

§7. Конечно порождённые абелевы группы

7.1. Фробениусово и жорданово представления. При $K = \mathbb{Z}$ теорема об инвариантных множителях¹ и теорема об элементарных делителях² дают две альтернативных полных классификации конечно порождённых абелевых групп.

ТЕОРЕМА 7.1 (ТЕОРЕМА ОБ ИНВАРИАНТНЫХ МНОЖИТЕЛЯХ)

Всякая конечно порождённая абелева группа изоморфна прямой сумме аддитивных групп

$$\mathbb{Z}^r \oplus \frac{\mathbb{Z}}{(n_1)} \oplus \dots \oplus \frac{\mathbb{Z}}{(n_g)}, \quad (7-1)$$

где r — целое неотрицательное, а натуральные $n_1, \dots, n_g \geq 2$ таковы, что $n_i \mid n_j$ при $i < j$. Две такие группы

$$\mathbb{Z}^r \oplus \frac{\mathbb{Z}}{(n_1)} \oplus \dots \oplus \frac{\mathbb{Z}}{(n_g)} \quad \text{и} \quad \mathbb{Z}^s \oplus \frac{\mathbb{Z}}{(m_1)} \oplus \dots \oplus \frac{\mathbb{Z}}{(m_h)}$$

изоморфны если и только если $r = s$, $g = h$ и $n_i = m_i$ при всех i . □

ТЕОРЕМА 7.2 (ТЕОРЕМА ОБ ЭЛЕМЕНТАРНЫХ ДЕЛИТЕЛЯХ)

Всякая конечно порождённая абелева группа изоморфна прямой сумме аддитивных групп

$$\mathbb{Z}^r \oplus \frac{\mathbb{Z}}{(p_1^{n_1})} \oplus \dots \oplus \frac{\mathbb{Z}}{(p_\alpha^{n_\alpha})}, \quad (7-2)$$

где $p_\nu \in \mathbb{N}$ — простые числа (не обязательно различные). Две такие 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 если и только если $r = s$, $\alpha = \beta$ и после надлежащей перестановки слагаемых будут выполняться равенства $n_\nu = m_\nu$ и $p_\nu = q_\nu$ при всех ν . □

При этом в разложениях (7-1) и (7-2) данной абелевой группы A целые неотрицательные r одинаковы, а упорядоченный набор натуральных чисел $n_1 \mid \dots \mid n_g$ из разложения (7-1) и неупорядоченное множество возможно повторяющихся степеней p^ν из разложения (7-2) однозначно определяют друг друга по лем. 6.2 на стр. 114: множество элементарных делителей является дизъюнктивным объединением степеней $p^{\nu_p(n_i)}$ с $\nu_p(m_i) > 0$ по всем $1 \leq i \leq g$ и всем простым $p \in \mathbb{N}$, а набор инвариантных множителей n_1, \dots, n_g является прочитанным справа налево набором произведений, взятых по столбцам диаграммы Юнга, в первую строку которой выписаны в порядке нестрого убывания показателей все степени того числа p , степеней которого больше всего, во вторую — все степени следующего по общему количеству степеней числа p и т. д. Единственная с точностью до перестановки прямых слагаемых аддитивная группа (7-2), изоморфная заданной конечно порождённой абелевой группе A , называется *стандартным* (или *жордановым*) *представлением* группы A или разложением группы A в прямую сумму неразложимых циклических подгрупп, а прямая сумма (7-1) — *фробениусовым представлением* группы A .

¹См. сл. 6.3 на стр. 118.

²См. теор. 6.4 на стр. 114.

Пример 7.1 (Абелевы группы порядка ≤ 10)

Абелевы группы из двух, трёх, пяти, шести, семи и десяти элементов с точностью до изоморфизма единственны и их стандартные представления (7-2) имеют, соответственно, вид:

$$\mathbb{Z}/(2), \mathbb{Z}/(3), \mathbb{Z}/(5), \mathbb{Z}/(3) \oplus \mathbb{Z}/(2), \mathbb{Z}/(7), \mathbb{Z}/(5) \oplus \mathbb{Z}/(2).$$

Групп из четырёх элементов с точностью до изоморфизма две: $\mathbb{Z}/(4)$ и $\mathbb{Z}/(2) \oplus \mathbb{Z}/(2)$.

