}+\beta E_{jj}) = (E+\alpha E_{ij})(E-\alpha\beta^2 E_{ij}) = E+\alpha(1-\beta^2)E_{ij}\,.$$

Упр. 10.35. Так как $\mathrm{SL}_2(\mathbb{F}_2) = \mathrm{GL}_2(\mathbb{F}_2) = S_3$, коммутанты $\mathrm{GL}_2'(\mathbb{F}_2) = \mathrm{SL}_2' = \{E, T, T^2\} \simeq A_3$, где

$$T = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \quad \text{и} \quad T^2 = T^{-1} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$

циклически переставляют ненулевые векторы $(1,0)$, $(0,1)$, $(1,1)$ пространства $\mathbb{F}_2^2$. Поскольку $(T_{ij}(\alpha), E_{ii}-E_{jj}) = T_{ij}(-\alpha)$, коммутант $\mathrm{GL}_2'(\mathbb{F}_3)$ содержит все трансвекции и равен $\mathrm{SL}_2(\mathbb{F}_3)$. Для вычисления $\mathrm{SL}_2'(\mathbb{F}_3)$ воспользуйтесь факторизацией $\mathrm{SL}_2(\mathbb{F}_3) \twoheadrightarrow \mathrm{PSL}_2(\mathbb{F}_3) \simeq A_4$ по нормальной подгруппе $\{\pm E\} \lhd \mathrm{SL}_2(\mathbb{F}_3)$. Она сюръективно отображает коммутант $\mathrm{SL}_2'(\mathbb{F}_3)$ на группу Клейна $A_4' = V_4$, состоящую независимых транспозиций двух пар точек проективной прямой

$$\mathbb{P}_1(\mathbb{F}_3) = \{(1:0), (0:1), (1:1), (1:-1)\}\,,$$

которые задаются следующими матрицами из $\mathrm{SL}_2(\mathbb{F}_3)$ с точностью до знака

$$I = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\,, \quad J = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\,, \quad K = \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix}\,.$$

Убедитесь, что $I^2 = J^2 = K^2 = -E$ и $IJ = -JI = K$, $JK = -KJ = I$, $KI = -IK = J$. Таким образом, коммутант $\mathrm{SL}_2(\mathbb{F}_3)'$ имеет порядок 8 и изоморфен группе *кватернионных единиц* $Q_8 \stackrel{\text{def}}{=} \{\pm E, \pm I, \pm J, \pm K\}$.

Упр. 11.1. Пусть $g \in A_n$, $h \in S_n \smallsetminus A_n$. Всякая перестановка, сопряжённая g в S_n, сопряжена в A_n либо g, либо $\mathrm{Ad}_h g$. Равенство $\mathrm{Ad}_p g = \mathrm{Ad}_h g$ равносильно равенству $\mathrm{Ad}_{p^{-1}h} g = g$. Поэтому существование чётной перестановки p удовлетворяющей первому равенству равносильно существованию нечётной перестановки $p^{-1}h$, коммутирующей с g, т. е. класс сопряжённости перестановки g в S_n не распадается на два класса сопряжённости в A_n если и только если централизатор $Z(g)$ содержит нечётную перестановку. Когда в цикловом типе g есть строка чётной длины или две строки одинаковой нечётной длины, то такая перестановка есть, а если g является произведением попарно разных циклов нечётной длины, то — нет.

Упр. 11.2. Правая часть равенства $|H| = 12\varepsilon_1 + 12\varepsilon_2 + 20\varepsilon_3 + 15\varepsilon_4 + 1$, приведённая по модулям 2, 3 и 5, равна, соответственно, $1+\varepsilon_4$, $1-\varepsilon_3$ и $1+2(\varepsilon_1+\varepsilon_2)$. Она делится на 2 или на 3 только если $\varepsilon_4 = 1$ или $\varepsilon_3 = 1$. В обоих случаях $|H| \geqslant 16$, так что $|H| \neq 2,\ 3,\ 4,\ 3\cdot 2,\ 3\cdot 4$. Если $|H|$ делится на 5, то $\varepsilon_1 = \varepsilon_2 = 1$ и $|H| \geqslant 25$, так что $|H| \neq 5,\ 2\cdot 5,\ 3\cdot 5,\ 4\cdot 5$. Если $|H|$ делится на $2\cdot 3\cdot 5$, то все $\varepsilon_i = 1$ и $|H| = 60$. Последняя возможность: $|H| = 1$.

