

§5. Векторы и матрицы

5.1. Модули над коммутативными кольцами. Аддитивная абелева группа¹ V называется *модулем* над коммутативным кольцом K или *K -модулем*, если задана операция умножения

$$K \times V \rightarrow V, \quad (x, v) \mapsto x \cdot v = xv,$$

с теми же свойствами, что известно из курса геометрии умножение векторов на числа²:

$$\forall x, y \in K \quad \forall v \in V \quad x(yv) = (xy)v \quad (5-1)$$

$$\forall x, y \in K \quad \forall v \in V \quad (x + y)v = xv + yv \quad (5-2)$$

$$\forall x \in K \quad \forall u, w \in V \quad x(u + w) = xu + xw. \quad (5-3)$$

Если в кольце K есть единица и выполняется дополнительное свойство

$$\forall v \in V \quad 1v = v, \quad (5-4)$$

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 — равенство³ $(-1) \cdot v = -v$.

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 $K \times V \rightarrow V$ — *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:

$$(vy)x = v(yx), \quad v(x + y) = vx + vy, \quad (u + w)x = ux + wx, \quad v1 = v.$$

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*.

¹См. н° 1.1.2 на стр. 23.

²См. 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 .

³Слева 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 унитарным. 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 подмодулей¹.

Пример 5.2 (координатный модуль K^r)

Декартово произведение r экземпляров кольца K обозначается $K^r = K \times \dots \times K$ и состоит из строк $a = (a_1, \dots, a_r)$, в которых $a_i \in K$. Сложение таких строк и их умножение их на скаляры $x \in K$ происходит покомпонентно: для $a = (a_1, \dots, a_r)$, $b = (b_1, \dots, b_r)$ и $x \in K$ мы полагаем

$$a + b \stackrel{\text{def}}{=} (a_1 + b_1, \dots, a_r + b_r) \quad \text{и} \quad xa \stackrel{\text{def}}{=} (xa_1, \dots, xa_r).$$

Пример 5.3 (модуль матриц $\text{Mat}_{m \times n}(K)$)

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 $\text{Mat}_{m \times n}(K)$. 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 $A \in \text{Mat}_{3 \times 4}(\mathbb{Z})$ 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 $\text{Mat}_{m \times n}(K)$ 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 унитарный \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 $(\pm n) \cdot a \stackrel{\text{def}}{=} \pm (a + \dots + a)$, 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 $\varphi : M \rightarrow N$ 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 $u, w \in M$

$$\varphi(u + w) = \varphi(u) + \varphi(w) \quad \text{и} \quad \varphi(xu) = x\varphi(u). \quad (5-5)$$

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 $\varphi, \psi : M \rightarrow N$ отображения $\varphi + \psi$ и $x\varphi$ тоже K -линейны.

¹См. предл. 4.1 на стр. 67.

Модуль K -линейных отображений $M \rightarrow N$ называется *модулем гомоморфизмов* из M в N и обозначается $\text{Hom}(M, N)$ или $\text{Hom}_K(M, N)$, если надо явно указать кольцо, над которым рассматриваются модули.

Так как K -линейные отображения $\varphi : M \rightarrow N$ являются гомоморфизмами абелевых групп, все они обладают перечисленными в п° 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 $\varphi : M \rightarrow N$ являются подмодулями в M и в N соответственно.

Биективные гомоморфизмы модулей называются *изоморфизмами*. K -линейное отображение $\varphi : M \rightarrow N$ является изоморфизмом если и только если $\ker \varphi = 0$ и $\text{im } \varphi = N$. Например, выписывание элементов матрицы в строку в произвольном порядке задаёт изоморфизм между модулем матриц $\text{Mat}_{m \times n}(K)$ 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 $D = \frac{d}{dx} : K[x] \rightarrow K[x]$, $f(x) \mapsto f'(x)$, 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 $\varphi : K \rightarrow K$, 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 п° 1.6 на стр. 34. Такие семейства можно поэлементно складывать и умножать на скаляры точно также, как мы это делали в п° 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 $\text{Mat}_{m \times n}(K)$ 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 $\bigoplus_{n \geq 0} Kt^n$ изоморфна модулю многочленов $K[t]$, а прямое произведение $\prod_{n \geq 0} Kt^n$ — модулю формальных степенных рядов $K[[t]]$.

Пример 5.7 (модуль функций со значениями в модуле)

Отображения $Z \rightarrow M$ из любого множества Z в произвольный K -модуль M можно складывать и умножать на числа из K по тем же правилам, что выше: для $\varphi, \psi : Z \rightarrow M$ 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 $Z \rightarrow M$ 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 $\varphi : Z \rightarrow M$ семейство его значений $(\varphi(z))_{z \in Z} \in \prod_{z \in Z} M_z$. Если Z является K -модулем, то K -линейные отображения $Z \rightarrow M$ составляют подмодуль $\text{Hom}_K(Z, M) \subset M^Z$.

Предложение 5.1

Для любого семейства K -модулей M_μ , занумерованных элементами μ произвольного множества \mathcal{M} , и любого K -модуля N имеется изоморфизм K -модулей

$$\prod_{\mu \in \mathcal{M}} \text{Hom}_K(M_\mu, N) \simeq \text{Hom}_K\left(\bigoplus_{\mu \in \mathcal{M}} M_\mu, N\right), \quad (5-6)$$

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

$$\bigoplus \varphi_\mu : \bigoplus_{\mu \in \mathcal{M}} M_\mu \rightarrow N, \quad (5-7)$$

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 $\psi : \bigoplus_{\mu \in \mathcal{M}} M_\mu \rightarrow N$ в семейство гомоморфизмов $\varphi_\mu : M_\mu \rightarrow N$, 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 $w_\nu = u$. \square

Пример 5.8 (продолжение прим. 5.6 на стр. 83)