Упражнение 7.1. Убедитесь явным образом, что эти две группы не изоморфны.

Групп из девяти элементов с точностью до изоморфизма тоже две: $\mathbb{Z}/(9)$ и $\mathbb{Z}/(3) \oplus \mathbb{Z}/(3)$. Группы из восьми элементов с точностью до изоморфизма исчерпываются тремя попарно не изоморфными группами $\mathbb{Z}/(8)$, $\mathbb{Z}/(4) \oplus \mathbb{Z}/(2)$ и $\mathbb{Z}/(2) \oplus \mathbb{Z}/(2) \oplus \mathbb{Z}/(2)$.

7.1.1. Канонические и не канонические слагаемые стандартного представления. Для каждого простого p , участвующего в стандартном представлении данной группы A , в A имеется единственная подгруппа, изоморфная прямой сумме всех прямых слагаемых вида $\mathbb{Z}/(p^m)$ в разложении (7-2) — это подгруппа p -кручения $\text{Tors}_p(A) \subset A$. Прямая сумма этих подгрупп, т. е. подгруппа кручения $\text{Tors}(A) = \bigoplus_p \text{Tors}_p(A)$ — это единственная подгруппа в A , изоморфная сумме всех отличных от \mathbb{Z}^r элементов разложения (7-2). В противоположность этому, дополнительная к $\text{Tors}(A)$ свободная подгруппа $B \subset A$, изоморфная $\mathbb{Z}^r \simeq A/\text{Tors}(A)$ может быть выбрана в A разными способами. Например, группа $A = \mathbb{Z} \oplus \mathbb{Z}/(3)$ иначе раскладывается как $B \oplus \mathbb{Z}/(3)$, где подгруппа $B \subset A$ порождена элементом $(1, [1]_3) \in A$.

Упражнение 7.2. Убедитесь в этом и перечислите для группы $A = \mathbb{Z} \oplus \mathbb{Z}/(3)$ все изоморфные \mathbb{Z} подгруппы $B \subset A$, дополнительные к $\text{Tors}(A)$.

Разложение подгруппы p -кручения в сумму неразложимых циклических подгрупп

$$\text{Tors}_p(A) = \frac{\mathbb{Z}}{(p^{v_1})} \oplus \dots \oplus \frac{\mathbb{Z}}{(p^{v_n})}$$

тоже не единственно: для каждого показателя v_i изоморфная $\mathbb{Z}/(p^{v_i})$ подгруппа в A может выбираться разными способами. Например, группа $A = \mathbb{Z}/(4) \oplus \mathbb{Z}/(2)$ иначе раскладывается в сумму $B \oplus C$ подгрупп $B \simeq \mathbb{Z}/(4)$ и $C \simeq \mathbb{Z}/(2)$, порождённых элементами $([1]_4, [1]_2)$ и $([2]_4, [1]_2)$ соответственно. Но цикловой тип группы A , т. е. набор (v_1, \dots, v_n) показателей p -кручения, от выбора разложения не зависит.

7.1.2. Циклические группы и минимальные наборы образующих. Пусть абелева группа A порождается как \mathbb{Z} -модуль элементами a_1, \dots, a_m . Наборы образующих с наименьшим возможным m называются *минимальными*. Группа (7-1)

$$A = \mathbb{Z}^r \oplus \frac{\mathbb{Z}}{(n_1)} \oplus \dots \oplus \frac{\mathbb{Z}}{(n_g)},$$

где $n_i \mid n_j$ при $i < j$, порождается $r + g$ элементами вида $(0, \dots, 0, 1, 0, \dots, 0)$. Покажем, что это минимальный набор образующих. Пусть A порождается m элементами a_1, \dots, a_m . Тогда

$$A \simeq \mathbb{Z}^m / R,$$

где $R \subset \mathbb{Z}^m$ — ядро сюръективного гомоморфизма $\mathbb{Z} \twoheadrightarrow A$, переводящего стандартные базисные векторы $e_1, \dots, e_m \in \mathbb{Z}^m$ в $a_1, \dots, a_m \in A$. Пусть векторы f_1, \dots, f_m и $\lambda_1 f_1, \dots, \lambda_k f_k$ образуют

