Глава IX. Модули над областями главных идеалов

§1. Модули и их гомоморфизмы

1°. **Модули над ассоциативными кольцами с 1.** Пусть Λ – ассоциативное кольцо с 1. Левым модулем над Λ, или левым Λ-модулем, называется множество M, на котором определено сложение, а также умножение слева на элементы из кольца Λ, обладающие следующими свойствами:

(1) $u + (v + w) = (u + v) + w$ для любых $u, v, w \in M$;
(2) $u + v = v + u$ для любых $u, v \in M$;
(3) существует такой элемент $0 \in V$, что $v + 0 = v$ для любого $v \in M$;
(4) для всякого $v \in M$ существует такой элемент $-v \in M$, что $v + (-v) = 0$;
(5) $\lambda(u + v) = \lambda u + \lambda v$ для любых $\lambda \in \Lambda$, $u, v \in M$;
(6) $(\lambda + \mu)v = \lambda v + \mu v$ для любых $\lambda, \mu \in \lambda$, $v \in M$;
(7) $(\lambda\mu)v = \lambda(\mu v)$ для любых $\lambda, \mu \in \lambda$, $v \in M$;
(8) $1 \cdot v = v$ для любого $v \in M$ (здесь 1 означает единицу кольца Λ).

Все эти аксиомы нам хорошо знакомы: они в точности совпадают с аксиомами векторного пространства. Единственное отличие состоит в том, что в случае векторного пространства в качестве множества операторов выступало не произвольное ассоциативное кольцо с 1, а поле, которое является частным случаем такого кольца.

2°. **Правые модули.** Иногда удобно операторы из кольца Λ писать не слева, а справа от элемента модуля; в этом случае мы говорим о правых модулях. Точнее говоря, правым Λ-модулем, называется множество M, на котором определено сложение, а также умножение справа на элементы из кольца Λ, обладающие следующими свойствами:

(1) $u + (v + w) = (u + v) + w$ для любых $u, v, w \in M$;
(2) $u + v = v + u$ для любых $u, v \in M$;
(3) существует такой элемент $0 \in V$, что $v + 0 = v$ для любого $v \in M$;
(4) для всякого $v \in M$ существует такой элемент $-v \in M$, что $v + (-v) = 0$;
(5) $(u + v)\lambda = u\lambda + v\lambda$ для любых $\lambda \in \Lambda$, $u, v \in M$;
(6) $v(\lambda + \mu) = v\lambda + v\mu$ для любых $\lambda, \mu \in \lambda$, $v \in M$;
(7) $v(\lambda\mu) = (v\lambda)\mu$ для любых $\lambda, \mu \in \lambda$, $v \in M$;
(8) $v \cdot 1 = v$ для любого $v \in M$ (здесь 1 означает единицу кольца Λ).

Отметим, что разница между левым и правым модулями – не только в форме записи; для них принципиально различным образом выглядит аксиома 7. В случае левых модулей действие произведения $\lambda\mu$ на элемент v осуществляется так: сначала действует второй сомножитель, а затем результат умножают на первый сомножитель. В правых модулях все как раз наоборот: сначала элемент умножается на первый сомножитель, а затем – на второй. Если кольцо Λ коммутативно, то эта разница не принципиальна; именно так обстояло дело в векторных пространствах над полями, где мы часто записывали коэффициенты не только слева, но и справа от вектора. Для модулей же над некоммутативными кольцами такая путаница недопустима.

В дальнейшем мы будем работать только с левыми модулями, часто не оговаривая это специально.

3°. **Примеры модулей.** 1. Как мы уже отметили, всякое векторное пространство над полем k является k-модулем.

2. Пусть Γ – ассоциативное кольцо с 1, и пусть Λ – его подкольцо, содержащее 1. По сложению Γ является группой; кроме того, для любого $\gamma \in \Gamma$ и любого $\lambda \in \Lambda$ определено произведение $\lambda\gamma \in \Gamma$. Из аксиом ассоциативного кольца с 1 следуют все свойства, нужные для того, чтобы Γ было левым Λ-модулем. Часто

для обозначения того, что кольцо Γ рассматривается как левый Λ-модуль, мы обозначаем его ${}_\Lambda\Gamma$. Точно так же, кольцо Γ может рассматриваться как правый Λ-модуль Γ_Λ. В частности, само кольцо Λ является левым Λ-модулем ${}_\Lambda\Lambda$ и правым Λ-модулем Λ_Λ.

3. Всякая абелева группа A (аддитивно записанная) может рассматриваться как модуль над кольцом целых чисел $\mathbb{Z}$. Действительно, для всякого $a \in A$ и всякого целого числа n определено кратное na элемента a (в мультипликативной записи вместо "кратное" мы бы сказали "n-я степень" и записали бы это в форме a^n). Все аксиомы $\mathbb{Z}$-модуля выполняются автоматически; например, свойство $(m+n)a = ma + na$ является аддитивной записью доказанного ранее свойства степеней элемента в любой группе $a^{m+n} = a^m a^n$.

4. Пусть $M_1, \ldots, M_n$ – левые Λ-модули. Относительно сложения они являются группами, и определена их (внешняя) прямая сумма M, которую в аддитивной записи мы будем записывать не $M_1 \times \cdots \times M_n$, а $M_1 \oplus \ldots \oplus M_n$. Напомним, что элементы прямой суммы $M = M_1 \oplus \ldots \oplus M_n$ – это элементы $(a_1, \ldots, a_n)$ декартова произведения множеств $M_1, \ldots, M_n$, так что

$$M = M_1 \oplus \ldots \oplus M_n = \{(a_1, \ldots, a_n) \,|\, a_1 \in M_1, \ldots, a_n \in M_n\},$$

а сложение в этом декартовом произведении осуществляется покомпонентно. Превратим M в Λ-модуль, положив

$$\lambda(a_1, \ldots, a_n) = (\lambda a_1, \ldots, \lambda a_n) \quad \text{для любых } \lambda \in \Lambda,\ a_1 \in M_1,\ \ldots,\ a_n \in M_n.$$

Все аксиомы Λ-модуля выполняются, потому что они выполняются покомпонентно (мы опускаем проверку этого ввиду ее полной тривиальности). Так построенный Λ-модуль называется (внешней) прямой суммой Λ-модулей $M_1, \ldots, M_n$ и, как мы уже сказали, обозначается $M_1 \oplus \ldots \oplus M_n$.

Особо важен случай, когда все модули M_i совпадают с кольцом Λ, рассматриваемым как левый Λ-модуль. Прямая сумма $\Lambda \oplus \ldots \oplus \Lambda$ n экземпляров модуля Λ обозначается Λ^n; этот модуль называется свободным Λ-модулем ранга n. Оправдание для такого названия будет дано немного ниже. Отметим, что элементами Λ^n являются строчки $(\lambda_1, \ldots, \lambda_n)$ элементов $\lambda_i \in \Lambda$, а не столбцы, как это было у нас раньше (например, через k^n, где k – поле, мы обозначали пространство столбцов). С той точки зрения, что Λ^n – прямая сумма, "горизонтальная"запись элементов Λ^n более удобна, чем вертикальная.

4°. **Подмодули.** Пусть M – Λ-модуль. Подмножество N множества M называется подмодулем M, если оно является Λ-модулем относительно тех же операций сложения и умножения на элементы из Λ. Точнее говоря, N является подмодулем M, если выполняются условия: $0 \in N$; если $a, b \in N$, то $a + b \in N$; если $a \in N$, то $\lambda a \in N$ для любого $\lambda \in \Lambda$. Заметим, что сам модуль M и подмножество модуля M, состоящее из единственного элемента 0, являются подмодулями модуля M.

Как и в случае векторных пространств, для доказательства того, что подмножество является подмодулем, нам будет полезно пользоваться следующим простым критерием.

Предложение 1. *Пусть M – Λ-модуль, и пусть N – его непустое подмножество. Следующие условия равносильны.*

(1) *N – подмодуль M.*
(2) *Для любых $a, b \in N$ и любого $\lambda \in \Lambda$ элемент $\lambda a + b$ принадлежит N.*

Доказательство. (1) $\Rightarrow$ (2) – очевидно. (2) $\Rightarrow$ (1). Пусть $a \in N$; тогда по (2) элемент $0 = (-1)a + a$ принадлежит N. Далее, опять по (2) элемент $\lambda a = \lambda a + 0$ принадлежит U. Наконец, полагая в (2) $\lambda = 1$, получаем, что $a + b = 1 \cdot a + b$ принадлежит N для любых $a, b \in N$.

Предложение 2. *Пусть Λ – ассоциативное кольцо с 1. Подмножество I кольца Λ является подмодулем Λ, рассматриваемого как левый Λ-модуль, тогда и только тогда, когда I – левый идеал Λ.*

Доказательство. По определению левого идеала, подмножество I является левым идеалом кольца Λ тогда и только тогда, когда выполняются условия: $0 \in I$; если $a, b \in I$, то $a + b \in I$; если $a \in I$, то $\lambda a \in I$ для любого $\lambda \in \Lambda$. Но это в точности означает, что I – подмодуль ${}_\Lambda\Lambda$.

Предложение 3. *Пусть M – Λ-модуль, и пусть $a_1, \ldots, a_n \in M$. Тогда множество N всех элементов вида $\lambda_1 a_1 + \ldots + \lambda_n a_n$, где $\lambda_1, \ldots, \lambda_n \in \Lambda$, является подмодулем M.*

Доказательство. Пусть $u = \lambda_1 a_1 + \ldots + \lambda_n a_n$, $v = \mu_1 a_1 + \ldots + \mu_n a_n$ – элементы из N (здесь λ_i, μ_j – элементы из Λ), и пусть $\gamma \in \Lambda$. Тогда

$$\gamma u + v = \gamma(\lambda_1 a_1 + \ldots + \lambda_n a_n) + \mu_1 a_1 + \ldots + \mu_n a_n = (\gamma\lambda_1 + \mu_1)a_1 + \ldots + (\gamma\lambda_n + \mu_n)a_n \in N.$$

По предложению 1 отсюда следует, что N – подмодуль M.

Построенный в предыдущем предложении подмодуль N модуля M называется подмодулем Λ-модуля M, порожденным элементами $a_1, \ldots, a_n \in M$ и обозначается $\langle a_1, \ldots, a_n \rangle$. Таким образом,

$$\langle a_1, \ldots, a_n \rangle = \{\lambda_1 a_1 + \ldots + \lambda_n a_n \,|\, \lambda_1, \ldots, \lambda_n \in \Lambda\}.$$

Если $M = \langle a_1, \ldots, a_n \rangle$, то мы говорим, что элементы $a_1, \ldots, a_n$ порождают M, или что они составляют порождающую систему модуля M. Если в модуле M найдется конечная порождающая система, то модуль M называется конечно порожденным. Заметим еще, что подмодуль, порожденный пустым множеством элементов, считается равным нулевому подмодулю модуля M.

