§5. Векторы и матрицы

Всюду в этом параграфе K по умолчанию обозначает коммутативное кольцо с единицей.

5.1. Модули над коммутативными кольцами. Аддитивная абелева группа[1] M называется *модулем* над коммутативным кольцом K или *K-модулем*, если задана операция умножения

$$K \times M \to M\,, \quad (x, v) \mapsto x \cdot v = xv\,,$$

с теми же свойствами, что известное из курса геометрии умножение векторов на числа[2]:

$$\forall\, x, y \in K \quad \forall\, v \in M \quad x(yv) = (xy)v \tag{5-1}$$

$$\forall\, x, y \in K \quad \forall\, v \in M \quad (x + y)v = xv + yv \tag{5-2}$$

$$\forall\, x \in K \quad \forall\, u, w \in M \quad x(v + w) = xv + xw\,. \tag{5-3}$$

Если в кольце K есть единица и выполняется дополнительное свойство

$$\forall\, v \in V \quad 1v = v\,, \tag{5-4}$$

то модуль M называется *унитальным*. Всюду в этом курсе мы по умолчанию будем иметь дело именно с такими модулями. 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 $K \times M \to M$ — *умножением векторов на скаляры*. Часто бывает удобно записывать произведение вектора $v \in M$ на скаляр $x \in K$ не как xv, а как vx. Для коммутативного кольца K мы по определению считаем эти две записи эквивалентными обозначениями $xv = vx$ для одного и того же вектора из M.

Упражнение 5.1. Выведите из свойств (5-1) – (5-3), что в любом K-модуле M для всех $v \in M$ 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] $(-1) \cdot v = -v$.

Аддитивная абелева подгруппа $N \subseteq M$ в K-модуле M называется *K-подмодулем*, если она образует K-модуль относительно имеющейся в M операции умножения векторов на скаляры. Для этого необходимо и достаточно, чтобы $xw \in N$ для всех $x \in K$ и $w \in N$. Подмодули $N \subsetneq M$ называются *собственными*. Собственный подмодуль 0, состоящий из одного нуля, называется *тривиальным*.

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[4].

[1] См. n° 1.1.2 на стр. 24.

[2] См. лекцию http://gorod.bogomolov-lab.ru/ps/stud/geom_ru/2122/lec_01.pdf. При этом в роли «векторов» выступают элементы модуля M, а в роли «чисел» — элементы кольца K.

[3] Слева стоит произведение вектора $v \in M$ на скаляр $-1 \in K$, а справа — противоположный к v вектор $-v \in M$.

[4] См. предл. 4.1 на стр. 71.

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 $P = \lambda A$ матрицы A на число $\lambda \in K$ имеет $p_{ij} = \lambda a_{ij}$.

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 5.2. 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 5.3. Покажите, 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 5.4. 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.

Модуль K-линейных отображений $M \to N$ называется *модулем гомоморфизмов* из M в N и обозначается $\mathrm{Hom}(M, N)$ или $\mathrm{Hom}_K(M, N)$, 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. 31 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 5.5. 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 $\mathrm{Mat}_{m\times n}(K)$ 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. 35. 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 $\mathrm{Mat}_{m\times n}(K)$ 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

$$\prod_{\mu\in\mathcal{M}} \mathrm{Hom}_K(M_\mu, N) \xrightarrow{\sim} \mathrm{Hom}_K\Big(\bigoplus_{\mu\in\mathcal{M}} M_\mu,\, N\Big), \tag{5-6}$$

который переводит семейство K-линейных гомоморфизмов $\varphi_\mu : M_\mu \to N$ в гомоморфизм

$$\bigoplus \varphi_\mu : \bigoplus_{\mu\in\mathcal{M}} M_\mu \to N, \tag{5-7}$$

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. 87)
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 $a(t) = a_0 + a_1t + \ldots + a_mt^m$ в число $\varphi(a) = f_0a_0 + f_1a_1 + \ldots + f_ma_m$. 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* $F(x) = \sum_{n\geqslant 0} f_nx^n \in K[\![x]\!]$. 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 $\sum_{n\geqslant 0} \alpha^nx^n = (1 - \alpha x)^{-1} \in K[\![x]\!]$.