взаимные базисы в \mathbb{Z}^m и R , и пусть $\lambda_1 = \dots = \lambda_s = 1$, а $\lambda_{s+1} \mid \dots \mid \lambda_k$ строго больше 1. Тогда фробениусово представление группы $A = \mathbb{Z}^m/R$ имеет вид

$$\frac{\mathbb{Z}}{(\lambda_{s+1})} \oplus \dots \oplus \frac{\mathbb{Z}}{(\lambda_k)} \oplus \mathbb{Z}^{m-k},$$

и в силу единственности фробениусова представления $r = (m - k)$, $g = k - s$ и $n_i = \lambda_{s+i}$ при всех $i = 1, \dots, g$. В частности $r + g = m - s \leq m$, что и утверждалось.

В терминах разложения (7-2) в прямую сумму неразложимых циклических подгрупп число g конечных слагаемых фробениусова разложения абелевой группы A равно максимальному числу элементарных делителей с одним и тем же простым основанием, т. е. длине верхней строки диаграммы Юнга, составленной из элементарных делителей группы A .

Абелевы группы, которые можно породить одним элементом, называются *циклическими*. Фробениусово разложение такой группы имеет ровно одно слагаемое. Тем самым, циклические абелевы группы исчерпываются группами \mathbb{Z} и $\mathbb{Z}/(n)$. В терминах элементарных делителей абелева группа A циклическая если и только если все простые числа в слагаемых $\mathbb{Z}/(p^m)$ её стандартного представления (7-2) попарно различны. Например, группа $\mathbb{Z}/(125) \oplus \mathbb{Z}/(9) \oplus \mathbb{Z}/(16)$ циклическая, а группа $\mathbb{Z}/(2) \oplus \mathbb{Z}/(3) \oplus \mathbb{Z}/(4) \simeq \mathbb{Z}/(2) \oplus \mathbb{Z}/(12)$ — нет.

7.1.3. Неразложимые группы. Абелева группа A называется *разложимой*, если она является прямой суммой $A = B \oplus C$ двух ненулевых собственных подгрупп $B, C \subsetneq A$. Из теор. 7.2 на стр. 120 вытекает, что каждая неразложимая абелева группа изоморфна \mathbb{Z} или $\mathbb{Z}/(p^m)$, где $p \in \mathbb{N}$ — простое, причём эти неразложимые группы попарно не изоморфны, а произвольная конечно порождённая абелева группа является прямой суммой неразложимых.

7.1.4. Простые и полупростые группы. Абелева группа A называется *простой*¹, если в ней нет ненулевых собственных подгрупп. Каждая простая группа автоматически неразложима. Обратное неверно: группы \mathbb{Z} и $\mathbb{Z}/(p^m)$, где $m \geq 2$ неразложимы, но не просты, поскольку содержат ненулевые собственные подгруппы.

УПРАЖНЕНИЕ 7.3. Опишите все ненулевые собственные подгруппы в \mathbb{Z} и в $\mathbb{Z}/(p^m)$, где $m \geq 2$.

Поскольку порядок любой подгруппы в конечной группе A делит порядок A , все конечные группы простого порядка просты. Мы заключаем, что конечно порождённые простые абелевы группы с точностью до изоморфизма исчерпываются группами $\mathbb{Z}/(p)$, где $p \in \mathbb{N}$ — простое, и при разных p такие группы не изоморфны.

Абелева группа называется *полупростой*, если она является прямой суммой простых подгрупп. Таким образом, конечно порождённые полупростые абелевы группы исчерпываются конечными прямыми суммами групп вида $\mathbb{Z}/(p)$, где $p \in \mathbb{N}$ — простое.

Предложение 7.1

Следующие свойства конечно порождённой абелевой группы A эквивалентны:

- (1) A полупроста
- (2) A порождается своими простыми подгруппами
- (3) каждая ненулевая собственная подгруппа $B \subsetneq A$ отщепляется прямым слагаемым, т. е. найдётся такая подгруппа $C \subset A$, что $A = B \oplus C$.

¹В другой терминологии — *неприводимой*.

