

§6. Конечно порождённые модули над областью главных идеалов

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

6.1. Метод Гаусса. Будем называть *элементарным преобразованием строк* прямоугольной матрицы $A \in \text{Mat}_{m \times n}(K)$ замену каких-нибудь двух строк r_i и r_j их линейными комбинациями

$$r'_i = \alpha r_i + \beta r_j \quad \text{и} \quad r'_j = \gamma r_i + \delta r_j$$

с обратимым определителем $\Delta = \alpha\delta - \beta\gamma \in K$. В этом случае матрица преобразования

$$\begin{pmatrix} r_i \\ r_j \end{pmatrix} \mapsto \begin{pmatrix} r'_i \\ r'_j \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} r_i \\ r_j \end{pmatrix}$$

обратима¹, и исходные строки r_i и r_j восстанавливаются из преобразованных строк r'_i и r'_j по формулам $r'_i = (\delta r_i - \beta r_j)/\Delta$ и $r'_j = (-\gamma r_i + \alpha r_j)/\Delta$.

УПРАЖНЕНИЕ 6.1. Убедитесь в этом.

В частности, прибавление к одной строке другой строки, умноженной на произвольное число $x \in K$, а также перестановка двух строк местами и умножение строк на обратимые элементы $s_1, s_2 \in K$ тоже являются элементарными преобразованиями, задаваемыми 2×2 матрицами

$$\begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \text{и} \quad \begin{pmatrix} s_1 & 0 \\ 0 & s_2 \end{pmatrix}.$$

Элементарное преобразование не меняет линейной оболочки строк матрицы A и заключается в умножении A слева на обратимую $m \times m$ матрицу L , которая получается из единичной $m \times m$ матрицы тем же самым элементарным преобразованием строк, что происходит в матрице A .

Симметричным образом, *элементарным преобразованием столбцов* матрицы A мы называем замену каких-нибудь двух столбцов c_i и c_j их линейными комбинациями $c'_i = \alpha c_i + \beta c_j$ и $c'_j = \gamma c_i + \delta c_j$ с обратимым в K определителем $\alpha\delta - \beta\gamma$. Такое преобразование не меняет линейной оболочки столбцов матрицы A и достигается умножением A справа на обратимую $n \times n$ матрицу R , которая получается из единичной $n \times n$ матрицы тем же самым элементарным преобразованием столбцов, что производится в матрице A . Прибавление к одному из столбцов другого, умноженного на произвольное число $x \in K$, а также перестановка столбцов местами и умножение столбцов на обратимые элементы из K являются частными примерами элементарных преобразований.

ЛЕММА 6.1

В области главных идеалов K любую пару ненулевых элементов (a, b) , стоящих в одной строке (соотв. в одном столбце) матрицы $A \in \text{Mat}_{m \times n}(K)$, можно подходящим элементарным преобразованием содержащих их столбцов (соотв. строк) заменить парой $(d, 0)$, где $d = \text{нод}(a, b)$.

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

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

¹См. прим. 5.15 на стр. 92.

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

ТЕОРЕМА 6.1

В области главных идеалов K любая матрица $A \in \text{Mat}_{m \times n}(K)$ конечным числом элементарных преобразований строк и столбцов преобразуется в матрицу $D_A = (d_{ij})$, у которой $d_{ij} = 0$ при $i \neq j$ и $d_{ii} \mid d_{jj}$ при $i < j$, где мы считаем, что $d \mid 0$ для всех $d \in K$, но $0 \nmid d$ при $d \neq 0$.

Доказательство. Если $A = 0$, то доказывать нечего. Если $A \neq 0$, то перестановками строк и столбцов добьёмся, чтобы $a_{11} \neq 0$. Если все элементы матрицы A делятся на a_{11} , то вычитая из всех строк подходящие кратности первой строки, а из всех столбцов — подходящие кратности первого столбца, добьёмся того, чтобы все элементы за исключением a_{11} в первом столбце и первой строке занулились. При этом все элементы матрицы останутся делящимися на a_{11} , и можно заменить A на матрицу размера $(m - 1) \times (n - 1)$, дополнительную к первой строке и первому столбцу матрицы A , после чего повторить процедуру.

Пусть в матрице A есть элемент a , не делящийся на a_{11} , и $d = \text{нод}(a, a_{11})$. Ниже мы покажем, что в этом случае можно элементарными преобразованиями перейти к новой матрице A' с $a'_{11} = d$. Так как $(a_{11}) \subsetneq (d)$, главный идеал, порождённый левым верхним угловым элементом матрицы, при таком переходе строго увеличится. Поскольку в области главных идеалов не существует бесконечно возрастающих цепочек строго вложенных друг в друга идеалов, после конечного числа таких переходов мы получим матрицу, все элементы которой делятся на a_{11} , и к этой матрице будут применимы предыдущие рассуждения.

Если не делящийся на a_{11} элемент a стоит в первой строке или первом столбце, достаточно заменить пару (a_{11}, a) на $(d, 0)$ по **лем. 6.1**. Если все элементы первой строки и первого столбца делятся на a_{11} , а не делящийся на a_{11} элемент a стоит строго ниже и правее a_{11} , то мы, как и выше, сначала занулим все элементы первой строки и первого столбца за исключением самого a_{11} , вычитая из всех строк подходящие кратности первой строки, а из всех столбцов — подходящие кратности первого столбца. К элементу a при этом будут добавляться числа, кратные a_{11} , и $\text{нод}(a, a_{11})$ не изменится. Далее, прибавим ту строку, где стоит a , к первой строке и получим в ней копию элемента a . Наконец, заменим пару (a_{11}, a) на $(d, 0)$ по **лем. 6.1**. □

6.1.1. Инвариантные множители и нормальная форма Смита. Ниже, в п° 6.3.4 на стр. 118 мы покажем, что «диагональная» матрица D_A , в которой $d_{ij} = 0$ при $i \neq j$ и $d_{ii} \mid d_{jj}$ при $i < j$, с точностью до умножения её элементов на обратимые элементы из K не зависит от выбора последовательности элементарных преобразований, приводящих матрицу A к такому виду. По этой причине диагональные элементы d_{ii} матрицы D_A называются *инвариантными множителями* матрицы A , а сама диагональная матрица D_A — *нормальной формой Смита* матрицы A .