В прим. 5.6 мы видели, что модуль многочленов $K[t] \simeq \bigoplus_{n \geq 0} Kt^n$ можно воспринимать как прямую сумму модулей $Kt^n \simeq K$. Применительно к этому случаю предл. 5.1 утверждает, что каждое K -линейное отображение $\varphi : K[t] \rightarrow K$ однозначно задаётся последовательностью K -линейных отображений $\varphi_n = \varphi|_{Kt^n} : Kt^n \rightarrow K$ — 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 $\varphi : K[t] \rightarrow K$ переводит многочлен $a(t) = a_0 + a_1 t + \dots + a_m t^m$ в число $\varphi(a) = f_0 a_0 + f_1 a_1 + \dots + f_m a_m$. Мы заключаем, что модуль $\text{Hom}_K(K[t], K)$ изоморфен прямому произведению счётного множества копий модуля K , т. е. модулю формальных степенных рядов $K[[x]]$. Изоморфизм сопоставляет последовательности (f_n) её производящую функцию $F(x) = \sum_{n \geq 0} f_n x^n \in K[[x]]$. Например, для любого $\alpha \in K$ гомоморфизм вычисления $\text{ev}_\alpha : K[t] \rightarrow K, f \mapsto f(\alpha)$, 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 $\sum_{n \geq 0} \alpha^n x^n = (1 - \alpha x)^{-1} \in K[[x]]$.

Упражнение 5.7. В условиях предл. 5.1 постройте изоморфизм K -модулей

$$\bigoplus_{\mu \in \mathcal{M}} \text{Hom}_K(N, M_\mu) \simeq \text{Hom}_K\left(N, \bigoplus_{\mu \in \mathcal{M}} M_\mu\right). \quad (5-8)$$

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 $\text{span}(A)$ или $\text{span}_K(A)$, 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 $x_1 a_1 + \dots + x_n a_n$ 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 $\sum_\nu U_\nu \stackrel{\text{def}}{=} \text{span} \bigcup_\nu U_\nu$. Таким образом, сумма подмодулей представляет собою множество всевозможных конечных сумм векторов, принадлежащих этим подмодулям. Например,

$$\begin{aligned} U_1 + U_2 &= \{u_1 + u_2 \mid u_1 \in U_1, u_2 \in U_2\} \\ U_1 + U_2 + U_3 &= \{u_1 + u_2 + u_3 \mid u_1 \in U_1, u_2 \in U_2, u_3 \in U_3\} \end{aligned}$$

и т. д. Если подмодули $U_1, \dots, U_m \subset M$ таковы, что гомоморфизм сложения

$$U_1 \oplus \dots \oplus U_n \rightarrow U_1 + \dots + U_n \subset M, \quad (u_1, \dots, u_n) \mapsto u_1 + \dots + u_n, \quad (5-9)$$

является биекцией между $U_1 \oplus \dots \oplus U_n$ и $U_1 + \dots + U_n$, то сумму $U_1 + \dots + U_n$ называют прямой и обозначают $U_1 \oplus \dots \oplus U_n$, как в н° 5.1.2 выше. Биективность отображения (5-9) эквивалентна тому, что каждый вектор $w \in U_1 + \dots + U_n$ имеет единственное разложение $w = u_1 + \dots + u_n$, в котором $u_i \in U_i$ при каждом i .

Предложение 5.2

Сумма подмодулей $U_1, \dots, U_n \subset V$ 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 $u_i = u_1 + \dots + u_{i-1} + u_{i+1} + \dots + u_n$, где $u_i \in U_i$ при всех i , то у этого вектора имеется два различных представления¹

$$0 + \dots + 0 + u_i + 0 + \dots + 0 = u_1 + \dots + u_{i-1} + 0 + u_{i+1} + \dots + u_n.$$

Поэтому такая сумма не прямая. Наоборот, если $U_i \cap W_i = 0$ при всех i , то переписывая равенство $u_1 + \dots + u_n = w_1 + \dots + w_n$, 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 $i = 1, \dots, n$. \square

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 $L \cap N = 0$. \square

¹В левом отлично от нуля только i -е слагаемое, а в правом оно нулевое.

5.1.4. Фактор модуля. 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 $m \equiv m' \pmod{N}$ сравнимости по модулю N , означающему, что $m' - m \in N$. Сложение классов и их умножение на элементы кольца определяются обычными формулами $[m_1]_N + [m_2]_N \stackrel{\text{def}}{=} [m_1 + m_2]_N$ 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, фактор кольцо K/I кольца K по идеалу $I \subseteq K$ 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 $\varphi : M \rightarrow N$ 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, $\iota_\varphi : M/\ker \varphi \xrightarrow{\simeq} \text{im } \varphi$ является изоморфизмом K -модулей.

Упражнение 5.10. Пусть модуль M является прямой суммой своих подмодулей $L, N \subseteq M$. Покажите, что $M/N \simeq L$ и $M/L \simeq N$.

Пример 5.10 (дополнительные подмодули и разложимость)

Подмодули $L, N \subseteq M$ 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 $I \subseteq \mathbb{Z}$ представляет собою главный идеал $I = (d)$. Согласно упр. 5.10, разложение $\mathbb{Z} = (d) \oplus N$ означает наличие в \mathbb{Z} подмодуля $N \subseteq \mathbb{Z}$, 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 $N \subseteq \mathbb{Z}^2$, 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 $L \subseteq \mathbb{Z}^2$, что $\mathbb{Z}^2 = L \oplus N$.

Пример 5.11 (фактор модуля по идеалу кольца)

Для произвольных K -модуля M и идеала $I \subseteq K$ обозначим через

$$IM \stackrel{\text{def}}{=} \{x_1 a_1 + \dots + x_n a_n \in M \mid x_i \in I, a_i \in M, n \in \mathbb{N}\}$$

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 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 5.13. Убедитесь, что оно корректно.