Следующее утверждение – совершенно очевидная переформулировка определения, но его очень часто бывает удобно применять.

Предложение 4. *Пусть M – Λ-модуль, а N – его подмодуль. Если элементы $a_1, \ldots, a_n \in M$ принадлежат подмодулю N, то N содержит подмодуль $\langle a_1, \ldots, a_n \rangle$ модуля M, порожденный этими элементами.*

5°. **Гомоморфизмы модулей.** Пусть M, N – два Λ-модуля; отображение $\varphi : M \to N$ называется гомоморфизмом Λ-модулей, или Λ-гомоморфизмом, если оно является гомоморфизмом групп (относительно сложения) и если для любого $a \in M$ и любого $\lambda \in \Lambda$ выполняется соотношение $\varphi(\lambda a) = \lambda\varphi(a)$. Иными словами, φ – гомоморфизм модулей, если $\varphi(a + b) = \varphi(a) + \varphi(b)$, $\varphi(\lambda a) = \lambda\varphi(a)$ для любых $a, b \in M$ и любого $\lambda \in \Lambda$. Эти два условия можно обычным образом свести к одному: отображение $\varphi : M \to N$ является гомоморфизмом Λ-модулей, если $\varphi(\lambda a + b) = \lambda\varphi(a) + \varphi(b)$ для любых $a, b \in M$ и любого $\lambda \in \Lambda$.

Поскольку гомоморфизм модулей является частным случаем гомоморфизма групп, для него определены ядро и образ. Напомним, что ядром гомоморфизма $\varphi : M \to N$ называется множество $\operatorname{Ker}\varphi$ всех элементов $a \in M$, таких что $\varphi(a) = 0$, а образом $\operatorname{Im}\varphi$ – множество всех тех элементов $b \in N$, для которых существует элемент $a \in M$, такой что $\varphi(a) = b$.

Предложение 5. *Пусть $\varphi : M \to N$ – гомоморфизм Λ-модулей. Тогда $\operatorname{Ker}\varphi$ – подмодуль M, а $\operatorname{Im}\varphi$ – подмодуль N.*

Доказательство. Если $a_1, a_2 \in \operatorname{Ker}\varphi$, $\lambda \in \Lambda$, то $\varphi(a_1) = \varphi(a_2) = 0$, и потому $\varphi(\lambda a_1 + a_2) = \lambda\varphi(a_1) + \varphi(a_2) = 0$, т.е. $\lambda a_1 + a_2 \in \operatorname{Ker}\varphi$. По предлжению 1 это значит, что $\operatorname{Ker}\varphi$ – подмодуль M. Если $b_1, b_2 \in \operatorname{Im}\varphi$, то существуют элементы $a_1, a_2 \in M$, такие что $\varphi(a_1) = b_1$, $\varphi(a_2) = b_2$, и для любого $\lambda \in \Lambda$ получаем, что $\lambda b_1 + b_2 = \lambda\varphi(a_1) + \varphi(a_2) = \varphi(\lambda a_1 + a_2) \in \operatorname{Im}\varphi$. Опять по предложению 1 заключаем, что $\operatorname{Im}\varphi$ – подмодуль N.

Для гомоморфизмов модулей сохраняется терминология, которая использовалась для гомоморфизмов групп. В частности, изоморфизмом Λ-модулей называется гомоморфизм Λ-модулей $\varphi : M \to N$, у которого ядро равно 0, а образ – всему модулю N. Иными словами, изоморфизм Λ-модулей – это биективный Λ-гомоморфизм. Два Λ-модуля M, N называются изоморфными, если существует Λ-изоморфизм $\varphi : M \to N$.

6°. **Фактормодуль. Теорема о гомоморфизме.** Пусть M – Λ-модуль, а N – его подмодуль. В частности, N является подгруппой (аддитивно записанной) группы M, и поэтому определена факторгруппа M/N. Напомним, что элементами факторгруппы являются классы смежности $a + N$ группы M по подгруппе N ($a \in M$). Определим на M/N действие операторов из кольца Λ следующим образом: для смежного класса $a + N \in M/N$ и элемента $\lambda \in \Lambda$ положим $\lambda(a + N) = \lambda a + N$. Это определение, которое на первый взгляд кажется зависящим от выбора представителя a в классе смежности $a + N$, на самом деле корректно: если $a_1 + N = a + N$, то разность $a_1 - a$ принадлежит N, и, поскольку N – подмодуль M, а не просто подгруппа, $\lambda(a_1 - a) \in N$. Таким образом, $\lambda a_1 + N = \lambda a + \lambda(a_1 - a) + N \subseteq \lambda a + N$, и аналогично доказывается обратное включение.

Взглянем на наше определение с другой точки зрения. Пусть $\pi : M \to M/N$ – канонический эпиморфизм группы на факторгруппу (напомним его определение: $\pi(a) = a + N$). Тогда для любого $a \in M$ мы получим, что $\pi(\lambda a) = \lambda a + N = \lambda(a + N) = \lambda\pi(a)$. На самом деле наше определение действия операторов из Λ на M/N является единственно возможным определением, при котором действие оператора перестановочно с каноническим эпиморфизмом π. Пользуясь этой перестановочностью, легко доказать, что для определенного нами действия Λ на M/N выполнены все аксиомы Λ-модуля. Докажем, например, что выполняется аксиома 7. Если $\bar{a} \in M/N$, то, поскольку отображение π сюръективно, найдется элемент $a \in M$, такой что $\pi(a) = \bar{a}$; пользуясь теперь перестановочностью π и действия операторов из Λ, а также тем, что для модуля M аксиома 7 выполняется, получаем для любых $\lambda, \mu \in \Lambda$:

$$(\lambda\mu)\bar{a} = (\lambda\mu)\pi(a) = \pi((\lambda\mu)a) = \pi(\lambda(\mu a)) = \lambda\pi(\mu a) = \lambda(\mu\pi(a)) = \lambda(\mu\bar{a}).$$

Выполнение остальных аксиом доказывается аналогично. Построенный Λ-модуль M/N называется фактормодулем Λ-модуля M по подмодулю N.

Теперь, когда мы знаем, что M/N – это Λ-модуль, мы можем утверждение о прерстановочности π и действия операторов из Λ сформулировать более удобным образом: канонический эпиморфизм $\pi : M \to M/N$ является гомоморфизмом Λ-модулей.

Как мы помним, в теории групп очень важную роль играет теорема о гомоморфизме. Ее аналогом в теории модулей является следующая теорема о гомоморфизме для модулей.

Теорема 1. *Пусть $\varphi : M \to N$ – гомоморфизм Λ-модулей. Тогда модули $M/\operatorname{Ker}\varphi$ и $\operatorname{Im}\varphi$ изоморфны.*

Доказательство. Обозначим через H ядро гомоморфизма φ, а через π – канонический эпиморфизм M на M/H. Напомним, как доказывалась теорема о гомоморфизме для групп. Мы там показали, что существует единственное отображение $\psi : M/H \to N$, такое что $\varphi(a) = \psi(\pi(a))$ для любого элемента $a \in A$, и затем показали, что это отображение является изоморфизмом группы M/H на $\operatorname{Im}\varphi$; поэтому все, что нам остается сделать, это показать, что ψ является не только гомоморфизмом групп, но и гомоморфизмом Λ-модулей. Но это делается автоматически. Пусть $\bar{a} \in M/H$, $\lambda \in \Lambda$; поскольку π – эпиморфизм, существует

такой элемент $a \in M$, что $\pi(a) = \bar{a}$. Теперь, пользуясь тем, что φ и π – гомоморфизмы Λ-модулей, получаем:

$$\psi(\lambda\bar{a}) = \psi(\lambda\pi(a)) = \psi(\pi(\lambda a)) = \varphi(\lambda a) = \lambda\varphi(a) = \lambda\psi(\pi(a)) = \lambda\psi(\bar{a}).$$

7°. **Циклические модули.** Как и в теории групп, одним из первых применений теоремы о гомоморфизме будет теорема о строении циклических модулей. Модуль M называется циклическим, если в нем есть порождающая система, состоящая из единственного элемента. Нулевой модуль тоже является циклическим: хотя он порождается уже пустым множеством, он может быть порожден и своим единственным элементом 0.

Теорема 2. *Пусть Λ – ассоциативное кольцо с 1. Для всякого левого идеала I кольца Λ фактормодуль Λ/I является циклическим Λ-модулем. Обратно, для всякого циклического Λ-модуля M существует левый идеал I кольца Λ, такой что Λ-модуль M изоморфен фактормодулю Λ/I.*

Доказательство. Фактормодуль Λ/I порождается смежным классом $1 + I$, так как всякий его элемент $\lambda+I$ может быть записан в виде $\lambda(1+I)$ ($\lambda \in \Lambda$). Обратно, пусть M – циклический Λ-модуль, порожденный элементом $a \in M$. Отображение $\varphi : \Lambda \to M$, определенное формулой $\varphi(\lambda) = \lambda a$ для любого $\lambda \in \Lambda$, является гомоморфизмом Λ-модулей, так как для любых $\lambda, \mu, \gamma \in \Lambda$ выполняется равенство

$$\varphi(\gamma\lambda + \mu) = (\gamma\lambda + \mu)a = \gamma(\lambda a) + \mu a = \gamma\varphi(\lambda) + \varphi(\mu).$$

Ядро I этого гомоморфизма является подмодулем Λ, рассматриваемого как левый Λ-модуль, а мы видели, что все такие подмодули являются идеалами Λ. Образ же гомоморфизма φ является подмодулем M, содержащим элемент $a = \varphi(1)$, порождающий модуль M, и потому по предложению 4 он совпадает с M. По теореме о гомоморфизме для модулей Λ-модуль $M = \operatorname{Im}\varphi$ изоморфен фактормодулю $\Lambda/\operatorname{Ker}\varphi = \Lambda/I$.

8°. **Разложение модуля в прямую сумму подмодулей.** В заключение этого вводного параграфа еще раз поговорим о прямых суммах модулей. Выше мы определили внешнюю прямую сумму модулей. Пусть теперь M – Λ-модуль, а $M_1, \ldots, M_n$ – его подмодули. Мы говорим, что модуль M разложен в прямую сумму своих подмодулей $M_1, \ldots, M_n$, если существует Λ-изоморфизм φ модуля M на внешнюю прямую сумму $M_1 \oplus \ldots \oplus M_n$, такой что

$$\varphi(a_i) = (0, \ldots, a_i, \ldots, 0) \quad \text{для любого } i,\ 1 \le i \le n, \text{ и любого } a_i \in M_i$$

(конечно, элемент a_i в строчке $(0, \ldots, a_i, \ldots, 0)$, фигурирующей в предыдущем соотношении, занимает i-ю позицию). Все, что говорилось о разложении группы в прямую сумму своих подгрупп, сохраняется и для разложения модуля в прямую сумму подмодулей, и даже с некоторыми упрощениями – сложение коммутативно, и поэтому не надо вспоминать о том, что элементы из разных слагаемых перестановочны друг с другом. В частности, справедливо утверждение, которое можно тоже было бы взять за определение разложения модуля в прямую сумму подмодулей.