Упражнение 5.6. В условиях предл. 5.1 постройте изоморфизм K-модулей

$$\bigoplus_{\mu\in\mathcal{M}} \mathrm{Hom}_K(N, M_\mu) \xrightarrow{\sim} \mathrm{Hom}_K\Big(N, \bigoplus_{\mu\in\mathcal{M}} M_\mu\Big). \tag{5-8}$$

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 $\mathrm{span}(A)$ или $\mathrm{span}_K(A)$, 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 5.7. 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 *фактор модуль* M/N, состоящий из классов $[m]_N = m \pmod N = m + N = \{m' \in M \mid m' - m \in N\}$, которые являются аддитивными сдвигами подмодуля N на всевозможные элементы $m \in M$ или, что тоже самое, классами эквивалентности по отношению $m \equiv n \pmod N$ сравнимости по модулю N, означающему, что $m' - m \in N$. Сложение классов и их умножение на элементы кольца определяются обычными формулами $[m_1]_N + [m_2]_N \overset{\text{def}}{=} [m_1 + m_2]_N$ и $x \cdot [m]_N \overset{\text{def}}{=} [xm]_N$.

Упражнение 5.8. Проверьте, что отношение сравнимости по модулю N является эквивалентностью, а операции корректно определены и удовлетворяют аксиомам (5-1) – (5-4).

В частности, фактор кольцо 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 сюрьективного 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, $\iota_\varphi : M/\ker\varphi \xrightarrow{\sim} \operatorname{im}\varphi$ является изоморфизмом K-модулей.

Упражнение 5.9. 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. 89 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. 5.9, 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 5.10. 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

$$IM \overset{\text{def}}{=} \{x_1a_1 + \ldots + x_na_n \in M \mid x_i \in I,\ a_i \in M,\ n \in \mathbb{N}\}$$

K-подмодуль, образованный всевозможными линейными комбинациями элементов модуля M с коэффициентами из идеала I.

Упражнение 5.11. Проверьте, что IM действительно является K-подмодулем в M.

Абелева фактор группа M/IM, элементы которой — это классы

$$[w]_{IM} = w + IM = \{v \in M \mid v - w \in IM\},$$

является модулем над фактор кольцом K/I. Умножение векторов на скаляры задаётся правилом

$$[x]_I \cdot [w]_{IM} = [xw]_{[IM]}.$$

Упражнение 5.12. 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 5.13. 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. $v = x_1 u_1 + \ldots + x_m u_m$ 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 $x_1 e_1 + \ldots + x_n e_n = 0$, 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. 86 свободен, так как каждый вектор $(x_1, \ldots, x_n)$ единственным образом представляется в виде линейной комбинации $x_1 e_1 + \ldots + x_n e_n$ 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. 90 мы видели, что фактор модуль $F/\mathfrak{m}F$ является векторным пространством над полем $\Bbbk = K/\mathfrak{m}$ и изоморфен $\bigoplus_{e \in E} \Bbbk[e]$ в силу форм. (5-10) на стр. 91. Таким образом, классы 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 $a, b \in A$ выполняются равенства

$$0 \cdot b = (a + (-1) \cdot a)\, b = ab + (-1) \cdot ab = 0 \quad \text{и} \quad a \cdot 0 = a\,(b + (-1) \cdot b)a = ab + (-1)ab = 0,$$

мы заключаем, что $0 \cdot a = a \cdot 0 = 0$ 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. 74.

[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. $\varphi(a_1a_2) = \varphi(a_1)\varphi(a_2)$. Будучи гомоморфизмами K-модулей, гомоморфизмы K-алгебр обладают всеми свойствами из n° 5.1.1 на стр. 86 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. 75. 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 5.14. Проверьте, что композиция отображений ассоциативна и линейно зависит от каждого из двух компонуемых отображений.

5.2.1. Алгебра матриц $\mathrm{Mat}_n(K)$. 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 $w = x_1e_1 + \dots + x_ie_i$,

$$\varphi(w) = \varphi(x_1e_1 + \dots + x_ne_n) = x_1\varphi(e_1) + \dots + x_n\varphi(w_n) = x_1w_1 + \dots + x_nw_n,$$

и наоборот, для любого набора векторов $w_1, \dots, w_n \in K^n$ отображение

$$\varphi_{w_1,\dots,w_n} : K^n \to K^n, \quad x_1e_1 + \dots + x_ne_n \mapsto x_1w_1 + \dots + x_nw_n,$$

является K-линейным и переводит каждый базисный вектор e_i в вектор w_i.

