

§10. Конечны порождённые модули над кольцами главных идеалов

10.1. Модули над коммутативными кольцами. Напомним, что абелева группа M называется *унитальным модулем* над коммутативным кольцом K с единицей, если задана операция $K \times M \rightarrow M$, обладающая всеми свойствами умножения векторов на числа, перечисленными в [опр. 6.1](#) на стр. 83. Всюду далее, если специально не оговаривается противное, мы рассматриваем именно такие модули.

Абелева подгруппа $N \subset M$ в K -модуле M называется K -подмодулем, если она выдерживает умножение на элементы кольца, т. е. для всех $a \in N$ и $\lambda \in K$ $\lambda a \in N$. Подмодуль называется *собственным*, если он отличен от нуля и от всего модуля.

Фактор модуль M/N по подмодулю $N \subset M$ определяется как множество смежных классов $[m]_N = m \pmod{N} = m + N = \{m' \in M \mid m' - m \in N\}$, которые являются классами эквивалентности по отношению $m \sim_N m'$, означающему, что $m' - m \in N$. Сложение классов и их умножение на элементы кольца определяются обычными формулами:

$$[m_1] + [m_2] = [m_1 + m_2] \quad \text{и} \quad \lambda[m] = [\lambda m].$$

Упражнение 10.1. Проверьте, что эти операции корректно определены и удовлетворяют аксиомам модуля.

Гомоморфизм, или K -линейное отображение между K -модулями M и M' это гомоморфизм абелевых групп $M \rightarrow M'$, перестановочный с умножением на элементы кольца:

$$\varphi(\lambda v) = \lambda \varphi(v) \quad \forall \lambda \in K, \forall v, w \in M.$$

Таким образом, гомоморфизм модулей обладает всеми свойствами гомоморфизма абелевых групп. Например, $\varphi(0) = 0$, $\varphi(v-w) = \varphi(v) - \varphi(w)$ и т. п.. Инъективность K -линейного отображения φ равносильна тому, что φ имеет нулевое ядро $\ker(\varphi) = \{a \in M_1 \mid \varphi(a) = 0\}$.

Упражнение 10.2. Убедитесь, что ядро и образ произвольного гомоморфизма K -модулей $\varphi : M_1 \rightarrow M_2$ являются K -подмодулями в M_1 и M_2 соответственно, и постройте канонический изоморфизм $M_1/\ker(\varphi) \simeq \text{im}(\varphi)$.

K -линейные отображения $M \rightarrow N$ образуют K -модуль, который обозначается $\text{Hom}(M, N)$ или $\text{Hom}_K(M, N)$, если важно указать, над каким именно кольцом K рассматриваются модули.

10.1.1. Образующие и соотношения. Понятия линейной зависимости, линейной оболочки и линейных порождающих сохраняют смысл в любом модуле M . Набор векторов $\{e_v\}$ называется *базисом* модуля M , если каждый вектор $w \in M$ допускает единственное представление в виде конечной линейной комбинации $w = \sum \lambda_i e_{v_i}$.

Упражнение 10.3. Докажите, что набор векторов тогда и только тогда является базисом, когда он линейно независим и линейно порождает модуль.

Модуль, обладающий базисом, называется *свободным*. Примером свободного модуля является координатный модуль K^n . Число элементов в базисе свободного модуля M называется *рангом* этого модуля и обозначается $\text{rk } M$. В [теор. 10.2](#) на стр. 151 ниже мы покажем, что ранг свободного модуля не зависит от выбора базиса.

С каждым набором векторов w_1, w_2, \dots, w_m , линейно порождающих M , связан сюръективный гомоморфизм координатного модуля ранга m на модуль M , переводящий стандартный базисный вектор $e_i \in K^m$ в образующую w_i :

$$\pi_w : K^m \rightarrow M, \quad e_i \mapsto w_i, \quad (10-1)$$

Ядро $R_w \stackrel{\text{def}}{=} \ker \pi_w$ этого эпиморфизма называется *модулем соотношений* между образующими w_i , поскольку векторы $(\lambda_1, \lambda_2, \dots, \lambda_m) \in R_w$ суть коэффициенты всевозможных линейных зависимостей между векторами w_i :

$$\sum \lambda_i w_i = 0 \iff (\lambda_1, \lambda_2, \dots, \lambda_m) \in R_w.$$

Таким образом, любой конечно-порождённый K -модуль M представляется в виде

$$M = K^m / R. \quad (10-2)$$

Это представление называется *заданием M образующими и соотношениями*. Если кольцо K не является полем, наиболее интересные K -модули, как правило, *не свободны*, и любая их система образующих оказывается связанной линейными соотношениями с необратимыми коэффициентами.

Пример 10.1 (идеалы)

Каждое кольцо K является модулем над самим собой. Его подмодули $I \subset K$ — это в точности идеалы кольца K . Если идеал не является главным, то любое множество его образующих содержит хотя бы два элемента и, тем самым, линейно зависимо, поскольку любые два элемента $a, b \in K$ линейно зависимы над K : $a \cdot b - b \cdot a = 0$. Например, идеал $I = (x, y) \subset \mathbb{Q}[x, y]$, рассматриваемый как модуль над кольцом $K = \mathbb{Q}[x, y]$, порождается двумя векторами x и y . Эпиморфизм (10-1) имеет вид

$$\pi_{(x,y)} : K^2 \rightarrow I, \quad (f, g) \mapsto xf + yg.$$

Его ядро $R_{(x,y)} = \ker \pi_{(x,y)}$ представляет собою свободный модуль ранга 1 с базисным вектором $(y, -x)$. В самом деле, из факториальности кольца $\mathbb{Q}[x, y]$ вытекает, что равенство $xf = -yg$ возможно только при $f = yh, g = -xh$ для некоторого $h \in \mathbb{Q}[x, y]$. Тем самым, любое K -линейное соотношение между x и y пропорционально соотношению с коэффициентами $(y, -x)$.

Пример 10.2 (абелевы группы)

Всякая абелева группа A имеет каноническую структуру модуля над кольцом целых чисел \mathbb{Z} , заданную правилом $n \cdot a \stackrel{\text{def}}{=} \text{sgn}(n) \cdot (\underbrace{a + a + \dots + a}_{|n| \text{ слагаемых}})$, где $\text{sgn}(n) = n/|n| = \pm 1$.

Упражнение 10.4. Проверьте выполнение аксиом \mathbb{Z} -модуля.

Например, аддитивная группа вычетов $M = \mathbb{Z}/(k)$ может рассматриваться как \mathbb{Z} -модуль с операцией $n \cdot [m]_k \stackrel{\text{def}}{=} [nm]_k$, где мы обозначаем через $[m]_k = m \pmod{k}$ класс числа m по модулю k . Модуль M порождается одним элементом $[1]_k$, который удовлетворяет соотношению $k \cdot [1]_k = 0$, т.е. линейно зависим и, в частности, не является базисом. Обратите внимание, что запись $M = \mathbb{Z}/(k)$ есть ни что иное как представление (10-2) модуля M одной образующей и модулем соотношений $R = (k) \subset \mathbb{Z}$, который является

свободным \mathbb{Z} -модулем с базисным элементом k . Отметим, что соотношение $k \cdot [1]_k = 0$ влечёт за собой отсутствие ненулевых гомоморфизмов $\mathbb{Z}/(k) \rightarrow \mathbb{Z}$. В самом деле, для такого гомоморфизма φ в кольце \mathbb{Z} выполняется равенство $k \cdot \varphi([1]_k) = \varphi(k \cdot [1]_k) = \varphi(0) = 0$, откуда $\varphi([1]_k) = 0$, поскольку в \mathbb{Z} нет делителей нуля. Но тогда для всех m

$$\varphi([m]_k) = \varphi(m \cdot [1]_k) = m \cdot \varphi([1]_k) = 0.$$

Упражнение 10.5. Покажите, что класс $[n]_k$ порождает \mathbb{Z} -модуль $\mathbb{Z}/(k)$ тогда и только тогда, когда n взаимно просто с k .