Доказательство. Импликация (1) \Rightarrow (2) очевидна. Докажем импликацию (2) \Rightarrow (3). Так как все простые абелевы группы являются группами кручения, группа A , удовлетворяющая условию (2), тоже является группой кручения и по теор. 7.2 на стр. 120 конечна. Пересечение любой простой подгруппы $U \subset A$ с любой подгруппой $W \subsetneq A$, будучи подгруппой в U , либо нулевое, либо совпадает с U . Так как \mathbb{Z} -линейная оболочка простых подгрупп совпадает с A , для любой собственной подгруппы $B \subsetneq A$ найдётся простая подгруппа $U_1 \subsetneq B$. Сумма подгрупп B и U_1 прямая. Если $B \oplus U_1 \neq A$, заменяем B на $B \oplus U_1$ и повторяем рассуждение, до тех пор пока не получим равенство $A = B \oplus U_1 \oplus \dots \oplus U_k$, где все U_k просты. Остаётся положить $C = U_1 \oplus \dots \oplus U_k$.

Чтобы установить импликацию (3) \Rightarrow (1), докажем сначала, что если группа A обладает свойством (3), то им обладает и каждая подгруппа $B \subset A$. Пусть $V \subset B$ — любая подгруппа. Тогда в A существуют такие подгруппы C, U , что $A = B \oplus C = V \oplus C \oplus U$. Обозначим через

$$\pi : A \rightarrow B, \quad b + c \mapsto b,$$

проекцию A на B вдоль C и положим $W = \pi(U)$.

УПРАЖНЕНИЕ 7.4. Проверьте, что $B = V \oplus W$.

Поскольку группы \mathbb{Z}^n и $\mathbb{Z}/(p^m)$ с $m \geq 2$ не просты и неразложимы, они не обладают свойством (3) и по доказанному не могут входить в стандартное представление группы, которая обладает свойством (3). Тем самым, каждая группа, обладающая свойством (3) является прямой суммой простых групп. \square

УПРАЖНЕНИЕ 7.5. Убедитесь непосредственно, что группы \mathbb{Z} и $\mathbb{Z}/(p^m)$ с $m \geq 2$ не порождаются своими простыми подгруппами.

7.2. Группы, заданные образующими и соотношениями. На практике конечно порождённые абелевы группы часто задаются образующими и соотношениями. Это описание обычно звучит так: «рассмотрим абелеву группу A , порождённую элементами a_1, \dots, a_m , которые связаны соотношениями

$$\begin{cases} a_1 r_{11} + a_2 r_{21} + \dots + a_m r_{m1} = 0 \\ a_1 r_{12} + a_2 r_{22} + \dots + a_m r_{m2} = 0 \\ \dots \dots \dots \dots \dots \dots \dots \\ a_1 r_{1n} + a_2 r_{2n} + \dots + a_m r_{mn} = 0, \end{cases} \tag{7-3}$$

где $R = (r_{ij}) \in \text{Mat}_{m \times n}(\mathbb{Z})$. Оно означает, что $A = \mathbb{Z}^m / M$, где подмодуль $M \subset \mathbb{Z}^m$ порождается над \mathbb{Z} строками r_1, \dots, r_m матрицы R , а образующие $a_j = [e_j]_M \in A$ суть классы стандартных базисных векторов $e_j \in \mathbb{Z}^m$ по модулю подрешётки $M \subset \mathbb{Z}^m$.

7.2.1. Стандартное представление. Рассмотрим векторное пространство $\mathbb{Q}^m \supset \mathbb{Z}^m$, в которое координатный модуль \mathbb{Z}^m естественным образом вложен, и обозначим через

$$\mathbb{Q} \otimes M \stackrel{\text{def}}{=} \text{span}_{\mathbb{Q}}(M) \subset \mathbb{Q}^m$$

\mathbb{Q} -линейную оболочку строк матрицы R в \mathbb{Q}^m . Её размерность $\dim_{\mathbb{Q}}(\mathbb{Q} \otimes M) = \text{rk} R = \text{rk} M$ совпадает как с рангом матрицы R над полем \mathbb{Q} , так и с рангом свободного \mathbb{Z} -модуля $M \subset \mathbb{Z}^n$, поскольку любой базис решётки M над \mathbb{Z} одновременно является базисом пространства $\mathbb{Q} \otimes M$ над \mathbb{Q} .