Предложение 6. *Для того, чтобы Λ-модуль M был прямой суммой своих подмодулей $M_1, \ldots, M_n$, необходимо и достаточно, чтобы всякий элемент $a \in M$ представлялся, и притом единственным образом, в виде $a = a_1 + \ldots + a_n$, где $a_i \in M_i$ для всех i, $1 \le i \le n$.*

Для обозначения того, что модуль M разложен в прямую сумму своих подмодулей $M_1, \ldots, M_n$, мы будем использовать ту же запись, что и для обозначения внешней прямой суммы: $M = M_1 \oplus \ldots \oplus M_n$. Это не приведет к путанице, так как из контекста всегда будет ясно, о чем идет речь; к тому же, эти два понятия очень близки.

§ 2. Свободные модули

Пусть M – Λ-модуль. Система элементов $a_1, \ldots, a_n$ называется базисом модуля M, если всякий элемент $b \in M$ может быть представлен в виде $b = \lambda_1 a_1 + \ldots + \lambda_n a_n$, причем это представление единственно. В отличие от векторных пространств, в случае, когда Λ не является телом, далеко не всякий модуль, даже конечно порожденный, имеет базис. Если в модуле есть хоть один базис, то модуль называется свободным Λ-модулем. Хотелось бы сказать, что модуль, в котором есть базис, состоящий из n элементов, называется свободным модулем ранга n; однако, в общем случае один и тот же модуль может иметь базисы, состоящие из разного числа элементов, и потому понятие ранга свободного модуля некорректно.

Важнейшим свойством свободного модуля является то, что легко строить гомоморфизмы этого модуля в любой другой модуль.

Предложение 1. *Пусть S – свободный Λ-модуль с базисом $a_1, \ldots, a_n$, и пусть M – произвольный Λ-модуль, а $b_1, \ldots, b_n$ – любые элементы из M. Тогда существует, и притом единственный, гомоморфизм Λ-модулей $\varphi : S \to M$, такой что $\varphi(a_i) = b_i$ для всех i, $1 \leq i \leq n$.*

Доказательство. Единственность такого гомоморфизма очевидна: поскольку любой элемент $a \in S$ представляется в виде $a = \lambda_1 a_1 + \ldots + \lambda_n a_n$, то элемент $\varphi(a)$ обязан быть равным $\lambda_1 \varphi(a_1) + \ldots + \lambda_n \varphi(a_n) = \lambda_1 b_1 + \ldots + \lambda_n b_n$. Осталось доказать существование φ. Для любого $a \in S$ существуют единственные элементы $\lambda_1, \ldots, \lambda_n \in \Lambda$, такие что $a = \lambda_1 a_1 + \ldots + \lambda_n a_n$; положим $\varphi(a) = \lambda_1 b_1 + \ldots + \lambda_n b_n$. Покажем, что так определенное отображение $\varphi : S \to M$ является гомоморфизмом Λ-модулей. Пусть $a' = \lambda'_1 a_1 + \ldots + \lambda'_n a_n$ – еще один элемент из S, и пусть λ – любой элемент из Λ. Тогда $\lambda a + a' = ((\lambda\lambda_1 + \lambda'_1)a_1 + \ldots + (\lambda\lambda_n + \lambda'_n)a_n)$, и по определению отображения φ мы имеем:

$$\varphi(\lambda a + a') = (\lambda\lambda_1 + \lambda'_1)b_1 + \ldots + (\lambda\lambda_n + \lambda'_n)b_n =$$
$$= \lambda(\lambda_1 b_1 + \ldots + \lambda_n b_n) + (\lambda'_1 b_1 + \ldots + \lambda'_n b_n) = \lambda\varphi(a) + \varphi(a'),$$

а это и значит, что отображение φ – гомоморфизм Λ-модулей.

Предложение 2. *Для любого кольца Λ модуль Λ^n является свободным Λ-модулем, и в нем есть базис, состоящий из n элементов. Всякий свободный Λ-модуль, в котором есть базис, состоящий из n элементов, изоморфен Λ^n.*

Доказательство. Напомним, что элементы из Λ_n – это строки $(\lambda_1, \ldots, \lambda_n)$ длины n с компонентами из Λ. Обозначим через e_i строку $(0, \ldots, 1, \ldots, 0) \in \Lambda^n$, у которой на i-м месте стоит единица 1 кольца Λ, а остальные компоненты равны 0. Очевидно, что для для любых $\lambda_1, \ldots, \lambda_n \in \Lambda$ выполняется равенство

$$\lambda_1 e_1 + \ldots + \lambda_n e_n = (\lambda_1, \ldots, \lambda_n),$$

которое показывает, во-первых, что всякий элемент $(\lambda_1, \ldots, \lambda_n) \in \Lambda_n$ представим в виде $\lambda_1 e_1 + \ldots + \lambda_n e_n$ с коэффициентами $\lambda_i \in \Lambda$, а во-вторых, что такое представление единственно: если

$$(\lambda_1, \ldots, \lambda_n) = \mu_1 e_1 + \ldots + \mu_n e_n \qquad (\lambda_1, \ldots, \lambda_n \in \Lambda)$$

– другое такое представление, то

$$(\lambda_1, \ldots, \lambda_n) = \mu_1 e_1 + \ldots + \mu_n e_n = (\mu_1, \ldots, \mu_n),$$

откуда следует, что $\mu_1 = \lambda_1$, ... , $\mu_n = \lambda_n$. Таким образом, $e_1, \ldots, e_n$ – базис Λ_n.

Пусть теперь S – свободный Λ-модуль с базисом $a_1, \ldots, a_n$. По основному свойству свободных модулей, существует Λ-гомоморфизм $\varphi : \Lambda^n \to S$, такой что

$\varphi(e_i) = a_i$ для любого i, $1 \leq i \leq n$. Образ этого гомоморфизма содержит порождающую систему $a_1, \ldots, a_n$ модуля S и потому совпадает с S; таким образом, φ – эпиморфизм. Если $(\lambda_1, \ldots, \lambda_n) \in \operatorname{Ker} \varphi$, то

$$0 \cdot a_1 + \ldots + 0 \cdot a_n = 0 = \varphi((\lambda_1, \ldots, \lambda_n)) = \varphi(\lambda_1 e_1 + \ldots + \lambda_n e_n) = \lambda_1 a_1 + \ldots + \lambda_n a_n;$$

из единственности разложения элемента свободного модуля S по базису $a_1, \ldots, a_n$ тогда следует, что $\lambda_1 = \ldots = \lambda_n = 0$, т.е. $(\lambda_1, \ldots, \lambda_n) = 0$. Итак, ядро гомоморфизма φ состоит только из 0, а это значит, что φ – мономорфизм. Таким образом, гомоморфизм φ является эпиморфизмом и мономорфизмом, а значит, изоморфизмом.

§ 3. Базисы свободного модуля

Если $u_1, \ldots, u_n$ – система образующих некоторого Λ-модуля M (в частности, если модуль свободен, то это может быть базис), то всякий элемент $a \in M$ может быть представлен в виде $a = c_1 u_1 + \ldots + c_n u_n$, где $c_1, \ldots, c_n \in \Lambda$. Аналогично, если у нас есть несколько элементов $a_1, \ldots, a_m \in \Lambda$, то существуют такие элементы $c_{ij} \in \Lambda$, что для каждого i, $1 \leq i \leq m$, элемент a_i равен $c_{i1} u_1 + \ldots + c_{in} u_n$. Обозначая матрицу с компонентами c_{ij} через C, мы можем записать это в виде одного матричного равенства

$$\begin{pmatrix} a_1 \\ \vdots \\ a_m \end{pmatrix} = \begin{pmatrix} c_{11} & \ldots & c_{1n} \\ \vdots & \ddots & \vdots \\ c_{m1} & \ldots & c_{mn} \end{pmatrix} \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix} = C \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix}.$$

Таким образом, для любой порождающей системы $u_1, \ldots, u_n$ Λ-модуля M и любых элементов $a_1, \ldots, a_m \in \Lambda$ найдется матрица $C \in \Lambda^{m \times n}$, такая что

$$(a_1, \ldots, a_m)^{\intercal} = C(u_1, \ldots, u_n)^{\intercal}.$$

Теорема 1. *Пусть M – Λ-модуль, и пусть $u_1, \ldots, u_n$; $v_1, \ldots, v_m$ – два набора элементов из M, связанных соотношением $(v_1, \ldots, v_m)^{\intercal} = C(u_1, \ldots, u_n)^{\intercal}$, где C – матрица из $\Lambda^{m \times n}$.*

(1) *Если элементы $u_1, \ldots, u_n$ порождают M, то для того, чтобы элементы $v_1, \ldots, v_m$ порождали M достаточно, чтобы существовала такая матрица $D \in \Lambda^{n \times m}$, что $DC = E_n$.*

(2) *Если $u_1, \ldots, u_n$ – базис M, то для того, чтобы элементы $v_1, \ldots, v_m$ тоже составляли базис M, необходимо и достаточно, чтобы существовала такая матрица $D \in \Lambda^{n \times m}$, что $DC = E_n$, $CD = E_m$.*

Доказательство. (1) В условиях утверждения мы имеем:

$$\begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix} = E_n \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix} = DC \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix} = D \begin{pmatrix} v_1 \\ \vdots \\ v_m \end{pmatrix};$$

поэтому элементы $u_1, \ldots, u_n$, порождающие M, принадлежат подмодулю модуля M, порожденному $v_1, \ldots, v_m$. Следовательно, подмодуль модуля M, порожденный $v_1, \ldots, v_m$, совпадает со всем модулем M.

(2) *Необходимость.* Пусть $v_1, \ldots, v_m$ – базис M; элементы $v_1, \ldots, v_m$ порождают M, и потому существует такая матрица $D \in \Lambda^{n \times m}$, что

$$\begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix} = D \begin{pmatrix} v_1 \\ \vdots \\ v_m \end{pmatrix}.$$

Мы имеем:

$$\begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix} = D \begin{pmatrix} v_1 \\ \vdots \\ v_m \end{pmatrix} = D\Big(C \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix}\Big) = (DC) \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix};$$

поэтому для любого i, $1 \le i \le n$, будет

$$0 \cdot u_1 + \ldots + 1 \cdot u_i + \ldots + 0 \cdot u_n = u_i = (DC)_{i1}u_1 + \ldots + (DC)_{ii}u_i + \cdots + (DC)_{in}u_n.$$

Но по определению базиса каждый элемент из M лишь единственным образом выражается через базис, и потому мы получаем, что $(DC)_{ii} = 1$, $(DC)_{ij} = 0$ для $j \ne i$, $1 \le j \le n$. Эти соотношения равносильны тому, что $DC = E_n$. Точно так же показываем, что $CD = E_m$.