Упр. 11.3. Чтобы перевести одномерные подпространства, порождённые непропорциональными векторами e_1, e_2, в одномерные подпространства, порождённые непропорциональными векторами v_1, v_2, дополним эти пары векторов до базисов $\boldsymbol{e} = (e_1, \ldots, e_n)$ и $\boldsymbol{v} = (v_1, \ldots, v_n)$. Матрица перехода $C_{\boldsymbol{ee}}$ имеет ненулевой определитель δ. Умножая её первый столбец на δ^{-1} получаем матрицу $F \in \mathrm{SL}_n$. Оператор $x \mapsto Fx$ переводит e_1 в $\delta^{-1}v_1$, а e_2 в v_2.

Упр. 11.4. Пусть $1 \leqslant k \leqslant m$. Класс $[k] \in \mathbb{Z}/(m)$ удовлетворяет уравнению $n[k] = 0$ если и только если $m \mid kn$. Полагая $m = \mu\,\mathrm{нод}(m,n)$, $n = \nu\,\mathrm{нод}(m,n)$, где $\mathrm{нод}(\mu,\nu) = 1$, заключаем, что $m \mid kn$ если и только если $\mu \mid k$, откуда $k = i\mu$, где $i = 1, \ldots, \mathrm{нод}(m,n)$.

Упр. 11.7. $a_1n_1a_2n_2n_1^{-1}a_1^{-1}n_2^{-1}a_2^{-1} = (a_1n_1a_1^{-1})(a_1a_2n_2n_1^{-1}a_1^{-1}a_2^{-1})(a_2n_2^{-1}a_2^{-1})$. Так как N нормальна, а A абелева, заключённые в скобки слагаемые лежат в N.

Упр. 11.8. При эпиморфизме S_4 на группу треугольника из прим. 10.9 подгруппа чётных перестановок $A_4 \subset S_4$ переходит в группу вращений треугольника.

Упр. 11.9. Не вполне очевидно, разве что последнее равенство

$$(Q_k \cap P_i) \cap ((Q_{k+1} \cap P_i)P_{i+1}) = (Q_{k+1} \cap P_i)(Q_k \cap P_{i+1})\,.$$

Левая часть содержит правую, поскольку $Q_{k+1}Q_k \subset Q_k$ и $P_iP_{i+1} \subset P_i$. Правая часть содержит левую, так как если элемент $c \in Q_k \cap P_i$ имеет вид $c = ab$, где $a \in Q_{k+1} \cap P_i$, $b \in P_{i+1}$, то $b = a^{-1}c$ лежит в Q_k, а значит, и в $Q_k \cap P_{i+1}$.

Упр. 11.10. $\mathbb{Z}/(p^n) \supsetneq A_1 \supsetneq \ldots \supsetneq A_{n-1} \supsetneq 0$, где $A_k = \{[zp^{k-1}] \in \mathbb{Z}/(p^n) \mid z \in \mathbb{Z}\}$.

Упр. 11.11. Проверка ассоциативности:

$$\big((x_1,h_1)\cdot(x_2,h_2)\big)\cdot(x_3,h_3) = \big(x_1\psi_{h_1}(x_2)\,,\ h_1h_2\big)\cdot(x_3,h_3) = \big(x_1\psi_{h_1}(x_2)\psi_{h_1h_2}(x_3)\,,\ h_1h_2h_3\big)$$
$$(x_1,h_1)\cdot\big((x_2,h_2)\cdot(x_3,h_3)\big) = (x_1,h_1)\cdot\big(x_2\psi_{h_2}(x_3)\,,\ h_2h_3\big) = \Big(x_1\psi_{h_1}\big(x_2\psi_{h_2}(x_3)\big)\,,\ h_1h_2h_3\Big)\,.$$

Но $\psi_{h_1}\big(x_2\psi_{h_2}(x_3)\big) = \psi_{h_1}(x_2)\psi_{h_1}\circ\psi_{h_2}(x_3) = \psi_{h_1}(x_2)\psi_{h_1h_2}(x_3)$. Существование единицы:

$$(x,h)\cdot(e,e) = (x,\psi_h(e),he) = (x,h)\,,$$

поскольку $\psi_h(e) = e$ в силу того, что ψ_h гомоморфизм. Существование обратного:

$$\big(\psi_h^{-1}(x^{-1})\,,\ h^{-1}\big)\cdot(x,h) = \big(\psi_h^{-1}(x^{-1})\psi_h^{-1}(x^{-1})\,,\ h^{-1}h\big) = (e,e)\,.$$