УПРАЖНЕНИЕ 7.6. Докажите, что набор векторов $v_1, \dots, v_k \in \mathbb{Z}^m \subset \mathbb{Q}^m$ линейно независим над \mathbb{Z} если и только если он линейно независим над \mathbb{Q} .

Мы заключаем, что ранг свободного слагаемого $A/\text{Tors}(A)$ в стандартном представлении¹ группы $A = \mathbb{Z}^m / M$ равен $m - \text{rk } R$, причём ранг матрицы R можно вычислять над полем \mathbb{Q} . Для вычисления остальных слагаемых стандартного представления необходимо найти все ненулевые инвариантные множители $\lambda_1, \dots, \lambda_r$ матрицы R . Тогда фробениусово представление группы $A = \mathbb{Z}^m / M$ будет иметь вид $\mathbb{Z}^{m-r} \oplus \mathbb{Z}/(\lambda_1) \oplus \dots \oplus \mathbb{Z}/(\lambda_r)$, а стандартное представление получится из него разложением каждого фактора $\mathbb{Z}/(\lambda_i)$ по китайской теореме об остатках.

УПРАЖНЕНИЕ 7.7. Найдём стандартное представление абелевой группы, порождённой элементами a_1, a_2, a_3 , которые связаны соотношениями

$$\begin{cases} -57a_1 + 58a_2 - 55a_3 = 0 \\ -34a_1 + 40a_2 - 22a_3 = 0 \\ 5a_1 - 10a_2 - 5a_3 = 0 \\ 9a_1 - 11a_2 + 5a_3 = 0. \end{cases}$$

Для этого методом Гаусса найдём инвариантные множители матрицы

$$R = \begin{pmatrix} -57 & -34 & 5 & 9 \\ 58 & 40 & -10 & -11 \\ -55 & -22 & -5 & 5 \end{pmatrix}$$

Прибавим к 1-й строке 2-ю:

$$\begin{pmatrix} 1 & 6 & -5 & -2 \\ 58 & 40 & -10 & -11 \\ -55 & -22 & -5 & 5 \end{pmatrix}$$

Зануляем верхнюю строку и левый столбец вне левого верхнего угла:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -308 & 280 & 105 \\ 0 & 308 & -280 & -105 \end{pmatrix}$$

Так как 3-я строка кратна 2-й, и наибольший общий делитель второй строки равен 7, ненулевые множители матрицы R суть 1 и 7, а её ранг равен 2. Мы заключаем, что

$$A = \mathbb{Z}^3 / M \simeq \mathbb{Z} \oplus \mathbb{Z}/(7).$$

7.2.2. Порядки элементов. На практике часто бывает важно знать, отлична ли от нуля та или иная \mathbb{Z} -линейная комбинация $w = k_1a_1 + \dots + k_ma_m$ образующих a_i , и если да, то каков порядок² $\text{ord}([w])$ элемента $[w]$ в группе A . Для ответа на эти вопросы необходимо выяснить, лежит или нет какое-нибудь целое кратное zw вектора $w = (k_1, \dots, k_m)$ в целочисленной линейной оболочке строк $r_1, \dots, r_n \in \mathbb{Z}^m$ матрицы соотношений R из формулы (7-3). Если строки матрицы R линейно независимы над \mathbb{Q} , т. е. образуют базис модуля $M \subset \mathbb{Z}^m$ соотношений между образующими a_1, \dots, a_m над \mathbb{Z} , то достаточно решить над полем \mathbb{Q} систему уравнений

$$r_1x_1 + \dots + r_mx_m = w \tag{7-4}$$

¹См. теор. 7.2 на стр. 120.

²Напомним, что порядком $\text{ord}(w)$ элемента w в аддитивной абелевой группе называется наименьшее такое $n \in \mathbb{N}$, что $nw = 0$, а если такого n нет, то $\text{ord}(w) = \infty$, см. н° 2.5.1 на стр. 51.