Достаточность. Пусть существует такая матрица D, что $CD = E_m$, $DC = E_n$. Поскольку базис $u_1, \ldots, u_n$ порождает модуль M, из (1) следует, что элементы $v_1, \ldots, v_m$ порождают M. Осталось показать, что любые два разложения одного и того же элемента $a \in M$ в линейную комбинацию элементов $v_1, \ldots, v_m$ совпадают. Пусть $a = \lambda_1 v_1 + \ldots + \lambda_m v_m = \mu_1 v_1 + \ldots + \mu_m v_m$. Тогда

$$a = (\lambda_1, \ldots, \lambda_m) \begin{pmatrix} v_1 \\ \vdots \\ v_m \end{pmatrix} = (\lambda_1, \ldots, \lambda_m)\Big(C \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix}\Big) = \big((\lambda_1, \ldots, \lambda_m)C\big) \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix}$$

и точно так же $a = \big((\mu_1, \ldots, \mu_m)C\big)(u_1, \ldots, u_n)^{\mathtt{T}}$. Но по условию $u_1, \ldots, u_n$ – базис M, поэтому разложение элемента $a \in M$ по этому базису единственно. Следовательно, $(\lambda_1, \ldots, \lambda_m)C = (\mu_1, \ldots, \mu_m)C$. Домножая полученное равенство на D, получаем требуемое равенство:

$$(\lambda_1, \ldots, \lambda_m) = (\lambda_1, \ldots, \lambda_m)E_m = (\lambda_1, \ldots, \lambda_m)(CD) = ((\lambda_1, \ldots, \lambda_m)C)D =$$
$$= ((\mu_1, \ldots, \mu_m)C)D = (\mu_1, \ldots, \mu_m)(CD) = (\mu_1, \ldots, \mu_m)E_m = (\mu_1, \ldots, \mu_m).$$

Следствие. *Если Λ – область целостности, и в Λ-модуле S есть базис, состоящий из n элементов, то всякий базис S состоит из n элементов.*

Доказательство. Пусть $u_1, \ldots, u_n$, $v_1, \ldots, v_m$ – два базиса модуля S; как мы только что показали, тогда существует матрица $C \in \Lambda^{m \times n}$, такая что $(v_1, \ldots, v_m)^{\mathtt{T}} = C(u_1, \ldots, u_n)^{\mathtt{T}}$, причем для матрицы C существует обратная ей матрица $D \in \Lambda^{n \times m}$. Но поскольку кольцо Λ – область целостности, оно может быть вложено в поле отношений K, и матрица D, обратная к матрице C над Λ, будет, конечно, обратной к C и над K. Но над полем только квадратные матрицы обратимы; следовательно, C – квадратная матрица, и $m = n$.

Доказанное следствие показывает, что число элементов в базисе свободного модуля S над областью целостности зависит только от модуля, а не от конкретно выбранного базиса; оно называется рангом свободного модуля S и обозначается $\operatorname{rank} S$. Еще раз подчеркнем, что понятие ранга свободного модуля является корректным понятием только для модулей над некоторыми кольцами, в число которых, как мы только что показали, входят области целостности.

§ 4. Периодические модули над областью главных идеалов

1°. **Модуль кручения.** Мы займемся теперь систематиическим изучением конечно порожденных модулей над областями главных идеалов. Но в этом пункте мы еще будем работать в немного более общей ситуации.

Пусть Λ – область целостности, и пусть M – левый Λ-модуль. Периодом элемента $a \in M$ называется любой элемент $\lambda \in \Lambda$, такой что $\lambda a = 0$. Нулевой элемент кольца Λ является периодом любого элемента. Элемент $a \in M$ называется периодическим, если у него есть хоть один период, отличный от 0, т.е. если

существует такой элемент $\lambda \neq 0$ из кольца Λ, что $\lambda a = 0$. В любом модуле элемент 0 является периодическим, так как, например, $1_\Lambda \cdot 0 = 0$; если в модуле M нет других периодических элементов, кроме 0, то модуль M называется модулем без кручения.

Предложение 1. *Пусть Λ – область целостности, и пусть M – левый Λ-модуль. Множество всех периодических элементов модуля M является подмодулем модуля A, а фактормодуль M по этому подмодулю уже является модулем без кручения.*

Доказательство. Пусть $X \subseteq M$ – множество всех периодических элементов модуля M. Пусть $x, y \in X$; тогда существуют такие элементы $\lambda, \mu \in \Lambda$, что $\lambda \neq 0$, $\mu \neq 0$, $\lambda x = 0$, $\mu y = 0$. Поскольку Λ – область целостности, $\lambda\mu \neq 0$. Пользуясь аксиомами модуля и области целостности (в частности, тем, что Λ – коммутативное кольцо), легко получаем, что для любого $\gamma \in \Lambda$

$$\lambda\mu(\gamma x + y) = \lambda\mu\gamma x + \lambda\mu y = (\mu\gamma)(\lambda x) + \lambda(\mu y) = \mu\gamma \cdot 0 + \lambda \cdot 0 = 0,$$

и потому $\gamma x + y$ принадлежит множеству X периодических элементов модуля M; это и доказывает, что X – подмодуль M.

Пусть теперь $\bar{a}$ – периодический элемент фактормодуля M/X. Элементы фактормодуля являются смежными классами по X; пусть $a \in M$ – какой-то представитель смежного класса $\bar{a}$, так что $\bar{a} = a + X$. Поскольку $\bar{a}$ – периодический элемент фактормодуля M/X, существует ненулевой элемент $\lambda \in \Lambda$, такой что $\lambda a + X = \lambda\bar{a} = 0_{M/X} = 0 + X = X$, так что λa принадлежит множеству X периодических элементов модуля M. Поэтому существует такой элемент $\mu \in \Lambda$, $\mu \neq 0$, что $\mu\lambda a = 0$. Но в области целостности Λ произведение $\mu\lambda$ двух ненулевых элементов отлично от 0, и, значит, a – периодический элемент, т.е. $a \in X$. Мы получили, таким образом, что $\bar{a} = a + X = X = 0_{M/X}$. Итак, в M/X нет периодических элементов, кроме $0_{M/X}$.

Множество всех периодических элементов модуля M обозначается через $T(M)$ и называется модулем кручения модуля M. Мы уже отметили выше, что если $T(M) = 0$, то модуль M называется модулем без кручения.

Аналогично периоду элемента из M, элемент $\lambda \in \Lambda$ называется периодом всего модуля M, если $\lambda a = 0$ для всех элементов $a \in M$. Нулевой элемент кольца Λ является периодом любого модуля. Λ-модуль M называется периодическим, если у него есть хоть один ненулевой период, т.е. если существует такой элемент $\lambda \in \Lambda$, $\lambda \neq 0$, что $\lambda a = 0$ для всех элементов $a \in M$. Конечно, если модуль M периодический, то все его элементы периодические, т.е. $T(M) = M$. Обратное, однако, не верно: если $T(M) = M$, то для каждого элемента $a \in M$ существует свой период λ_a, но периода, общего для всех элементов модуля A, может не быть. Примером является $\mathbb{Z}$-модуль $\mathbb{Q}^+/\mathbb{Z}^+$: класс смежности $\dfrac{m}{n} + \mathbb{Z}$ аннулируется элементом $n \in \mathbb{Z}$, однако целого числа, умножение на которое делало бы целыми все рациональные числа, не существует.

Ясно, что множество всех периодов любого элемента Λ-модуля и множество периодов всего Λ-модуля являются идеалами Λ. В случае, если Λ – область главных идеалов, этот идеал порождается одним элементом, который естественно назвать наименьшим периодом элемента или модуля. Наименьший период определен однозначно с точностью до ассоциированности.

В заключение этого пункта отметим некоторые простые свойства модулей кручения.

Предложение 2. *Свободный модуль над областью целостности Λ является модулем без кручения. Всякий подмодуль модуля без кручения – модуль без кручения. Если M – периодический Λ-модуль, то $T(M) = M$. Если M_1, M_2 – два*

Λ-*модуля, то* $T(M_1 \oplus M_2) = T(M_1) \oplus T(M_2)$. *Если при этом* M_1 – *периодический модуль, а* M_2 – *модуль без кручения, то* $T(M_1 \oplus M_2) = M_1$.

Доказательство. Если S – свободный Λ-модуль с базисом $a_1, \ldots, a_n$, и если $a = \lambda_1 a_1 + \ldots + \lambda_n a_n$ – периодический элемент, то для некоторого $\lambda \in \Lambda$, $\lambda \neq 0$, мы получим

$$0 \cdot a_1 + \ldots + 0 \cdot a_n = 0 = \lambda a = \lambda(\lambda_1 a_1 + \ldots + \lambda_n a_n) = \lambda\lambda_1 a_1 + \ldots + \lambda\lambda_n a_n,$$

откуда из-за единственности разложения элемента свободного модуля по базису получаем: $\lambda\lambda_1 = \ldots = \lambda\lambda_n = 0$. Но Λ – область целостности, а $\lambda \neq 0$, поэтому из предыдущих равенств следует, что $\lambda_1 = \ldots = \lambda_n = 0$, т.е. $a = \lambda_1 a_1 + \ldots + \lambda_n a_n = 0$. Первое утверждение предложения доказано. Доказательства остальных мы опускаем ввиду их тривиальности.

2°. **Разложение периодического модуля над областью главных идеалов в прямую сумму.**

Теорема 1. *Пусть* Λ – *область главных идеалов, и пусть* M – *периодический* Λ-*модуль, один из преиодов которого* λ *разложен в произведение* $\lambda = \lambda_1 \ldots \lambda_n$ *попарно взаимно простых сомножителей. Тогда модуль* M *раскладывается в прямую сумму подмодулей* $M = M_1 \oplus \ldots \oplus M_n$, *таких что для любого* s, $1 \leq s \leq n$, s-*й сомножитель* λ_s *периода* λ *является периодом модуля* M_s.

