Лекция 7
Строение некоторых модулей

▷Прямые суммы ▷Фактор-модули ▷Разложение гомоморфизма ▷О сизигиях ▷Взаимные базисы ▷Инвариантные множители ▷Элементарные делители ▷Строение конечно порождённых модулей над кольцом главных идеалов ▷Строение конечно-порождённых абелевых групп ▷Целозначные многочлены

§1. Некоторые конструкции с модулями

1.1. Прямые суммы модулей. Прямая сумма модулей определяется аналогично прямой сумме колец. Если $V_1, V_2, \dots, V_m$ — некоторый набор K-модулей, то их *прямой суммой* называется модуль, обозначаемый

$$\bigoplus_{i=1}^{m} V_i = V_1 \oplus V_2 \oplus \cdots \oplus V_m$$

и состоящий из всевозможных наборов $(v_1, v_2, \dots, v_m)$, где $v_i \in V_i$, с покомпонентным сложением и умножением на числа:

$$\begin{aligned} (u_1, u_2, \dots, u_m) + (v_1, v_2, \dots, v_m) &\overset{\text{def}}{=} (u_1 + v_1\,,\ u_2 + v_2\,,\ \dots\,,\ u_m + v_m\,) \\ \lambda \cdot (v_1, v_2, \dots, v_m) &\overset{\text{def}}{=} (\lambda v_1, \lambda v_2, \dots, \lambda v_m) \end{aligned}$$

Задача 7.1. Проверьте, что прямая сумма K-модулей является K-модулем.

Говорят, что модуль V является *прямой суммой своих подмодулей*, $U_1, U_2, \dots, U_m \subset U$, если гомоморфизм сложения

$$\alpha\colon U_1 \oplus U_2 \oplus \cdots \oplus U_m \longrightarrow V : \quad (u_1, u_2, \dots, u_m) \longmapsto \sum u_i$$

является изоморфизмом. Это равносильно тому, что каждый вектор $v \in V$ допускает единственное разложение вида $v = \sum u_i$ с $u_i \in U_i$. Модуль, не представимый в виде прямой суммы своих собственных[1] подмодулей называется *неразложимым*.

1.1.1. Лемма. *Для того чтобы модуль V распадался в прямую сумму двух своих подмодулей U и W необходимо и достаточно, чтобы подмодули U, W порждали V и пересекались только по нулевому вектору.*

[1] т. е. ненулевых и отличных от самого модуля

Доказательство. Необходимость очевидна. Достаточность: то что U и W порождают V означает, что всякий $v \in V$ представим в виде $v = u + w$, а единственность такого представления вытекает из условия $U \cap W = 0$, ибо $v = u + w = u' + w'$ означает, что $u - u' = w - w' \in U \cap W$. □

1.1.2. Пример: свободный модуль K^n есть прямая сумма свободных модулей единичного ранга:

$$K^n = \underbrace{K \oplus K \oplus \cdots \oplus K}_{n} .$$

В частности, теорема о существовании базиса в векторном пространстве означает, что неразложимые модули над полем — это одномерные векторные пространства и только они.

1.1.3. Пример. Если число $m \in \mathbb{Z}$ разложено в произведение попарно взаимно простых множителей $m = q_1 q_2 \cdots q_s$, то построенный в лекции 2 изоморфизм колец

$$\mathbb{Z}/m\mathbb{Z} \xrightarrow{\sim} \bigoplus_i (\mathbb{Z}/q_i\mathbb{Z})$$

задаёт заодно разложение $\mathbb{Z}$-модуля $\mathbb{Z}/m\mathbb{Z}$ в прямую сумму $\mathbb{Z}$-модулей $\mathbb{Z}/q_i\mathbb{Z}$.

Задача 7.2. Вложите $\mathbb{Z}/q_i\mathbb{Z}$ в $\mathbb{Z}/m\mathbb{Z}$ в качестве подмодулей так, чтобы предыдущее разложение превратилось в разложение в прямую сумму *подмодулей*.

1.1.4. Пример: дополнительное подпространство. Если V — (конечномерное) векторное пространство над полем k, и $W \subset V$ — некоторое подпространство, то всегда можно (многими разными способами) подобрать подпространство $W' \subset V$, так чтобы $V = W \oplus W'$. Например, можно фиксировать какой-либо базис $(w_1, w_2, \ldots, w_m)$ в W и как-то дополнить его (по Сл.3.7.6 из лек. 5) до базиса $(w_1, w_2, \ldots, w_n)$ в V. После этого в качестве W' можно взять подпространство, порождённое последними $(n - m)$ базисными векторами $(w_{m+1}, \ldots, w_n)$.

Задача 7.3. Проверьте, что всякий вектор $v \in V$ действительно допускает единственное разложение $v = w + w'$ с $w \in W$, $w' \in W'$.

Задача 7.4. Проверьте, что в качестве W' можно взять любое подпространство в V, удовлетворяющее условиям $W' \cap W = 0$ и $\dim W' + \dim W = \dim V$.

Подпространство $W' \subset V$, такое что $V = W \oplus W'$, называется *дополнительным подпространством* к W в V.