10.1.2. Продолжение по линейности. Пусть K -модуль M линейно порождается векторами w_1, w_2, \dots, w_m . Тогда любой K -линейный гомоморфизм $F : M \rightarrow N$ однозначно определяется своими значениями $u_i = \varphi(w_i)$ на этих образующих: образ произвольного вектора $v = \sum x_i w_i \in M$ будет равен

$$Fv = F\left(\sum x_i w_i\right) = \sum x_i u_i. \quad (10-3)$$

Однако, если мы захотим *определить* гомоморфизм $F : M \rightarrow N$ произвольным образом указав в модуле N элементы $u_i = F(w_i)$ и по линейности продолжив F на все остальные векторы $v \in M$ формулой (10-3), то такое определение может оказаться некорректным из-за того, что линейное выражение $v = \sum x_i w_i$ через образующие *не единственно*.

Лемма 10.1

Для того, чтобы правило $w_i \mapsto u_i$ корректно продолжалось формулой (10-3) до гомоморфизма модулей $M \rightarrow N$, необходимо и достаточно, чтобы каждое линейное соотношение $\lambda \in R_w$ между образующими w_i в модуле M выполнялось также и между векторами u_i в модуле N : $\lambda_1 w_1 + \lambda_2 w_2 + \dots + \lambda_m w_m = 0 \Rightarrow \lambda_1 u_1 + \lambda_2 u_2 + \dots + \lambda_m u_m = 0$. Иначе говоря, если $M = K^m / R$, то $\text{Hom}(M, N) \simeq \{f : K^m \rightarrow N \mid f(R) = 0\}$.

Доказательство. Необходимость: если $\sum \lambda_i w_i = 0$, то $\sum \lambda_i u_i = F(\sum \lambda_i w_i) = F(0) = 0$. Наоборот, пусть каждое линейное соотношение между w_i выполняются и между u_i . Наличие двух разложений $v = x_1 w_1 + x_2 w_2 + \dots + x_n w_n = y_1 w_1 + y_2 w_2 + \dots + y_n w_n$ влечёт соотношение $\sum (x_i - y_i) \cdot w_i = 0$, а значит, и соотношение $\sum (x_i - y_i) \cdot u_i = 0$. Тогда $x_1 u_1 + x_2 u_2 + \dots + x_n u_n = y_1 u_1 + y_2 u_2 + \dots + y_n u_n$ в N , т. е. Fv не зависит от выбора разложения вектора v по образующим w_i . \square

Лемма 10.2

Набор векторов $\mathcal{E} = \{e_i\} \subset M$ тогда и только тогда является базисом K -модуля M , когда любое отображение множеств $\varphi : \mathcal{E} \rightarrow N$ в произвольный K -модуль N единственным способом продолжается до K -линейного гомоморфизма модулей $F_\varphi : M \rightarrow N$.

Доказательство. Необходимость следует из предыдущей леммы. Для доказательства достаточности образуем множество $\mathcal{E}' \simeq \mathcal{E}$, состоящее из формальных символов e'_i , взаимно однозначно соответствующих векторам $e_i \in \mathcal{E}$, и рассмотрим свободный K -модуль N с базисом \mathcal{E}' . Пусть отображение множеств $\mathcal{E} \rightarrow N$, переводящее e_i в e'_i , однозначно продолжается до гомоморфизма модулей $F : M \rightarrow N$. По предыдущей лемме отображение множеств $\mathcal{E}' \rightarrow M$, переводящее e'_i в e_i , также однозначно продолжается до гомоморфизма модулей $G : N \rightarrow M$. Поскольку и композиция $GF : M \rightarrow M$, и тождественный

гомоморфизм $\text{Id}_M : M \rightarrow M$ продолжают тавтологическое вложение $\mathcal{E} \subset M$ до K -линейного гомоморфизма $M \rightarrow M$, выполняется равенство $\psi\varphi = \text{Id}_M$. По той же самой причине $FG = \text{Id}_N$. Тем самым, F и G суть обратные друг другу изоморфизмы. \square

Упражнение 10.6. Убедитесь, что $\text{Hom}(K^m, N) \simeq N^{\oplus m}$ (прямая сумма m копий N).

10.1.3. Матрицы гомоморфизмов. Если векторы w_1, w_2, \dots, w_m порождают K -модуль M , а векторы u_1, u_2, \dots, u_n порождают K -модуль N , то каждому K -линейному гомоморфизму $F : M \rightarrow N$ можно сопоставить матрицу $F_{uw} \in \text{Mat}_{n \times m}(K)$, в j -том столбце которой стоят коэффициенты какого-нибудь линейного выражения вектора Fw_j через образующие u_i , так что $(Fw_1, Fw_2, \dots, Fw_m) = (u_1, u_2, \dots, u_n) \cdot F_{uw}$. Если образующие u_i линейно зависимы, такое матричное представление не единственно, а если линейно независимы образующие w_j , то не всякая матрица является матрицей гомоморфизма $F : M \rightarrow N$. Тем не менее, если гомоморфизм $F : M \rightarrow N$ корректно определён тем или иным способом, то для любого его матричного представления F_{uw} и любого линейного выражения $v = \sum w_j x_j$ произвольного вектора $v \in M$ через образующие w_j произведение $F_{uw} x$ матрицы F_{uw} на столбец коэффициентов x даст столбец коэффициентов одного из разложений вектора Fv по образующим u_i .

10.1.4. Тождество Гамильтона – Кэли. Пусть K — произвольное кольцо с единицей, $A \in \text{Mat}_n(K)$ — любая квадратная матрица, и $f(t) = f_0 + f_1 t + \dots + f_m t^m$ — любой многочлен с коэффициентами из K . Обозначим через $f(A) \in \text{Mat}_n(K)$ результат *вычисления*¹ многочлена f на элементе A в алгебре $\text{Mat}_n(K)$:

$$f(A) \stackrel{\text{def}}{=} f_0 E + f_1 A + f_2 A^2 + \dots + f_m A^m \in \text{Mat}_n(K).$$

Наделим координатный K -модуль K^n , векторы которого будем записывать в виде столбцов, структурой модуля над кольцом $K[t]$, полагая $f(t) \cdot v$ равным произведению столбца v на матрицу $f(A)$:

$$f(t) \cdot v \stackrel{\text{def}}{=} f(A)v = f_0 v + f_1 A v + f_2 A^2 v + \dots + f_m A^m v. \quad (10-4)$$

Упражнение 10.7. Проверьте выполнения аксиом $K[t]$ -модуля для K^n .

Векторы e_1, e_2, \dots, e_n стандартного базиса модуля K^n над K линейно порождают K^n над $K[t]$, однако над $K[t]$ они линейно зависимы. Поэтому $K[t]$ -линейное отображение умножения на t : $v \mapsto tv$ имеет в этой системе порождающих два различных матричных представления: $t \cdot E$ и A , а нулевой гомоморфизм, отображающий все векторы в нуль, можно задать ненулевой матрицей $tE - A$. По [предл. 9.4](#) умножение на $\det(tE - A)$ отображает любой вектор K^n в нуль. В силу определения (10-4) оператор умножения на $\det(tE - A)$, рассматриваемый как K -линейный оператор $K^n \rightarrow K^n$, задаётся в стандартном базисе матрицей $\chi_A(A)$ — результатом подстановки матрицы A вместо переменной t в *характеристический многочлен*

$$\chi_A(t) \stackrel{\text{def}}{=} \det(tE - A) \in K[t].$$

Поскольку K^n свободен над K , K -линейные эндоморфизмы $K^n \rightarrow K^n$ однозначно представляются своими матрицами в стандартном базисе. Поэтому матрица $\chi_A(A) \in \text{Mat}_n(K)$ это нулевая матрица. Нами установлена

¹см. н° 8.1.2 на стр. 118

Теорема 10.1 (тождество Гамильтона – Кэли)

Над любым коммутативным кольцом K с единицей при подстановке матрицы $A \in \text{Mat}_n(K)$ вместо переменной t в характеристический многочлен $\chi_A(t) = \det(tE - A) \in K[t]$ получается нулевая матрица $\chi_A(t) = \det(tE - A) \in \text{Mat}_n(K)$. \square

Пример 10.3

Всякая 2×2 матрица A удовлетворяет квадратному уравнению¹ $t^2 - \text{tr}(A) \cdot t + \det(A) = 0$, а всякая 3×3 матрица — кубическому уравнению $t^3 - \text{tr}(A) \cdot t^2 + \sigma_2(A) \cdot t - \det(A) = 0$, где

$$\sigma_2 \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} = (a_{11}a_{22} - a_{12}a_{21}) + (a_{11}a_{33} - a_{13}a_{31}) + (a_{22}a_{33} - a_{23}a_{32}).$$

10.1.5. Кручение. Пусть в кольце K нет делителей нуля. Элемент m из K -модуля M называется *элементом кручения*, если $\lambda m = 0$ для некоторого ненулевого $\lambda \in K$.

