§9. Конечно порождённые модули над кольцами главных идеалов

Всюду в этом параграфе K по умолчанию означает произвольное кольцо главных идеалов. Все рассматриваемые нами K-модули предполагаются конечно порождёнными. Под свободным K-модулем ранга нуль понимается нулевой K-модуль.

9.1. Метод Гаусса. Рассмотрим произвольную матрицу $A \in \mathrm{Mat}_{m\times n}(K)$ над кольцом главных идеалов K. Элементарным преобразованием строк матрицы A называется замена каких-либо её двух строк a_i и a_j их линейными комбинациями $a_i' = \alpha a_i + \beta a_j$ и $a_j' = \gamma a_i + \delta a_j$ с определителем $\alpha\delta - \beta\gamma = \pm 1$. В этом случае матрица преобразования

$$\begin{pmatrix} a_i \\ a_j \end{pmatrix} \mapsto \begin{pmatrix} a_i' \\ a_j' \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} a_i \\ a_j \end{pmatrix}$$

обратима, и строки a_i и a_j могут быть выражены обратно через преобразованные строки a_i' и a_j' по формулам $a_i' = \delta a_i - \beta a_j$, $a_j' = -\gamma a_i + \alpha a_j$, если $\alpha\delta - \beta\gamma = 1$, и по формулам $a_i' = -\delta a_i + \beta a_j$, $a_j' = \gamma a_i - \alpha a_j$, если $\alpha\delta - \beta\gamma = -1$.

Упражнение 9.1. Убедитесь в этом.

Таким образом, элементарное преобразование строк матрицы A не меняет линейной оболочки строк матрицы и заключается в умножении матрицы A слева на такую обратимую матрицу $L \in \mathrm{GL}_m(K)$, которая получается из единичной $m \times m$ матрицы E тем же самым элементарным преобразованием строк, которое производится в матрице A.

Симметричным образом, элементарное преобразование столбцов матрицы A заключается в замене каких-либо её двух столбцов a_i и a_j их линейными комбинациями $a_i' = \alpha a_i + \beta a_j$ и $a_j' = \gamma a_i + \delta a_j$ с определителем $\alpha\delta - \beta\gamma = \pm 1$. Такое преобразование не меняет линейной оболочки столбцов матрицы A и заключается в умножении матрицы A справа на обратимую матрицу $R \in \mathrm{GL}_n(K)$, которая получается из единичной $n \times n$ матрицы E тем же самым элементарным преобразованием столбцов, которое производится в матрице A.

Лемма 9.1
Любую пару стоящих в одной строке (соотв. в одном столбце) матрицы A ненулевых элементов (a, b) можно подходящим элементарным преобразованием содержащих их столбцов (соотв. строк) заменить парой $(d, 0)$, где $d = \mathrm{нод}(a, b)$ — наибольший общий делитель[1] a и b.

Доказательство. Запишем $d = \mathrm{нод}(a, b)$ как $d = ax + by$ и пусть $a = da'$, $b = db'$. Тогда $a'x + b'y = 1$ и $a'b - b'a = 0$. Таким образом,

$$(a, b) \cdot \begin{pmatrix} x & -b' \\ y & a' \end{pmatrix} = (d, 0) \quad \text{и} \quad \begin{pmatrix} x & y \\ -b' & a' \end{pmatrix} \cdot \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} d \\ 0 \end{pmatrix},$$

где $\det \begin{pmatrix} x & -b' \\ y & a' \end{pmatrix} = \det \begin{pmatrix} x & y \\ -b' & a' \end{pmatrix} = 1$. □

[1] Напомню, что он определён с точностью до умножения на обратимые элементы кольца K, см. n° 5.3.2 на стр. 72.

Теорема 9.1
Любая прямоугольная матрица C над кольцом главных идеалов конечным числом элементарных преобразований строк и столбцов может быть преобразована в такую матрицу D, у которой $d_{ij} = 0$ при $i \neq j$ и $d_{ii} \mid d_{jj}$ при $i < j$, причём эта матрица D не зависит от выбора последовательности элементарных преобразований.

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 всегда можно сделать элементарными преобразованиями.

Если не делящийся на c_{11} элемент a стоит в первой строке или первом столбце, достаточно заменить пару (c_{11}, a) на $(d, 0)$ согласно лем. 9.1. Если все элементы первой строки и первого столбца делятся на c_{11}, а не делящийся на c_{11} элемент a стоит строго ниже и правее 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 и получим в первой строке копию элемента a. Наконец, заменим пару (c_{11}, a) на $(d, 0)$ по лем. 9.1.