Упражнение 5.15. 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 5.16. 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:

$$w_1, w_2, \dots, w_n = \begin{pmatrix} \varphi_{11} \\ \vdots \\ \varphi_{n1} \end{pmatrix}, \begin{pmatrix} \varphi_{12} \\ \vdots \\ \varphi_{n2} \end{pmatrix}, \dots, \begin{pmatrix} \varphi_{1n} \\ \vdots \\ \varphi_{nn} \end{pmatrix} \rightsquigarrow \Phi = \begin{pmatrix} \varphi_{11} & \varphi_{12} & \cdots & \varphi_{1n} \\ \vdots & \vdots & \cdots & \vdots \\ \varphi_{n1} & \varphi_{n2} & \cdots & \varphi_{nn} \end{pmatrix}.$$

[1] Терминологию, относящуюся к отображениям множеств, см. на стр. 6.

[2] См. прим. 5.3 на стр. 86.

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 $\varphi :\ K^n \to K^n$ в базисе $e_1, \dots , e_n$. Таким образом, сопоставляя эндоморфизму φ его матрицу Φ, мы получаем изоморфизм K-модулей

$$\mathrm{End}(K^n) \simeq \mathrm{Mat}_{n\times n}(K)\,, \quad \varphi \mapsto \Phi\,, \tag{5-11}$$

где $\mathrm{Mat}_n(K) \stackrel{\text{def}}{=} \mathrm{Mat}_{n\times n}(K)$ — 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 $\mathrm{End}(K^n)$ из прим. 5.13 выше и задаётся композицией отображений. Возникающая таким образом билинейная ассоциативная операция

$$\mathrm{Mat}_{n\times n}(K) \times \mathrm{Mat}_{n\times n}(K) \to \mathrm{Mat}_{n\times n}(K)\,, \quad (\Phi, \Psi) \mapsto \Phi\Psi\,,$$

где Φ и Ψ суть матрицы K-линейных отображений $\varphi, \psi :\ K^n \to K^n$, а $\Phi\Psi$ — матрица их композиции $\varphi\psi :\ K^n \to K^n$, $w \mapsto \varphi(\psi(w))$, 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 $\psi_{1j}\varphi_{i1} + \ldots + \psi_{nj}\varphi_{in}$. 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 $\mathrm{Mat}_{n\times n}(K)$ является матрица тождественного отображения $\mathrm{Id} :\ K^n \to K^n$

$$E = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & 1 \end{pmatrix} \in \mathrm{Mat}_{n\times n}(K)\,, \tag{5-12}$$

(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 $\mathrm{Mat}_n(K)$ изоморфна координатному модулю K^{n^2} и тем самым свободна. Стандартный базис в $\mathrm{Mat}_n(K)$ 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 $E_{ij} :\ K^n \to K^n$, которые

[1] См. прим. 5.3 на стр. 86.

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 5.17. 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^{2020} для матрицы $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Поскольку $A = E + E_{12}$ и матрицы E и E_{12} коммутируют, вычислить $(E + E_{12})^{2020}$ можно по формуле для раскрытия бинома[1], а так как $E_{12}^n = 0$ при $n > 1$, на ответ влияют только первые два члена:

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{2020} = (E + E_{12})^{2020} = E + 2020\,E_{12} = \begin{pmatrix} 1 & 2020 \\ 0 & 1 \end{pmatrix}.$$

Упражнение 5.18. 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 $a', a'' \in A$, что $a'a = aa'' = e$. В самом деле, выкладка $a' = a'e = a'(aa'') = (a'a)a'' = ea'' = a''$ показывает, что любые два таких элемента a', a'' друг с другом. Из проделанного вычисления также следует, что обратный к a элемент a^{-1}, если он существует, однозначно определяется по a из равенств $aa^{-1} = a^{-1}a = e$.

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 равенство вида

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix}$$

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 (0-9) на стр. 10.