которая в матричных обозначениях имеет вид $R^t x = w^t$, и в силу линейной независимости векторов r_1, \dots, r_n либо несовместна, либо имеет единственное рациональное решение. В первом случае никакое целое кратное zw не лежит в M . Поэтому класс $[w]_M$ отличен от нуля в группе $A = \mathbb{Z}^m / M$ и имеет в ней бесконечный порядок. Если же система (7-4) имеет рациональное решение $x_i = p_i / q_i \in \mathbb{Q}$, где $\text{нод}(p_i, q_i) = 1$ при всех i , то

$$w = \frac{p_1}{q_1} r_1 + \dots + \frac{p_n}{q_n} r_n$$

и $\text{ord}([w]_M) = \text{нод}(q_1, \dots, q_n)$. В частности, $[w]_M = 0$ если и только если все $q_i = 1$, т. е. когда система (7-4) решается в целых числах.

7.2.3. Подрешётки в \mathbb{Z}^m . Абелевы подгруппы $L \subset \mathbb{Z}^m$ обычно называют *подрешётками* в \mathbb{Z}^m . Согласно теор. 6.2 на стр. 111 каждая подрешётка $L \subset \mathbb{Z}^m$ является свободным \mathbb{Z} -модулем ранга $\text{rk } L \leq m$. Если $\text{rk } L = m$, подрешётка L называется *соизмеримой* с \mathbb{Z}^m . Из сказанного выше вытекает

Предложение 7.2 (соизмеримые подрешётки)

Следующие свойства подрешётки $L_A \subset \mathbb{Z}^m$, порождённой столбцами матрицы $A \in \text{Mat}_{m \times n}(\mathbb{Z})$, эквивалентны друг другу:

- (1) $\text{rk } L = m$
- (2) факторгруппа \mathbb{Z}^m / L конечна
- (3) ранг матрицы A над полем \mathbb{Q} равен m . □

Решётка $L \subset \mathbb{Z}^m$ называется *отщепимой*, если она удовлетворяет следующему предложению.

Предложение 7.3 (отщепимые подрешётки)

Следующие свойства подрешётки $L \subset \mathbb{Z}^m$ эквивалентны друг другу:

- (1) все ненулевые инвариантные множители подрешётки L равны единице
- (2) факторгруппа \mathbb{Z}^m / L не имеет кручения
- (3) существует такая подрешётка $N \subset \mathbb{Z}^m$, что $\mathbb{Z}^m = L \oplus N$
- (4) решётка L является множеством всех целых решений системы однородных линейных уравнений $Ax = 0$ с целочисленной матрицей A высоты m .

Доказательство. Равносильность условий (1), (2) и импликации $(1) \Rightarrow (3)$, (4) вытекают из теоремы о взаимном базисе: если первые r базисных векторов базиса u_1, \dots, u_m в \mathbb{Z}^m образуют базис в L , то дополнительная к L подрешётка N является линейной оболочкой последних $m - r$ базисных векторов, а решётка L задаётся линейными однородными уравнениями, констатирующими обнуление последних $m - r$ координат вектора в базисе u_1, \dots, u_m .

Импликация $(3) \Rightarrow (2)$ очевидна, так как $(L \oplus N) / L \simeq N$.

Докажем импликацию $(4) \Rightarrow (2)$. Пусть $A \in \text{Mat}_{k \times m}(\mathbb{Z})$ и подрешётка $L \subset \mathbb{Z}^m$ является ядром линейного отображения $\alpha : \mathbb{Z}^m \rightarrow \mathbb{Z}^k$, $x \mapsto Ax$. Тогда отображение $\bar{\alpha} : \mathbb{Z}^m / L \hookrightarrow \mathbb{Z}^k$, $[x] \mapsto Ax$, корректно определено и инъективно.

Упражнение 7.8. Убедитесь в этом.