Так как кольцо главных идеалов нётерово, идеал (c_{11}) не может увеличиваться бесконечно долго, и после конечного числа описанных выше переходов мы получим матрицу C, все элементы которой делятся на c_{11}. У этой матрицы, как уже объяснялось выше, можно обнулить все элементы первой строки и первого столбца за исключением c_{11}. Все элементы подматрицы, стоящей в остальных строках и столбцах, при этом останутся делящимися на c_{11}. По индукции, эту подматрицу можно диагонализовать элементарными преобразованиями строк и столбцов. При этом первая строка и первый столбец не поменяются.

Чтобы доказать независимость получающейся в результате диагональной матрицы D от выбора цепочки элементарных преобразований, обозначим через $\Delta_k(C) \in K$ наибольший общий делитель всех $k \times k$-миноров прямоугольной матрицы $C \in \mathrm{Mat}_{m\times n}(K)$. Для матрицы D, ненулевые элементы которой исчерпываются стоящими на главной диагонали числами

$$d_{11} \mid d_{22} \mid \ldots \mid d_{rr}\,,$$

каждое из которых делит все последующие, $\Delta_k(D) = d_{11}d_{22}\ldots d_{kk}$, откуда $d_{kk} = \Delta_k(D)/\Delta_{k-1}(D)$. В силу идущей ниже леммы $\Delta_k(D) = \Delta_k(C)$, поскольку матрица $D = LCR$ получается из матрицы C умножением слева и справа на обратимые матрицы $L \in \mathrm{GL}_m(K)$ и $R \in \mathrm{GL}_n(K)$. Это доказывает независимость итоговых диагональных элементов $d_{kk} = \Delta_k(C)/\Delta_{k-1}(C)$ от выбора преобразований. □

Лемма 9.2
При умножении матрицы C слева или справа на обратимую квадратную матрицу наибольший общий делитель $\Delta_k(C)$ её $k \times k$-миноров не меняется[1].

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

Упражнение 9.2. Убедитесь в этом.

[1] С точностью до умножения на обратимые элементы кольца K.

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. □

Определение 9.1
Числа $\lambda_k(C) \stackrel{\text{def}}{=} \Delta_k(C)/\Delta_{k-1}(C)$ называются *инвариантными множителями* прямоугольной матрицы $C \in \mathrm{Mat}_{m\times n}(K)$.

Следствие 9.1
Для любой матрицы $C \in \mathrm{Mat}_{m\times n}(K)$ над кольцом главных идеалов K существуют такие обратимые матрицы $L \in \mathrm{GL}_m(K)$ и $R \in \mathrm{GL}_n(K)$, что матрица $D = LCR$ имеет $d_{kk} = \lambda_k = \Delta_k(C)/\Delta_{k-1}(C)$ и $d_{ij} = 0$ при $i \neq j$. □

Замечание 9.1. Обратимые матрицы L и R, преобразующие матрицу C в диагональную матрицу $D = LCR$, представляют собою произведения $L = L_\ell \dots L_2 L_1$ и $R = R_1 R_2 \dots R_r$ обратимых матриц L_i и R_j, осуществляющих последовательные элементарные преобразования строк и столбцов матрицы C. Таким образом, $L = L_\ell \dots L_1 E$ и $R = E R_1 \dots R_r$ получаются применением к единичным матрицам E размеров $m \times m$ и $n \times n$ тех же самых цепочек элементарных преобразований строк и соответственно столбцов, которые осуществляются с матрицей C. Поэтому для явного отыскания матриц L и R следует приписать к матрице $C \in \mathrm{Mat}_{m\times n}(K)$ справа и снизу единичные матрицы размеров $m \times m$ и $n \times n$ соответственно, так что получится Г-образная таблица вида $\left[\begin{array}{c|c} C & E \\ \hline E & \end{array}\right]$, и в процессе приведения матрицы C к диагональному виду осуществлять элементарные преобразования строк и столбцов сразу во всей Г-образной таблице. Тогда на выходе получится Г-образная таблица $\left[\begin{array}{c|c} D & L \\ \hline R & \end{array}\right]$, содержащая наряду с итоговой диагональной матрицей D искомые матрицы L и R, такие что $LCR = D$.