Упражнение 10.8. Убедитесь, что элементы кручения образуют в M подмодуль.

Этот подмодуль называется *подмодулем кручения* и обозначается

$$\text{Tors } M \stackrel{\text{def}}{=} \{m \in M \mid \exists \lambda \neq 0 : \lambda m = 0\}.$$

Если $\text{Tors } M = 0$, то говорят, что M *без кручения*. Например, любой идеал кольца K и любой свободный K -модуль не имеют кручения.

Упражнение 10.9. Покажите, что любой гомоморфизм $\varphi : M \rightarrow N$ в свободный от кручения модуль N переводит $\text{Tors}(M)$ в нуль.

Если $\text{Tors } M = M$, то M называется *модулем кручения*. Например, фактор K/I по любому ненулевому идеалу $I \subset K$ является K -модулем кручения.

10.1.6. Факторизация модуля по идеалу кольца. Для любого идеала $I \subset K$ и произвольного K -модуля M обозначим через $IM \subset M$ подмодуль, образованный всевозможными линейными комбинациями элементов модуля M с коэффициентами из идеала I :

$$IM = \{x_1 a_1 + x_2 a_2 + \dots + x_n a_n \mid x_i \in I, a_i \in M\}.$$

Упражнение 10.10. Проверьте, что IM действительно является K -подмодулем в M .

Фактор модуль M/IM обладает канонической структурой модуля над фактор кольцом K/I , которая корректно задаётся правилом $[\lambda]_I \cdot [w]_{IM} = [\lambda w]_{IM}$, где $[\lambda]_I = \lambda \pmod{I}$ и $[a]_{IM} = a \pmod{IM}$ обозначают классы эквивалентности элементов $\lambda \in K$ и $w \in M$.

Упражнение 10.11. Убедитесь, что это определение корректно.

10.1.7. Прямые разложения. Прямые суммы и прямые произведения модулей определяются как прямые суммы и прямые произведения соответствующих абелевых групп и наделяются покомпонентной модульной структурой дословно также, как и векторные пространства (см. н° 6.4.4 на стр. 96).

Упражнение 10.12. Покажите, что прямая сумма свободных модулей с базисами \mathcal{E}_1 и \mathcal{E}_2 (\mathcal{E}_1 и \mathcal{E}_2 обозначают множества базисных векторов) является свободным модулем с базисом $\mathcal{E}_1 \sqcup \mathcal{E}_2$.

¹ср. с форм. (8-4) на стр. 121

Если набор подмодулей $N_1, N_2, \dots, N_s \subset M$ таков, что гомоморфизм сложения

$$N_1 \oplus N_2 \oplus \dots \oplus N_s \rightarrow M, \quad (u_1, u_2, \dots, u_s) \mapsto u_1 + u_2 + \dots + u_s, \quad (10-5)$$

является изоморфизмом, то говорят, что модуль M является *прямой суммой* этих подмодулей и пишут $M = \bigoplus_i N_i$. Биjectивность гомоморфизма (10-5) означает, что каждый вектор $w \in M$ имеет единственное разложение $w = u_1 + u_2 + \dots + u_s$, в котором $u_i \in N_i$. Например, свободный K -модуль с базисом e_1, e_2, \dots, e_n является прямой суммой свободных подмодулей ранга 1, порождённых базисными векторами: $K^n = Ke_1 \oplus Ke_2 \oplus \dots \oplus Ke_n$.

Лемма 10.3

Для того чтобы модуль M распадался в прямую сумму собственных подмодулей $L, N \subset M$ необходимо и достаточно, чтобы L и N линейно порождали M и $L \cap N = 0$.

Доказательство. Сюръективность гомоморфизма сложения $\sigma : L \oplus N \rightarrow M$, $(a, b) \mapsto a + b$, равносильна тому, что L и N порождают M , а тривиальность его ядра — условию $L \cap N = 0$, ибо $(a, b) \in \ker \sigma \Rightarrow a = -b \in L \cap N$, и наоборот, $a \in L \cap N \Rightarrow (a, -a) \in \ker \sigma$. \square

Упражнение 10.13. Пусть модуль M является прямой суммой $M = L \oplus N$ подмодулей $L, N \subset M$. Покажите, что $M/N \simeq L$ и $M/L \simeq N$.

10.1.8. Разложимость и полупростота. Модули, не представимые в виде прямой суммы двух своих собственных подмодулей называются *неразложимыми*.

Например, \mathbb{Z} -модуль \mathbb{Z} неразложим, т. к. всякий собственный подмодуль $I \subset \mathbb{Z}$ — это главный идеал $I = (d)$, и из наличия разложения $\mathbb{Z} = (d) \oplus N$ вытекает, что в \mathbb{Z} есть подмодуль N , изоморфный по [упр. 10.13](#) модулю $\mathbb{Z}/(d)$. Но это невозможно, поскольку в \mathbb{Z} нет кручения.

Этот пример показывает, что над кольцом K , содержащим необратимые элементы, у подмодуля $N \subset M$ может не оказаться *дополнительного подмодуля* $L \subset M$, такого что $M = L \oplus N$, как это имело место для векторных пространств над полем.

Упражнение 10.14. Пусть $M = \mathbb{Z}^2 = \mathbb{Z} \oplus \mathbb{Z}$ и $N \subset M$ — подмодуль, порождённый векторами $(2, 1)$ и $(1, 2)$. Покажите, что $N \simeq \mathbb{Z}^2$, $M/N \simeq \mathbb{Z}/(3)$, и не существует подмодуля $L \subset M$, такого что $M = L \oplus N$.

Модуль M называется *полупростым*, если любой его собственный подмодуль $N \subset M$ отщепляется прямым слагаемым, т. е. обладает дополнительным подмодулем $L \subset M$, таким что $M = L \oplus N$. Например, \mathbb{Z} -модуль $M = \mathbb{Z}/(p) \oplus \mathbb{Z}/(p) \oplus \dots \oplus \mathbb{Z}/(p) = \mathbb{Z}^n/p\mathbb{Z}^n$, где $p \in \mathbb{N}$ — простое, полупрост, поскольку одновременно является векторным пространством над полем $\mathbb{F}_p = \mathbb{Z}/(p)$, а всякий \mathbb{Z} -подмодуль $N \subset M$ одновременно является векторным подпространством, и дополнительное к нему векторное подпространство является также и дополнительным \mathbb{Z} -подмодулем.

Упражнение 10.15. Убедитесь, что для любого разложения $M = M_1 \oplus M_2 \oplus \dots \oplus M_m$ и любого идеала $I \subset K$ выполняются равенства $IM = IM_1 \oplus IM_2 \oplus \dots \oplus IM_m$ и

$$M/IM = (M_1/IM_1) \oplus (M_2/IM_2) \oplus \dots \oplus (M_m/IM_m).$$

В частности, результатом факторизации свободного K -модуля $M = K^n$ по идеалу $I \subset K$ является свободный K/I -модуль $M/IM = (K/I)^n$ того же ранга.

Теорема 10.2 (о ранге свободного модуля)

Все базисы свободного модуля M над произвольным коммутативным кольцом K с единицей равносильны.