Если $M = N_1 \oplus \dots \oplus N_m$ раскладывается в прямую сумму своих подмодулей $N_i \subset M$, то возникает аналогичное разложение $IM = IN_1 \oplus \dots \oplus IN_m$ в сумму подмодулей $IN_i = N_i \cap IM$.

УПРАЖНЕНИЕ 5.14. Убедитесь в этом.

Мы заключаем, что в этом случае $M/IM = (N_1/IN_1) \oplus \dots \oplus (N_m/IN_m)$. В частности,

$$K^n / IK^n = (K/I)^n. \quad (5-10)$$

для любого идеала $I \subset K$.

ПРЕДЛОЖЕНИЕ 5.3

Для любых K -модулей M, N и подмодуля $L \subset M$ гомоморфизмы $\varphi : M \rightarrow N$, переводящие L в нуль, образуют подмодуль $\text{Ann}_N(L) \stackrel{\text{def}}{=} \{\varphi : M \rightarrow N \mid \varphi(L) = 0\} \subset \text{Hom}(M, N)$. Каждый гомоморфизм $\varphi \in \text{Ann}_N(L)$ корректно задаёт K -линейное отображение $\varphi_L : M/L \rightarrow N, [v]_L \mapsto \varphi(v)$. При этом отображение $\text{Ann}_N(L) \rightarrow \text{Hom}_K(M/L, N), \varphi \mapsto \varphi_L$, является изоморфизмом K -модулей, и обратный к нему изоморфизм $\text{Hom}_K(M/L, N) \rightarrow \text{Ann}_N(L), \psi \mapsto \psi\pi_L$, переводит гомоморфизм $\psi : M/L \rightarrow N$ в его композицию с эпиморфизмом факторизации $\pi_L : M \twoheadrightarrow M/L$.

Доказательство. Если $\varphi_1, \varphi_2 : M \rightarrow N$ аннулируют L , то линейная комбинация $x_1\varphi_1 + x_2\varphi_2$ тоже аннулирует L . Поэтому $\text{Ann}_N(L)$ является K -подмодулем в $\text{Hom}_K(M, N)$. Если $\varphi \in \text{Ann}_N(L)$, 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

$$\text{Ann}_N(L) \rightarrow \text{Hom}_K(M/L, N), \quad \varphi \mapsto \varphi_L,$$

является гомоморфизмом K -модулей. Поскольку для любого гомоморфизма $\psi : M/L \rightarrow N$ выполняется равенство $(\psi\pi_L)_L = \psi$, а для любого гомоморфизма $\varphi \in \text{Ann}_N(L)$ — равенство $\varphi_L\pi_L = \varphi$, отображения $\varphi \mapsto \varphi_L$ и $\psi \mapsto \psi\pi_L$ обратны друг другу и тем самым биективны. \square

5.1.5. Образующие и соотношения. Говорят, что вектор v из K -модуля M линейно выражается над K через векторы w_1, \dots, w_m , если $v = x_1w_1 + \dots + x_mw_m$ для некоторых $x_1, \dots, x_m \in K$. 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. $x_1u_1 + \dots + x_ku_k = 0$ для некоторых $u_1, \dots, u_k \in Z$ и $x_1, \dots, x_k \in K$, 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. $v = x_1 u_1 + \dots + x_m u_m$ 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 $\bigoplus_{e \in E} K e$ одинаковых копий $K e = K$ 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 $x_1 e_1 + \dots + x_n e_n = 0$, в котором $e_i \in E$ и $x_1 \neq 0$, то оно у нулевого вектора $0 \in M$ имеет 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 обеих 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 . \square

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 нуля 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, \dots, x_n) единственным образом представляется в виде линейной комбинации $x_1 e_1 + \dots + x_n e_n$ стандартных базисных векторов $e_i = (0, \dots, 0, 1, 0, \dots, 0)$, 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

$$\pi : K^m \rightarrow M, \quad (x_1, \dots, x_m) \mapsto x_1 w_1 + \dots + x_m w_m.$$

Его ядро $R = \ker \pi$ называется *модулем соотношений* между образующими w_i , поскольку оно состоит из всех тех строк $(x_1, \dots, x_m) \in K^m$, 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 $\text{rk } F$ 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 идеал¹ $\mathfrak{m} \subset K$. В прим. 5.11 на стр. 86 мы видели, что фактор модуль $F/\mathfrak{m}F$ является векторным пространством над полем $\mathbb{k} = K/\mathfrak{m}$ и изоморфен $\bigoplus_{e \in E} \mathbb{k}[e]$ в силу форм. (5-10) на стр. 87. Таким образом, классы векторов $e \in E$ составляют базис векторного пространства $F/\mathfrak{m}F$ над полем $\mathbb{k} = K/\mathfrak{m}$. Но из курса линейной алгебры известно², что все базисы векторного пространства имеют одинаковую мощность. \square

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

$$A \times A \rightarrow A, \quad (a, b) \mapsto ab,$$

которая K -линейна по a при фиксированном b и K -линейна по b при фиксированном³ 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

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

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.

¹См. прим. 4.3 на стр. 70.

²См. теор. 7.3 на стр. 93 лекции http://gorod.bogomolov-lab.ru/ps/stud/geom_ru/2122/lec_07.pdf.

³Такие функции от двух аргументов называются *билинейными*.

Отображение $\varphi : A \rightarrow B$ 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 $\text{н}^\circ 5.1.1$ 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 $\text{Hom}_K(M, M)$ всех K -линейных отображений $M \rightarrow M$ обозначается $\text{End } M$ или $\text{End}_K M$ и называется *алгеброй эндоморфизмов*¹ K -модуля M , поскольку композиция эндоморфизмов

$$\text{End}(M) \times \text{End}(M) \rightarrow \text{End}(M), \quad (\varphi, \psi) \mapsto (\varphi \circ \psi : w \mapsto \varphi(\psi(w))),$$

задаёт на $\text{End } M$ структуру ассоциативной K -алгебры с единицей, в роли которой выступает тождественный эндоморфизм $\text{Id}_M : w \mapsto w$.