9.2. Теорема об инвариантных множителях. Как мы видели в прим. 6.12 на стр. 87, произвольный K-модуль M, линейно порождённый над K векторами $w_1, \dots, w_m$, является фактором $M \simeq K^m/R_{\boldsymbol{w}}$ координатного модуля K^m по подмодулю $R_{\boldsymbol{w}} \subset K^m$ линейных соотношений между порождающими векторами $\boldsymbol{w}$. Подмодуль $R_{\boldsymbol{w}}$ состоит из всех таких $(x_1, \dots, x_m) \in K^m$, что $x_1 w_1 + \dots + x_m w_m = 0$ в M и представляет собою ядро эпиморфизма

$$\pi_{\boldsymbol{w}} : K^m \twoheadrightarrow M\,, \quad (x_1, \dots, x_m) \mapsto x_1 w_1 + \dots + x_m w_m\,. \tag{9-1}$$

Согласно теор. 6.5 на стр. 93 подмодуль соотношений тоже свободен и имеет $\mathrm{rk}\, R_{\boldsymbol{w}} \leqslant m$. Следующая теорема позволяет выбрать в модуле соотношений особенно удобный базис.

Теорема 9.2 (об инвариантных множителях)
Для любого подмодуля N в свободном модуле F ранга m над кольцом главных идеалов K существует такой базис $\boldsymbol{e} = (e_1, \dots, e_m)$ модуля F над K, что подходящие кратности $\lambda_1 e_1, \dots, \lambda_n e_n$ первых $n \leqslant m$ его базисных векторов составляют базис в N, причём каждый из множителей λ_i делится на все предыдущие множители λ_j с $j < i$. Набор множителей $\lambda_1, \dots, \lambda_n$ с точностью до умножения на обратимые элементы из K не зависит от выбора такого базиса.

Доказательство. Зафиксируем произвольный базис $\boldsymbol{w} = (w_1, \dots, w_m)$ в F и какой-нибудь набор векторов $\boldsymbol{u} = (u_1, \dots, u_k) = \boldsymbol{w}\, C_{\boldsymbol{wu}}$, порождающих подмодуль $N \subset F$. Напомню, что в j-м столбце матрицы $C_{\boldsymbol{wu}}$ стоят координаты образующей u_j в базисе $\boldsymbol{w}$. По сл. 9.1 существуют такие обратимые матрицы $L \in \mathrm{GL}_m(K)$ и $R \in \mathrm{GL}_k(K)$, что матрица $D = L C_{\boldsymbol{wu}} R$ имеет $d_{ij} = 0$

при $i \neq j$, а каждый её диагональный элемент $d_{ii} = \lambda_i$ делится на все предыдущие. Так как матрица L обратима, набор векторов $\boldsymbol{e} = \boldsymbol{w}\,L^{-1}$ является базисом в F. Набор векторов $\boldsymbol{v} = \boldsymbol{u}\,R$ выражается через этот базис по формуле $\boldsymbol{v} = \boldsymbol{u}\,R = \boldsymbol{w}\,C_{\boldsymbol{wu}}R = \boldsymbol{e}\,LC_{\boldsymbol{wu}}R = \boldsymbol{e}\,D$. Тем самым, в наборе $\boldsymbol{v}$ отличны от нуля в точности первые n векторов $v_i = \lambda_i e_i$. Будучи пропорциональны базисным векторам свободного модуля F, они линейно независимы. Исходный набор образующих $\boldsymbol{u}$ подмодуля N линейно выражается через $\boldsymbol{v}$ по формуле $\boldsymbol{u} = \boldsymbol{v}\,L^{-1}$. Тем самым, ненулевые векторы v_i с $1 \leqslant i \leqslant n$ линейно порождают подмодуль N, а значит, образуют в нём базис. Это устанавливает существование базисов с требуемыми свойствами.

Если в F имеются такие базисы $\boldsymbol{e}' = (e'_1, \dots, e'_m)$ и $\boldsymbol{e}'' = (e''_1, \dots, e''_m)$, что некоторые кратности $v'_i = \lambda'_i e'_i$ и $v''_i = \lambda''_i e''_i$ первых их n векторов составляют базисы подмодуля $N \subset F$, а множители $\lambda'_i \mid \lambda'_j$ и $\lambda''_i \mid \lambda''_j$ при $i < j$, то обе диагональные матрицы перехода $C_{\boldsymbol{v''e''}} = C_{\boldsymbol{v''v'}}C_{\boldsymbol{v'e'}}C_{\boldsymbol{e'e''}}$ и $C_{\boldsymbol{v'e'}} = E_n C_{\boldsymbol{v'e'}} E_m$, где E_n и E_m суть единичные $n\times n$ и $m\times m$ матрицы, удовлетворяют условиям сл. 9.1 для одной и той же $n\times m$ матрицы $C = C_{\boldsymbol{v'e'}}$ и, стало быть, совпадают. Это устанавливает независимость инвариантных множителей от выбора взаимных базисов. □