Доказательство. Выберем произвольный максимальный идеал $\mathfrak{m} \subset K$. Фактор $M/\mathfrak{m}M$ представляет собою векторное пространство над полем $\mathbb{k} = K/\mathfrak{m}$. Если e_1, e_2, \dots, e_m образуют базис K -модуля M , то $M = Ke_1 \oplus Ke_2 \oplus \dots \oplus Ke_m$ и $\mathfrak{m}M = \mathfrak{m}e_1 \oplus \mathfrak{m}e_2 \oplus \dots \oplus \mathfrak{m}e_m$, а $M/\mathfrak{m}M = \mathbb{k}e_1 \oplus \mathbb{k}e_2 \oplus \dots \oplus \mathbb{k}e_m \simeq \mathbb{k}^m$. Таким образом, $m = \dim_{\mathbb{k}}(M/\mathfrak{m}M)$ не зависит от выбора базиса¹. \square

Замечание 10.1. Согласно зам. 6.4. на стр. 91, доказанная выше теор. 10.2 верна и для свободных модулей бесконечного ранга.

10.2. Теорема об инвариантных множителях. Начиная с этого места и до конца параграфа мы обозначаем через K произвольное кольцо главных идеалов и по умолчанию предполагаем, что все рассматриваемые нами K -модули конечно порождены. Договоримся также понимать под свободным модулем ранга 0 нулевой модуль.

Лемма 10.4

Всякий подмодуль N конечно порождённого модуля M над произвольным кольцом главных идеалов K тоже свободен и $\text{rk } N \leq \text{rk } M$.

Доказательство. Индукция по $m = \text{rk } M$. При $m = 1$ $M \simeq K$ и подмодуль $N \subset K$ это некий главный идеал $(d) \subset K$. Если $d = 0$, то $N = 0$ свободен ранга 0. Если $d \neq 0$, то (d) свободен с базисом d , поскольку $xd = yd \Rightarrow (x - y)d = 0 \Rightarrow x = y$, т. к. в K нет делителей нуля.

Пусть теперь $m > 1$. Зафиксируем в M базис e_1, e_2, \dots, e_m и будем записывать векторы $w \in M$ строчками их координат. Первые координаты $x_1(v)$ всевозможных векторов $v \in N$ образуют идеал $(d) \subset K$. Если $d = 0$, подмодуль N содержится в свободном модуле ранга $m-1$ с базисом e_2, \dots, e_m и по индукции свободен, и $\text{rk } N \leq (m-1)$. Если $d \neq 0$, обозначим через $v_1 \in N$ какой-нибудь вектор с первой координатой d . Тогда $N = K \cdot v_1 \oplus N'$, где $N' \subset N$ — подмодуль, состоящий из векторов с нулевой первой координатой. Действительно, $(K \cdot v_1) \cap N' = 0$, и любой вектор $v \in N$ представляется в виде $\lambda v_1 + w$, где $\lambda = x_1(v)/d$ и $w = v - \lambda v_1 \in N'$. Модуль Kv_1 , порождённый вектором v_1 , свободен ранга 1, поскольку в объёмлющем свободном модуле M нет кручения. Модуль N' содержится в свободном модуле ранга $m-1$ с базисом e_2, \dots, e_m . По индукции N' свободен и $\text{rk } M \leq (m-1)$. Поэтому $N = K \cdot v_1 \oplus N'$ свободен и $\text{rk } N \leq m$. \square

Теорема 10.3 (об инвариантных множителях)

Для любого подмодуля N свободного модуля M конечного ранга над кольцом главных идеалов K в модуле M существует базис (e_1, e_2, \dots, e_m) , такой что некоторые кратности $\lambda_1 e_1, \lambda_2 e_2, \dots, \lambda_n e_n$ первых $n \leq m$ базисных векторов составляют базис в N и каждый из множителей λ_i делится на все предыдущие множители λ_j с $j < i$. Набор множителей $\lambda_1, \lambda_2, \dots, \lambda_n$ с точностью до умножения на обратимые элементы кольца не зависит от выбора такого базиса.

¹а также от выбора максимального идеала $\mathfrak{m} \subset K$

Определение 10.1

Множители $\lambda_1, \lambda_2, \dots, \lambda_n$, о которых идёт речь в [теор. 10.3](#), называются *инвариантными множителями* подмодуля $N \subset M$, а базисы e_1, e_2, \dots, e_m в M и $\lambda_1 e_1, \lambda_2 e_2, \dots, \lambda_n e_n$ в N — *взаимными базисами* модуля M и подмодуля $N \subset M$.

Доказательство [теор. 10.3](#) разбивается на несколько шагов, которым посвящены [н° 10.2.1](#) — [н° 10.2.4](#) ниже. Мы начнём с переформулировки теоремы об инвариантных множителях на языке матриц.

Предложение 10.1

Для любой матрицы $C \in \text{Mat}_{m \times k}(K)$ с элементами из кольца главных идеалов K существуют такие обратимые матрицы $F \in \text{GL}_m(K)$ и $G \in \text{GL}_k(K)$, что матрица

$$D = FCG = \begin{pmatrix} \lambda_1 & & 0 & \mathbf{0} \\ & \ddots & & \vdots \\ 0 & & \lambda_n & \vdots \\ \mathbf{0} & \dots & \dots & \mathbf{0} \end{pmatrix} \quad (10-6)$$

имеет $d_{ij} = 0$ при $i \neq j$, а каждый её диагональный элемент $d_{ii} = \lambda_i$ делится на все предшествующие диагональные элементы $d_{jj} = \lambda_j$ с $j < i$. При этом матрица D зависит только от матрицы C , и не зависит от выбора матриц F и G .

10.2.1. Вывод [теор. 10.3](#) из [предл. 10.1](#). Зафиксируем в модуле M какой-нибудь базис $w = (w_1, w_2, \dots, w_m)$, а в подмодуле $N \subset M$ — любой порождающий набор векторов $u = (u_1, u_2, \dots, u_k) = w \cdot C_{wu}$, где матрица перехода $C_{wu} \in \text{Mat}_{k \times m}$ имеет в j -том столбце координаты вектора u_j в базисе w . Применим [предл. 10.1](#) к матрице $C = C_{wu}$: пусть матрицы $F \in \text{GL}_m(K)$ и $G \in \text{GL}_k(K)$ таковы, что матрица $D = FC_{wu}G$ имеет диагональный вид (10-6). Так как матрица F обратима, набор векторов $e = wF^{-1}$ является базисом в M . Набор векторов $\varepsilon = uG$ выражается через этот базис как $\varepsilon = uG = wC_{wu}G = eFC_{wu}G = eD$, т. е. в наборе ε отличны от нуля в точности первые n векторов $\varepsilon_i = \lambda_i e_i$. Будучи пропорциональны базисным векторам модуля M , они линейно независимы. Исходный набор векторов u , порождающий N , линейно выражается через набор ε по формуле $u = \varepsilon G^{-1}$. Поэтому ненулевые векторы ε_i , $1 \leq i \leq n$, линейно порождают N и образуют базис. Это устанавливает существование взаимных базисов.

Если имеются два таких базиса $e' = (e'_1, e'_2, \dots, e'_m)$ и $e'' = (e''_1, e''_2, \dots, e''_m)$ модуля M , что некоторые кратности $\varepsilon'_i = \lambda'_i e'_i$ и $\varepsilon''_i = \lambda''_i e''_i$ их начальных n векторов составляют базисы подмодуля $N \subset M$ и удовлетворяют условиям делимости из [предл. 10.1](#), то обе диагональные матрицы перехода $C_{\varepsilon'' e''} = C_{\varepsilon' e'} C_{e' e''}$ и $C_{\varepsilon' e'} = E_n C_{\varepsilon'' e''} E_m$, где E_n и E_m — единичные $n \times n$ и $m \times m$ матрицы, удовлетворяют условиям [предл. 10.1](#) для одной и той же $n \times m$ матрицы $C = C_{\varepsilon' e'}$ и, стало быть, совпадают. Это устанавливает независимость инвариантных множителей от выбора взаимных базисов.