Так как каждое элементарное преобразование строк (соотв. столбцов) матрицы A является результатом умножения матрицы A слева (соотв. справа) на квадратную обратимую матрицу, которая получается из единичной матрицы E ровно тем же преобразованием, что совершается в матрице A , мы заключаем, что $D_A = LAR$, где $L = L_\rho \dots L_2 L_1$ и $R = R_1 R_2 \dots R_r$ — обратимые матрицы размеров $m \times m$ и $n \times n$, являющиеся произведениями обратимых матриц L_i и R_j , осуществляющих последовательные элементарные преобразования строк и столбцов матрицы A . Мы будем называть L и R *матрицами перехода* от матрицы A к её нормальной форме Смита. Так как $L = L_\rho \dots L_1 E$ и $R = E R_1 \dots R_r$, матрицы L и R получаются из единичных матриц размеров $m \times m$ и $n \times n$ теми же цепочками элементарных преобразований строк и соответственных столбцов, которые производились с матрицей A . Поэтому для явного отыскания матриц L

и R следует приписать к матрице $A \in \text{Mat}_{m \times n}(K)$ справа и снизу единичные матрицы размеров $m \times m$ и $n \times n$ так, что получится Γ -образная таблица вида

$$\begin{array}{|c|c|} \hline A & E \\ \hline E & \\ \hline \end{array},$$

и в процессе приведения матрицы A к диагональному виду осуществлять элементарные преобразования строк и столбцов сразу во всей Γ -образной таблице. В результате на выходе получится Γ -образная таблица

$$\begin{array}{|c|c|} \hline D_A & L \\ \hline R & \\ \hline \end{array}.$$

ПРИМЕР 6.1

Вычислим нормальную форму Смита и матрицы перехода к ней для целочисленной матрицы

$$A = \begin{pmatrix} -9 & -18 & 15 & -24 & 24 \\ 15 & 30 & -27 & 42 & -36 \\ -6 & -12 & 6 & -12 & 24 \\ 31 & 62 & -51 & 81 & -87 \end{pmatrix} \in \text{Mat}_{4 \times 5}(\mathbb{Z}).$$

Составляем Γ -образную матрицу

$$\begin{array}{|c|c|} \hline A & E \\ \hline E & \\ \hline \end{array} = \begin{array}{|c|c|c|c|c|c|c|c|c|c|} \hline -9 & -18 & 15 & -24 & 24 & 1 & 0 & 0 & 0 & 0 \\ 15 & 30 & -27 & 42 & -36 & 0 & 1 & 0 & 0 & 0 \\ -6 & -12 & 6 & -12 & 24 & 0 & 0 & 1 & 0 & 0 \\ 31 & 62 & -51 & 81 & -87 & 0 & 0 & 0 & 1 & 0 \\ \hline 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ \hline \end{array}.$$

Прибавим к 4-й строке третью, умноженную на 5 и переставим полученную строку наверх:

$$\begin{array}{|c|c|c|c|c|c|c|c|c|c|} \hline 1 & 2 & -21 & 21 & 33 & 0 & 0 & 5 & 1 & 0 \\ -9 & -18 & 15 & -24 & 24 & 1 & 0 & 0 & 0 & 0 \\ 15 & 30 & -27 & 42 & -36 & 0 & 1 & 0 & 0 & 0 \\ -6 & -12 & 6 & -12 & 24 & 0 & 0 & 1 & 0 & 0 \\ \hline 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ \hline \end{array}.$$

Теперь обнулим 1-ю строку и 1-й столбец левой матрицы вне левого верхнего угла, прибавив

ко всем строкам и столбцам надлежащие кратности 1-й строки и 1-го столбца:

1	0	0	0	0	0	0	5	1
0	0	-174	165	321	1	0	45	9
0	0	288	-273	-531	0	1	-75	-15
0	0	-120	114	222	0	0	31	6
1	-2	21	-21	-33				
0	1	0	0	0				
0	0	1	0	0				
0	0	0	1	0				
0	0	0	0	1				

Делаем второй столбец пятым, а к 3-му столбцу прибавляем 4-й:

1	0	0	0	0	0	0	5	1
0	-9	165	321	0	1	0	45	9
0	15	-273	-531	0	0	1	-75	-15
0	-6	114	222	0	0	0	31	6
1	0	-21	-33	-2				
0	0	0	0	1				
0	1	0	0	0				
0	1	1	0	0				
0	0	0	1	0				

Вычитаем из 2-й строки 4-ю:

1	0	0	0	0	0	0	5	1
0	-3	51	99	0	1	0	14	3
0	15	-273	-531	0	0	1	-75	-15
0	-6	114	222	0	0	0	31	6
1	0	-21	-33	-2				
0	0	0	0	1				
0	1	0	0	0				
0	1	1	0	0				
0	0	0	1	0				

Все элементы 3×4 матрицы, стоящей в строках со 2-й по 4-ю и столбцах со 2-го по 5-й, делятся на 3. Поэтому мы обнуляем в этой матрице верхнюю строку и левый столбец, вычитая из 3-й и 4-й строк подходящие кратности 2-й строки, а потом из 3-го и 4-го столбцов — подходящие кратности 2-го:

1	0	0	0	0	0	0	5	1
0	-3	0	0	0	1	0	14	3
0	0	-18	-36	0	5	1	-5	0
0	0	12	24	0	-2	0	3	0
1	0	-21	-33	-2				
0	0	0	0	1				
0	1	17	33	0				
0	1	18	33	0				
0	0	0	1	0				

Теперь прибавляем к 3-й строке 4-ю:

1	0	0	0	0	0	0	5	1	
0	-3	0	0	0	0	1	0	14	3
0	0	-6	-12	0	0	3	1	-2	0
0	0	12	24	0	0	-2	0	3	0
1	0	-21	-33	-2	0	0	0	0	0
0	0	0	0	1	0	0	0	0	0
0	1	17	33	0	0	0	0	0	0
0	1	18	33	0	0	0	0	0	0
0	0	0	1	0	0	0	0	0	0

и видим, что можно занулить все недиагональные элементы исходной матрицы, прибавляя к 4-й строке удвоенную 3-ю и вычитая из 4-го столбца удвоенный 3-й:

1	0	0	0	0	0	0	0	5	1
0	-3	0	0	0	0	1	0	14	3
0	0	-6	0	0	0	3	1	-2	0
0	0	0	0	0	0	4	2	-1	0
1	0	-21	9	-2	0	0	0	0	0
0	0	0	0	1	0	0	0	0	0
0	1	17	-1	0	0	0	0	0	0
0	1	18	-3	0	0	0	0	0	0
0	0	0	1	0	0	0	0	0	0

Таким образом, инвариантные множители матрицы A суть 1, -3, -6, 0 и

$$L = \begin{pmatrix} 0 & 0 & 5 & 1 \\ 1 & 0 & 14 & 3 \\ 3 & 1 & -2 & 0 \\ 4 & 2 & -1 & 0 \end{pmatrix}, \quad R = \begin{pmatrix} 1 & 0 & -21 & 9 & -2 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 17 & -1 & 0 \\ 0 & 1 & 18 & -3 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}, \quad D_A = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & -3 & 0 & 0 & 0 \\ 0 & 0 & -6 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

УПРАЖНЕНИЕ 6.2. Проверьте равенство $LAR = D_A$ прямым вычислением.

6.1.2. Отыскание обратной матрицы. Пусть квадратная матрица $A \in \text{Mat}_n(K)$ обратима. Тогда и любая матрица вида $B = LAR$, где $L, R \in \text{Mat}_n(K)$ обратимы, тоже обратима, ибо матрица $R^{-1}A^{-1}L^{-1}$ обратна к B . В частности, обратимы все матрицы, которые получаются из A элементарными преобразованиями строк и столбцов, включая нормальную форму Смита D_A .

УПРАЖНЕНИЕ 6.3. Убедитесь, что диагональная матрица обратима если и только если обратимы все её диагональные элементы.