УПРАЖНЕНИЕ 5.15. Проверьте, что композиция отображений ассоциативна и линейно зависит от каждого из двух компонентных отображений.

5.2.1. Алгебра матриц $\text{Mat}_n(K)$. Рассмотрим свободный координатный модуль $M = K^n$ с базисом из векторов e_1, \dots, e_n . Каждый K -линейный эндоморфизм $\varphi : K^n \rightarrow K^n$ 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 $w = x_1 e_1 + \dots + x_n e_n$,

$$\varphi(w) = \varphi(x_1 e_1 + \dots + x_n e_n) = x_1 \varphi(e_1) + \dots + x_n \varphi(e_n) = x_1 w_1 + \dots + x_n w_n,$$

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

$$\varphi_{w_1, \dots, w_n} : K^n \rightarrow K^n, \quad x_1 e_1 + \dots + x_n e_n \mapsto x_1 w_1 + \dots + x_n w_n,$$

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 $K^n \rightarrow K^n$, т. е. элементами K -модуля $\text{End } K^n$, 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 $\varphi : K^n \rightarrow K^n$, принято записывать в виде квадратной матрицы² Φ размера $n \times n$, помещая координаты j -го вектора w_j в j -й столбец этой таблицы:

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

¹Терминологию, относящуюся к отображениям множеств, см. на стр. 5.

²См. [прим. 5.3](#) на стр. 82.

Матрица $\Phi = (\varphi_{ij})$ в i -й строке и j -м столбце которой находится i -я координата вектора $\varphi(e_j)$, называется *матрицей* отображения $\varphi : K^n \rightarrow K^n$ в базисе e_1, \dots, e_n . Таким образом, сопоставляя эндоморфизму φ его матрицу Φ , мы получаем изоморфизм K -модулей

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

где $\text{Mat}_n(K) \stackrel{\text{def}}{=} \text{Mat}_{n \times n}(K)$ — модуль $n \times n$ матриц¹ с элементами из K . Изоморфизм (5-11) позволяет перенести на K -модуль матриц ассоциативное умножение с единицей, которое имеется в алгебре $\text{End}(K^n)$ из прим. 5.13 выше и задаётся композицией отображений. Возникающая таким образом билинейная ассоциативная операция

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

где Φ и Ψ суть матрицы K -линейных отображений $\varphi, \psi : K^n \rightarrow K^n$, а $\Phi\Psi$ — матрица их композиции $\varphi\psi : K^n \rightarrow K^n$, $w \mapsto \varphi(\psi(w))$, 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 $A = (a_{ij})$ и $B = (b_{ij})$ 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 $\text{Mat}_{n \times n}(K)$ является матрица тождественного отображения $\text{Id} : K^n \rightarrow K^n$

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

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

¹См. 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} :

$$E_{ik}E_{\ell j} = \begin{cases} E_{ij} & \text{при } k = \ell \\ 0 & \text{при } k \neq \ell, \end{cases} \quad (5-13)$$

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 биннома¹, 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 $\text{Mat}_{2 \times 2}(K)$ из п. 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

$$(\alpha, \beta) = (d, -b) \quad \text{и} \quad (\gamma, \delta) = (-c, a).$$

¹См. 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 $A, B \in \text{Mat}_{2 \times 2}(K)$.

Из упражнения вытекает, что для всех $A, B \in \text{Mat}_{2 \times 2}(K)$

$$\det(AB) \cdot E = AB(AB)^\vee = ABB^\vee A^\vee = A \cdot \det(B) \cdot E \cdot A^\vee = \det(B) \cdot AA^\vee = \det(A) \cdot \det(B) \cdot E,$$

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 подалгебрами¹ в $\text{Mat}_n(K)$.

Треугольные матрицы с единицами на главной диагонали называются *унитреугольными*. Покажем, что каждая верхняя унитреугольная матрица $A = (a_{ij})$ обратима² и обратная к ней матрица $B = A^{-1}$ тоже верхняя унитреугольная с наддиагональными элементами

$$\begin{aligned} b_{ij} &= \sum_{s=0}^{j-i-1} (-1)^{s+1} \sum_{i < v_1 < \dots < v_s < j} a_{iv_1} a_{v_1 v_2} a_{v_2 v_3} \dots a_{v_{s-1} v_s} a_{v_s j} = \\ &= -a_{ij} + \sum_{i < k < j} a_{ik} a_{kj} - \sum_{i < k < \ell < j} a_{ik} a_{k\ell} a_{\ell j} + \sum_{i < k < \ell < m < j} a_{ik} a_{k\ell} a_{\ell m} a_{mj} - \dots \end{aligned} \quad (5-14)$$

Для этого запишем матрицу A в виде линейной комбинации базисных матриц E_{ij} :

$$A = E + \sum_{i < j} a_{ij} E_{ij} = E + N,$$

¹Т. е. являются подмодулями, замкнутыми относительно умножения.

²Причём 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 $j - i \geq k$ представляет собою сумму всевозможных произведений¹

$$\underbrace{a_{iv_1} a_{v_1 v_2} \cdots a_{v_{k-2} v_{k-1}} a_{v_{k-1} j}}_{k \text{ сомножителей}}, \quad \text{где } i < v_1 < \cdots < v_{k-1} < j.$$

В частности, он заведомо зануляется, когда k превышает размер матрицы A . Полагая $x = E$, $y = N$ в равенстве² $(x + y)(x^{m-1} - x^{m-2}y + \cdots + (-1)^{m-1}y^{m-1}) = x^m - y^m$, при достаточно большом m мы получим матричное равенство $A(E - N + N^2 - N^3 + \cdots) = E$, откуда

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

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 $\text{Mat}_{m \times n}(R)$ 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 $L \times M \rightarrow N$, $(u, w) \rightarrow uw$, что $(x_1 u_1 + x_2 u_2)(y_1 w_1 + y_2 w_2) = x_1 y_1 u_1 w_1 + x_1 y_2 u_1 w_2 + x_2 y_1 u_2 w_1 + x_2 y_2 u_2 w_2$ 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

$$\text{Mat}_{m \times s}(L) \times \text{Mat}_{s \times n}(M) \rightarrow \text{Mat}_{m \times n}(N), \quad (A, B) \mapsto AB.$$

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:

$$(a_1, \dots, a_s) \begin{pmatrix} b_1 \\ \vdots \\ b_s \end{pmatrix} \stackrel{\text{def}}{=} a_1 b_1 + \dots + a_s b_s = \sum_{k=1}^s a_k b_k. \quad (5-15)$$

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):

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

¹Продуктивно 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.