Доказательство. Напомним, что в любой области целостности выполняется китайская теорема об остатках; поэтому для каждого s, $1 \leq s \leq n$, существует такой элемент $\pi_s \in \Lambda$, что

$$\pi_s \equiv 1 \pmod{\lambda_s}, \qquad \pi_s \equiv 0 \pmod{\lambda_i} \text{ при } i \neq s.$$

Из этого определения сразу следует, что каждый из элементов

$$(\pi_1 + \ldots + \pi_n) - 1, \quad \pi_s^2 - \pi_s, \quad \pi_s\pi_t, \quad \lambda_s\pi_s \quad (1 \leq s, t \leq n,\ s \neq t)$$

делится на каждый из попарно взаимно простых элементов $\lambda_1, \ldots, \lambda_n$, а потому и на их произведение $\lambda_1 \ldots \lambda_n = \lambda$. Поскольку λ является периодом модуля M, умножение на любой из перечисленных выше элементов превращает в 0 любой элемент $a \in M$; таким образом, для любого $a \in M$ и любых $s \neq t$ $(1 \leq s, t \leq n)$ выполняются соотношения

$$\pi_1 a + \ldots + \pi_n a = (\pi_1 + \ldots + \pi_n)a = a, \quad \pi_s^2 a = \pi_s a, \quad \pi_s\pi_t a = 0, \quad \lambda_s\pi_s a = 0.$$

Положим $M_s = \pi_s M = \{\pi_s a \,|\, a \in M\}$. Для любых $a_s, b_s \in M_s$ существуют такие элементы $a, b \in M$, что $a_s = \pi_s a$, $b_s = \pi_s b$, и тогда для любого $\gamma \in \Lambda$ элемент $\gamma a_s + b_s = \gamma\pi_s a + \pi_s b = \pi_s(\gamma a + b)$ принадлежит M_s; это означает, что M_s – подмодуль Λ-модуля M. Далее, пусть $a_s = \pi_s a \in M_s$; тогда

$$\pi_s a_s = \pi_s^2 a = \pi_s a = a_s, \qquad \pi_t a_s = \pi_t\pi_s a = 0 \ \ (t \neq s), \qquad \lambda_s a_s = \lambda_s\pi_s a = 0.$$

Последнее из этих равенств показывает, что λ_s является периодом модуля M_s.

Остается доказать, что $M = M_1 \oplus \ldots \oplus M_n$. Если $a \in M$, то $a = \pi_1 a + \ldots + \pi_n a$, и каждое слагаемое $\pi_s a$ в этой сумме принадлежит подмодулю $\pi_s M = M_s$ модуля M. Если $a = a_1 + \ldots + a_s + \ldots + a_n$, где $a_s \in M_s$ для всех s, то

$$\pi_s a = \pi_s a_1 + \ldots + \pi_s a_s + \ldots + \pi_s a_n = a_s.$$

Таким образом, s-я компонента в разложении $a = a_1 + \ldots + a_s + \ldots + a_n$ обязана равняться $\pi_s a$, и разложение $a = \pi_1 a + \ldots + \pi_n a$ является единственным представлением элемента $a \in M$ в виде суммы элементов из подмодулей $M_1, \ldots, M_n$.

Чаще всего доказанная теорема применяется в случае, когда все сомножители λ_s периода λ являются степенями простых элементов кольца Λ. Модуль, для которого степень некоторого простого элемента кольца является периодом,

называется примарным периодическим модулем. Следующее утверждение непосредственно вытекает из теоремы.

Следствие. *Всякий периодический модуль над областью главных идеалов раскладывается в прямую сумму примарных периодических модулей.*

Доказательство. Пусть Λ – область главных идеалов, и пусть M – периодический Λ-модуль. Его период λ раскладывается в области главных идеалов в произведение $\lambda = \varepsilon\pi_1^{i_1}\dots\pi_n^{i_n}$, где ε – делитель 1, а $\pi_1,\dots,\pi_n$ – попарно не ассоциированные простые элементы кольца Λ. Тогда асоциированное с λ произведение $\pi_1^{i_1}\dots\pi_n^{i_n}$ тоже является периодом M, его сомножители $\pi_s^{i_s}$ попарно взаимно просты, и потому по нашей теореме модуль M раскладывается в прямую сумму модулей M_s, период каждого из которых равен $\pi_s^{i_s}$ $(1 \le s \le n)$.

3°. **Циклические периодические модули.** Пусть Λ – область целостности. Напомним, что Λ-модуль M называется циклическим, если он порождается одним элементом $a \in M$. Пусть I – идеал всех периодов элемента a; тогда I ядро эпиморфизма $\varphi : \Lambda \to M$, определенного формулой $\varphi(\lambda) = \lambda a$, и потому модуль M изоморфен фактормодулю кольца Λ по идеалу периодов I. Если этот идеал периодов отличен от 0, то циклический модуль M периодический, поскольку все элементы $\lambda \in I$ являются, очевидно, периодами не только порождающего элемента a, но и всего модуля M.

Предложение 3. *Всякий периодический циклический модуль над областью главных идеалов раскладывается в прямую сумму примарных циклических модулей.*

Доказательство. Предложение сразу следует из следствия теоремы 1 и следующей простой леммы.

Лемма 1. *Всякое прямое слагаемое циклического модуля над любым кольцом – циклический модуль.*

Доказательство. Пусть $A =< a >$ – циклический модуль над кольцом Λ, и пусть $A = B \oplus C$, где B, C – подмодули A. Элемент a, как и всякий элемент прямой суммы $A = B \oplus C$, представляется в виде суммы $a = b + c$, где $b \in B$, $c \in C$. Пусть b_1 – любой элемент из B. Поскольку модуль A – циклический, существует такой элемент $\gamma \in \Lambda$, что $b_1 = \gamma a$. Но тогда

$$b_1 + 0 = b_1 = \gamma a = \gamma(b + c) = \gamma b + \gamma c$$

– два представления элемента b_1 в виде суммы элементов из модулей B, C; поскольку сумма прямая, эти два представления совпадают, и, в частности, $b_1 = \gamma b$. Таким образом, прямое слагаемое B циклического модуля A порождается единственным элементом b.

§ 5. Теорема об элементарных делителях

1°. **Теорема об элементарных делителях.** Следующая теорема, доказательству которой посвящен этот параграф, играет главную роль в изучении строения конечно порожденных модулей над областями главных идеалов.

Теорема 1. *Пусть Λ – область главных идеалов, и пусть $A \in \Lambda^{m\times n}$ – матрица с компонентами из Λ. Тогда существуют такие матрицы $C \in \Lambda_m^*$, $D \in \Lambda_n^*$, что в матрице $B = CAD \in \Lambda^{m\times n}$ равны 0 все недиагональные элементы (т.е. $B_{ij} = 0$ для всех пар индексов i, j, таких что $i \ne j$).*

Напомним, что для любого кольца R через R^* обозначается группа всех обратимых элементов кольца. Таким образом, матрицы C и D в формулировки

теоремы – это матрицы с компонентами из Λ, для которых существуют обратные матрицы, причем все компоненты этих обратных матриц тоже принадлежат Λ.

Для удобства доказательства введем одно определение. Две матрицы $A, B \in \Lambda^{m\times n}$ назовем эквивалентными, если существуют такие матрицы $C \in \Lambda_m^*$, $D \in \Lambda_n^*$, что $B = CAD$. Из того, что Λ_m^*, Λ_n^* – группы, легко выводится, что введенное отношение действительно является отношением эквивалентности. В этих терминах наша теорема формулируется так: для всякой матрицы $A \in \Lambda^{m\times n}$ существует эквивалентная ей матрица B указанного выше вида. Сразу отметим, что матрица, получающаяся из матрицы A перестановкой строк или столбцов, эквивалентна матрице A, потому что такая перестановка равносильна умножению матрицы A слева или справа на матрицу, в каждой строчке и каждом столбце которой ровно один элемент равен 1, а все остальные элементы матрицы равны 0.

2°. **Основные леммы.** Для матрицы $A \in \Lambda^{m\times n}$ будем обозначать через $\lambda(A)$ элемент $(A)_{11}$, стоящий в левом верхнем углу матрицы A.

Лемма 1. *Если не все элементы первой строки и первого столбца матрицы $A \in \Lambda^{m\times n}$ делятся на $\lambda(A)$, то существует матрица A_1, эквивалентная A и такая, что $\lambda(A)$ делится на $\lambda(A_1)$, но $\lambda(A)$ и $\lambda(A_1)$ не ассоциированы.*

Доказательство. Пусть $\lambda(A) = a$ и пусть на a не делится элемент b, стоящий в первой строке и j-м столбце матрицы A; переставив 2-й и j-й столбцы матрицы A, заменим матрицу A на эквивалентную ей матрицу A', имеющую вид

$$A' = \begin{pmatrix} a & b & * \\ * & * & * \end{pmatrix}$$

(остальные элементы матрицы A', кроме первых двух элементов первой строки, нас сейчас не интересуют).

Поскольку Λ – область главных идеалов, существует наибольший общий делитель d элементов a, b. При этом $d \neq 0$: иначе элемент b, делящийся на $d = 0$, был бы сам равен 0 и потому делился бы на a. Далее, a делится на общий делитель d элементов a, b, но элементы d и a не ассоциированы, потому что b делится на d, но не делится на a.

Как мы знаем из главы I, в области главных идеалов наибольший общий нескольких элементов линейно выражается через них; поэтому существуют такие элементы $x, y \in \Lambda$, что $ax+by = d$. Далее, поскольку a и b делятся на d, существуют такие элементы $a_1, b_1 \in \Lambda$, что $a = a_1 d$, $b = b_1 d$. Подставляя эти выражения в предыдущее равенство, получим, что $d = a_1 dx + b_1 dy$, откуда, сокращая на $d \neq 0$ находим: $a_1 x + b_1 y = 1$. Пусть

$$D = \begin{pmatrix} x & -b_1 & \mathbf{0} \\ y & a_1 & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & E_{n-2} \end{pmatrix} \in \Lambda_n.$$

Матрица D обратима – обратной к ней будет, очевидно, матрица

$$\begin{pmatrix} a_1 & b_1 & \mathbf{0} \\ -y & x & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & E_{n-2} \end{pmatrix} \in \Lambda_n;$$

поэтому матрица

$$A_1 = E_m A' D = \begin{pmatrix} a & b & * \\ * & * & * \end{pmatrix} \begin{pmatrix} x & -b_1 & \mathbf{0} \\ y & a_1 & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & E_{n-2} \end{pmatrix} = \begin{pmatrix} ax+by & * \\ * & * \end{pmatrix} = \begin{pmatrix} d & * \\ * & * \end{pmatrix}$$

эквивалентна матрицам A' и A. При этом $\lambda(A_1) = d$, а мы отметили выше, что d – делитель $a = \lambda(A)$, не ассоциированный с a.

Аналогично лемма доказывается в случае, когда элемент, не делящийся на $\lambda(A)$, есть в первом столбце матрицы A.