Определение 9.2
Множители $\lambda_1, \dots, \lambda_n$ из теор. 9.2 называются *инвариантными множителями* подмодуля N в свободном модуле F, а построенные в теор. 9.2 базисы $e_1, \dots, e_m$ в F и $\lambda_1 e_1, \dots, \lambda_n e_n$ в N называются *взаимными базисами* свободного модуля F и его подмодуля N.

Пример 9.1 (подрешётки в $\mathbb{Z}^m$)
По теореме об инвариантных множителях для любой абелевой подгруппы $L \subset \mathbb{Z}^m$ существует такой базис $u_1, \dots, u_m$ в $\mathbb{Z}^m$, что подходящие кратности первых ℓ его базисных векторов $m_1 u_1, \dots, m_\ell u_\ell$ составляют базис в L. Тем самым, L тоже является свободным $\mathbb{Z}$-модулем, а фактор модуль

$$\mathbb{Z}^m / L \simeq \frac{\mathbb{Z}}{(m_1)} \oplus \cdots \oplus \frac{\mathbb{Z}}{(m_\ell)} \oplus \mathbb{Z}^{m-\ell}. \tag{9-2}$$

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

$$C = \begin{pmatrix} 126 & 51 & 72 & 33 \\ 30 & 15 & 18 & 9 \\ 60 & 30 & 36 & 18 \end{pmatrix} \tag{9-3}$$

Для этого перейдём к взаимным базисам. Заметим, что нод элементов матрицы (9-3) равен 3, и мы можем получить -3 в позиции $(1,4)$, прибавляя к 1-й строке учетверённую 2-ю:

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

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

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

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

подходящие кратности 1-го столбца

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

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

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

Остаётся 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 $\mathbb{Z}^3 / L \simeq \mathbb{Z}/(3) \oplus \mathbb{Z}/(6) \oplus \mathbb{Z}$.

Проделанные элементарные преобразования строк состояли в последовательном умножении слева на матрицы

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

а преобразования столбцов — в последовательном умножении справа на матрицы

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

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

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

Пример 9.2 (соизмеримые подрешётки)
Из существования взаимных базисов вытекает, что следующие свойства абелевой подгруппы $L \subset \mathbb{Z}^m$, порождённой столбцами матрицы $C \in \mathrm{Mat}_{m\times n}(\mathbb{Z})$, эквивалентны друг другу:

(1) $\mathrm{rk}\, L = m$

(2) фактор группа $\mathbb{Z}^m / L$ конечна

(3) решётка $L \subset \mathbb{Z}^m$ линейно порождает векторное пространство $\mathbb{Q}^m$ над $\mathbb{Q}$

(4) ранг матрицы C над полем $\mathbb{Q}$ равен m.

Решётки $L \subset \mathbb{Z}^m$, удовлетворяющие этим условиям, называются *соизмеримыми* с $\mathbb{Z}^m$. Если решётка $L \subset \mathbb{Z}^m$ задана как $\mathbb{Z}$-линейная оболочка столбцов некоторой матрицы $C \in \mathrm{Mat}_{m\times n}(\mathbb{Z})$, то чтобы убедиться в её соизмеримости с $\mathbb{Z}^m$ достаточно указать в матрице C ненулевой минор порядка m. Для отыскания ранга решётки L достаточно гауссовыми элементарными преобразованиями строк над полем $\mathbb{Q}$ привести матрицу C или[1] C^t к ступенчатому виду с рациональными элементами.

Предложение 9.1
Столбцы матрицы $C \in \mathrm{Mat}_n(\mathbb{Z})$ порождают соизмеримую с $\mathbb{Z}^n$ абелеву подгруппу $L \subset \mathbb{Z}^n$ если и только если $\det C \neq 0$, и в этом случае $|\mathbb{Z}^n / L| = |\det C|$, т. е. число элементов в факторе по соизмеримой подрешётке равно абсолютной величине объёма параллелепипеда, натянутого на любой её базис.