²Поскольку 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

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \end{pmatrix} \quad (5-17)$$

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 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 $C^t = (c_{ij}^t)$ размера $n \times m$, по строкам которой записаны столбцы $m \times n$ матрицы $C = (c_{ij})$, называется *транспонированной* к матрице C . Её элементы $c_{ij}^t = c_{ji}$ 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 $c_{ij} = \sum_k a_{ik} b_{kj} = \sum_k a_{ki}^t b_{jk}^t = \sum_k b_{jk}^t a_{ki}^t = d_{ji}$. \square

УПРАЖНЕНИЕ 5.25. Убедитесь, что если операция умножения $L \times M \rightarrow N$ билинейна, то произведение матриц $\text{Mat}_{m \times s}(L) \times \text{Mat}_{s \times n}(M) \rightarrow \text{Mat}_{m \times n}(N)$ 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 $A, A_1, A_2 \in \text{Mat}_{m \times s}(L)$, $B, B_1, B_2 \in \text{Mat}_{s \times n}(M)$ 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 ассоциативные¹ умножения

$$L_1 \times L_2 \rightarrow L_{12}, \quad L_{12} \times L_3 \rightarrow L_{123}, \quad L_2 \times L_3 \rightarrow L_{23}, \quad L_1 \times L_{23} \rightarrow L_{123},$$

то при всех $m, k, \ell, n \in \mathbb{N}$ умножения матриц

$$\begin{aligned} \text{Mat}_{m \times k}(L_1) \times \text{Mat}_{k \times \ell}(L_2) &\rightarrow \text{Mat}_{m \times \ell}(L_{12}), & \text{Mat}_{m \times \ell}(L_{12}) \times \text{Mat}_{\ell \times n}(L_3) &\rightarrow \text{Mat}_{m \times n}(L_{123}), \\ \text{Mat}_{k \times \ell}(L_2) \times \text{Mat}_{\ell \times n}(L_3) &\rightarrow \text{Mat}_{k \times n}(L_{23}), & \text{Mat}_{m \times k}(L_1) \times \text{Mat}_{k \times n}(L_{23}) &\rightarrow \text{Mat}_{m \times n}(L_{123}). \end{aligned}$$

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:

$$\begin{aligned} \sum_k p_{ik} c_{kj} &= \sum_k \left(\sum_{\ell} a_{i\ell} b_{\ell k} \right) c_{kj} = \sum_{k\ell} (a_{i\ell} b_{\ell k}) c_{kj} = \\ &= \sum_{k\ell} a_{i\ell} (b_{\ell k} c_{kj}) = \sum_{\ell} a_{i\ell} \left(\sum_k b_{\ell k} c_{kj} \right) = \sum_{\ell} a_{i\ell} q_{\ell j}. \end{aligned}$$

Обратите внимание, что 2-е и 4-е равенства используют билинейность умножений. \square

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

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

причём первый из них содержится в линейной оболочке второго, т. е. каждый вектор u_j имеет вид $u_j = w_1 c_{1j} + w_2 c_{2j} + \dots + w_m c_{mj}$, где $c_{ij} \in K$. Эти n равенств собираются в одну матричную формулу $\mathbf{u} = \mathbf{w} C_{\mathbf{w}\mathbf{u}}$, где $\mathbf{u} = (u_1, \dots, u_n)$ и $\mathbf{w} = (w_1, \dots, w_m)$ суть матрицы-строки с элементами из M , а матрица $C_{\mathbf{w}\mathbf{u}} = (c_{ij})$ получается подстановкой в матрицу \mathbf{u} вместо каждого из векторов u_j столбца коэффициентов его линейного выражения через векторы w_i . Матрица $C_{\mathbf{w}\mathbf{u}}$ называется *матрицей перехода* от векторов \mathbf{u} к векторам \mathbf{w} . Название объясняется тем, что если имеется набор векторов $\mathbf{v} = (v_1, \dots, v_k)$, линейно выражающихся через векторы \mathbf{u} по формулам $\mathbf{v} = \mathbf{u} C_{\mathbf{u}\mathbf{v}}$, то выражение векторов \mathbf{v} через векторы \mathbf{w} задаётся матрицей

$$C_{\mathbf{w}\mathbf{v}} = C_{\mathbf{w}\mathbf{u}} C_{\mathbf{u}\mathbf{v}}, \tag{5-18}$$

которая возникает при подстановке $\mathbf{u} = \mathbf{w} C_{\mathbf{w}\mathbf{u}}$ в разложение $\mathbf{v} = \mathbf{u} C_{\mathbf{u}\mathbf{v}}$. В частности, если вектор $v \in \text{span}(u_1, \dots, u_n) \subset \text{span}(w_1, \dots, w_n)$ линейно выражается через векторы \mathbf{u} по формуле $v = u_1 x_1 + \dots + u_n x_n = \mathbf{u} \mathbf{x}$, где $\mathbf{x} = (x_1, \dots, x_n)^t \in K^n$ — столбец коэффициентов, то этот

¹Т. е. $(ab)c = a(bc)$ всякий раз, когда произведения определены.