Лемма 2. *Для всякой матрицы $A \in \Lambda^{m\times n}$ существует эквивалентная ей матрица A', все элементы первой строки и первого столбца которой делятся на ее левый верхний элемент $\lambda(A')$.*

Доказательство. Строим цепочку матриц по следующему правилу. Полагаем $A_0 = A$; до тех пор, пока не все элементы первой строки и первого столбца матрицы A_i делятся на $\lambda(A_i)$, находим по лемме 1 такую матрицу A_{i+1}, эквивалентную A_i, что $\lambda(A_i)$ делится на $\lambda(A_{i+1})$, но $\lambda(A_i)$ и $\lambda(A_{i+1})$ не ассоциированы. Поскольку в области главных идеалов выполняется условие обрыва цепей делителей, цепочка $\lambda(A_0), \lambda(A_1), \ldots$, в которой каждый следующий элемент делит предыдущий и не ассоциирован с ним, не может быть бесконечной, и потому при некотором n все элементы первой строки и первого столбца матрицы A_n, эквивалентной матрице A, делятся на ее левый верхний элемент $\lambda(A_n)$.

Лемма 3. *Для всякой матрицы $A \in \Lambda^{m\times n}$ существует эквивалентная ей матрица вида*

$$\begin{pmatrix} a & 0 & \ldots & 0 \\ 0 & * & \ldots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & * & \ldots & * \end{pmatrix}.$$

Доказательство. По лемме 2 существует эквивалентная A матрица вида

$$A' = \begin{pmatrix} a & ab_2 & \ldots & ab_n \\ ac_2 & * & \ldots & * \\ \vdots & \vdots & \ddots & \vdots \\ ac_m & * & \ldots & * \end{pmatrix},$$

где $b_2, \ldots, b_n$; $c_2, \ldots, c_m$ – какие-то элементы из Λ. Матрица

$$A'' = \begin{pmatrix} a & ab_2 & \ldots & ab_n \\ ac_2 & * & \ldots & * \\ \vdots & \vdots & \ddots & \vdots \\ ac_m & * & \ldots & * \end{pmatrix} \begin{pmatrix} 1 & -b_2 & \ldots & -b_n \\ 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & 1 \end{pmatrix} = \begin{pmatrix} a & 0 & \ldots & 0 \\ ac_2 & * & \ldots & * \\ \vdots & \vdots & \ddots & \vdots \\ ac_n & * & \ldots & * \end{pmatrix}$$

эквивалентна матрице A', а матрица

$$A''' = \begin{pmatrix} 1 & 0 & \ldots & 0 \\ -c_2 & 1 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ -c_m & 0 & \ldots & 1 \end{pmatrix} \begin{pmatrix} a & 0 & \ldots & 0 \\ ac_2 & * & \ldots & * \\ \vdots & \vdots & \ddots & \vdots \\ ac_m & * & \ldots & * \end{pmatrix} = \begin{pmatrix} a & 0 & \ldots & 0 \\ 0 & * & \ldots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & * & \ldots & * \end{pmatrix}$$

– матрице A''. По транзитивности эквивалентности, A''' – матрица, эквивалентная матрице A. (Неформально говоря, мы сделали следующее: прибавляя первый столбец, умноженный на соответствующие элементы, к остальным столбцам, мы превратили в 0 все элементы первой строки, кроме начального, а затем таким же образом "заработали" нули в первом столбце).

3°. **Доказательство теоремы 1.** Мы доказываем теорему индукцией по тому из чисел m, n, которое не больше другого. Если $m = 1$ или $n = 1$, то утверждение теоремы вытекает уже из леммы 3. Пусть $m, n > 1$ и для матриц из $\Lambda^{(m-1)\times(n-1)}$ все уже доказано. По лемме 3 существует эквивалентная A матрица вида

$$\begin{pmatrix} a & \mathbf{0} \\ \mathbf{0} & A_1 \end{pmatrix}, \qquad A_1 \in \Lambda^{(m-1)\times(n-1)}.$$

По предположению индукции, существуют матрицы $C_1 \in \Lambda^*_{m-1}$, $D_1 \in \Lambda^*_{n-1}$, такие что в матрице $B_1 = C_1 A_1 D_1$ все элементы, не лежащие на диагонали, проходящей через левый верхний элемент этой матрицы, равны 0. Тогда матрица

$$B = \begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{0} & C_1 \end{pmatrix} \begin{pmatrix} a & \mathbf{0} \\ \mathbf{0} & A_1 \end{pmatrix} \begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{0} & D_1 \end{pmatrix} = \begin{pmatrix} a & \mathbf{0} \\ \mathbf{0} & C_1 A_1 D_1 \end{pmatrix} = \begin{pmatrix} a & \mathbf{0} \\ \mathbf{0} & B_1 \end{pmatrix}$$

тоже эквивалентна матрице A, и, очевидно, в ней, как и в матрице B_1, все элементы, не лежащие на диагонали, проходящей через левый верхний элемент этой матрицы, равны 0.

4°. **Замечание об элементарных делителях.** Доказанная нами теорема 1, которую мы назвали теоремой об элементарных делителях, не содержит никакого упоминания об элементарных делителях. На самом деле теоремой об элементарных делителях называется чуть более точное утверждение, легко получаемое из теоремы 1:

Пусть Λ – область главных идеалов, и пусть $A \in \Lambda^{m\times n}$ – матрица с компонентами из Λ. Тогда существуют такие матрицы $C \in \Lambda^*_m$, $D \in \Lambda^*_n$, что

$$CAD = \begin{pmatrix} \varepsilon_1 & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & \varepsilon_2 & \dots & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & \varepsilon_r & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 \end{pmatrix},$$

где $r \geq 0$, а $\varepsilon_1, \varepsilon_2, \dots \varepsilon_r$ – ненулевые элементы из Λ, причем при $1 \leq s < r$ элемент ε_{s+1} делится на ε_s.

Элементарными делителями матрицы A называются элементы $\varepsilon_1, \dfrac{\varepsilon_2}{\varepsilon_1}, \dots, \dfrac{\varepsilon_r}{\varepsilon_{r-1}}$, принадлежащие кольцу Λ. Можно доказать, что элементарные делители матрицы определены однозначно с точностью до ассоциированности. Например, первый элементарный делитель ε_1 является наибольшим общим делителем всех компонент матрицы A.

Для наших целей вполне хватит теоремы 1, а более точное утверждение, о котором мы говорили в этом пункте, нам не понадобится.

§ 6. Конечно порожденные модули над областью главных идеалов

1°. Подмодули конечно порожденного модуля над областью главных идеалов.

Теорема 1. *Пусть Λ – область главных идеалов, и пусть M – конечно порожденный Λ-модуль. Тогда всякий подмодуль N модуля M является конечно порожденным Λ-модулем.*

Доказательство. Пусть элементы $u_1, \dots, u_n$ порождают модуль M. Теорему будем доказывать индукцией по числу элементов n в порождающем множестве. Если $n = 0$, то $M = 0$ и утверждение бессодержательно. Пусть $n \geq 1$ и утверждение уже доказано для модулей, порожденных $n-1$ элементами. Обозначим

через I множество элементов $\lambda \in \Lambda$, для которых существуют такие $\lambda_2, \ldots, \lambda_n$, что элемент $\lambda u_1 + \lambda_2 u_2 + \ldots + \lambda_n u_n \in N$. Говоря иначе и не вполне строго, I – это множество первых "координат" элементов из N (слово "координат" поставлено в кавычки, потому что $u_1, \ldots, u_n$ – не обязательно базис, и коэффициенты в разложении элементов из M по $u_1, \ldots, u_n$, в том числе, и первый коэффициент, определены не однозначно).

Лемма 1. *I – идеал кольца Λ.*

Доказательство. Множество I непусто, так как, очевидно, $0 \in I$. Пусть $\lambda, \mu \in I$ и пусть γ – произвольный элемент из Λ. Существуют такие $\lambda_2, \ldots, \lambda_n; \mu_2, \ldots, \mu_n \in \Lambda$, что элементы $a = \lambda u_1 + \lambda_2 u_2 + \ldots + \lambda_n u_n$, $b = \mu u_1 + \mu_2 u_2 + \ldots + \mu_n u_n$ принадлежат подмодулю N модуля M. Тогда подмодулю N принадлежит и элемент

$$\gamma a + b = \gamma(\lambda u_1 + \lambda_2 u_2 + \ldots + \lambda_n u_n) + \mu u_1 + \mu_2 u_2 + \ldots + \mu_n u_n = \\ = (\gamma\lambda + \mu)u_1 + (\gamma\lambda_2 + \mu_2)u_2 + \ldots + (\gamma\lambda_n + \mu_n)u_n,$$

а потому первый коэффициент в этом представлении элемента $\gamma a + b$ принадлежит I. Итак, непустое множество I вместе с любыми λ, μ содержит и все элементы $\gamma\lambda + \mu$ ($\gamma \in \Lambda$), а это и значит, что I – идеал Λ. Лемма доказана.

Как и всякий идеал кольца Λ, идеал I – главный. Поэтому существует такой элемент $\xi \in I$, что I состоит из всех элементов $\mu\xi$, где μ пробегает кольцо Λ. По определению идеала I, существует такой элемент $v_1 \in N$, что $v_1 = \xi u_1 + \xi_2 u_2 + \ldots + \xi_n u_n$ для каких-то элементов $\xi_2, \ldots, \xi_n$ из кольца Λ.

Обозначим теперь через M_0 подмодуль M, порожденный $n-1$ элементами $u_2, \ldots, u_n$, а через N_0 – пересечение $N \cap M_0 \subseteq M_0$. По предположению индукции подмодуль N_0 модуля M_0 конечно порожден; пусть $v_2, \ldots, v_m \in N_0$ – какая-то порождающая его система элементов. Покажем, что элементы $v_1, v_2, \ldots, v_m$ порождают весь модуль N. В самом деле, если элемент $b = \lambda_1 u_1 + \lambda_2 u_2 + \ldots + \lambda_n u_n$ модуля M принадлежит подмодулю N, то по определению идеала I первый коэффициент λ_1 принадлежит идеалу $I = (\xi)$, и потому существует такой элемент $\mu_1 \in \Lambda$, что $\lambda_1 = \mu_1\xi$. Тогда элемент $b' = b - \mu_1 v_1$ принадлежит N; с другой стороны, тот же элемент

$$b' = b - \mu_1 v_1 = \lambda_1 u_1 + \lambda_2 u_2 + \ldots + \lambda_n u_n - \mu_1(\xi u_1 + \xi_2 u_2 + \ldots + \xi_n u_n) = \\ = (\lambda_2 - \mu_1\xi_2)u_2 + \ldots + (\lambda_n - \mu_1\xi_n)u_n$$

принадлежит M_0. Таким образом, $b' \in N \cap M_0 = N_0$, и потому существуют такие элементы $\mu_2, \ldots, \mu_m \in \Lambda$, что $b' = \mu_2 v_2 + \ldots + \mu_m v_m$. Тогда $b = b' + \mu_1 v_1 = \mu_1 v_1 + \mu_2 v_2 + \ldots + \mu_m v_m$. Итак, элементы $v_1, v_2, \ldots, v_m$ действительно порождают весь модуль N.