Таким образом, матрица A обратима если и только если обратимы все её инвариантные множители, и в этом случае существуют такие обратимые матрицы $L = L_\rho \dots L_1$ и $R = R_1 \dots R_r$,

Уравнения системы $D_A y = c$ имеют вид $d_{ii} y_i = c_i$. Такое уравнение не имеет решений, если и только если $d_{ii} \nmid c_i$. Если же $d_{ii} \mid c_i$, то при $d_{ii} = c_i = 0$ решениями уравнения являются все числа $y_i \in K$, а при $d_{ii} \neq 0$ уравнение имеет единственное решение $y_i = c_i / d_{ii}$.

Пусть $d_{ii} \neq 0$ при $i \leq r$ и $d_{jj} = 0$ при $j > r$. Мы заключаем, что система $D_A y = c$ несовместна если и только если $d_{ii} \nmid c_i$ хотя бы при одном $i \leq r$ или $c_j \neq 0$ хотя бы при одном $j > r$, и в этом случае исходная система (6-1) тоже несовместна. Если же система $D_A y = c$ совместна, то её решения имеют вид $y = w_0 + w$, где $w_0 = (c_1 / d_{11}, \dots, c_r / d_{rr}, 0, \dots, 0)^t$, а вектор $w \in K^n$ пробегает свободный подмодуль ранга $\min(m, n) - r$ с базисом из векторов

$$w_k = (0, \dots, 0, 1, 0, \dots, 0)^t, \text{ где } 1 \text{ стоит на } (r + k)\text{-м месте,}$$

и в этом случае все решения исходной системы (6-1) имеют вид $x = u_0 + u$, где $u_0 = R w_0$, а $u \in K^n$ пробегает свободный подмодуль ранга $\min(m, n) - r$ с базисом из векторов $u_k = R w_k$.

Отметим, что столбец $c = Lb$ правых частей системы $D_A y = c$ получается из столбца b правых частей исходной системы (6-1) теми же преобразованиями строк, что производятся с матрицей A в процессе её приведения к виду D_A , а матрица R получается из единичной матрицы E теми же преобразованиями столбцов, что производятся с матрицей A в том же процессе. Поэтому для отыскания c и R можно составить Γ -образную матрицу вида

$$\left[\begin{array}{c|c} A & b \\ \hline E & \end{array} \right],$$

привести A к нормальной форме Смита и получить на выходе

$$\left[\begin{array}{c|c} D_A & c \\ \hline R & \end{array} \right].$$

ПРИМЕР 6.3

Найдём все целые решения системы уравнений

$$\begin{cases} -65x_1 - 156x_2 + 169x_3 + 104x_4 = 117 \\ -143x_1 - 351x_2 + 364x_3 + 221x_4 = 195 \\ 52x_1 + 117x_2 - 143x_3 - 91x_4 = -156 \end{cases} \quad (6-2)$$

Для этого составим Γ -образную таблицу из матрицы коэффициентов при неизвестных, к которой справа приписана матрица правых частей уравнений, а снизу — единичная матрица:

-65	-156	169	104	117
-143	-351	364	221	195
52	117	-143	-91	-156
1	0	0	0	
0	1	0	0	
0	0	1	0	
0	0	0	1	

Вычтем из 2-й строки 1-ю, умноженную на 2, и поменяем две верхние строки местами:

-13	-39	26	13	-39
-65	-156	169	104	117
52	117	-143	-91	-156
1	0	0	0	
0	1	0	0	
0	0	1	0	
0	0	0	1	

Поскольку все элементы матрицы коэффициентов делятся на 13, зануляем в ней верхнюю строку и левый столбец, за исключением верхнего левого углового элемента, прибавляя ко 2-й и 3-й строкам надлежащие кратности 1-й строки, а ко 2-му, 3-му и 4-му столбцам — надлежащие кратности 1-го столбца:

-13	0	0	0	-39
0	39	39	39	312
0	-39	-39	-39	-312
1	-3	2	1	
0	1	0	0	
0	0	1	0	
0	0	0	1	

Прибавляем к 3-й строке 2-ю, после чего вычитаем 2-й столбец из 3-го и 4-го:

-13	0	0	0	-39
0	39	0	0	312
0	0	0	0	0
1	-3	5	4	
0	1	-1	-1	
0	0	1	0	
0	0	0	1	

Мы заключаем, что система (6-2) равносильна системе

$$\begin{cases} -13y_1 = -39 \\ 39y_2 = 312 \end{cases} \quad (6-3)$$

на *четыре* неизвестные y_1, \dots, y_4 , через которые исходные неизвестные x_1, \dots, x_4 выражаются по формуле:

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 1 & -3 & 5 & 4 \\ 0 & 1 & -1 & -1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{pmatrix}. \quad (6-4)$$

Все решения системы (6-3) описываются формулой:

$$(y_1, y_2, y_3, y_4) = (3, 8, z_1, z_2), \quad \text{где } z_1, z_2 \in \mathbb{Z} \text{ — любые.}$$

Решения исходной системы получаются из них по формуле (6-4):

$$(x_1, x_2, x_3, x_4) = (5z_1 + 4z_2 - 21, 8 - z_1 - z_2, z_1, z_2), \quad \text{где } z_1, z_2 \in \mathbb{Z} \text{ — любые.}$$

6.2. Инвариантные множители. Как мы видели в [прим. 5.12](#) на стр. 88, произвольный K -модуль M , линейно порождённый над K конечным набором векторов

$$\mathbf{w} = (w_1, \dots, w_m),$$

представляет собою фактор $M \simeq K^m / R_{\mathbf{w}}$ свободного координатного модуля K^m по подмодулю $R_{\mathbf{w}} \subset K^m$ линейных соотношений между порождающими векторами \mathbf{w} . Подмодуль $R_{\mathbf{w}}$ состоит из всех таких строк $(x_1, \dots, x_m) \in K^m$, что $x_1 w_1 + \dots + x_m w_m = 0$ в M , и является ядром эпиморфизма

$$\pi_{\mathbf{w}} : K^m \twoheadrightarrow M, \quad (x_1, \dots, x_m) \mapsto x_1 w_1 + \dots + x_m w_m. \quad (6-5)$$

ТЕОРЕМА 6.2

Каждый подмодуль N в свободном модуле F конечного ранга над областью главных идеалов K тоже свободен, и $\text{rk } N \leq \text{rk } F$.

Доказательство. Индукция по $m = \text{rk } F$. При $m = 1$ модуль $N \simeq K$, и каждый ненулевой подмодуль $N \subset K$ представляет собою главный идеал $(d) \subset K$, который является свободным K -модулем ранга 1 с базисом d . Пусть теперь $m > 1$. Зафиксируем в F базис e_1, \dots, e_m и будем записывать векторы из N строками их координат в этом базисе. Первые координаты всевозможных векторов $v \in N$ образуют идеал $(d) \subset K$. Если $d = 0$, подмодуль N содержится в свободном модуле ранга $m - 1$ с базисом e_2, \dots, e_m . По индукции, такой модуль N свободен и $\text{rk } N \leq (m - 1)$. Если $d \neq 0$, обозначим через $u \in N$ какой-нибудь вектор с первой координатой d . Порождённый вектором u модуль Ku свободен ранга 1, поскольку равенство $xu = 0$ влечёт равенство $xd = 0$, возможное в целостном кольце K только при $x = 0$. Покажем, что $N = Ku \oplus N'$, где $N' \subset N$ — подмодуль, состоящий из векторов с нулевой первой координатой. Очевидно, что $Ku \cap N' = 0$. Если первая координата вектора $v \in N$ равна xd , то $v = xu + w$, где $w = v - xu \in N'$. Поэтому $N = Ku + N'$, и $N = Ku \oplus N'$ по [предл. 5.2](#) на стр. 85. Модуль N' содержится в свободном модуле ранга $m - 1$ с базисом e_2, \dots, e_m . По индукции он свободен и $\text{rk } N' \leq (m - 1)$. Поэтому $N = Ku \oplus N'$ тоже свободен и $\text{rk } N = 1 + \text{rk } N' \leq m$. \square