же вектор выражается через векторы \mathbf{w} по формуле $v = w_1 y_1 + \dots + w_m y_m = \mathbf{w}\mathbf{y}$ со столбцом коэффициентов $\mathbf{y} = (y_1, \dots, y_m)^t \in K^m$, который связан со столбцом \mathbf{x} соотношением

$$\mathbf{y} = C_{\mathbf{w}\mathbf{u}}\mathbf{x}.$$

Отметим, что когда набор векторов $\mathbf{w} = (w_1, \dots, w_m)$ линейно зависим, у каждого вектора v из их линейной оболочки имеется много *разных* линейных выражений через векторы w_j . Поэтому обозначение $C_{\mathbf{w}\mathbf{v}}$ в этой ситуации не корректно в том смысле, что элементы матрицы $C_{\mathbf{w}\mathbf{v}}$ определяются наборами векторов \mathbf{w} и \mathbf{v} не однозначно. Тем не менее, равенство (5-18) вполне осмысленно и означает, что имея какие-нибудь линейные выражения $C_{\mathbf{w}\mathbf{u}}$ и $C_{\mathbf{u}\mathbf{v}}$ векторов \mathbf{u} через \mathbf{w} и векторов \mathbf{v} через \mathbf{u} , мы можем явно предъявить одно из линейных выражений $C_{\mathbf{w}\mathbf{v}}$ векторов \mathbf{v} через векторы \mathbf{w} , перемножив матрицы $C_{\mathbf{w}\mathbf{u}}$ и $C_{\mathbf{u}\mathbf{v}}$.

Если же набор векторов $\mathbf{e} = (e_1, \dots, e_n)$ является базисом своей линейной оболочки, то матрица перехода $C_{\mathbf{e}\mathbf{w}}$, выражающая произвольный набор векторов $\mathbf{w} = (w_1, \dots, w_m)$ через \mathbf{e} однозначно определяется наборами \mathbf{e} и \mathbf{w} , т. е. $\mathbf{u} = \mathbf{w}$ если и только если $C_{\mathbf{e}\mathbf{u}} = C_{\mathbf{e}\mathbf{w}}$. Отсюда получается следующий критерий обратимости матрицы с элементами из коммутативного кольца.

Предложение 5.6

Следующие условия на квадратную матрицу $C \in \text{Mat}_n(K)$ эквивалентны:

- 1) матрица C обратима в $\text{Mat}_n(K)$
- 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 $C^t B^t = B^t C^t = E$, и тем самым обратимость матрицы C влечёт обратимость транспонированной матрицы C^t и наоборот. Чтобы доказать равносильность первых двух условий, обозначим через $\mathbf{u} = (u_1, \dots, u_n)$ набор столбцов матрицы C , рассматриваемых как векторы координатного модуля K^n . Тогда $C = C_{\mathbf{e}\mathbf{u}}$ является матрицей перехода от векторов \mathbf{u} к стандартному базису $\mathbf{e} = (e_1, \dots, e_n)$ модуля K^n . Если векторы \mathbf{u} образуют базис в K^n , то векторы \mathbf{e} линейно через них выражаются: $\mathbf{e} = \mathbf{u} C_{\mathbf{u}\mathbf{e}}$, где $C_{\mathbf{u}\mathbf{e}} \in \text{Mat}_n(K)$. Из формулы (5-18) вытекают равенства $C_{\mathbf{e}\mathbf{e}} = C_{\mathbf{e}\mathbf{u}} C_{\mathbf{u}\mathbf{e}}$ и $C_{\mathbf{u}\mathbf{u}} = C_{\mathbf{u}\mathbf{e}} C_{\mathbf{e}\mathbf{u}}$. Так как оба набора векторов являются базисами, $C_{\mathbf{e}\mathbf{e}} = C_{\mathbf{u}\mathbf{u}} = E$. Поэтому матрицы $C_{\mathbf{u}\mathbf{e}}$ и $C_{\mathbf{e}\mathbf{u}}$ обратны друг другу. Наоборот, если матрица $C_{\mathbf{e}\mathbf{u}}$ обратима, то умножая обе части равенства $\mathbf{u} = \mathbf{e} C_{\mathbf{e}\mathbf{u}}$ справа на $C_{\mathbf{e}\mathbf{u}}^{-1}$, получаем линейное выражение $\mathbf{e} = \mathbf{u} C_{\mathbf{e}\mathbf{u}}^{-1}$ векторов \mathbf{e} через векторы \mathbf{u} . Поэтому последние линейно порождают модуль K^n . Пусть столбец $\mathbf{x} = (x_1, \dots, x_n)^t \in K^n$ таков, что $\mathbf{u}\mathbf{x} = 0$. Поскольку векторы \mathbf{e} составляют базис в K^n и $\mathbf{e} C_{\mathbf{e}\mathbf{u}}\mathbf{x} = \mathbf{u}\mathbf{x} = 0$, столбец $C_{\mathbf{e}\mathbf{u}}\mathbf{x} \in K^n$ является нулевым. Умножая его слева на $C_{\mathbf{e}\mathbf{u}}^{-1}$, заключаем, что и столбец \mathbf{x} нулевой, т. е. векторы \mathbf{u} линейно независимы. \square

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 переменных, т. е. когда $f(x_1, \dots, x_n) = f(x_{g(1)}, \dots, x_{g(n)})$ для всех биекций

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

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 $\lambda_1 \geq \dots \geq \lambda_n$, мы заключаем, что однородные симметрические многочлены степени d образуют свободный \mathbb{Z} -модуль с базисом из многочленов

$$m_\lambda = (\text{сумма всех различных мономов вида } x_1^{\lambda_{g(1)}} \dots x_n^{\lambda_{g(n)}}), \quad (5-19)$$

где $\lambda = (\lambda_1, \dots, \lambda_n)$ пробегает диаграммы Юнга¹ 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 $1 \leq k \leq n$, называются *элементарными*. Они появляются в *формулах Виета*: если $\alpha_1, \dots, \alpha_n$ — корни приведённого многочлена

$$t^n + a_1 t^{n-1} + \dots + a_n = \prod_{i=1}^n (x - \alpha_i), \quad (5-20)$$

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 $(m_1, \dots, m_n) \in \mathbb{Z}_{\geq 0}^n$ 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 Юнга². Таким образом, разложение многочлена e_μ по базису (5-19) имеет вид:

$$e_\mu = m_{\mu^t} + (\text{лексикографически младшие члены}). \quad (5-21)$$

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 унитарной. 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 $(\alpha_1 - \alpha_2)^2 = (\alpha_1 + \alpha_2)^2 - 4\alpha_1\alpha_2 = p^2 - 4q$. 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 5.29. Вычислите дискриминант кубического трёхчлена $x^3 + px + q$.