Упр. 11.12. Так как $\psi\colon H \to \operatorname{Aut} N$ — гомоморфизм, $\psi_e = \mathrm{Id}_N$ и

$$(x_1,e)\cdot(x_2,e) = (x_1\psi_e(x_2),e) = (x_1x_2,e)\,,$$

т. е. элементы (x,e) образуют подгруппу, изоморфную N. Она нормальна, поскольку

$$(y,h)\cdot(x,e)\cdot\big(\psi_h^{-1}(y^{-1}),h^{-1}\big) = (y\psi_h(x),h)\cdot\big(\psi_h^{-1}(y^{-1}),h^{-1}\big) = \big(y\psi_h(x)y^{-1},e\big)\ .$$

Элементы (e,h) очевидно образуют дополнительную подгруппу, изоморфную H, и

$$\mathrm{Ad}_{(e,h)}(x,e) = (\psi_h(x),e)\,.$$

Упр. 11.15. Пусть центр $Z(G) = C$. Если $|C| = p$, то $C \simeq \mathbb{Z}/(p) \simeq G/C$. Пусть $a \in C$ — образующая центра, а $b \in G$ — такой элемент, что смежный класс bC является образующей в G/C. Тогда любой элемент группы имеет вид b^ka^m. Так как a централен, любые два таких элемента коммутируют.

Упр. 11.16. Аддитивные автоморфизмы группы $\mathbb{Z}/(p)$ суть линейные автоморфизмы одномерного векторного пространства над полем $\mathbb{F}_p$. Они образуют группу $\mathrm{GL}_1(\mathbb{F}_p) \simeq \mathbb{F}_p^\times$ ненулевых элементов поля $\mathbb{F}_p$ по умножению. Как и всякая конечная мультипликативная подгруппа поля, она циклическая[1].

[1] См. сл. 2.3 на стр. 52.

Упр. 12.1. Первое очевидно, второе вытекает из того, что при вставке фрагмента $x^\varepsilon x^{-\varepsilon}$ в произвольное слово w получится такое слово, в котором сокращение любого фрагмента вида $y^\varepsilon y^{-\varepsilon}$ приведёт либо обратно[1] к слову w, либо к слову, получающемуся из w сначала сокращением *того же самого фрагмента* $y^\varepsilon y^{-\varepsilon}$, а уже затем вставкой $x^\varepsilon x^{-\varepsilon}$ в *то же самое место*, что и в w.

Упр. 12.2. Отобразите $n \in \mathbb{N}$ в $x^n y x^n \in F_2$ и воспользуйтесь предл. 12.1 на стр. 199.

Упр. 12.3. Поскольку отображение $F\colon \mathbb{R}^n \to \mathbb{R}^n$ биективно, достаточно убедиться, что отображения $\sigma_{F(\pi)}$ и $F \circ \sigma_\pi \circ F^{-1}$ одинаково действуют на точку вида $F(p)$ с произвольным $p \in \mathbb{R}^n$.

Упр. 12.4. Обозначим через v_i вектор, идущий из центра симплекса Δ в вершину i. Вектор $n_{ij} = v_i - v_j$ ортогонален гиперплоскости π_{ij}, поскольку для любого $k \neq i, j$ скалярное произведение $\bigl(n_{ij}, v_k - (v_i + v_j)/2\bigr) = (v_i, v_k) - (v_j, v_k) + (v_i, v_i)/2 - (v_j, v_j)/2 = 0$, т. к. все произведения (v_i, v_j) с $i \neq j$ и все скалярные квадраты (v_i, v_i) одинаковы. Аналогичная выкладка показывает, что при $\{i, j\} \cap \{k, m\} = \varnothing$ векторы n_{ij} и n_{km} ортогональны. Векторы $v_i - v_k$ и $v_k - v_j$ образуют в натянутой на них двумерной плоскости стороны правильного треугольника с вершинами в концах векторов v_i, v_j и v_k, и угол между ними равен 60°.

[1] Обратите внимание, что такое происходит *не только* при сокращении того же самого фрагмента $x^\varepsilon x^{-\varepsilon}$, который был перед этим вставлен, но и при сокращении одной из букв $x^{\pm\varepsilon}$ с её соседкой.