10.2.2. Единственность диагональной формы D в [предл. 10.1](#). Обозначим наибольший общий делитель¹ всех $k \times k$ -миноров прямоугольной матрицы C через $\Delta_k(C)$. Для

¹напомним, что он определён с точностью до умножения на обратимые элементы кольца K

диагональной матрицы

$$D = \begin{pmatrix} \lambda_1 & & 0 & \mathbf{0} \\ & \ddots & & \vdots \\ 0 & & \lambda_n & \vdots \\ \mathbf{0} & \dots & \dots & \mathbf{0} \end{pmatrix},$$

каждый диагональный элемент λ_i которой делится на все предыдущие λ_j с $j < i$,

$$\Delta_k(D) = \lambda_1 \lambda_2 \dots \lambda_k,$$

откуда $\lambda_k = \Delta_k(D) / \Delta_{k-1}(D)$. Поэтому независимость диагональной матрицы D от выбора диагонализующих матриц F и G вытекает из следующего простого утверждения.

Лемма 10.5

При умножении матрицы C слева или справа на обратимую квадратную матрицу числа $\Delta_k(C)$ не меняются¹.

Доказательство. Поскольку $\Delta_k(C) = \Delta_k(C^t)$ достаточно рассмотреть только левое умножение. Пусть $F = AC$, где A обратима. Тогда каждый $k \times k$ минор матрицы F является линейной комбинацией $k \times k$ миноров матрицы C .

Упражнение 10.16. Убедитесь в этом.

Поэтому $\Delta_k(F)$ делится на $\Delta_k(C)$. Аналогично, из равенства $C = A^{-1}F$ вытекает, что $\Delta_k(C)$ делится на $\Delta_k(F)$. Тем самым, $\Delta_k(C)$ и $\Delta_k(F)$ отличаются обратимым множителем. \square

10.2.3. Обобщённые элементарные преобразования. Матрицы F и G , приводящие заданную матрицу к диагональному виду, удовлетворяющему условиям [предл. 10.1](#), мы будем строить как композиции $F = F_r F_{r-1} \dots F_1$ и $G = G_1 G_2 \dots G_s$ последовательных умножений $A \mapsto F_i A$ (соотв. $A \mapsto A G_i$) на обратимые матрицы F_i (соотв. G_i), которые заменяют какие-либо две строки (соотв. столбца) a_i, a_j матрицы A их линейными комбинациями $a'_i = \alpha a_i + \beta a_j$ и $a'_j = \gamma a_i + \delta a_j$, а все остальные строки (соотв. столбцы) оставляют на месте. Для обратимости матрицы F_i (соотв. G_i), осуществляющей такое преобразование, достаточно чтобы её определитель $\alpha\delta - \beta\gamma$ был равен 1. Мы будем называть такие преобразования строк (соотв. столбцов) *обобщёнными элементарными преобразованиями*.

Лемма 10.6

Любую пару стоящих в одной строке (соотв. в одном столбце) матрицы A элементов (a_i, a_j) , таких что $a_i \nmid a_j$ и $a_j \nmid a_i$, можно подходящим обобщённым элементарным преобразованием содержащих их столбцов (соотв. строк) заменить парой $(d, 0)$, где $d = \text{нод}(a_i, a_j)$.

Доказательство. Запишем $d = \text{нод}(a_i, a_j)$ как $d = a_i x + a_j y$, и пусть $a_i = ad, a_j = bd$. Тогда $-a_i b + a_j a = 0$. Поэтому $(a_i, a_j) \cdot \begin{pmatrix} x & -b \\ y & a \end{pmatrix} = (d, 0)$ и $\begin{pmatrix} x & y \\ -b & a \end{pmatrix} \cdot \begin{pmatrix} a_i \\ a_j \end{pmatrix} = \begin{pmatrix} d \\ 0 \end{pmatrix}$, причём

$$\det \begin{pmatrix} x & -b \\ y & a \end{pmatrix} = \det \begin{pmatrix} x & y \\ -b & a \end{pmatrix} = ax + by = 1$$

в силу того, что $d = xa_i + ya_j = xad + ybd = (ax + by) \cdot d$. \square

¹с точностью до умножения на обратимые элементы кольца K

10.2.4. Метод Гаусса над кольцом главных идеалов. Доказательство [предл. 10.1](#), а с ним и теоремы об инвариантных множителях, завершает

Предложение 10.2

Любая прямоугольная матрица C над кольцом главных идеалов обобщёнными элементарными преобразованиями строк и столбцов приводится к диагональному виду (10-6), в котором каждый диагональный элемент делится на все предыдущие.

Доказательство. Сначала перестановками строк и столбцов добьёмся того, чтобы $c_{11} \neq 0$. Пусть в матрице C есть элемент a , не делящийся на c_{11} , и пусть $d = \text{нод}(a, c_{11})$. Тогда $(c_{11}) \subsetneq (d)$, и если мы перейдём от матрицы C к матрице C' с $c'_{11} = d$, то идеал, порождаемый левым верхним угловым элементом, строго увеличится. Покажем, что это можно сделать обобщёнными элементарными преобразованиями.

Если не делящийся на c_{11} элемент a имеется в первой строке или первом столбце, достаточно заменить пару (c_{11}, a) на $(d, 0)$ согласно [лем. 10.6](#). Если все элементы первой строки и первого столбца делятся на c_{11} , а не делящийся на c_{11} элемент a стоит строго ниже и строго левее c_{11} , то мы сначала занулим все элементы первой строки и первого столбца за исключением самого c_{11} , добавляя ко всем столбцам подходящие кратные первого столбца, а ко всем строкам — подходящие кратные первой строки. К элементу a при этом будут добавляться числа, кратные c_{11} , и он останется не делящимся на c_{11} . Далее, прибавим ту строку, где стоит a , к первой строке — получим в ней копию элемента a . Наконец, заменим пару (c_{11}, a) на $(d, 0)$ по [лем. 10.6](#).

Так как кольцо K нётерово, идеал (c_{11}) не может увеличиваться бесконечно долго, и после конечного числа таких переходов мы получим матрицу C , все элементы которой делятся на c_{11} . У этой матрицы мы обычными гауссовыми преобразованиями занулим все элементы первой строки и первого столбца кроме c_{11} . Все элементы подматрицы, стоящей в остальных строках и столбцах, при этом останутся делящимися на c_{11} . По индукции, эту подматрицу можно диагонализировать элементарными преобразованиями строк и столбцов. При этом первая строка и первый столбец не поменяются. \square

Упражнение 10.17. Припишем к матрице $C \in \text{Mat}_{m \times n}(K)$ справа и снизу единичные матрицы размеров $m \times m$ и $n \times n$ соответственно, так что получится Γ -образная таблица вида $\begin{bmatrix} C & E \\ E & \end{bmatrix}$, и приведём матрицу C к диагональному виду D , делая элементарные преобразования строк и столбцов сразу во всей Γ -образной таблице. Покажите, что в получившейся в результате таблице $\begin{bmatrix} D & F \\ G & \end{bmatrix}$ матрицы F и G таковы, что $FCG = D$.

10.2.5. Пример: абелевы подгруппы в \mathbb{Z}^m . По теореме об инвариантных множителях для любой абелевой подгруппы $L \subset \mathbb{Z}^m$ существует такой базис u_1, u_2, \dots, u_m в \mathbb{Z}^m , что некоторые кратности $m_1 u_1, m_2 u_2, \dots, m_\ell u_\ell$ первых ℓ его базисных векторов составляют базис в L . Тем самым, L тоже является свободным \mathbb{Z} -модулем, а фактор модуль

$$\mathbb{Z}^m / L \simeq \frac{\mathbb{Z}}{(m_1)} \oplus \dots \oplus \frac{\mathbb{Z}}{(m_\ell)} \oplus \mathbb{Z}^{m-\ell}. \quad (10-7)$$

Выясним, к примеру, как устроена подгруппа $L \subset \mathbb{Z}^3$, порождённая столбцами матрицы

$$C = \begin{pmatrix} 126 & 51 & 72 & 33 \\ 30 & 15 & 18 & 9 \\ 60 & 30 & 36 & 18 \end{pmatrix} \quad (10-8)$$