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
$$\Phi^\vee \overset{\text{def}}{=} \begin{pmatrix} d & -b \\ -c & d \end{pmatrix}$$
называется *присоединённой* к матрице Φ, а число $\det \Phi \overset{\text{def}}{=} ad - bc \in K$ — *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 $\Phi^{-1} = \det(\Phi)^{-1}\Phi$.

Упражнение 5.19. 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 5.20. 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 $A = \left(a_{ij}\right)$ обратима[2] и обратная к ней матрица $B = A^{-1}$ тоже верхняя унитреугольная с наддиагональными элементами
$$\begin{aligned} b_{ij} &= \sum_{s=0}^{j-i-1}(-1)^{s+1}\sum_{i<\nu_1<\ldots<\nu_s<j} a_{i\nu_1}a_{\nu_1\nu_2}a_{\nu_2\nu_3}\,\ldots\,a_{\nu_{s-1}\nu_s}a_{\nu_s j} = \\ &= -a_{ij} + \sum_{i<k<j}a_{ik}a_{kj} - \sum_{i<k<\ell<j}a_{ik}a_{k\ell}a_{\ell j} + \sum_{i<k<\ell<m<j}a_{ik}a_{k\ell}a_{\ell m}a_{mj} - \,\ldots\,. \end{aligned} \tag{5-14}$$
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. 96 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]

$$\underbrace{a_{i\nu_1}a_{\nu_1\nu_2}\dots a_{\nu_{k-2}\nu_{k-1}}a_{\nu_{k-1}j}}_{k\text{ сомножителей}}\,, \quad \text{где} \quad i < \nu_1 < \ldots < \nu_{k-1} < j\,.$$

В частности, он заведомо зануляется, когда k превышает размер матрицы A. Полагая $x = E$, $y = N$ в равенстве[2] $(x+y)(x^{m-1} - x^{m-2}y + \ldots + (-1)^{m-1}y^{m-1}) = x^m - y^m$, при достаточно большом m мы получим матричное равенство $A(E - N + N^2 - N^3 + \ldots) = E$, откуда

$$A^{-1} = E - N + N^2 - N^3 + \ldots\,,$$

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:

$$(a_1,\ldots,a_s)\begin{pmatrix} b_1\\ \vdots\\ b_s\end{pmatrix} \overset{\text{def}}{=} a_1b_1 + \ldots + a_sb_s = \sum_{k=1}^{s} a_kb_k\,. \tag{5-15}$$

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):

$$c_{ij} = \begin{pmatrix} a_{i1}, \ldots & a_{is}\end{pmatrix}\cdot\begin{pmatrix} b_{1j}\\ \vdots\\ b_{sj}\end{pmatrix} = \sum_{k=1}^{s} a_{ik}b_{kj}\,. \tag{5-16}$$

[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 5.21. 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 5.22. 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 5.23. 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 $c_{ij} = \sum_k a_{ik} b_{kj} = \sum_k a^t_{ki} b^t_{jk} = \sum_k b^t_{jk} a^t_{ki} = d_{ji}$. □

Упражнение 5.24. 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.

$$(x_1 A_1 + x_2 A_2)B = x_1 A_1 B + x_2 A_2 B \quad \text{и} \quad A(y_1 B_1 + y_2 B_2) = y_1 A B_1 + y_2 A B_2$$

для всех $A, A_1, A_2 \in \mathrm{Mat}_{m\times s}(L)$, $B, B_1, B_2 \in \mathrm{Mat}_{m\times s}(M)$ и $x_i, y_j \in K$.

Предложение 5.5
Если на абелевых группах L_1, L_2, L_3, L_{12}, L_{23}, L_{123} заданы дистрибутивные[1] и ассоциативные[2] умножения $L_1 \times L_2 \to L_{12}$, $L_{12} \times L_3 \to L_{123}$, $L_2 \times L_3 \to L_{23}$, $L_1 \times L_{23} \to L_{123}$, то при всех $m, k, \ell, n \in \mathbb{N}$ умножения матриц

$$\begin{gathered}\mathrm{Mat}_{m\times k}(L_1) \times \mathrm{Mat}_{k\times \ell}(L_2) \to \mathrm{Mat}_{m\times \ell}(L_{12}), \quad \mathrm{Mat}_{m\times \ell}(L_{12}) \times \mathrm{Mat}_{\ell\times n}(L_3) \to \mathrm{Mat}_{m\times n}(L_{123}), \\ \mathrm{Mat}_{k\times \ell}(L_2) \times \mathrm{Mat}_{\ell\times n}(L_3) \to \mathrm{Mat}_{k\times n}(L_{23}), \quad \mathrm{Mat}_{m\times k}(L_1) \times \mathrm{Mat}_{k\times n}(L_{23}) \to \mathrm{Mat}_{m\times n}(L_{123}).\end{gathered}$$