5.3.3. Матрицы линейных отображений. Пусть K -модули N и M линейно порождаются наборами векторов $\mathbf{u} = (u_1, \dots, u_n)$ и $\mathbf{w} = (w_1, \dots, w_m)$ соответственно. Всякое K -линейное отображение $F : N \rightarrow M$ однозначно задаётся набором $F(\mathbf{u}) \stackrel{\text{def}}{=} (F(u_1), \dots, F(u_n))$ своих значений на порождающих векторах и действует на произвольный вектор $v = \mathbf{u}\mathbf{x}$, где $\mathbf{x} \in K^n$ — столбец коэффициентов линейного выражения вектора v через образующие \mathbf{u} , по правилу

$$F(\mathbf{u}\mathbf{x}) = F\left(\sum_{i=1}^n u_i x_i\right) = \sum_{i=1}^n F(u_i) x_i = F(\mathbf{u})\mathbf{x}. \quad (5-22)$$

Матрица перехода от набора векторов $F(\mathbf{u})$ к образующим \mathbf{w} модуля M обозначается

$$F_{\mathbf{w}\mathbf{u}} = C_{\mathbf{w}F(\mathbf{u})} \in \text{Mat}_{m \times n}(K)$$

и называется *матрицей отображения*¹ F в образующих \mathbf{w} и \mathbf{u} . Её j -й столбец состоит из коэффициентов линейного выражения вектора $F(u_j)$ через векторы \mathbf{w} . Согласно (5-22) произвольный вектор $v = \mathbf{u}\mathbf{x} \in N$, выражающийся через образующие \mathbf{u} со столбцом коэффициентов \mathbf{x} , переводится отображением F в вектор $F(v) = \mathbf{w}F_{\mathbf{w}\mathbf{u}}\mathbf{x} \in M$, который выражается через образующие \mathbf{w} со столбцом коэффициентов $F_{\mathbf{w}\mathbf{u}}\mathbf{x}$.

Вычисление (5-22) также показывает, что для любого набора векторов $\mathbf{v} = (v_1, \dots, v_k)$ в N , любой матрицы $A \in \text{Mat}_{\ell \times k}(K)$ и любого K -линейного отображения $F : N \rightarrow M$ выполняется равенство $F(\mathbf{v}A) = F(\mathbf{v})A$.

Если K -модуль L порождается векторами $\mathbf{v} = (v_1, \dots, v_\ell)$ и K -линейные отображения

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

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

$$H(\mathbf{u}) = G(F(\mathbf{u})) = G(\mathbf{v}F_{\mathbf{v}\mathbf{u}}) = G(\mathbf{v})F_{\mathbf{v}\mathbf{u}} = \mathbf{w}G_{\mathbf{w}\mathbf{v}}F_{\mathbf{v}\mathbf{u}}.$$

¹Ср. с н° 5.2.1 на стр. 90.

Предостережение 5.3. (некорректность обозначения F_{wu}) Если образующие w линейно зависимы, то как и в п° 5.3.2, матрица F_{wu} линейного отображения F определяется образующими w и u не однозначно, поскольку набор векторов $F(u)$ имеет много разных линейных выражений через векторы w . Предыдущие формулы означают при этом, что если задано какое-то выражение $v = ux$ вектора v через образующие u , то столбец коэффициентов $y = F_{wu}x$ даёт одно из возможных линейных выражений $F(v) = wy$ вектора $F(v)$ через образующие 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 u линейно зависимы, то матрица F_{wu} не может быть произвольной: для любого линейного соотношения $ux = 0$ между векторами u в N в модуле M должно выполняться соотношение

$$0 = F(0) = F(ux) = wF_{wu}x,$$

т. е. отображение $x \mapsto F_{wu}x$ должно переводить коэффициенты любого линейного соотношения между образующими u в коэффициенты линейного соотношения между образующими w . Наоборот, если матрица F_{wu} обладает этим свойством, то правило $ux \mapsto wF_{wu}x$ корректно задаёт K -линейное отображение $N \rightarrow M$, поскольку равенство $ux_1 = ux_2$ означает, что $u(x_1 - x_2) = 0$, откуда $wF_{wu}(x_1 - x_2) = 0$, и значит, $wF_{wu}x_1 = wF_{wu}x_2$. 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 $A \in \text{Mat}_{m \times n}(K)$ тогда и только тогда является матрицей некоторого линейного отображения $F : N \rightarrow M$, когда для любого столбца $x \in R_N$ столбец $Ax \in R_M$. Две такие матрицы A и B задают одинаковые отображения $N \rightarrow M$ если и только если $(A - B)x \in R_M$ для всех $x \in K^n$. \square

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 $A \rightarrow B$ является гомоморфизмом абелевых групп¹ 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 $\mathbb{Z} \rightarrow \mathbb{Z}/(m)$, $z \mapsto [z]_m$, 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 $\mathbb{Z}/(n) \rightarrow \mathbb{Z}/(m)$ получается из некоторого \mathbb{Z} -линейного отображения $\mathbb{Z} \rightarrow \mathbb{Z}$, отправляющего n в подмодуль $(m) \subset \mathbb{Z}$. Но $\text{End}_{\mathbb{Z}}(\mathbb{Z}) \simeq \text{Mat}_1(\mathbb{Z}) \simeq \mathbb{Z}$, 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 $\mathbb{Z}/(n) \rightarrow \mathbb{Z}/(m)$ 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 $(k_1 - k_2) \text{ нок}(m, n) / n$