Для этого перейдём к взаимным базисам. Заметим, что нод всех элементов матрицы (10-8) равен 3, и мы можем получить -3 в позиции $(1, 4)$, прибавляя к 1-й строке учтёрённую 2-ю:

$$\begin{pmatrix} 6 & -9 & 0 & -3 \\ 30 & 15 & 18 & 9 \\ 60 & 30 & 36 & 18 \end{pmatrix}.$$

Умножаем 1-ю строку на -1 и меняем местами первый и последний столбцы

$$\begin{pmatrix} 3 & 9 & 0 & -6 \\ 9 & 15 & 18 & 30 \\ 18 & 30 & 36 & 60 \end{pmatrix}.$$

Теперь мы можем занулить левый столбец и верхнюю строку вне левого углового элемента, отнимая из 2-й и 3-й строк подходящие кратности 1-й строки, а затем из 2-го и 4-го столбцов подходящие кратности 1-го столбца

$$\begin{pmatrix} 3 & 0 & 0 & 0 \\ 0 & -12 & 18 & 48 \\ 0 & -24 & 36 & 96 \end{pmatrix}$$

Зануляем 3-ю строку, отнимая из неё удвоенную 2-ю, и видим, что нод элементов второй строки можно получить, прибавляя ко 2-му столбцу 3-й

$$\begin{pmatrix} 3 & 0 & 0 & 0 \\ 0 & 6 & 18 & 48 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Остаётся переставить третий столбец на место второго и занулить 3-й и 4-й столбцы, добавляя к ним подходящие кратности второго

$$\begin{pmatrix} 3 & 0 & 0 & 0 \\ 0 & 6 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Таким образом, $L \simeq \mathbb{Z}^2$, а $\mathbb{Z}^3/L \simeq \mathbb{Z}/(3) \oplus \mathbb{Z}/(6) \oplus \mathbb{Z}$.

Согласно п° 8.2, проделанные нами элементарные преобразования строк заключались в последовательном умножении слева на

$$\begin{pmatrix} 1 & -4 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ -3 & 1 & 0 \\ -6 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -2 & 1 \end{pmatrix} = \begin{pmatrix} -1 & 4 & 0 \\ 3 & -11 & 0 \\ 0 & -2 & 1 \end{pmatrix},$$

а преобразования столбцов — в последовательном умножении справа на

$$\begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & -3 & 0 & 2 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & -3 & -8 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & -3 & -8 \\ 0 & 1 & -2 & -8 \\ 1 & -3 & 9 & 26 \end{pmatrix}.$$

Упражнение 10.18. Проверьте эти формулы проделав предыдущие преобразования строк и столбцов с Γ -образной матрицей $\begin{pmatrix} C & E \\ E & \end{pmatrix}$, как в упр. 10.17.

Таким образом базис в решётке L составляют векторы $3u_1 = c_4$ и $6u_2 = c_2 + c_3 - 3c_4$, где c_2, c_3, c_4 суть последние три столбца исходной матрицы C , а u_1, u_2 — первые два вектора взаимного с L базиса объемлющей решётки \mathbb{Z}^3 , образованного столбцами матрицы

$$U = \begin{pmatrix} -1 & 4 & 0 \\ 3 & -11 & 0 \\ 0 & -2 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 11 & 4 & 0 \\ 3 & 1 & 0 \\ 6 & 2 & 1 \end{pmatrix}$$

Упражнение 10.19. Убедитесь, что следующие условия на подрешётку $L \subset \mathbb{Z}^m \subset \mathbb{Q}^m$, порождённую столбцами матрицы $C \in \text{Mat}_{m \times n}(\mathbb{Z})$, эквивалентны друг другу:

- а) $\text{rk } L = m$ б) абелева группа \mathbb{Z}^m / L конечна
- в) \mathbb{Q} -линейная оболочка L в \mathbb{Q}^m равна всему пространству \mathbb{Q}^m
- г) ранг матрицы C (рассматриваемой как матрица над полем \mathbb{Q}) равен m

Абелевы подгруппы $L \subset \mathbb{Z}^m$, удовлетворяющие условиям упр. 10.19 называются *соизмеримыми* с \mathbb{Z}^m . Отметим, что для доказательства соизмеримости с \mathbb{Z}^m подгруппы L , заданной как \mathbb{Z} -линейная оболочка столбцов некоторой целочисленной матрицы C , достаточно указать в этой матрице ненулевой минор порядка m . Для отыскания ранга L достаточно гауссовыми элементарными преобразованиями строк над полем \mathbb{Q} привести матрицу C или C^t (смотря по тому, в какой из матриц меньше строк) к ступенчатому виду с рациональными элементами.

Предложение 10.3

Столбцы матрицы $C \in \text{Mat}_n(\mathbb{Z})$ порождают абелеву подгруппу $L \subset \mathbb{Z}^n$, соизмеримую с \mathbb{Z}^n , если и только если $\det C \neq 0$. В этом случае $|\mathbb{Z}^n / L| = |\det C|$, т. е. число элементов в факторе по соизмеримой подрешётке равно объёму параллелепипеда, натянутого на любой её базис.

Доказательство. Рассмотрим в \mathbb{Z}^m базис u_1, u_2, \dots, u_m , некоторые кратности первых ℓ векторов которого $m_1 u_1, m_2 u_2, \dots, m_\ell u_\ell$ составляют базис в L . Как мы видели в н° 10.2.1, переход к таким базисам от стандартного базиса e модуля \mathbb{Z}^m и произвольного набора u из m векторов, порождающих L , описывается матричным равенством $FCG = D$, где D — диагональная, а F и G — обратимые целочисленные $m \times m$ матрицы. Обратимость матриц F и G над кольцом \mathbb{Z} равносильна равенствам $\det F = \pm 1$ и $\det G = \pm 1$. Поэтому $|\det C| = \det D$ нулевой, если $\ell < m$, и равен $m_1 m_2 \dots m_\ell$, если $\ell = m$. Во втором случае $\mathbb{Z}^m / L = \bigoplus_i \mathbb{Z} / (m_i)$, откуда $|\det C| = |\mathbb{Z}^m / L|$. \square

10.3. Теорема об элементарных делителях. Вместо упорядоченного набора инвариантных множителей $\lambda_1, \lambda_2, \dots, \lambda_n$ иногда бывает удобнее иметь дело с неупорядоченным дизъюнктивным объединением всех степеней p^μ неприводимых элементов $p \in K$, входящих в разложения чисел $\lambda_1, \lambda_2, \dots, \lambda_n$ на неприводимые множители. Точнее, рассмотрим для каждого $i = 1, \dots, n$ разложение $\lambda_i = p_{i1}^{m_{i1}} p_{i2}^{m_{i2}} \dots p_{ik_i}^{m_{ik_i}}$, в котором все p_{ij} неприводимы и различны: $p_{ij} \neq p_{ik}$ при $j \neq k$. Неупорядоченное дизъюнктивное¹ объединение

¹дизъюнктивность означает, что степень p^m , входящая в разложение ровно k инвариантных множителей λ_i , присутствует в итоговом неупорядоченном наборе в точности k раз

всех степеней $p_{ij}^{m_{ij}}$, входящих в эти разложения при $i = 1, 2, \dots, n$, называется набором *элементарных делителей* набора инвариантных множителей $\lambda_1, \lambda_2, \dots, \lambda_n$.

Лемма 10.7

Описанная выше процедура устанавливает биекцию между упорядоченными наборами чисел¹ $\lambda_1, \lambda_2, \dots, \lambda_n \in K$, в которых $\lambda_i | \lambda_j$ при $i < j$, и всевозможными неупорядоченными наборами натуральных степеней p^μ неприводимых чисел из K , в которых разрешаются повторяющиеся элементы².