Доказательство. Рассмотрим в $\mathbb{Z}^m$ такой базис $u_1, \dots, u_m$, что векторы $\lambda_1 u_1, \dots, \lambda_\ell u_\ell$ образуют базис в L. Диагональная матрица D, единственными ненулевыми элементами которой являются $d_{ii} = \lambda_i$ с $1 \leqslant i \leqslant \ell$, связана с матрицей C соотношением $D = LCR$, где матрицы $L, R \in \mathrm{GL}_n(\mathbb{Z})$. Поскольку обратимость целочисленной матрицы равносильна тому, что её определитель равен[2] ± 1, мы заключаем, что $|\det D| = \prod_i |d_{ii}| = |\det C|$. Соизмеримость L с $\mathbb{Z}^m$ равносильна тому, что $\ell = m$ или, что то же самое, тому что все $d_{ii} = \lambda_i$ ненулевые. В этом случае $\mathbb{Z}^n / L = \bigoplus\limits_i \mathbb{Z}/(\lambda_i)$ состоит в точности из $\prod_i |\lambda_i| = |\det C|$ элементов. □

9.3. Теорема об элементарных делителях. Вместо упорядоченного набора инвариантных множителей $\lambda_1, \dots, \lambda_n$ иногда бывает удобнее иметь дело с неупорядоченным дизъюнктным объединением всех степеней p^μ неприводимых элементов $p \in K$, входящих в разложения чисел $\lambda_1, \dots, \lambda_n$ на неприводимые множители. Точнее, рассмотрим для каждого $i = 1, \dots, n$ разложение $\lambda_i = p_{i1}^{m_{i1}} \cdots p_{ik_i}^{m_{ik_i}}$, в котором все p_{ij} неприводимы и p_{ij} не ассоциировано с p_{ik} при $j \neq k$. Неупорядоченное дизъюнктное объединение всех степеней[3] $p_{ij}^{m_{ij}}$, входящих в эти разложения при $i = 1, \dots, n$, называется набором *элементарных делителей* набора инвариантных множителей $\lambda_1, \dots, \lambda_n$.

Лемма 9.3
Описанная только что процедура устанавливает биекцию между упорядоченными наборами чисел[4] $\lambda_1, \dots, \lambda_n \in K$, в которых $\lambda_i | \lambda_j$ при $i < j$, и всевозможными неупорядоченными наборами натуральных степеней p^μ неприводимых чисел[5] из K, в которых разрешаются повторяющиеся элементы[6].

[1] Смотря по тому, в какой из двух матриц меньше строк.

[2] См. сл. 7.1 на стр. 97.

[3] Эпитет «дизъюнктное» означает, что степень p^m, входящая в разложение ровно k инвариантных множителей λ_i, присутствует в итоговом неупорядоченном наборе в точности k раз.

[4] Рассматриваемых с точностью до умножения на обратимые элементы кольца K.

[5] Тоже рассматриваемых с точностью до умножения на обратимые элементы кольца K.

[6] Два таких набора считаются одинаковыми, если их можно привести в биективное соответствие друг с другом так, что у соответственных степеней p^μ и q^ν натуральные показатели μ и ν будут равны другу, а простые основания p и q будут ассоциированы друг с другом.

Доказательство. Набор инвариантных множителей $\lambda_1, \dots, \lambda_n$ однозначно восстанавливается по набору элементарных делителей следующим образом. Расставим элементарные делители в клетки диаграммы Юнга так, чтобы в первой строке шли в порядке нестрого убывания степени того простого числа, степеней которого в наборе элементарных делителей имеется больше всего. Во вторую строку поместим в порядке нестрого убывания все степени простого числа, следующего за первым по общему количеству вхождений его степеней в набор элементарных делителей и т. д. Поскольку наибольший инвариантный множитель λ_n делится на все остальные, его разложение на простые множители содержит *все* встречающиеся среди элементарных делителей простые числа, причём каждое из них — с максимальным показателем. Таким образом, λ_n является произведением всех элементарных делителей, стоящих в первом столбце построенной нами диаграммы Юнга. По индукции мы заключаем, что произведения элементарных делителей по столбцам диаграммы образуют прочитанную справа налево последовательность инвариантных множителей. □

Пример 9.3
Набор элементарных делителей

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

возникает из такого набора инвариантных множителей:

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

9.3.1. Формулировка основной теоремы. Остаток этого раздела будет посвящён доказательству следующего результата.