тоже дистрибутивны и ассоциативны, т. е. $A(B + C) = AB + AC$, $(A + B)C = AC + BC$ и $(AB)C = A(BC)$ для всех матриц A, B, C, на которых эти операции определены.

Доказательство. Дистрибутивность вытекает из упр. 5.24. Докажем ассоциативность. Полагаем $AB = P$, $BC = Q$ и проверяем, что (i, j)-е элементы произведений PC и AQ равны друг другу:

$$\sum_k p_{ik} c_{kj} = \sum_k \Big(\sum_\ell a_{i\ell} b_{\ell k} \Big) c_{kj} = \sum_{k\ell} (a_{i\ell} b_{\ell k}) c_{kj} = \\ = \sum_{k\ell} a_{i\ell} (b_{\ell k} c_{kj}) = \sum_\ell a_{i\ell} \Big(\sum_k b_{\ell k} c_{kj} \Big) = \sum_\ell a_{i\ell} q_{\ell j}.$$

Обратите внимание, что второе и четвёртое равенство используют дистрибутивность умножений между абелевыми группами. □

5.3.2. Матрицы перехода. Пусть в K-модуле M заданы два набора векторов:

$$\boldsymbol{u} = (u_1, \dots, u_n) \quad \text{и} \quad \boldsymbol{w} = (w_1, \dots, w_m),$$

причём первый из них содержится в линейной оболочке второго, т. е. каждый вектор u_j имеет вид $u_j = w_1 c_{1j} + w_2 c_{2j} + \ldots + w_m c_{mj}$, где $c_{ij} \in K$. Эти n равенств собираются в одну матричную формулу $\boldsymbol{u} = \boldsymbol{w}\, C_{\boldsymbol{wu}}$, где $\boldsymbol{u} = (u_1, \dots, u_n)$ и $\boldsymbol{w} = (w_1, \dots, w_m)$ 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 $\boldsymbol{v} = (v_1, \dots, v_k)$, 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 $\boldsymbol{v} = \boldsymbol{u} C_{\boldsymbol{uv}}$. Таким образом, если записывать линейные выражения $v = u_1 x_1 + \ldots + u_n x_n = w_1 y_1 + \ldots + w_m y_m$ произвольного

[1] Т. е. $(a + b)c = ac + bc$ и $a(b + c) = ab + ac$
[2] Т. е. $(ab)c = a(bc)$.

вектора $v \in \mathrm{span}(u_1, \dots, u_n)$ через векторы $\boldsymbol{u}$ и $\boldsymbol{w}$ в виде $v = \boldsymbol{ux} = \boldsymbol{wy}$, где $\boldsymbol{x} = (x_1, \dots, x_n)^t$ и $\boldsymbol{y} = (y_1, \dots, y_m)^t$ суть столбцы коэффициентов, то эти столбцы будут связаны соотношением