2°. Согласованный выбор базисов модуля и подмодуля (над областью главных идеалов).

Теорема 2. *Пусть S – свободный модуль конечного ранга над областью главных идеалов Λ, и пусть M – подмодуль модуля S. Тогда M – тоже свободный Λ-модуль, и можно так выбрать базис $e_1, \ldots, e_n$ модуля S и базис $u_1, \ldots, u_r$ подмодуля M, что $u_1 = \varepsilon_1 e_1, \ldots, u_r = \varepsilon_r e_r$, где $\varepsilon_1, \ldots, \varepsilon_r$ – ненулевые элементы из Λ. В частности, отсюда следует, что ранг r любого подмодуля свободного модуля S не больше ранга n модуля S.*

Доказательство. Пусть $d_1, \ldots, d_n$ – какой-то базис свободного Λ-модуля S, а $v_1, \ldots, v_m$ – какая-то порождающая система подмодуля M. Тогда существует такая матрица $A \in \Lambda^{m\times n}$, что

$$\begin{pmatrix} v_1 \\ \vdots \\ v_m \end{pmatrix} = A \begin{pmatrix} d_1 \\ \vdots \\ d_n \end{pmatrix}.$$

По теореме об элементарных делителях существуют такие матрицы $C \in \Lambda_m^*$, $D \in \Lambda_n^*$, такие что в матрице $B = CAD$ все элементы, не лежащие на диагонали, проходящей через левый верхний элемент этой матрицы, равны 0. Переставляя, если надо, строки и столбцы матрицы B (напомним, что это делается умножением матрицы B слева и справа на невырожденные матрицы), добьемся того, чтобы первые r диагональных элементов $\varepsilon_1, \ldots, \varepsilon_r$ матрицы $B = CAD$ были ненулевыми, а остальные равнялись 0. Положим

$$\begin{pmatrix} u_1 \\ \vdots \\ u_m \end{pmatrix} = C \begin{pmatrix} v_1 \\ \vdots \\ v_m \end{pmatrix}, \qquad \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix} = D^{-1} \begin{pmatrix} d_1 \\ \vdots \\ d_n \end{pmatrix};$$

по теореме ??? $u_1, \ldots, u_m$ – порождающая система модуля M, а $e_1, \ldots, e_n$ – базис модуля S, и мы имеем:

$$\begin{pmatrix} u_1 \\ \vdots \\ u_r \\ \vdots \\ u_m \end{pmatrix} = C \begin{pmatrix} v_1 \\ \vdots \\ v_r \\ \vdots \\ v_m \end{pmatrix} = CA \begin{pmatrix} d_1 \\ \vdots \\ d_r \\ \vdots \\ d_n \end{pmatrix} = CAD \begin{pmatrix} e_1 \\ \vdots \\ e_r \\ \vdots \\ e_n \end{pmatrix} = \begin{pmatrix} \varepsilon_1 & \ldots & 0 & \ldots & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & \ldots & \varepsilon_r & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \ldots & 0 & \ldots & 0 \end{pmatrix} \begin{pmatrix} e_1 \\ \vdots \\ e_r \\ \vdots \\ e_n \end{pmatrix},$$

т.е. $u_1 = \varepsilon_1 e_1, \ldots, u_r = \varepsilon_r e_r, u_{r+1} = \ldots = u_m = 0$. Нулевые элементы $u_{r+1}, \ldots, u_m$ можно выбросить из порождающей системы; остается доказать, что всякий элемент из M лишь единственным образом может быть выражен через элементы $u_1, \ldots, u_r$, порождающие M. Действительно, если

$$\alpha_1 u_1 + \ldots + \alpha_r u_r = \beta_1 u_1 + \ldots + \beta_r u_r$$

для некоторых $\alpha_i, \beta_i \in \Lambda$, то

$$\alpha_1\varepsilon_1 e_1 + \ldots + \alpha_r\varepsilon_r e_r = \beta_1\varepsilon_1 e_1 + \ldots + \beta_r\varepsilon_r e_r,$$

и, поскольку $e_1, \ldots, e_n$ – базис S, мы получаем, что $\alpha_1\varepsilon_1 = \beta_1\varepsilon_1$, ... , $\alpha_r\varepsilon_r = \beta_r\varepsilon_r$. Но Λ – область целостности, а все элементы $\varepsilon_1, \ldots, \varepsilon_r$ отличны от 0; поэтому можно сократить на них предыдущие равенства, и мы получим желаемые соотношения $\alpha_1 = \beta_1$, ... , $\alpha_r = \beta_r$.

§ 7. Конечнопорожденные модули над областью главных идеалов

1°. **Строение конечно порожденных модулей над областью главных идеалов.** Все предыдущие рассмотрения проводились ради доказательства следующего важнейшего результата.

Теорема 1. *Всякий конечно порожденный модуль над областью главных идеалов раскладывается в прямую сумму конечного числа циклических модулей.*

Доказательство. Пусть Λ – область главных идеалов, и пусть M – Λ-модуль, порожденный конечным числом элементов $a_1, \ldots, a_n$. По предложению 2.1 существует гомоморфизм φ из свободного Λ-модуля $S = \Lambda^n$ в модуль M, такой что $\varphi(e_i) = a_i$, где $e_1, \ldots, e_n$ – стандартный базис модуля Λ_n (напомним, что Λ^n состоит из столбцов высоты n с компонентами из Λ, а e_i – столбец, у которого на

i-й позиции стоит 1, а на остальных позициях – нули). Образ гомоморфизма φ является подмодулем модуля M и содержит элементы $a_1, \dots, a_n$, порождающие этот модуль; поэтому $\operatorname{Im}\varphi = M$, и по теореме о гомоморфизмах для модулей мы получаем, что модуль $M = \operatorname{Im}\varphi$ изоморфен фактормодулю модуля S по его подмодулю $\operatorname{Ker}\varphi$. Таким образом, достаточно доказать, что фактормодуль свободного модуля конечного ранга по любому его подмодулю раскладывается в прямую сумму конечного числа циклических модулей.

Итак, пусть S – свободный Λ-модуль конечного ранга, и пусть B – его подмодуль. По теореме о согласованном выборе базисов свободного модуля и его подмодуля (теорема 6.2) существуют такие базис $d_1, \dots, d_n$ модуля S и порождающая система $u_1, \dots, u_r$ подмодуля B, что $u_1 = \varepsilon_1 d_1, \dots, u_r = \varepsilon_r d_r$, где $r \le n$, а $\varepsilon_1, \dots, \varepsilon_r$ – ненулевые элементы кольца Λ.

Каждый из модулей $\Lambda/(\varepsilon_i)$ является циклическим; обозначим через D прямую сумму всех этих модулей и $n - r$ экземпляров модуля Λ, который тоже циклический:

$$D = \Lambda/(\varepsilon_1) \oplus \dots \oplus \Lambda/(\varepsilon_r) \oplus \Lambda \oplus \dots \oplus \Lambda.$$

Поскольку модуль S свободен, и $d_1, \dots, d_n$ – его базис, отображение $\psi : S \to D$, заданное формулой

$$\psi(\lambda_1 d_1 + \dots + \lambda_r d_r + \lambda_{r+1} d_{r+1} + \dots + \lambda_n d_n) = (\lambda_1 + (\varepsilon_1), \dots, \lambda_r + (\varepsilon_r), \lambda_{r+1}, \dots, \lambda_n),$$

представляет собой гомоморфизм Λ-модулей. Этот гомоморфизм является эпиморфизмом, потому что для любого элемента

$$d = (\lambda_1 + (\varepsilon_1), \dots, \lambda_r + (\varepsilon_r), \lambda_{r+1}, \dots, \lambda_n) \in \Lambda/(\varepsilon_1) \oplus \dots \oplus \Lambda/(\varepsilon_r) \oplus \Lambda \oplus \dots \oplus \Lambda = D$$

найдется элемент $s = \lambda_1 d_1 + \dots + \lambda_r d_r + \lambda_{r+1} d_{r+1} + \dots + \lambda_n d_n \in S$, такой что $\psi(s) = d$. Элемент $s = \lambda_1 d_1 + \dots + \lambda_r d_r + \lambda_{r+1} d_{r+1} + \dots + \lambda_n d_n$ принадлежит ядру ψ тогда и только тогда, когда

$$\psi(s) = (\lambda_1 + (\varepsilon_1), \dots, \lambda_r + (\varepsilon_r), \lambda_{r+1}, \dots, \lambda_n) = (0 + (\varepsilon_1), \dots, 0 + (\varepsilon_r), 0, \dots, 0),$$

т.е. когда $\lambda_1 \in (\varepsilon_1), \dots, \lambda_r \in (\varepsilon_r)$, $\lambda_{r+1} = \dots = \lambda_n = 0$. Это в точности равносильно условию: существуют $\alpha_1, \dots, \alpha_r \in \Lambda$, такие что $\lambda_1 = \alpha_1 \varepsilon_1, \dots, \lambda_r = \alpha_r \varepsilon_r$, $\lambda_{r+1} = \dots = \lambda_n = 0$, что бывает тогда и только тогда, когда элемент

$$\lambda_1 d_1 + \dots + \lambda_r d_r + \lambda_{r+1} d_{r+1} + \dots + \lambda_n d_n = \alpha_1 \varepsilon_1 d_1 + \dots + \alpha_r \varepsilon_r d_r = \alpha_1 u_1 + \dots + \alpha_r u_r$$

принадлежит B. Таким образом, $\operatorname{Ker}\psi = B$, и потому фактормодуль $S/B = S/\operatorname{Ker}\psi$ изоморфен модулю $\operatorname{Im}\psi = D$, который представляет собой прямую сумму циклических модулей.

2°. **Уточнения и следствия.** По теореме 1 всякий конечно порожденный модуль M над областью главных идеалов Λ раскладывается в прямую сумму своих подмодулей

$$M = M_1 \oplus \dots \oplus M_r \oplus M_{r+1} \oplus \dots \oplus M_n,$$

в котором каждое из последних $n - r$ слагаемых изоморфно Λ, а при $1 \le i \le r$ модуль M_i изоморфен циклическому модулю $\Lambda/(\varepsilon_i)$, где $\varepsilon_i \in \Lambda$, $\varepsilon_i \ne 0$. Обозначим

$$T = M_1 \oplus \dots \oplus M_r, \qquad S = M_{r+1} \oplus \dots \oplus M_n.$$

Тогда $M = T \oplus S$, причем T – периодический Λ-модуль (элемент $\varepsilon_1 \dots \varepsilon_r \ne 0$ является одним из его периодов), а модуль $S \approx \Lambda^{n-r}$ – свободный Λ-модуль. По предложению 4.2 мы получаем, что T совпадает с подмодулем кручения $T(M)$ модуля M. Вспомнив еще, что, по предложению 4.3, каждый из периодических циклических модулей M_i $(1 \le i \le r)$ раскладывается дальше в прямую сумму примарных циклических модулей, мы получим следующий результат, уточняющий теорему 1.