Теорема 9.3 (об элементарных делителях)
Всякий конечно порождённый модуль над кольцом главных идеалов K изоморфен

$$K^{n_0} \oplus \frac{K}{\left(p_1^{n_1}\right)} \oplus \dots \oplus \frac{K}{\left(p_\alpha^{n_\alpha}\right)} \tag{9-4}$$

где $m_\nu \in \mathbb{N}$, все $p_\nu \in K$ просты, и слагаемые в прямой сумме могут повторяться. Два модуля

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

изоморфны если и только если $n_0 = m_0$, $\alpha = \beta$ и слагаемые можно перенумеровать так, чтобы $n_\nu = m_\nu$ и $p_\nu = s_\nu q_\nu$, где все $s_\nu \in K$ обратимы.

Определение 9.3
Набор (возможно повторяющихся) степеней $p_i^{n_i}$, по которым происходит факторизация в (9-4), называется *набором элементарных делителей* модуля (9-4).

9.3.2. Существование разложения (9-4)**.** Пусть K-модуль M порождается векторами

$$w_1, \dots, w_m .$$

Тогда $M = K^m/R$, где R — ядро эпиморфизма $K^m \twoheadrightarrow M$, переводящего стандартные базисные векторы $e_i \in K^m$ в образующие $w_i \in M$, как в форм. (9-1) на стр. 123. По теор. 9.2 в K^m существует такой базис $u_1, \dots, u_m$, что некоторые кратности $\lambda_1 u_1, \dots, \lambda_k u_k$ первых K базисных векторов составляют базис в R. Таким образом,

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

Пусть i-й инвариантный множитель $\lambda_i = p_1^{m_1} \cdots p_s^{m_s}$, где $p_j \in K$ — попарно неассоциированные простые элементы. Тогда по китайской теореме об остатках

$$K/(\lambda_i) = K/\left(p_1^{m_1}\right) \oplus \dots \oplus K/\left(p_s^{m_s}\right) ,$$

что и даёт разложение (9-4). Чтобы установить его единственность, мы дадим инвариантное описание всех слагаемых разложения (9-4) во внутренних терминах модуля M.

9.3.3. Отщепление кручения. Сумма $K/\left(p_1^{n_1}\right) \oplus \dots \oplus K/\left(p_\alpha^{n_\alpha}\right)$ в разложении (9-4) совпадает с подмодулем кручения[1] $\operatorname{Tors} M = \{w \in M \mid \exists \lambda \neq 0 : \lambda w = 0\}$, а число n_0 в разложении (9-4) равно рангу свободного модуля $M/\operatorname{Tors} M$ и не зависит от выбора разложения. Из существования разложения (9-4) вытекает

Следствие 9.2
Всякий конечно порождённый модуль над кольцом главных идеалов является прямой суммой свободного модуля и подмодуля кручения. В частности, любой модуль без кручения автоматически свободен. □

9.3.4. Отщепление p-кручения. Для каждого неприводимого $p \in K$ назовём *p-кручением* в K-модуле M подмодуль, образованный всеми векторами, которые аннулируются умножением на какую-нибудь степень числа p, и обозначим этот подмодуль

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

Если простое $q \in K$ не ассоциировано с p, то класс p^k обратим в $K/\left(q^m\right)$, и гомоморфизм умножения на $p^k : K/\left(q^m\right) \to K/\left(q^m\right)$, $x \mapsto p^k x$, является изоморфизмом. В частности, он не имеет ядра. Напротив, каждый модуль $K/\left(p^\ell\right)$ полностью аннулируется умножением на достаточно большую степень p. Поэтому прямая сумма всех слагаемых вида $K/\left(p^m\right)$ в разложении (9-4) совпадает с подмодулем p-кручения $\operatorname{Tors}_p M \subset M$ и тоже не зависит от выбора разложения, а из наличия разложения (9-4) вытекает

Следствие 9.3
Всякий конечно порождённый модуль кручения над кольцом главных идеалов является прямой суммой подмодулей p-кручения по всем простым $p \in K$, для которых p-кручение ненулевое. □

Упражнение 9.3. Обозначим через $\varphi : K/\left(p^m\right) \to K/\left(p^m\right)$, $x \mapsto px$, гомоморфизм умножения на p. Покажите, что: а) $\varphi^n = 0$ при $n \geqslant m$ б) $\ker \varphi^n \supset \ker \varphi^{n-1}$ в) $\ker \varphi^n = \operatorname{im} \varphi^{m-n} \simeq K/\left(p^n\right)$ при $0 < n < m$ г) $\ker \varphi^n / \ker \varphi^{n-1}$ нулевой при $n > m$ и изорфен $K/(p)$ при $1 \leqslant n \leqslant m$.