Тем самым, \mathbb{Z}^m / L изоморфен подмодулю модуля без кручения. □

7.3. Общие замечания о полупростоте. Пусть K — произвольное ассоциативное кольцо, т. е. абелева группа с операцией умножения $K \times K \rightarrow K$, которая дистрибутивна по отношению к сложению: $(x + y)z = xz + yz$, $x(y + z) = xy + xz$, и ассоциативна: $(xy)z = x(yz)$, где $x, y, z \in K$. Абелева группа V называется *левым K -модулем*, если задано умножение (или действие)

$$K \times V \rightarrow V,$$

которое тоже дистрибутивно и ассоциативно:

$$\begin{aligned} \forall z \in K, \forall u, w \in V \quad z(u + w) = zu + zw \quad \text{и} \quad \forall x, y \in K, \forall v \in V \quad (x + y)v = xv + yv, \\ \forall x, y \in K, \forall v \in V \quad (xy)v = x(yv). \end{aligned}$$

Подмодуль в V — это абелева подгруппа, выдерживающая умножение на все элементы из K . Модуль U называется *простым*, если в нём нет ненулевых собственных подмодулей, и *полупростым*, если он является прямой суммой простых (не обязательно конечной).

ЛЕММА 7.1

Пусть K -модуль W линейно порождается над K некоторым множеством \mathcal{S} своих простых K -подмодулей. Тогда у любого собственного подмодуля $U \subsetneq W$ имеется дополнительный¹ подмодуль V , являющийся прямой суммой подходящих подмодулей из множества \mathcal{S} . Для нулевого подмодуля $U = 0$ это означает, что весь модуль W является прямой суммой подходящих подмодулей из множества \mathcal{S} . В частности, такой модуль W автоматически полупрост.

Доказательство. Так как $U \neq W$ и W линейно порождается подмодулями $S \in \mathcal{S}$, в множестве \mathcal{S} найдётся подмодуль $S \not\subset U$. Сумма $U + S$ является прямой, поскольку пересечение $S \cap U \subsetneq S$ и S прост. Обозначим через \mathcal{S}' множество всех полупростых подмодулей $M \subset W$, которые являются прямыми суммами модулей из \mathcal{S} и имеют нулевое пересечение с U . По предыдущему, множество \mathcal{S}' непусто. Введём на нём частичный порядок, полагая $M_1 < M_2$, когда $M_2 = M_1 \oplus M$ для ненулевого $M \in \mathcal{S}'$.

УПРАЖНЕНИЕ 7.9. Убедитесь, что \mathcal{S}' является полным чумом².

По лемме Цорна³ в множестве \mathcal{S}' имеется максимальный элемент V . По построению $U \cap V = 0$. Покажем, что $U + V = W$. Если $U + V \neq W$, то повторяя проведённое в начале доказательства рассуждение для подмодуля $U' = U + V$ в роли подмодуля U , мы найдём в \mathcal{S} такой подмодуль $S \subset W$, что сумма $U' + S$ прямая. Это означает, что $V \oplus S \in \mathcal{S}'$ строго больше, чем V . Всё сказанное работает и для $U = 0$. \square

ТЕОРЕМА 7.3

Модуль W полупрост если и только если каждый ненулевой подмодуль в W содержит простой ненулевой подмодуль и для каждого ненулевого собственного подмодуля $U \subset W$ найдётся такой подмодуль $V \subset W$, что $W = U \oplus V$.

Доказательство. Если модуль W полупрост, т. е. является прямой суммой простых подмодулей, подмодуль $V \subset W$, дополнительный к произвольно заданному подмодулю $U \subset W$, существует по лем. 7.1, применённой к множеству \mathcal{S} всех простых подмодулей в W .

¹Т. е. такой подмодуль $V \subset W$, что $W = U \oplus V$, см. прим. 5.10 на стр. 86.

²См. опр. 0.3 на стр. 20.

³См. сл. 0.1 на стр. 20.

Упражнение 7.10. Убедитесь, что проекция $\pi : W = U \oplus V \rightarrow U, u + v \mapsto u$, K -линейна, т. е. $\pi(xw) = x\pi(w)$ для всех $x \in K$ и $w \in W$.

Так как W линейно порождается простыми подмодулями, проекция π переводит хотя бы один из них в ненулевой подмодуль в U .

Упражнение 7.11. Убедитесь, что этот ненулевой подмодуль прост.