ПРИМЕР 6.4 (качественный анализ систем линейных уравнений)

Каждая матрица $A \in \text{Mat}_{m \times n}(K)$ задаёт K -линейное отображение $F_A : K^n \rightarrow K^m$, $x \mapsto Ax$, переводящее стандартные базисные векторы $e_1, \dots, e_n \in K^n$ в столбцы матрицы A . Множество решений системы линейных уравнений $Ax = b$ является полным прообразом $F^{-1}(b)$ данного вектора $b \in K^m$ при отображении F_A . Если $b \notin \text{im } F_A$, то этот прообраз пуст и система $Ax = b$ несовместна. Если $b \in \text{im } F_A$, то $F_A^{-1}(b) = w + \ker F_A$ представляет собою сдвиг свободного модуля $\ker F_A \subset K^n$ на такой вектор $w \in K^n$, что $F(w) = b$. На языке уравнений ядро $\ker F_A$ является множеством решений системы однородных линейных уравнений $Ax = 0$ с теми же самыми левыми частями, что и система $Ax = b$. Наличие у такой системы ненулевого решения означает, что $\ker F_A \neq 0$, и в этом случае любая система $Ax = b$ либо несовместна, либо множество её решений является сдвигом свободного модуля положительного ранга, что согласуется с [п. 6.1.3](#) на стр. 108.

ТЕОРЕМА 6.3 (ТЕОРЕМА О ВЗАИМНОМ БАЗИСЕ)

Пусть F — свободный модуль ранга m над областью главных идеалов K , и $N \subset F$ — произвольный его подмодуль. Тогда в модуле F существует такой базис $e = (e_1, \dots, e_m)$, что подходящие кратности $\lambda_1 e_1, \dots, \lambda_n e_n$ первых $n = \text{rk } N$ его базисных векторов составляют базис в N и $\lambda_i \mid \lambda_j$ при $i < j$.

Доказательство. Зафиксируем произвольные базисы $\mathbf{w} = (w_1, \dots, w_m)$ в F и $\mathbf{u} = \mathbf{w} C_{\mathbf{w}\mathbf{u}}$ в N . Последний существует по теор. 6.2 и состоит из $n \leq m$ векторов. Обозначим через $D = LC_{\mathbf{w}\mathbf{u}}R$ нормальную форму Смита матрицы перехода $C_{\mathbf{w}\mathbf{u}}$. Поскольку матрицы L и R обратимы, набор векторов $\mathbf{e} = \mathbf{w} L^{-1}$ является базисом в F , а набор векторов $\mathbf{v} = \mathbf{u} R$ — базисом в N . Так как

$$\mathbf{v} = \mathbf{u} R = \mathbf{w} C_{\mathbf{w}\mathbf{u}} R = \mathbf{e} L C_{\mathbf{w}\mathbf{u}} R = \mathbf{e} D$$

векторы $v_i = d_{ii} e_i$ базиса \mathbf{v} имеют предписанный теоремой вид, в котором $\lambda_i = d_{ii}$ суть инвариантные множители матрицы $C_{\mathbf{w}\mathbf{u}}$. \square

ОПРЕДЕЛЕНИЕ 6.1

Множители $\lambda_1, \dots, \lambda_n$ из теор. 6.3 называются *инвариантными множителями* подмодуля N в свободном модуле F , а построенные в теор. 6.3 базисы e_1, \dots, e_m в F и $\lambda_1 e_1, \dots, \lambda_n e_n$ в N называются *взаимными базисами* свободного модуля F и его подмодуля N . В н° 6.3.4 на стр. 118 ниже мы покажем, что множители λ_i не зависят от выбора взаимных базисов, что оправдывает эпитет «инвариантные» в их названии.

ПРИМЕР 6.5

Построим взаимные базисы целочисленной решётки \mathbb{Z}^3 и её подрешётки $L \subset \mathbb{Z}^3$, порождённой столбцами матрицы

$$A = \begin{pmatrix} 126 & 51 & 72 & 33 \\ 30 & 15 & 18 & 9 \\ 60 & 30 & 36 & 18 \end{pmatrix}. \quad (6-6)$$

Обозначим через $\mathbf{e} = (e_1, e_2, e_3)$ стандартный базис в \mathbb{Z}^3 . По условию, столбцы матрицы A , т. е. векторы $\mathbf{a} = (a_1, a_2, a_3, a_4) = \mathbf{e} A$ порождают решётку L . Пусть $D_A = LAR$ — нормальная форма Смита матрицы A . Тогда векторы $\mathbf{w} = \mathbf{a} R = \mathbf{e} AR$ тоже порождают L , поскольку образующие $\mathbf{a} = \mathbf{w} R^{-1}$ линейно через них выражаются. По предл. 5.6 на стр. 97 векторы $\mathbf{u} = \mathbf{e} L^{-1}$ составляют базис в \mathbb{Z}^3 , так как матрица перехода от них к стандартному базису обратима. При этом $\mathbf{e} = \mathbf{u} L$. В силу равенств $\mathbf{w} = \mathbf{e} AR = \mathbf{u} LAR = \mathbf{u} D_A$, образующие $w_i = d_{ii} u_i$ пропорциональны базисным векторам u_i . Поэтому взаимные базисы в \mathbb{Z}^3 и L состоят из векторов \mathbf{u} , т. е. столбцов матрицы L^{-1} , и векторов $w_i = d_{ii} u_i$ с ненулевыми d_{ii} . Для их отыскания приведём матрицу A к нормальной форме Смита. Так как матрица R нас сейчас не интересует, в вычислении из прим. 6.1 на стр. 104 можно ограничиться только верхней частью Γ -образной таблицы:

$$\boxed{A \mid E} = \begin{array}{|cccc|ccc} \hline 126 & 51 & 72 & 33 & 1 & 0 & 0 \\ 30 & 15 & 18 & 9 & 0 & 1 & 0 \\ 60 & 30 & 36 & 18 & 0 & 0 & 1 \\ \hline \end{array}.$$

Отнимаем из первой строки удвоенную третью:

$$\begin{array}{|cccc|ccc} \hline 6 & -9 & 0 & -3 & 1 & 0 & -2 \\ 30 & 15 & 18 & 9 & 0 & 1 & 0 \\ 60 & 30 & 36 & 18 & 0 & 0 & 1 \\ \hline \end{array}$$

и делаем четвёртый столбец первым:

$$\begin{array}{|cccc|ccc} \hline -3 & 6 & -9 & 0 & 1 & 0 & -2 \\ 9 & 30 & 15 & 18 & 0 & 1 & 0 \\ 18 & 60 & 30 & 36 & 0 & 0 & 1 \\ \hline \end{array}.$$