Теорема 2. *Всякий конечно порожденный модуль M над областью главных идеалов Λ раскладывается в прямую сумму подмодуля кручения $T(M)$ и свободного модуля конечного ранга S. При этом модуль кручения $T(M)$ периодический, и он раскладывается в прямую сумму конечного числа примарных циклических модулей.*

В отличие от разложения теоремы 1, можно доказать, что если в новом разложении выбросить все нулевые слагаемые, то оно будет уже единственно с точностью до порядка слагаемых.

По предложению 4.2, если M – периодический модуль, то $T(M) = M$, а если M – модуль без кручения, то $T(M) = 0$. Поэтому мы получаем как частные случаи теоремы 2 такие утверждения.

Следствие 1. *Всякий конечно порожденный периодический модуль над областью главных идеалов раскладывается в прямую сумму конечного числа примарных циклических модулей.*

Следствие 2. *Всякий конечно порожденный модуль без кручения над областью главных идеалов является свободным модулем.*

§ 8. Конечно порожденные абелевы группы

1°. **Строение конечнопорожденных абелевых групп.** Как мы уже отмечали, абелевы группы – это то же самое, что модули над кольцом целых чисел $\mathbb{Z}$. Поскольку $\mathbb{Z}$ – область главных идеалов, к абелевым группам применимы все результаты предыдущих параграфов. Но перед тем, как их формулировать, сделаем несколько замечаний, связанных с тем, что некоторые понятия для групп определялись для модулей и для групп независимо друг от друга. Если абелева группа конечно порождена, т.е. всякий ее элемент может быть получен из конечной системы элементов использованием только сложений и вычитаний, то этой же системы элементов тем более достаточно, если допустить еще умножения на целые числа (хотя пири этом ничего нового не получится, так как умножение на целые числа тоже сводится к сложениям и вычитаниям); таким образом, всякая конечно порожденная абелева группа является конечно порожденным $\mathbb{Z}$-модулем. Далее, всякий циклический $\mathbb{Z}$-модуль изоморфен фактормодулю $\mathbb{Z}$ по главному идеалу n, причем можно считать, что $n \geq 0$; поэтому при $n > 0$ циклический $\mathbb{Z}$-модуль оказывается циклической группой порядка n, а при $n = 0$ – свободной циклической группой. Далее, примарный модуль – это циклическая группа периода p^s, где p – простое число, а $s \geq 1$, а примарная циклическая группа – это циклическая группа порядка p^s. Наконец, заметим, что каждая циклическая группа, не являющаяся свободной, конечна, и прямая сумма конечного числа таких групп – конечная группа.

Свободный $\mathbb{Z}$-модуль ранга n называется свободной абелевой группой ранга n. Легче всего ее представить как прямую сумму n экземпляров группы $\mathbb{Z}$ или как группу строк $(a_1, \ldots, a_n)$ с целыми компонентами a_i.

Теперь мы можем сформулировать основные теоремы об абелевых группах.

Теорема 1. *Пусть A – периодическая абелева группа, и пусть $n = p_1^{s_1} \ldots p_r^{s_r}$ – ее период (здесь $p_1, \ldots, p_r$ – попарно различные положительные простые числа). Тогда A раскладывается в прямую сумму $A = A_1 \oplus \ldots \oplus A_r$, каждое слагаемое A_i в которой является примарной периодической группой, период которой равен $p_i^{s_i}$.*

Теорема 2. *Всякая конечно порожденная абелева группа A раскладывается в прямую сумму подгруппы кручения $T(A)$ и свободной абелевой группы S конечного ранга. Группа $T(A)$ конечна, и она раскладывается в прямую сумму конечного числа примарных циклических групп.*

Следствие 1. *Всякая конечно порожденная периодическая абелева группа конечна. Всякая конечная абелева группа раскладывается в прямую сумму конечного числа примарных циклических групп..*

Следствие 2. *Всякий конечно порожденная абелева группа без кручения является свободной абелевой группой конечного ранга.*

2°. **Факторгруппа свободной группы по коммутанту.** У нас раньше изучались свободные группы; теперь появились свободные абелевы группы. Связь между ними установлена в следующей теореме.

Теорема 3. *Факторгруппа свободной группы с n образующими F_n по коммутанту изоморфна свободной абелевой группе ранга n.*

Следствие. *Если $m \neq n$, то свободная группа с n образующими F_n не изоморфна свободной группе с m образующими F_m.*

Действительно, если бы были изоморфны группы F_n и F_m, то были бы изоморфны их факторгруппы по коммутантам. Но тогда мы получили бы, что свободный $\mathbb{Z}$-модуль ранга n изоморфен свободному $\mathbb{Z}$-модулю ранга m, а это возможно только при $m = n$.

Доказательство теоремы 3. Мы воспользуемся следующей леммой.

Лемма 1. *Пусть A, B – Λ-модули, порожденные соответственно элементами $a_1, \ldots, a_n$ и элементами $b_1, \ldots, b_n$. Если существуют такие Λ-гомоморфизмы $\varphi : A \to B$, $\psi : B \to A$, что $\varphi(a_i) = b_i$, $\psi(b_i) = a_i$ для всех i, $1 \leq i \leq n$, то Λ-модули A, B изоморфны.*

Доказательство. Для любого элемента $\lambda_1 a_1 + \ldots + \lambda_n a_n \in A$ мы имеем:

$$\psi(\varphi(\lambda_1 a_1 + \ldots + \lambda_n a_n)) = \psi(\lambda_1 b_1 + \ldots + \lambda_n b_n) = \lambda_1 a_1 + \ldots + \lambda_n a_n;$$

поэтому $\psi \circ \varphi = \mathrm{id}_A$. Точно так же доказываем, что $\varphi \circ \psi = \mathrm{id}_B$. Значит, отображения φ и ψ взаимно обратны, и потому биективны. Итак, каждое из отобрахений $\varphi : A \to B$, $\psi : B \to A$ – биективный Λ-гомоморфизм модулей, т.е. изоморфизм Λ-модулей.

Вернемся к доказательству теоремы. Пусть $F = F_n$ – группа со свободными порождающими $x_1, \ldots, x_n$. Обозначим через π канонический эпиморфизм группы F на ее факторгруппу по коммутанту $F/[F, F]$. Поскольку каждый элемент из группы F равен произведению нескольких сомножителей, каждый из которых равен одному из элементов x_i или x_i^{-1} $(1 \leq i \leq n)$, а π – эпиморфизм групп, каждый элемент из группы $F/[F, F]$ равен произведению нескольких сомножителей, каждый из которых равен одному из элементов $\pi(x_i)$ или $(\pi(x_i))^{-1}$. Следовательно, группа $F/[F, F]$ порождается элементами $\bar{x}_i = \pi(x_i)$ $(1 \leq i \leq n)$.

Далее, пусть $A = A_n$ – свободная абелева группа с базисом $a_1, \ldots, a_n$. По лемме 1 для доказательства теоремы достаточно построить такие гомоморфизмы абелевых групп $\varphi : A \to F/[F, F]$, $\psi : F/[F, F] \to A$, что $\varphi(a_i) = \bar{x}_i$, $\psi(\bar{x}_i) = a_i$ для всех i, $1 \leq i \leq n$. Существование первого из них очевидно: любое отображение базиса свободной абелевой группы A в другую абелеву группу продолжается до гомоморфизма групп, и потому, в частности, существует гомоморфизм $\varphi : A \to F/[F, F]$, такой что $\varphi(a_i) = \bar{x}_i$ для всех i. Осталось построить гомоморфизм ψ.

Поскольку $x_1, \ldots, x_n$ – свободные образующие свободной группы F, существует такой гомоморфизм $\psi' : F \to A$, что $\psi'(x_i) = a_i$ для всех i, $1 \leq i \leq n$. Группа A абелева; поэтому факторгруппа F по $\operatorname{Ker} \psi'$, изоморфная $\operatorname{Im} \psi' \subseteq A$, тоже абелева, и значит, $\operatorname{Ker} \psi' \supseteq [F, F] = \operatorname{Ker} \pi$. Покажем, что тогда существует гомоморфизм $\psi : F/[F, F] \to A$, такой что $\psi'(g) = \psi(\pi(g))$ для всех $g \in F$; в частности, этот гомоморфизм ψ обладает нужным нам свойством: для любого

i выполняется равенство $\psi(\bar{x}_i) = \psi(\pi(x_i)) = \psi'(x_i) = a_i$. Существование такого гомоморфизма ψ вытекает из следующего общего утверждения, похожего на 3-ю теорему о гомоморфизмах.

Лемма 2. *Пусть G, H, K – произвольные группы, и пусть $\psi' : G \to H$, $\pi : G \to K$ – такие гомоморфизмы групп, что π – эпиморфизм, а $\operatorname{Ker}\pi \subseteq \operatorname{Ker}\psi'$. Тогда существует такой гомоморфизм $\psi : K \to H$, что $\psi'(g) = \psi(\pi(g))$ для всех $g \in G$.*

Доказательство. Поскольку π – эпиморфизм, для любого элемента $x \in K$ существует такой элемент $g \in G$, что $\pi(g) = x$; положим $\psi(x) = \psi'(g)$. Определение корректно: если $g_1 \in G$ – другой элемент, такой что $\pi(g_1) = x$, то $\pi(g_1 g^{-1}) = \pi(g_1)(\pi(g))^{-1} = xx^{-1} = e$, и потому $g_1 g^{-1} \in \operatorname{Ker}\pi \subseteq \operatorname{Ker}\psi'$, а значит, $\psi'(g_1 g^{-1}) = e$, и $\psi'(g_1) = \psi'(g_1 g^{-1} g) = \psi'(g_1 g^{-1})\psi'(g) = e\psi'(g) = \psi'(g)$.

Построенное отображение ψ обладает свойством: $\psi'(g) = \psi(\pi(g))$ для всех $g \in G$; покажем, что оно является гомоморфизмом групп. Пусть $x_1, x_2 \in K$; существуют такие элементы $g_1, g_2 \in G$, что $\pi(g_1) = x_1$, $\pi(g_2) = x_2$. Поскольку π и ψ' – гомоморфизмы, мы получаем, что

$$\psi(x_1 x_2) = \psi(\pi(g_1)\pi(g_2)) = \psi(\pi(g_1 g_2)) = \psi'(g_1 g_2) = \psi'(g_1)\psi'(g_2) = \\ = \psi(\pi(g_1))\psi(\pi(g_2)) = \psi(x_1)\psi(x_2).$$

Полученное соотношение выполняется для любых $x_1, x_2 \in K$, а это в точности означает, что отображение ψ – гомоморфизм групп.