Доказательство. Набор инвариантных множителей $\lambda_1, \lambda_2, \dots, \lambda_n$ однозначно восстанавливается по набору элементарных делителей следующим образом. Занумеруем простые числа p , представленные в наборе элементарных делителей, в порядке (нестрогого) убывания количества имеющихся в нём степеней p^m с основанием p и разместим элементарные делители в клетки диаграммы Юнга, записав в k -тую строку все степени p_k^μ k -го числа p_k в порядке (нестрогого) убывания их показателей μ . Поскольку наибольший инвариантный множитель λ_n делится на все остальные, его разложение на простые множители содержит *все* простые элементы p_i , причём с максимальными показателями. Таким образом, λ_n является произведением всех элементарных делителей, стоящих в первом столбце диаграммы Юнга. По индукции мы заключаем, что произведения элементарных делителей по столбцам диаграммы образуют прочитанную справа налево последовательность инвариантных множителей. \square

Пример 10.4

Набор элементарных делителей

$$\begin{array}{ccccccc} 3^2 & 3^2 & 3 & 3 & 3 & & \\ 2^3 & 2^3 & 2^2 & 2 & & & \\ 5 & 5 & & & & & \\ 7 & & & & & & \end{array}$$

возникает из такого набора инвариантных множителей:

$$\lambda_1 = 3, \lambda_2 = 3 \cdot 2, \lambda_3 = 3 \cdot 2^2, \lambda_4 = 3^2 \cdot 2^3 \cdot 5, \lambda_5 = 3^2 \cdot 2^3 \cdot 5 \cdot 7.$$

Теорема 10.4 (об элементарных делителях)

Всякий конечно порождённый модуль M над произвольным кольцом главных идеалов K изоморфен модулю вида

$$M = K^{n_0} \oplus \frac{K}{(p_1^{n_1})} \oplus \dots \oplus \frac{K}{(p_\alpha^{n_\alpha})} \quad (10-9)$$

где элементы $p_\nu \in K$ просты и $m_\nu \in \mathbb{N}$ (и p_ν и m_ν могут повторяться). Два модуля

$$K^{n_0} \oplus \frac{K}{(p_1^{n_1})} \oplus \dots \oplus \frac{K}{(p_\alpha^{n_\alpha})} \quad \text{и} \quad K^{m_0} \oplus \frac{K}{(q_1^{m_1})} \oplus \dots \oplus \frac{K}{(q_\beta^{m_\beta})}$$

¹рассматриваемых с точностью до умножения на обратимые элементы кольца K

²два таких набора считаются одинаковыми, если их можно привести в биективное соответствие друг с другом так, что у соответственных элементов p^μ и q^ν числа p и q отличаются обратным множителем, а показатели степеней совпадают

изоморфны тогда и только тогда, когда $n_0 = m_0$, $\alpha = \beta$ и слагаемые можно перенумеровать так, что $n_\nu = m_\nu$, а $p_\nu = s_\nu q_\nu$ с обратимыми $s_\nu \in K$. \square

Определение 10.2

Набор (возможно повторяющихся) степеней $p_i^{n_i}$, по которым происходит факторизация в правых слагаемых разложения (10-9), называется *набором элементарных делителей* модуля M .

Доказательство теор. 10.4 проводится в н° 10.3.1 – н° 10.3.4 ниже.

10.3.1. Существование разложения (10-9). Пусть w_1, w_2, \dots, w_m порождают M . Тогда $M = K^m / R$, где R — ядро эпиморфизма $K^m \rightarrow M$, переводящего стандартные базисные векторы $e_i \in K^m$ в образующие $w_i \in M$, как в н° 7.4. По теор. 10.3 в K^m существует такой базис u_1, u_2, \dots, u_m , что некоторые кратности $\lambda_1 u_1, \lambda_2 u_2, \dots, \lambda_k u_k$ первых k базисных векторов составляют базис в R . Таким образом,

$$M = K^m / R = \frac{K}{(\lambda_1)} \oplus \dots \oplus \frac{K}{(\lambda_k)} \oplus K^{m-k}.$$

Разложим каждый инвариантный множитель $\lambda = \lambda_i$ в произведение степеней различных простых: $\lambda = p_1^{m_1} p_2^{m_2} \dots p_s^{m_s}$. По китайской теореме об остатках

$$K/(\lambda) = K/(p_1^{m_1}) \oplus K/(p_2^{m_2}) \oplus \dots \oplus K/(p_s^{m_s}),$$

что и даёт разложение (10-9). Чтобы установить его единственность, мы дадим инвариантное описание всех слагаемых во внутренних терминах модуля M .

10.3.2. Отщепление кручения. Сумма $K/(p_1^{n_1}) \oplus \dots \oplus K/(p_\alpha^{n_\alpha})$ в разложении (10-9) совпадает с подмодулем кручения $\text{Tors } M = \{w \in M \mid \exists \lambda \neq 0 : \lambda w = 0\}$, а число n_α в разложении (10-9) равно рангу свободного модуля $M / \text{Tors } M$ и не зависит от выбора разложения. Из существования разложения (10-9) вытекает

Следствие 10.1

Всякий конечно порождённый модуль над кольцом главных идеалов является прямой суммой свободного модуля и подмодуля кручения (в частности, любой модуль без кручения автоматически свободен). \square

10.3.3. Отщепление p -кручения. Для каждого неприводимого $p \in K$ назовём p -кручением в M подмодуль, образованный всеми векторами, которые аннулируются умножением на какую-нибудь степень числа p :

$$\text{Tors}_p M \stackrel{\text{def}}{=} \{w \in M \mid \exists k > 0 : p^k w = 0\}.$$

Если простое $q \in K$ не ассоциировано с p , то класс p^k обратим в $K/(q^m)$, и гомоморфизм умножения на $p^k : K/(q^m) \rightarrow K/(q^m)$, $x \mapsto p^k x$, является изоморфизмом, в частности — не имеет ядра. Напротив, каждый модуль $K/(p^\ell)$ полностью аннулируется умножением на достаточно большую степень p . Поэтому прямая сумма всех слагаемых вида $K/(p^m)$ в разложении (10-9) совпадает с подмодулем p -кручения $\text{Tors}_p M \subset M$ и тоже не зависит от выбора разложения, а из наличия разложения (10-9) вытекает

Следствие 10.2

Всякий конечно порождённый модуль кручения над кольцом главных идеалов является прямой суммой подмодулей p -кручения по всем простым $p \in K$, для которых p -кручение ненулевое. \square

Упражнение 10.20. Обозначим через $\varphi_n : K/(p^m) \rightarrow K/(p^m)$ гомоморфизм умножения на $p^n : x \mapsto p^n x$. Покажите, что $\varphi_n = 0$ при $n \geq m$, и $\ker \varphi_n = \text{im } \varphi_{m-n} \simeq K/(p^n)$ при $0 < n < m$, причём $\ker \varphi_n \supset \ker \varphi_{n-1}$ и фактор $\ker \varphi_n / \ker \varphi_{n-1}$ нулевой при $n > m$ и изоморфен $K/(p)$ при $1 \leq n \leq m$.

10.3.4. Инвариантность показателей p -кручения. Для завершения доказательства теор. 10.4 остаётся проверить, что (нестрого) убывающий набор $v_1 \geq v_2 \geq \dots \geq v_k$ показателей степеней простого числа $p \in K$ в разложении

$$M = \frac{K}{(p^{v_1})} \oplus \dots \oplus \frac{K}{(p^{v_k})}$$

однозначно определяется модулем M . Рассмотрим диаграмму Юнга v со строками длины v_1, v_2, \dots, v_k и обозначим через $\varphi_i : M \rightarrow M$ гомоморфизм умножения на $p^i : v \mapsto p^i v$. Согласно упр. 10.20 для каждого $i = 1, 2, \dots$ фактор модуль $\ker \varphi_i / \ker \varphi_{i-1}$ является прямой суммой одинаковых слагаемых $K/(p)$ в количестве, равном числу тех строк диаграммы v , длина которых не меньше i , т. е. высоте i -того столбца диаграммы v .

Упражнение 10.21. Убедитесь, что на фактор модуле $\ker \varphi_i / \ker \varphi_{i-1}$ имеется корректно определённая структура $K/(p)$ -модуля.

Поскольку $K/(p)$ — поле, фактор $\ker \varphi_i / \ker \varphi_{i-1}$ является векторным пространством над ним, и высота i -того столбца диаграммы¹ v равна размерности этого пространства

$$v_i^t = \dim_{K/(p)} \ker \varphi_i / \ker \varphi_{i-1}.$$

Таким образом, диаграмма v показателей p -кручения однозначно определяется модулем M . Теорема об элементарных делителях полностью доказана.