Это доказывает прямую импликацию «только если». Чтобы доказать обратную импликацию, обозначим через \mathcal{S} множество всех полупростых ненулевых подмодулей $S \subseteq W$. Это множество непусто, поскольку содержит ненулевой простой подмодуль, имеющийся в W по условию. Зададим на \mathcal{S} частичный порядок, полагая $S_1 < S_2$ когда $S_2 = S_1 \oplus S$ для некоторого $S \in \mathcal{S}$.

Упражнение 7.12. Убедитесь, что чум \mathcal{S} полон.

По лемме Цорна, в \mathcal{S} есть максимальный элемент M . Если он не совпадает с W , то найдётся такой нетривиальный подмодуль $V \subset W$, что $W = M \oplus V$. Поскольку в V есть нетривиальный простой подмодуль $S \subset V$, сумма $M \oplus S \in \mathcal{S}$ будет строго больше, чем M . Тем самым, $M = W$. \square

Следствие 7.1 (критерии полупростоты)

Пусть каждый ненулевой подмодуль K -модуля W содержит ненулевой простой K -подмодуль. Тогда следующие свойства модуля W эквивалентны:

- 1) W полупрост
- 2) W линейно порождается простыми подмодулями
- 3) для каждого ненулевого собственного подмодуля $U \subset W$ существует такой ненулевой собственный подмодуль $V \subset W$, что $W = U \oplus V$. \square

Упражнение 7.13. Пусть модуль V таков, что для любого ненулевого собственного подмодуля $U \subset V$ найдётся такой подмодуль $W \subset V$, что $V = U \oplus W$. Докажите, что любой подмодуль $V' \subset V$ тоже обладает этим свойством.

Ответы и указания к некоторым упражнениям

Упр. 7.1. В $\mathbb{Z}/(4)$ есть элемент порядка 4, а в $\mathbb{Z}/(2) \oplus \mathbb{Z}/(2)$ такого элемента нет.

Упр. 7.2. Имеется ровно три таких подгруппы. Они порождаются элементами $(1, [0]_3)$, $(1, [1]_3)$ и $(1, [-1]_3)$.

Упр. 7.3. Каждая ненулевая собственная подгруппа в \mathbb{Z} имеет вид $(n) = \{x \in \mathbb{Z} \mid x : n\}$, где $n \geq 2$, а каждая ненулевая собственная подгруппа в $\mathbb{Z}/(p^m)$ имеет вид $(p^k) = \{[x] \in \mathbb{Z}/(p^m) \mid x : p^k\}$, где $1 \leq k \leq m$.

Упр. 7.4. Так как любой вектор $b \in B$ представляется в A как $b = v + c + u$, где $u \in U$, $c \in C$, $u \in U$, выполняется равенство $b = \pi(b) = \pi(v + c + u) = v + \pi(u)$. Поэтому $B = V + W$. Если $b \in V \cap W$, то $b = \pi(u)$ для некоторого $u \in U$, и $\pi(b - u) = b - \pi(u) = 0$. Поэтому $b - u \in \ker \pi = C$, что возможно только при $b = u = 0$.

Упр. 7.6. Умножая \mathbb{Q} -линейную комбинацию векторов на общий знаменатель всех её коэффициентов, получаем \mathbb{Z} -линейную комбинацию тех же векторов.

Упр. 7.9. Верхней гранью цепи из S' является объединение всех модулей цепи.

Упр. 7.10. Пусть $w = u + v$. Тогда $fw = fu + fv$ и $fv \in V$. Поэтому $\pi(fw) = fu = f\pi(w)$.

Упр. 7.11. Пусть $S \subset W$ прост и $\pi(S) \neq 0$. Для любого K -подмодуля $M \subset \pi(S)$ пересечение

$$S \cap \pi^{-1}(M) = \{s \in S \mid \pi(s) \in M\}$$

является K -подмодулем в S : если $\pi(s) \in M$, то $\pi(fs) = f\pi(s) \in M$ для всех $f \in K$ и $s \in S$. Так как в S нет нетривиальных собственных подмодулей, их нет и в $\pi(S)$.

Упр. 7.12. Верхней гранью цепи из S является объединение или, что то же самое, прямая сумма всех модулей цепи.

Упр. 7.13. Воспользуйтесь рассуждением, которое использовалось при доказательстве импликации (3) \Rightarrow (1) в [предл. 7.1](#) на стр. 122.