[1] См. прим. 6.6 на стр. 82.

9.3.5. Инвариантность показателей p-кручения. Для завершения доказательства теор. 9.3 остаётся проверить, что если при простом $p \in K$ слагаемые прямого разложения

$$M = \frac{K}{(p^{\nu_1})} \oplus \cdots \oplus \frac{K}{(p^{\nu_k})} \tag{9-5}$$

выписаны в порядке нестрого убывания показателей $\nu_1 \geqslant \nu_2 \geqslant \cdots \geqslant \nu_k$, то этот набор показателей не зависит от выбора разложения и однозначно определяется модулем M. Для этого рассмотрим диаграмму Юнга ν, строки которой имеют длины $\nu_1, \ldots, \nu_k$, и дадим инвариантное описание длинам столбцов этой диаграммы. Обозначим через $\varphi : M \to M$, $x \mapsto px$, гомоморфизм умножения на p, как в упр. 9.3. Согласно этому упражнению, применённому к правой части разложения (9-5), при каждом $i = 1, 2, 3, \ldots$ фактор модуль $\ker \varphi^i / \ker \varphi^{i-1}$ изоморфен прямой сумме одинаковых слагаемых $K/(p)$ в количестве, равном числу строк диаграммы ν, длина которых не меньше i, т. е. высоте i-го столбца диаграммы ν. С другой стороны, фактор модуль $\ker \varphi^i / \ker \varphi^{i-1}$ никак не зависит от разложения (9-5) и является векторным пространством над полем $K/(p)$: умножение на класс $[x]_p \in K/(p)$ переводит класс $[z] \in \ker \varphi^i / \ker \varphi^{i-1}$ в класс $[xz] \in \ker \ker \varphi^i / \ker \varphi^{i-1}$.

Упражнение 9.4. Убедитесь, что это правило корректно и удовлетворяет аксиомам векторного пространства.

Мы заключаем, что высота i-того столбца диаграммы ν равна размерности векторного пространства $\ker \varphi^i / \ker \varphi^{i-1}$ над полем $K/(p)$. Теорема об элементарных делителях полностью доказана.

9.4. Строение конечно порождённых абелевых групп. При $K = \mathbb{Z}$ теорема об элементарных делителях даёт полную классификацию конечно порождённых абелевых групп.

Теорема 9.4
Всякая конечно порождённая абелева группа изоморфна прямой сумме аддитивных групп

$$\mathbb{Z}^r \oplus \frac{\mathbb{Z}}{\left(p_1^{n_1}\right)} \oplus \cdots \oplus \frac{\mathbb{Z}}{\left(p_\alpha^{n_\alpha}\right)} \tag{9-6}$$

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

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

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. □

Определение 9.4
Единственное представление заданной конечно порождённой абелевой группы A в виде прямой суммы аддитивных групп (9-6) называется её *каноническим представлением*.

Пример 9.4 (группы, заданные образующими и соотношениями)
На практике конечно порождённые абелевы группы часто задаются описанием вроде: абелева

группа A, порождённая элементами $a_1, \dots, a_n$, которые связаны соотношениями

$$\begin{cases} \mu_{11}a_1 + \mu_{12}a_2 + \cdots + \mu_{1n}a_n = 0 \\ \mu_{21}a_1 + \mu_{22}a_2 + \cdots + \mu_{2n}a_n = 0 \\ \mu_{31}a_1 + \mu_{32}a_2 + \cdots + \mu_{3n}a_n = 0 \\ \qquad \cdots\ \cdots\ \cdots\ \cdots\ \cdots \\ \mu_{\mu 1}a_1 + \mu_{\mu 2}a_2 + \cdots + \mu_{mn}a_n = 0\,, \end{cases} \tag{9-7}$$

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 $\mu_1, \dots, \mu_m$ матрицы $M = \left(\mu_{ij}\right)$. В каноническом разложении (9-6) группы A ранг r свободного слагаемого равен $n - \operatorname{rk} M$, а степени $p_i^{n_i}$ суть элементарные делители подмодуля $R \subset \mathbb{Z}^n$. Про конкретный элемент $w = x_1a_1 + \cdots + x_na_n$ часто бывает нужно знать, отличен он от нуля в A или нет, и если нет, то каков его порядок[1] $\operatorname{ord}(w)$.