10.4. Строеение конечно порождённых абелевых групп. Над кольцом $K = \mathbb{Z}$ теорема об элементарных делителях доставляет полную классификацию конечно порождённых абелевых групп.

Теорема 10.5

Всякая конечно порождённая абелева группа изоморфна прямой сумме аддитивных групп

$$\mathbb{Z}^r \oplus \frac{\mathbb{Z}}{(p_1^{n_1})} \oplus \dots \oplus \frac{\mathbb{Z}}{(p_\alpha^{n_\alpha})} \quad (10-10)$$

где $p_\nu \in \mathbb{N}$ — простые числа (не обязательно различные). Две аддитивных группы

$$\mathbb{Z}^r \oplus \frac{\mathbb{Z}}{(p_1^{n_1})} \oplus \dots \oplus \frac{\mathbb{Z}}{(p_\alpha^{n_\alpha})} \quad \text{и} \quad \mathbb{Z}^s \oplus \frac{\mathbb{Z}}{(q_1^{m_1})} \oplus \dots \oplus \frac{\mathbb{Z}}{(q_\beta^{m_\beta})}$$

изоморфны тогда и только тогда, когда $r = s$, $\alpha = \beta$ и после надлежащей перестановки слагаемых $n_\nu = m_\nu$ и $p_\nu = q_\nu$ при всех ν . \square

¹высота i -того столбца диаграммы v , это то же самое, что длина i -той строки диаграммы v^t , транспонированной к v .

Определение 10.3

Единственное представление заданной конечно порождённой абелевой группы A в виде прямой суммы аддитивных групп (10-10) называется её *каноническим представлением*.

Пример 10.5 (группы, заданные образующими и соотношениями)

На практике конечно порождённые абелевы группы часто задаются описанием вроде: абелева группа A , порождённая элементами a_1, a_2, \dots, a_n , связанными соотношениями

$$\begin{cases} \mu_{11}a_1 + \mu_{12}a_2 + \dots + \mu_{1n}a_n = 0 \\ \mu_{21}a_1 + \mu_{22}a_2 + \dots + \mu_{2n}a_n = 0 \\ \mu_{31}a_1 + \mu_{32}a_2 + \dots + \mu_{3n}a_n = 0 \\ \dots \dots \dots \dots \dots \\ \mu_{\mu 1}a_1 + \mu_{\mu 2}a_2 + \dots + \mu_{\mu n}a_n = 0, \end{cases} \quad (10-11)$$

где $\mu_{ij} \in \mathbb{Z}$. По определению, это означает, что $A = \mathbb{Z}^n / R$, где $R \subset \mathbb{Z}^n$ — подмодуль, порождённый строками $\mu_1, \mu_2, \dots, \mu_m$ матрицы (μ_{ij}) . В каноническом разложении (10-10) группы A ранг r свободного слагаемого равен $n - \text{rk}(\mu_{ij})$, а степени $p_i^{n_i}$ суть элементарные делители подмодуля $R \subset \mathbb{Z}^n$.

Про конкретный элемент $w = x_1a_1 + x_2a_2 + \dots + x_na_n$ часто бывает нужно знать, отличен он от нуля в A или нет, и если нет, то каков его порядок¹ $\text{ord}(w)$. Выяснить это можно посредством вычислений в векторном пространстве $\mathbb{Q}^n \supset \mathbb{Z}^n$ над полем \mathbb{Q} : если w не лежит в \mathbb{Q} -линейной оболочке строк матрицы (μ_{ij}) , то никакое его целое кратное mw не лежит в M , т. е. $w \neq 0$ в A и $\text{ord} w = \infty$; если же $w = x_1\mu_1 + x_2\mu_2 + \dots + x_m\mu_m$, где $x_i = p_i/q_i \in \mathbb{Q}$ — несократимые дроби, то $\text{ord}(w) = \text{нок}(q_1, q_2, \dots, q_m)$; в частности, если все $q_i = 1$ (т. е. все $x_i \in \mathbb{Z}$), то $w = 0$ в $A = \mathbb{Z}^n / R$.

¹напомним, что *порядком* $\text{ord}(w)$ элемента w в аддитивной абелевой группе называется наименьшее такое $n \in \mathbb{N}$, что $nw = 0$, или же $\text{ord}(w) = \infty$, если такого n нет (см. н° 3.5.1 на стр. 46)

Ответы и указания к некоторым упражнениям

- Упр. 10.1. Все проверки проводятся дословно также, как для классов вычетов по модулю идеала коммутативного кольца (ср. с [упр. 5.7](#) на стр. 72).
- Упр. 10.2. Изоморфизм $M_1/\ker(\varphi) \simeq \text{im}(\varphi)$ переводит класс $m \pmod{\ker \varphi}$ в $\varphi(m)$. Проверка корректности и биективности стандартна.
- Упр. 10.8. Если $\lambda_1 m_1 = 0$ и $\lambda_2 m_2 = 0$, то $\lambda_1 \lambda_2 (m_1 \pm m_2) = 0$, где $\lambda_1 \lambda_2 \neq 0$, т. к. в K нет делителей нуля. Кроме того, $\forall \mu \in K \quad \lambda_1 (\mu m_1) = \lambda_2 (\mu m_2) = 0$.
- Упр. 10.11. Если $\lambda' = \lambda + x$ и $a' = a + v$, где $x \in I$, $v \in IM$, то $\lambda' a' = \lambda a + (xa + \lambda v + xv)$, где взятая в скобки сумма лежит в IM .
- Упр. 10.16. Рассмотрим в грасмановой алгебре $K \langle \xi_1, \xi_2, \dots, \xi_m \rangle$ два набора линейных форм $\eta = \xi \cdot A$ и $\zeta = \eta \cdot C = \xi \cdot F$, где $F = AC$. Тогда грасмановы мономы степени k от η и ζ суть $\eta_I = \sum_J \xi_J a_{JI}$ и $\zeta_K = \sum_L \xi_L f_{LK}$. Поскольку $\zeta_I = \sum_J \eta_J c_{JI}$, мы получаем $f_{LK} = \sum_J a_{LJ} c_{JK}$.
- Упр. 10.17. Пусть проделанные с матрицей C преобразования строк заключаются в последовательном умножении слева на матрицы $S_k \dots S_2 S_1$, а проделанные преобразования столбцов — в умножении справа на $R_1 R_2 \dots R_\ell$. Тогда $F = S_k \dots S_2 S_1 E$ и $G = E R_1 R_2 \dots R_\ell$.
- Упр. 10.19. Равносильность условий (а), (б) и (в) очевидна после перехода к взаимным базисам \mathbb{Z}^m и подрешётки. Равносильность (в) и (г) вытекает прямо из определения ранга.
- Упр. 10.20. Равенство $\varphi_n = 0$ при $n \geq m$ очевидно. Пусть $0 \leq n < m$. Если $\varphi_n(x) = 0$, то $p^n x = p^m y$ для некоторого $y \in K$, откуда $x = p^{m-n} y$, т. к. в K нет делителей нуля. Наоборот, если $x = p^{m-n} y$, то $p^n x = 0 \pmod{p^m}$. Тем самым, $\ker \varphi_n = \text{im} \varphi_{m-n}$. Правило $x \pmod{p^n} \mapsto p^{m-n} x \pmod{p^m}$ корректно задаёт инъективный гомоморфизм K -модулей $K/(p^n) \rightarrow K/(p^m)$, который изоморфно отображает $K/(p^n)$ на $\text{im} \varphi_{m-n}$.
- Упр. 10.21. Достаточно проверить это для каждого отдельного слагаемого $K/(p^m)$. В этом случае фактор $\ker \varphi_i \ker \varphi_{i-1}$ состоит из классов вида $[p^{n-i} x] \in K/(p^m)$ по модулю классов вида $[p^{n-i+1} y]$, и все они аннулируются¹ умножением на p . Поэтому умножение на классы из $K/(p)$ определено корректно.

¹по модулю $p^{n-i+1} K$