$$\boldsymbol{y} = C_{\boldsymbol{wu}}\boldsymbol{x}\,.$$

Отметим, что когда набор векторов $\boldsymbol{w} = (w_1, \dots, w_m)$ 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 $\boldsymbol{e} = (e_1, \dots, e_n)$ является базисом своей линейной оболочки, то матрица перехода $C_{\boldsymbol{ew}}$, выражающая произвольный набор векторов $\boldsymbol{w} = (w_1, \dots, w_m)$ 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. 99 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 $u_1, \dots, u_n$ столбцы матрицы C, рассматриваемые как векторы координатного модуля K^n. Тогда $C = C_{\boldsymbol{ue}}$ является матрицей перехода от них к стандартному базису $\boldsymbol{e} = (e_1, \dots, e_n)$ модуля K^n. Если набор векторов $\boldsymbol{u} = (u_1, \dots, u_n)$ является базисом в K^n, набор векторов $\boldsymbol{e}$ линейно выражается через $\boldsymbol{u}$, т. е. $\boldsymbol{e} = \boldsymbol{u}\,C_{\boldsymbol{eu}}$, где $C_{\boldsymbol{eu}} \in \mathrm{Mat}_n(K)$. Из формулы (5-18) получаем равенства $C_{\boldsymbol{ee}} = C_{\boldsymbol{eu}}C_{\boldsymbol{ue}}$ и $C_{\boldsymbol{uu}} = C_{\boldsymbol{ue}}C_{\boldsymbol{eu}}$, и поскольку оба набора являются базисами, заключаем, что $C_{\boldsymbol{ee}} = C_{\boldsymbol{uu}} = E$. Тем самым, 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. Если столбец $\boldsymbol{x}$ коэффициентов $x_i \in K$ таков, что $0 = \boldsymbol{ux} = \boldsymbol{e}\,C_{\boldsymbol{eu}}\boldsymbol{x}$, то поскольку векторы $\boldsymbol{e}$ составляют базис в K^n, 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 $f \in \mathbb{Z}[x_1, \dots, x_n]$ называется *симметрическим*, если он не меняется при перестановках номеров переменных, т. е. когда $f(x_1, \dots, x_n) = f(x_{g(1)}, \dots, x_{g(n)})$ для всех биекций

$$g:\ \{1, \dots, n\} \xrightarrow{\sim} \{1, \dots, n\}\,.$$

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 5.25. 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 5.26. Убедитесь в этом.

Для каждой диаграммы Юнга $\mu = (\mu_1, \dots, \mu_n)$ положим $e_\mu \overset{\text{def}}{=} e_{\mu_1} \dots e_{\mu_n}$. 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 5.27. 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 выписать все диаграммы λ из d клеток в одну строку в порядке лексикографического возрастания наборов чисел $(\lambda_1, \dots, \lambda_n)$, а все диаграммы μ с $m_1 + 2m_2 + \dots + nm_n = d$, где m_i — число строк длины i, — в порядке лексикографического возрастания транспонированных диаграмм μ^t, то согласно формуле (5-21) матрица перехода от многочленов e_μ к многочленам m_λ является верхней унитреугольной. В прим. 5.16 на стр. 97 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 базис модуля однородных симметрических

[1] См. прим. 0.3 на стр. 10.
[2] Её строками являются столбцы диаграммы μ также, как при транспонировании матриц.

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 $(\alpha_1 - \alpha_2)^2 = (\alpha_1 + \alpha_2)^2 - 4\alpha_1\alpha_2 = p^2 - 4q$. 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 5.28. 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 $F : N \to M$ однозначно задаётся набором $F(\boldsymbol{u}) \overset{\text{def}}{=} \big(F(u_1), \dots, F(u_n)\big)$ 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

$$F_{\boldsymbol{wu}} = C_{\boldsymbol{w}\,F(\boldsymbol{u})} \in \mathrm{Mat}_{m\times n}(K)$$

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 $F(v) = \boldsymbol{w}F_{\boldsymbol{wu}}\boldsymbol{x} \in M$, который выражается через образующие $\boldsymbol{w}$ со столбцом коэффициентов $F_{\boldsymbol{wu}}\boldsymbol{x}$.

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 $F : N \to M$ 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

$$F : N \to L \quad \text{и} \quad G : L \to M$$

имеют матрицы $F_{\boldsymbol{vu}}$ и $G_{\boldsymbol{wv}}$, соответственно, в образующих $\boldsymbol{v}$, $\boldsymbol{u}$ и в образующих $\boldsymbol{w}$, $\boldsymbol{v}$, то композиция $H = GF : N \to M$ имеет в образующих $\boldsymbol{w}$, $\boldsymbol{u}$ матрицу $H_{\boldsymbol{wu}} = G_{\boldsymbol{wv}}F_{\boldsymbol{vu}}$, поскольку

$$H(\boldsymbol{u}) = G\big(F(\boldsymbol{u})\big) = G\big(\boldsymbol{v}F_{\boldsymbol{vu}}\big) = G(\boldsymbol{v})F_{\boldsymbol{vu}} = \boldsymbol{w}G_{\boldsymbol{wv}}F_{\boldsymbol{vu}}\,.$$

[1] Ср. с n° 5.2.1 на стр. 94.