Так как все элементы левой матрицы делятся на 3, зануляем в ней 1-ю строку и 1-й столбец вне левого верхнего угла:

$$\left[\begin{array}{cccc|ccc} -3 & 0 & 0 & 0 & 1 & 0 & -2 \\ 0 & 48 & -12 & 18 & 3 & 1 & -6 \\ 0 & 96 & -24 & 36 & 6 & 0 & -11 \end{array} \right].$$

Теперь зануляем 3-ю строку, отнимая из неё удвоенную 2-ю:

$$\left[\begin{array}{cccc|ccc} -3 & 0 & 0 & 0 & 1 & 0 & -2 \\ 0 & 48 & -12 & 18 & 3 & 1 & -6 \\ 0 & 0 & 0 & 0 & 0 & -2 & 1 \end{array} \right].$$

Прибавляем к 3-му столбцу 4-й и переставляем результат во 2-й столбец:

$$\left[\begin{array}{cccc|ccc} -3 & 0 & 0 & 0 & 1 & 0 & -2 \\ 0 & 6 & 48 & 18 & 3 & 1 & -6 \\ 0 & 0 & 0 & 0 & 0 & -2 & 1 \end{array} \right].$$

Отнимаем из 3-го и 4-го столбцов 2-й, умноженный на 8 и на 3, меняем знак в первой строке и получаем окончательно:

$$\boxed{D_A} \mid L = \left[\begin{array}{cccc|ccc} 3 & 0 & 0 & 0 & -1 & 0 & 2 \\ 0 & 6 & 0 & 0 & 3 & 1 & -6 \\ 0 & 0 & 0 & 0 & 0 & -2 & 1 \end{array} \right].$$

Из проделанного вычисления уже видно, что $L \simeq \mathbb{Z}^2$, а $\mathbb{Z}^3/L \simeq \mathbb{Z}/(3) \oplus \mathbb{Z}/(6) \oplus \mathbb{Z}$. Для отыскания матрицы L^{-1} действуем как в [прим. 6.2](#) на стр. 107: приписываем к L единичную матрицу

$$L = \left[\begin{array}{ccc|ccc} -1 & 0 & 2 & 1 & 0 & 0 \\ 3 & 1 & -6 & 0 & 1 & 0 \\ 0 & -2 & 1 & 0 & 0 & 1 \end{array} \right],$$

прибавляем ко 2-й строке утроенную 1-ю:

$$\left[\begin{array}{ccc|ccc} -1 & 0 & 2 & 1 & 0 & 0 \\ 0 & 1 & 0 & 3 & 1 & 0 \\ 0 & -2 & 1 & 0 & 0 & 1 \end{array} \right],$$

затем прибавляем к 3-й строке удвоенную 2-ю:

$$\left[\begin{array}{ccc|ccc} -1 & 0 & 2 & 1 & 0 & 0 \\ 0 & 1 & 0 & 3 & 1 & 0 \\ 0 & 0 & 1 & 6 & 2 & 1 \end{array} \right],$$

наконец, отнимаем из 1-й строки удвоенную 3-ю, меняем в ней знак и получаем

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

Таким образом, взаимные базисы решётки \mathbb{Z}^3 и её подрешётки L состоят из векторов

$$u_1 = (11, 3, 6), \quad u_2 = (4, 1, 2), \quad u_3 = (2, 0, 1)$$

и векторов $w_1 = 3u_1 = (33, 9, 18)$, $w_2 = 6u_2 = (24, 6, 12)$.

УПРАЖНЕНИЕ 6.6. Выразите последние два вектора через столбцы матрицы (6-6).

6.3. Элементарные делители. Зафиксируем в каждом классе ассоциированных простых элементов кольца K какого-нибудь представителя и обозначим множество всех этих попарно неассоциированных представителей через $P(K)$. Как и ранее, будем обозначать через $v_p(m)$ показатель, с которым $p \in P(K)$ входит в разложение элемента $m \in K$ на простые множители. Сопоставим каждому упорядоченному набору необратимых чисел

$$\lambda_1, \dots, \lambda_n \in K, \text{ где } \lambda_i \mid \lambda_j \text{ при } i < j, \quad (6-7)$$

неупорядоченное дизъюнктивное объединение по всем $i = 1, \dots, n$ степеней $p^{v_p(\lambda_i)}$ с ненулевыми показателями $v_p(\lambda_i)$. Иначе говоря, рассмотрим для каждого $i = 1, \dots, n$ разложение на простые множители $\lambda_i = \prod_{p \in P(K)} p^{v_p(\lambda_i)}$ и соберём все участвующие в этих разложениях сомножители p^v с $v > 0$ в одно неупорядоченное множество, где каждая степень p^v , присутствующая в разложении ровно k чисел λ_i , тоже присутствует ровно k раз. Получающееся таким образом неупорядоченное множество (возможно повторяющихся) степеней p^v называется *набором элементарных делителей* упорядоченного набора (6-7).

Лемма 6.2

Описанная выше процедура устанавливает биекцию между рассматриваемыми с точностью до умножения каждого элемента на обратимое число из K упорядоченными наборами необратимых чисел $\lambda_1, \dots, \lambda_n \in K$, в которых $\lambda_i \mid \lambda_j$ при $i < j$, и всевозможными неупорядоченными наборами степеней p^v , где $p \in P(K)$, $n \in \mathbb{N}$, элементы в которых могут повторяться.

Доказательство. Набор $\lambda_1, \dots, \lambda_n$ однозначно восстанавливается по своему набору элементарных делителей следующим образом. Расставим элементарные делители в клетки диаграммы Юнга так, чтобы в первой строке шли в порядке нестрого убывания степени того $p \in P(K)$, степеней которого в наборе элементарных делителей имеется больше всего. Во вторую строку поместим в порядке нестрого убывания степени простого числа, следующего за p по общему количеству вхождений его степеней в набор элементарных делителей и т. д. Поскольку λ_n делится на все остальные λ_i , в его разложение на простые множители входят все встречающиеся среди элементарных делителей простые основания, причём каждое из них — с максимально возможным показателем. Таким образом, λ_n является произведением всех элементарных делителей, стоящих в первом столбце построенной диаграммы Юнга. По индукции мы заключаем, что произведения элементарных делителей по столбцам диаграммы, перебираемым слева направо, суть $\lambda_n, \dots, \lambda_1$, т. е. прочитанный справа налево набор (6-7). \square

Пример 6.6

Набор элементарных делителей

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

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

ТЕОРЕМА 6.4 (ТЕОРЕМА ОБ ЭЛЕМЕНТАРНЫХ ДЕЛИТЕЛЯХ)

Всякий конечно порождённый модуль над областью главных идеалов K изоморфен

$$K^{n_0} \oplus \frac{K}{(p_1^{n_1})} \oplus \dots \oplus \frac{K}{(p_\alpha^{n_\alpha})} \quad (6-8)$$

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

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

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

ОПРЕДЕЛЕНИЕ 6.2

Набор (возможно повторяющихся) степеней $p_i^{n_i}$, по которым происходит факторизация в (6-8), называется *набором элементарных делителей* модуля (6-8).