¹См. п° 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 $\text{Hom}_{\mathbb{Z}}(\mathbb{Z}/(n), \mathbb{Z}/(m)) \simeq \mathbb{Z}/(\text{нод}(m, n))$. При этом изоморфизме классу $[k] \in \mathbb{Z}/(\text{нод}(m, n))$ отвечает гомоморфизм $\mathbb{Z}/(n) \rightarrow \mathbb{Z}/(m)$, $[z]_n \mapsto [kz \text{ нок}(n, m)/n]_m$. В частности, для всех n, m

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

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

ПРИМЕР 5.20 (матрицы гомоморфизмов свободных модулей)

Если оба модуля N и M свободны и наборы векторов \mathbf{u} и \mathbf{w} являются их базисами, то, как мы видели в н° 5.2.1 на стр. 90, сопоставление K -линейному отображению $F : N \rightarrow M$ его матрицы $F_{\mathbf{wu}}$ в этих базисах задаёт K -линейный изоморфизм $\text{Hom}_K(N, M) \simeq \text{Mat}_{m \times n}(K)$, $F \mapsto F_{\mathbf{wu}}$. В других базисах $\mathbf{e} = \mathbf{w} C_{\mathbf{we}}$ и $\mathbf{f} = \mathbf{u} C_{\mathbf{uf}}$ матрица гомоморфизма F примет вид

$$F_{\mathbf{fe}} = C_{\mathbf{fu}} F_{\mathbf{uw}} C_{\mathbf{we}} = C_{\mathbf{uf}}^{-1} F_{\mathbf{u}} C_{\mathbf{we}} = C_{\mathbf{fu}} F_{\mathbf{u}} C_{\mathbf{ew}}^{-1}, \quad (5-23)$$

поскольку $F(\mathbf{e}) = F(\mathbf{w} C_{\mathbf{we}}) = F(\mathbf{w}) C_{\mathbf{we}} = \mathbf{u} F_{\mathbf{uw}} C_{\mathbf{uw}} = \mathbf{f} C_{\mathbf{fu}} F_{\mathbf{uw}} C_{\mathbf{uw}}$.

ПРИМЕР 5.21 (матрицы эндоморфизмов)

Пусть модуль M свободен и набор векторов \mathbf{u} составляет его базис. Матрица $F_{\mathbf{uu}}$ линейного эндоморфизма $F : M \rightarrow M$ в базисах \mathbf{u} и \mathbf{u} обозначается просто $F_{\mathbf{u}}$ и называется *матрицей эндоморфизма F в базисе \mathbf{u}* . По формуле (5-23) любом другом базисе $\mathbf{w} = \mathbf{u} C_{\mathbf{uw}}$ матрица оператора F имеет вид

$$F_{\mathbf{w}} = C_{\mathbf{wu}} F_{\mathbf{u}} C_{\mathbf{uw}} = C_{\mathbf{uw}}^{-1} F_{\mathbf{u}} C_{\mathbf{uw}} = C_{\mathbf{wu}} F_{\mathbf{u}} C_{\mathbf{wu}}^{-1}. \quad (5-24)$$

Ответы и указания к некоторым упражнениям

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 н° 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 $\varphi_\mu : N \rightarrow M_\mu$, в котором лишь конечное число ненулевых гомоморфизмов, отображение $\bigoplus_{\mu \in \mathcal{M}} \varphi_\mu : N \rightarrow \bigoplus_{\mu \in \mathcal{M}} M_\mu$, переводящее вектор $u \in N$ в семейство векторов $(\varphi_\mu(u))_{\mu \in \mathcal{M}}$ с конечным числом ненулевых членов.

Упр. 5.8. Пусть $A \not\subseteq B$ — две подгруппы в абелевой группе. Выберем $a \in A \setminus B$. 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 $\pi_N : M \rightarrow N$ и $\pi_L : M \rightarrow L$, 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 $\iota_{\pi_N} : M/L \rightarrow N$ и $\iota_{\pi_L} : M/L \rightarrow L$ из прим. 5.9 на стр. 86 являются искомыми изоморфизмами.

Упр. 5.13. Если $x' = x + u$ и $w' = w + u$, где $u \in I$, $x \in IM$, то $[x'w'] = [xw + (xu + uw + xu)] = [xw]$, 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 $IN_i \subseteq N_i \cap IM$, и при этом каждый подмодуль $N_i \cap IM$ имеет нулевое пересечение с суммой подмодулей $N_v \cap IM$ по всем $v \neq i$, ибо $N_i \cap \sum_{v \neq i} N_v = 0$.

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:

$$\begin{aligned} (AB)^\vee &= \left(\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} \right)^\vee = \begin{pmatrix} a_{11}b_{11} + a_{12}b_{21} & a_{11}b_{21} + a_{12}b_{22} \\ a_{21}b_{11} + a_{22}b_{21} & a_{21}b_{21} + a_{22}b_{22} \end{pmatrix}^\vee = \\ &= \begin{pmatrix} a_{21}b_{21} + a_{22}b_{22} & -a_{11}b_{21} - a_{12}b_{22} \\ -a_{21}b_{11} - a_{22}b_{21} & a_{11}b_{11} + a_{12}b_{21} \end{pmatrix} = \begin{pmatrix} b_{22} & -b_{12} \\ -b_{21} & b_{11} \end{pmatrix} \begin{pmatrix} a_{22} & -a_{12} \\ -a_{21} & a_{11} \end{pmatrix} = B^\vee A^\vee \end{aligned}$$

Упр. 5.25. Оба равенства проверяются прямым вычислением.