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. 92, то матрица $A \in \mathrm{Mat}_{m\times n}(K)$ тогда и только тогда является матрицей некоторого линейного отображения $F : N \to M$, 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 $x \in K^n$. □

Замечание 5.1. Если оба модуля N и M свободны и наборы векторов $\boldsymbol{u}$ и $\boldsymbol{w}$ являются их базисами, сопоставление K-линейному отображению $F : N \to M$ его матрицы $F_{\boldsymbol{wu}}$ в этих базисах задаёт K-линейный изоморфизм $\mathrm{Hom}_K(N, M) \xrightarrow{\sim} \mathrm{Mat}_{m\times n}(K)$, $F \mapsto F_{\boldsymbol{wu}}$, что проверяется дословно тем же рассуждением, как в n° 5.2.1 на стр. 94 выше, т. е. абсолютно также, как и для векторных пространств над полем.

Пример 5.19 (гомоморфизмы между аддитивными группами вычетов)
Как мы уже отмечали в прим. 5.4 на стр. 86, любые две абелевы группы A и B могут рассматриваться как модули над кольцом $\mathbb{Z}$.

Упражнение 5.29. 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 класс $[1]_m$ порождает $\mathbb{Z}/(m)$ над $\mathbb{Z}$ и отображение факторизации $\mathbb{Z} \twoheadrightarrow \mathbb{Z}/(m)$, $z \mapsto [z]_m$, является сюрьективным 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

[1] См. n° 1.5 на стр. 31.

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 $a : z \mapsto az$. Так как $an \in (m)$ если и только если an является общим кратным m и n, мы заключаем, что $a = k\,\text{нок}(m,n)/n$, где $k \in \mathbb{Z}$ — любое. Два таких числа $a_1 = k_1\,\text{нок}(m,n)/n$ и $a_2 = k_2\,\text{нок}(m,n)/n$ 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 $(k_1 - k_2)\,\text{нок}(m,n)/n$ 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 $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/(n), \mathbb{Z}/(m)) \simeq \mathbb{Z}/(\text{нод}(m,n))$. 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

$$\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/(n), \mathbb{Z}/(m)) \simeq \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/(m), \mathbb{Z}/(n))\,,$$

и если m и n взаимно просты, то $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/(n), \mathbb{Z}/(m)) \simeq \mathbb{Z}/(1) = 0$.

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. 5.3. Прямая проверка: если φ и ψ K-линейны, то $\varphi\psi(xu+yw) = \varphi(x\psi(u)+y\psi(w)) = x\varphi\psi(u)+y\varphi\psi(w)$ для любых скаляров x, y и векторов u, w.

Упр. 5.4. 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. 5.5. Ядро и образ любого гомоморфизма абелевых групп являются абелевыми подгруппами согласно n° 1.5 на стр. 31. 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. 5.6. 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 $\left(\varphi_\mu(u)\right)_{\mu\in\mathcal{M}}$ с конечным числом ненулевых членов.

Упр. 5.7. Пусть $A \nsubseteq B$ — 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. 5.8. Все проверки проводятся дословно также, как для классов вычетов по модулю идеала коммутативного кольца (ср. с упр. 4.7 на стр. 74).

Упр. 5.9. 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 сюрьекции $\pi_N : M \twoheadrightarrow N$ 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. 90 являются искомыми изоморфизмами.

Упр. 5.12. 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. 5.13. 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. 5.17. Ответ:

$$[E_{ij}, E_{k\ell}] \overset{\text{def}}{=} E_{ij}E_{k\ell} - E_{k\ell}E_{ij} = \begin{cases} E_{ii} - E_{jj} & \text{при } j = k \text{ и } i = \ell \\ E_{i\ell} & \text{при } j = k \text{ и } i \neq \ell \\ -E_{kj} & \text{при } j \neq k \text{ и } i = \ell \\ 0 & \text{в остальных случаях.} \end{cases}$$

Упр. 5.19. 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. 5.24. Оба равенства проверяются прямым вычислением.