Доказательство существования разложения (6-8). Пусть K -модуль M порождается векторами

$$w_1, \dots, w_m.$$

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 форм. (6-5) на стр. 111. По теор. 6.3 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, $M = K^m / R = K / (\lambda_1) \oplus \dots \oplus K / (\lambda_k) \oplus K^{m-k}$. Если i -й инвариантный множитель λ_i обратим, то отвечающее ему слагаемое $K / (\lambda_i) = K / K$ нулевое. Если λ_i необратим, то $\lambda_i = p_1^{m_1} \dots p_s^{m_s}$, где $p_j \in K$ — попарно не ассоциированные простые элементы, и по китайской теореме об остатках $K / (\lambda_i) = K / (p_1^{m_1}) \oplus \dots \oplus K / (p_s^{m_s})$, что и даёт разложение (6-8). \square

Чтобы установить единственность разложения (6-8) для заданного K -модуля M , мы дадим инвариантное описание его ингредиентов во внутренних терминах модуля M . Этому посвящены идущие ниже разделы н° 6.3.1 – н° 6.3.3. Далее, в н° 6.3.4 мы установим обещанные ранее независимость инвариантных множителей матрицы A от способа её приведения к нормальной форме Смита D_A и независимость инвариантных множителей подмодуля $N \subset F$ в свободном модуле F от выбора взаимных базисов в F и N .

6.3.1. Отщепление кручения. Вектор w из модуля M над целостным¹ кольцом K называется *элементом кручения*, если $xw = 0$ для какого-нибудь ненулевого $x \in K$. Например, любой класс $[k]_n \in \mathbb{Z}/(n)$ является элементом кручения в \mathbb{Z} -модуле $\mathbb{Z}/(n)$, так как $n[k]_n = [nk]_n = [0]_n$. В общем случае элементы кручения составляют подмодуль в M , который обозначается

$$\text{Tors } M \stackrel{\text{def}}{=} \{w \in M \mid \exists x \neq 0 : xw = 0\} \quad (6-9)$$

и называется *подмодулем кручения* в M .

УПРАЖНЕНИЕ 6.7. Убедитесь в том, что $\text{Tors } M$ действительно является подмодулем в M .

Если $\text{Tors } M = 0$, то говорят, что модуль M *не имеет кручения*. Например, любой идеал целостного кольца K и любой подмодуль в координатном модуле K^n над таким кольцом не имеют кручения. Если $\text{Tors } M = M$, то M называется *модулем кручения*. Например, фактор K/I по любому ненулевому идеалу $I \subset K$ является K -модулем кручения, поскольку для любого класса $[a] \in K/I$ и любого ненулевого $x \in I$ класс $x[a] = [xa] = [0]$, так как $xa \in I$.

¹См. н° 1.4.1 на стр. 28.

ПРЕДЛОЖЕНИЕ 6.1

Для любого модуля M над целостным кольцом K фактормодуль $M/\text{Tors}(M)$ не имеет кручения. Если подмодуль $N \subset M$ таков, что $\text{Tors}(M/N) = 0$, то $\text{Tors}(M) \subset N$.

Доказательство. При ненулевом $x \in K$ равенство $x[w] = [xw] = [0]$ в $M/\text{Tors}(M)$ означает, что $xw \in \text{Tors}(M)$, т. е. $uxw = 0$ для некоторого ненулевого $u \in K$. Так как в K нет делителей нуля, $xu \neq 0$ и $w \in \text{Tors}(M)$, т. е. $[w] = [0]$. Это доказывает первое утверждение. Для доказательства второго заметим, что если $w \in \text{Tors}(M) \setminus N$, то класс $[w] \in M/N$ является ненулевым элементом кручения. \square

ТЕОРЕМА 6.5

Всякий конечно порождённый модуль M над областью главных идеалов K является прямой суммой свободного модуля и подмодуля кручения. В частности, любой модуль без кручения автоматически свободен.

Доказательство. По уже доказанному $M \simeq K^{n_0} \oplus K/(p_1^{n_1}) \oplus \dots \oplus K/(p_\alpha^{n_\alpha})$, где первое слагаемое свободно от кручения, а сумма остальных $N = K/(p_1^{n_1}) \oplus \dots \oplus K/(p_\alpha^{n_\alpha})$ является модулем кручения, и тем самым содержится в $\text{Tors}(M)$. Так как $M/N \simeq K^{n_0}$ не имеет кручения, $\text{Tors}(M) \subset N$ по [предл. 6.1](#). Тем самым, $\text{Tors}(M) = N$, $M = K^{n_0} \oplus \text{Tors}(M)$ и $M/\text{Tors}(M) \simeq K^{n_0}$. \square

Следствие 6.1 (из существования разложения из [теор. 6.5](#))

В форм. (6-8) на стр. 114 сумма $K/(p_1^{n_1}) \oplus \dots \oplus K/(p_\alpha^{n_\alpha}) = \text{Tors}(M)$ и число n_0 , равное рангу свободного модуля $M/\text{Tors}(M)$, не зависят от выбора разложения (6-8). \square

6.3.2. Отщепление p -кручения. Для каждого простого $p \in P(K)$ назовём подмодуль

$$\text{Tors}_p(M) \stackrel{\text{def}}{=} \{w \in M \mid \exists k \in \mathbb{N} : p^k w = 0\}$$

подмодулем p -кручения в M , а его элементы — *элементами p -кручения*.

УПРАЖНЕНИЕ 6.8. Убедитесь, что $\text{Tors}_p(M)$ действительно является подмодулем в M и докажите для него аналог [предл. 6.1](#): фактор $M/\text{Tors}_p(M)$ не имеет p -кручения, и если подмодуль $N \subset M$ таков, что $\text{Tors}_p(M/N) = 0$, то $\text{Tors}_p(M) \subset N$.

ТЕОРЕМА 6.6

Всякий конечно порождённый модуль кручения $M = \text{Tors}(M)$ над областью главных идеалов K является прямой суммой своих подмодулей p -кручения: $M = \bigoplus_p \text{Tors}_p(M)$, где сумма берётся по всем таким $p \in P(K)$, что $\text{Tors}_p(M) \neq 0$. При этом каждый конечно порождённый модуль p -кручения имеет вид $K/(p^{v_1}) \oplus \dots \oplus K/(p^{v_k})$, где $v_1, \dots, v_k \in \mathbb{N}$.