Выяснить первое 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 M, то никакое его целое кратное mw не лежит в R, т. е. $w \neq 0$ в A и $\operatorname{ord} w = \infty$. Если же w лежит в $\mathbb{Q}$-линейной оболочке строк матрицы M, то подходящее целое кратное mw этого элемента лежит в R и класс w в группе $A = \mathbb{Z}^n/R$ имеет конечный порядок. Оценить этот порядок сверху тоже можно при помощи вычислений над полем $\mathbb{Q}$. Если строки $\mu_{i_1}, \dots, \mu_{i_k}$, где $k = \operatorname{rk} M = n - r$, образуют базис в $\mathbb{Q}$-линейной оболочке строк матрицы M, то $\mathbb{Z}$-линейная оболочка этих строк соизмерима[2] с R. Если $w = x_{i_1}\mu_{i_1} + \cdots + x_{i_k}\mu_{i_k}$, где $x_j = p_j/q_j \in \mathbb{Q}$ несократимы, то вектор mw с $m = \text{нок}(q_{i_1}, \dots, q_{i_k})$ лежит в $\mathbb{Z}$-линейной оболочке строк $\mu_{i_1}, \dots, \mu_{i_k}$, а значит, и в R. Поэтому $\operatorname{ord} w \leqslant m$ в группе A. Для точного отыскания порядка $\operatorname{ord} w$ вычислений над $\mathbb{Q}$ уже не достаточно, и требуется явный базис $e_1, \dots, e_k$ модуля R над $\mathbb{Z}$. Если такой базис найден[3], и $w = \sum x_ie_i$, где $x_i = p_i/q_i \in \mathbb{Q}$ несократимы, то $\operatorname{ord} w = \text{нок}(q_1, \dots, q_k)$. В частности, если все $q_i = 1$, то $w = 0$ в $A = \mathbb{Z}^n/R$.

[1] Напомню, что *порядком* $\operatorname{ord}(w)$ элемента w в аддитивной абелевой группе называется наименьшее такое $n \in \mathbb{N}$, что $nw = 0$, или же $\operatorname{ord}(w) = \infty$, если такого n нет (см. n° 3.5.1 на стр. 49).

[2] Т. е. является подгруппой конечного индекса в R, см. прим. 9.2 на стр. 125.

[3] Например, методом Гаусса, как это объяснялось в прим. 9.1 на стр. 124.

Упр. 9.1. $\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}^{-1} = \frac{1}{\alpha\delta-\beta\gamma}\begin{pmatrix}\delta & -\beta\\ -\gamma & \alpha\end{pmatrix}$.

Упр. 9.2. Рассмотрим в грассмановой 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 грассмановы мономы степени k от η и ζ суть $\eta_I = \sum\limits_J \xi_J a_{JI}$ и $\zeta_K = \sum\limits_L \xi_L f_{LK}$. Поскольку $\zeta_I = \sum\limits_J \eta_J c_{JI}$, мы получаем $f_{LK} = \sum\limits_J a_{LJ} c_{JK}$.

Упр. 9.3. Утверждения (а) и (б) очевидны. Пусть $0 < n < m$, как в (в). 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 $p^n x = 0$ в $K/(p^m)$. Тем самым, $\ker\varphi^n = \operatorname{im}\varphi^{m-n}$. Правило $[x]_{p^n} \mapsto [p^{m-n}x]_{p^m}$ корректно задаёт инъективный гомоморфизмом K-модулей $\psi\colon K/(p^n) \hookrightarrow K/(p^m)$, который изоморфно отображает $K/(p^n)$ на $\operatorname{im}\varphi^{m-n} = \ker\varphi^n \subset K/(p^m)$. Это доказывает (в). Изоморфизм

$$\frac{\ker\varphi^n}{\ker\varphi^{n-1}} = \frac{p^{m-n}K/(p^m)}{p^{m-n+1}K/(p^m)} \xrightarrow{\sim} \frac{K}{p}$$

из (г) сопоставляет классу элемента $p^{n-m}x$ по модулю элементов вида $p^{n-m+1}y$ класс элемента x по модулю (p).

Упр. 9.4. Если $z' = z + q$, где $p^{i-1}q = 0$, а $x' = x + py$, то $x'z' = xz + q(x+py) + pyz$ и $p^{i-1}\big(q(x+py) + pyz\big) = 0$, поскольку $p^i z = 0$.