Доказательство. Если простое $q \in K$ не ассоциировано с p , то $\text{нод}(p^k, q^m) = 1$ для всех k, m , и класс $[p^k]$ обратим в факторкольце $K/(q^m)$. Поэтому гомоморфизм умножения на p^k :

$$K/(q^m) \rightarrow K/(q^m), \quad x \mapsto p^k x,$$

биективен и, в частности, не имеет ядра. Напротив, модуль $K/(p^v)$ аннулируется умножением на p^v . Тем самым, в разложении из форм. (6-8) на стр. 114

$$M = \text{Tors}(M) = \left(\frac{K}{(p^{v_1})} \oplus \dots \oplus \frac{K}{(p^{v_k})} \right) \oplus \left(\bigoplus_{q \neq p} \left(\frac{K}{(q^{\mu_{q,1}})} \oplus \dots \oplus \frac{K}{(q^{\mu_{q,m_q}})} \right) \right)$$

слагаемое в левых скобках содержится в $\text{Tors}_p(M)$, а фактор по нему, изоморфный сумме в правых скобках, не имеет p -кручения. Поэтому $\text{Tors}_p(M)$ совпадает с левым слагаемым, $M/\text{Tors}_p(M)$ изоморфен правому слагаемому, и $M \simeq \text{Tors}_p(M) \oplus (M/\text{Tors}_p(M))$. \square

Следствие 6.2 (из существования разложения из теор. 6.6)

В форм. (6-8) на стр. 114 сумма всех подмодулей $K/(p^v)$ с заданным $p \in P(K)$ является подмодулем p -кручения в M и не зависит от выбора разложения (6-8). \square

6.3.3. Инвариантность показателей p -кручения. Согласно теор. 6.6 каждый конечно порождённый модуль p -кручения M над областью главных идеалов K имеет вид

$$M = \frac{K}{(p^{v_1})} \oplus \dots \oplus \frac{K}{(p^{v_n})}. \quad (6-10)$$

Упорядоченные по нестрогому убыванию натуральные числа $v_1 \geq v_2 \geq \dots \geq v_n$ называются *показателями p -кручения* модуля M . Они образуют диаграмму Юнга $\nu = \nu(M) = (v_1, \dots, v_n)$, которая называется *цикловым типом* модуля p -кручения M . Для завершения доказательства теор. 6.4 остаётся проверить, что цикловой тип зависит только от модуля M , а не от выбора конкретного разложения (6-10). Для этого рассмотрим гомоморфизм умножения на p

$$\varphi : M \rightarrow M, \quad w \mapsto pw$$

и обозначим через $\varphi^k = \varphi \circ \dots \circ \varphi : w \mapsto p^k w$ его k -кратную итерацию, считая, что $\varphi^0 = \text{Id}_M$. Очевидно, что $\ker \varphi^k \subseteq \ker \varphi^{k+1}$ при всех k , и $\ker \varphi^k = M$ при $k \geq v_1$, но $\ker \varphi^k \neq M$ при $k < v_1$. Таким образом, мы имеем конечную цепочку возрастающих подмодулей

$$0 = \ker \varphi^0 \subseteq \ker \varphi^1 \subseteq \dots \subseteq \ker \varphi^{v_1-1} \subsetneq \ker \varphi^{v_1} = M, \quad (6-11)$$

которая зависит только от модуля M . В частности, v_1 зависит только от M .

Лемма 6.3

Для каждого $k = 1, \dots, v_1$ фактормодуль $\ker \varphi^k / \ker \varphi^{k-1}$ является векторным пространством над полем $\mathbb{k} = K/(p)$ размерности, равной высоте k -го столбца диаграммы Юнга $\nu(M)$.

Доказательство. Зададим умножение класса $[x] \in K/(p)$ на класс $[w] \in \ker \varphi^k / \ker \varphi^{k-1}$ правилом $[x][z] \stackrel{\text{def}}{=} [xz]$. Оно корректно, поскольку для $x' = x + py$ и $w' = w + u$, где $p^{k-1}u = 0$, имеем $x'w' = xw + (x + py)u + puw$, где $p^{k-1}((x + py)u + puw) = 0$, так как $p^{k-1}u = 0$ и $p^k w = 0$. Аксиомы дистрибутивности и ассоциативности очевидно выполняются. Это доказывает первое утверждение. Для доказательства второго рассмотрим произвольное разложение (6-10). Гомоморфизм φ переводит каждое слагаемое этого разложения в себя. Обозначим через $\varphi_i = \varphi|_{K/(p^{v_i})}$ ограничение φ на i -е слагаемое $K/(p^{v_i})$ разложения (6-10). Фактор модуль $\ker \varphi^k / \ker \varphi^{k-1}$ изоморфен прямой сумме фактормодулей $\ker \varphi_i^k / \ker \varphi_i^{k-1}$.

УПРАЖНЕНИЕ 6.9. Убедитесь, что при каждом i для каждого $k = 1, \dots, v_i$ отображение

$$K/(p) \rightarrow \ker \varphi_i^k / \ker \varphi_i^{k-1}, \quad x \pmod{p} \mapsto p^{v_i-k} x \pmod{\ker \varphi_i^{k-1}},$$

корректно определено, \mathbb{k} -линейно и биективно.

Таким образом, на каждом слагаемом разложения (6-10) цепочка ядер (6-11) имеет вид

$$0 = \ker \varphi_i^0 \subsetneq \ker \varphi_i^1 \subsetneq \dots \subsetneq \ker \varphi_i^{v_i-1} \subsetneq \ker \varphi_i^{v_i} = K/(p^{v_i}),$$

и каждый из её факторов $\ker \varphi_i^k / \ker \varphi_i^{k-1}$ при $k = 1, \dots, v_i$ является одномерным векторным пространством над полем $\mathbb{k} = K/(p)$, а во всём модуле (6-10) пространство $\ker \varphi^k / \ker \varphi^{k-1}$ является прямой суммой этих одномерных пространств в количестве, равном числу строк диаграммы ν , длина которых не меньше k , т. е. длине k -го столбца диаграммы ν . \square

На этом доказательство теоремы об элементарных делителях заканчивается.

Следствие 6.3 (ТЕОРЕМА ОБ ИНВАРИАНТНЫХ МНОЖИТЕЛЯХ)

Всякий конечно порождённый модуль над областью главных идеалов K изоморфен

$$K^{n_0} \oplus \frac{K}{(\lambda_1)} \oplus \dots \oplus \frac{K}{(\lambda_g)} \quad (6-12)$$

где n_0, g — целые неотрицательные, а $\lambda_1, \dots, \lambda_g \in K$ — такие ненулевые необратимые элементы, что $\lambda_i \mid \lambda_j$ при $i < j$. Два таких модуля

$$K^{n_0} \oplus \frac{K}{(\lambda_1)} \oplus \dots \oplus \frac{K}{(\lambda_g)} \quad \text{и} \quad K^{m_0} \oplus \frac{K}{(\mu_1)} \oplus \dots \oplus \frac{K}{(\mu_h)}$$

изоморфны если и только если $n_0 = m_0, g = h$ и $\lambda_i = s_i \mu_i$, где все $s_i \in K$ обратимы. \square

6.3.4. Единственность инвариантных множителей. Пусть F — свободный модуль конечного ранга m над областью главных идеалов K и $N \subset F$ — его подмодуль. Покажем, что множители $\lambda_1, \dots, \lambda_n$ из теоремы о взаимном базисе¹ не зависят от выбора взаимных базисов. В самом деле, фактормодуль $M = F/N$ ничего не знает о взаимных базисах, и по теореме об элементарных делителях² он имеет вид

$$M \simeq K^{m_0} \oplus \frac{K}{(p_1^{m_1})} \oplus \dots \oplus \frac{K}{(p_\alpha^{m_\alpha})}. \quad (6-13)$$

С другой стороны, если базис e_1, \dots, e_m модуля F таков, что векторы $\lambda_1 e_1, \dots, \lambda_n e_n$ составляют базис в N и $\lambda_i \mid \lambda_j$ при $i < j$, то $M = F/N \simeq K^{m-n} \oplus K/(\lambda_1) \oplus \dots \oplus K/(\lambda_n)$, где каждый фактор $K/(\lambda)$ либо нулевой (если λ обратим), либо — когда λ необратим — распадается по китайской теореме об остатках в прямую сумму модулей вида $K/(p^{v_p(\lambda)})$, где $p^{v_p(\lambda)}$ берутся из разложения $\lambda = \prod_{p \in P(K)} p^{v_p(\lambda)}$ на простые множители. Мы заключаем, что $m_0 = m - n$, а набор степеней $p^{v_p(\lambda)}$ является набором элементарных делителей упорядоченного по отношению делимости набора всех необратимых множителей λ , который по лем. 6.2 на стр. 114 однозначно восстанавливается по набору своих элементарных делителей. Таким образом число $n = m - m_0$ и все ненулевые необратимые инвариантные множители подмодуля N однозначно считываются с разложения (6-13), что и доказывает независимость инвариантных множителей подмодуля N от выбора взаимного базиса.

Применительно к модулю $F = K^m$ со стандартным базисом $e = (e_1, \dots, e_m)$ и его подмодулю $N \subset K^m$, порождённому столбцами $a = (a_1, \dots, a_n)$ матрицы $A \in \text{Mat}_{m \times n}(K)$, это утверждение означает, что элементы d_{ii} нормальной формы Смита матрицы A не зависят от способа её приведения к нормальной форме и даже собственно от матрицы, а зависят лишь от подмодуля N . В самом деле, если $D = LAR$ — это (какая-нибудь) нормальная форма Смита матрицы A , то из равенства $a = eA$ вытекает равенство $aR = eL^{-1}LAR = eL^{-1}D$. В силу обратимости матрицы R

¹См. теор. 6.3 на стр. 111.

²См. теор. 6.4 на стр. 114.

и L векторы $\mathbf{u} = \mathbf{e} L^{-1}$ тоже составляют базис в K^m , а векторы $\mathbf{w} = \mathbf{a}R$ линейно порождают N . Так как $\mathbf{w} = \mathbf{u}D$, векторы $\mathbf{u} = (u_1, \dots, u_m)$ и векторы $w_i = d_{ii}u_i$ с ненулевыми d_{ii} образуют взаимные базисы модуля K^m и его подмодуля N , а ненулевые диагональные элементы d_{ii} являются инвариантными множителями этого подмодуля.

Ответы и указания к некоторым упражнениям

Упр. 6.1. $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}^{-1} = \frac{1}{\Delta} \begin{pmatrix} \delta & -\beta \\ -\gamma & \alpha \end{pmatrix}$ как мы видели в [прим. 5.15](#) на стр. 92.

Упр. 6.3. Если матрица D диагональна, то матрица DA (соотв. AD) получается из матрицы A умножением её i -й строки (соотв. i -го столбца) на диагональный элемент d_{ii} матрицы D . Поэтому равенство $AD = DA = E$ равносильно тому, что $a_{ii}d_{ii} = 1$ и $a_{ij} = 0$ при всех $i \neq j$.

Упр. 6.4. Последовательно заменяя в данном столбце пары ненулевых элементов a, b по [лем. 6.1](#) на стр. 102 парами $\text{нод}(a, b), 0$, получаем столбец в котором отличен от нуля ровно один элемент $d \in K$, равный нод элементов исходного столбца. Если матрица A обратима, то её столбцы (a_1, \dots, a_n) образуют базис в K^n , причём $a_j = de_i$, где (e_1, \dots, e_n) — стандартный базис в K^n . Пусть стандартный базисный вектор e_i выражается через столбцы матрицы A по формуле $e_i = \sum x_\nu a_\nu$. Тогда $a_j - \sum dx_\nu a_\nu = 0$, и вектор a_j входит в эту линейную комбинацию с коэффициентом $1 - dx_j$, откуда $dx_j = 1$.

Упр. 6.6. Векторы w_1, w_2 — это первые два вектора набора $w = aR$, где матрица $R = R_1R_2R_3R_4$ задаёт совершенные в [прим. 6.5](#) на стр. 112 преобразования столбцов:

$$R_1 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

делает четвёртый столбец первым,

$$R_2 = \begin{pmatrix} 1 & 2 & -3 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

прибавляет ко 2-у и 3-у столбцам 1-й, умноженный на 2 и на -3 ,

$$R_3 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$$

записывает во 2-й столбец сумму к 3-го и 4-го, а в 3-й столбец — бывший 2-й,

$$R_4 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & -8 & -3 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

отнимает из 3-го и 4-го столбцов 2-й, умноженный на 8 и на 3. Вычисляя произведение¹, получаем

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

¹Или, что тоже самое, применяя указанные четыре преобразования к единичной матрице 4×4 .

откуда $w_1 = a_4$ и $w_2 = a_2 + a_3 - 3a_4$.

Упр. 6.7. Если $x_1 w_1 = 0$ и $x_2 w_2 = 0$ для ненулевых $x_1, x_2 \in K$, то $x_1 x_2 (w_1 \pm w_2) = 0$ и $x_1 x_2 \neq 0$, так как в K нет делителей нуля, и $x_1 (y w_1) = x_2 (y w_2) = 0$ для всех $y \in K$.

Упр. 6.8. Если $p^{k_1} w_1 = 0$ и $p^{k_2} w_2 = 0$, то $p^{k_1+k_2} (w_1 \pm w_2) = 0$ и $p^{k_1} y w_1 = 0$ для всех $y \in K$. Равенство $p^{k_1} [w] = [0]$ в $M / \text{Tors}_p(M)$ означает, что $p^{k_1} w \in \text{Tors}_p(M)$, т.е. $p^{k_2} p^{k_1} w = 0$ для некоторого $k_2 \in \mathbb{N}$, откуда $p^{k_1+k_2} w = 0$ и $w \in \text{Tors}_p(M)$, т.е. $[w] = [0]$. Если $w \in \text{Tors}_p(M) \setminus N$, то класс $[w] \in M/N$ является ненулевым элементом p -крючения.

Упр. 6.9. Класс $[p^{v_i-k} x] \in K / (p^{v_i})$ лежит в $\ker \varphi_i^k$, поскольку $p^k [p^{v_i-k} x] = [p^{v_i} x] = [0]$. Если $x' = x + py$, то $p^{v_i-k} x' = p^{v_i-k} x + p^{v_i-k+1} y$ и класс $[p^{v_i-k+1} y] \in K / (p^{v_i})$ лежит в $\ker \varphi_i^{k-1}$, так как $p^{k-1} [p^{v_i-k+1} y] = [p^{v_i} y] = [0]$. Линейность отображения очевидна. Оно сюръективно, поскольку каждый класс $[y] \in K / (p^{v_i})$, такой что $[p^k y] = [0]$, имеет $y = p^{v_i-k} x$ для некоторого $x \in K$ в силу того, что $p^k x$ делится на p^{v_i} в факториальном кольце K если и только если x делится на p^{v_i-k} . Ядро отображения нулевое по той же причине: если класс $[p^{v_i-k} x] \in K / (p^{v_i})$ лежит в $\ker \varphi_i^{k-1}$, то $p^{k-1} p^{v_i-k} x = p^{v_i-1} x$ делится на p^{v_i} , а значит $x \in p$ и класс $[x] \in K / (p)$ нулевой.