1.1.5. Пример-предупреждение. Если кольцо K не является полем, то *неверно* что всякий подмодуль W в K-модуле V имеет дополнительный подмодуль, даже в случае, когда $V = K^n$ – свободен. Например, подмодуль $W = 2\mathbb{Z} \subset \mathbb{Z}$ чётных чисел не имеет никакого дополнительного подмодуля $W' \subset \mathbb{Z}$. Действительно, как и всякий подмодуль в $\mathbb{Z}$, W' был бы тогда главным идеалом: $W' = d\mathbb{Z}$, и изоморфизм $\mathbb{Z} = W \oplus W'$ означал бы, что всякое целое число m *единственным способом* разложимо в сумму $m = 2x + dy$, что невозможно.

Задача 7.5. Убедитесь, что представлений числа m в виде $m = 2x + dy$ либо нет вообще, либо бесконечно много.

Тем не менее, с парой $W \subset V$ всегда можно связать новый модуль, V/W называемый *фактор-модулем V по подмодулю W*. Этот модуль обладает многими интуитивными свойствами “дополнения” к W в в V, с той только разницей, что он не будет подмодулем в V, а будет “отдельно стоящим”.

1.2. Факторизация K-модуля V по подмодулю $W \subset V$, опять-таки, аналогична факторизации кольца по идеалу. А именно, рассмотрим разбиение V на классы эквивалентности, относя два элемента $v_1, v_2 \in V$ в один класс $[v_1] = [v_2]$, если и только если их разность $(v_1 - v_2)$ лежит в W. Это действительно разбиение, ибо если классы $[v_1]$ и $[v_2]$ пересекаются по некоторому u, то $v_1 - u = w_1$ и $v_2 - u = w_2$ для каких-то $w_1, w_2 \in W$, и значит, $v_1 - v_2 = w_1 - w_2 \in W$, т. е. $[v_1] = [v_2]$. Класс $[v]$ называется *смежным классом элемента* $v \in V$ *по подмодулю* W. Два элемента v_1, v_2, лежащие в одном кдассе, называются *сравнимыми по подмодулю* W. Множество смежных классоы обозначается V/W и наделяется структурой K-модуля, инуцированной с V:

$$\begin{aligned} [v_1] + [v_2] &\stackrel{\text{def}}{=} [v_1 + v_2] \qquad \forall\, v_1, v_2 \in V \\ \lambda[v] &\stackrel{\text{def}}{=} [\lambda v] \qquad \forall\, \lambda \in K \ , \quad \forall\, v \in V \end{aligned}$$

Эти правила корректны, поскольку из равенств $[u_1] = [v_1]$, $[u_2] = [v_2]$ и $[u] = [v]$, означающих что $u_1 = v_1 + w_1$, $u_2 = v_2 + w_2$ и $u = v + w$, где w_1, w_2, $w \in V$, следует, что

$$\begin{aligned} u_1 + u_2 &= v_1 + v_2 + (w_1 + w_2) \equiv v_1 + v_2 \bmod (W) \\ \lambda u &= \lambda v + \lambda w \equiv \lambda v \bmod (W) \end{aligned}$$

Модуль V/W называется *фактор-модулем* V *по* W.

Задача 7.6. Проверьте выполнение аксиом модуля для V/W.

Задача 7.7. Проверьте, что каноническое отображение

$$\pi\colon\ V \longrightarrow V/W\ , \quad v \longmapsto [v]$$

является гомоморфизмом модулей (он называется *эпиморфизмом редукции по модулю* W).

Задача 7.8. Докажите, что фактор-множество модуля V по какому-либо разбиению тогда и только тогда корректно наследует модульную структуру с V, когда это разбиение является разбиением на смежные классы по некоторому подмодулю.
Подсказка: следуйте рассуждению из лекции 2 (т. е. убедитесь, что клясс $[0]$ — это подмодуль и т. д.).

1.3. Строение гомоморфизмов. Пусть $V \xrightarrow{\varphi} W$ — гомоморфизм модулей. Тогда имеется канонический изоморфизм $V/\ker(\varphi) \xrightarrow{\tilde\varphi} \mathrm{im}\,(\varphi)$, индуцированный гомоморфизмом φ, т. е. заданный правилом $v \bmod (\ker\varphi) \overset{\tilde\varphi}{\longmapsto} f(v) \in W$. Это правило корректно, поскольку выбирая другой $u = v + w$ (где $\varphi(w) = 0$), мы получим $f(u) = f(v) + f(w) = f(v)$. Биективность $\tilde\varphi$ вытекает из равносильности условий $f(v_1) = f(v_2)$ и $f(v_1 - v_2) = 0$ (последнее, означает, что $v_1 \equiv v_2 \bmod (\ker\varphi)$). Мы доказали

1.3.1. Предложение. (Теорема о строении гомоморфизма модулей.) *Всякий гомоморфизм* $\varphi\colon\ V \longrightarrow W$ *может быть разложен в композицию*

$$\begin{tikzcd} V \arrow[r, "\varphi"] \arrow[d, "\pi"'] & W \\ V/ker(\varphi) \arrow[r, "\tilde\varphi"] & \mathrm{im}\,(\varphi) \arrow[u, "\iota"'] \end{tikzcd} \quad ,$$

где $V \xrightarrow{\pi} V/ker(f)$ *– канонический эпиморфизм редукции по модулю* $\ker(f)$, $\tilde\varphi$ *– изоморфизм, а* ι *– вложение.*

□

1.3.2. Пример: линейные уравнения. Пусть $Ax = b$ — система из m линейных уравнений от n неизвестных над кольцом K. Рассмотрим гомоморфизм $K^n \xrightarrow{\mu_A} K^m$, переводящий вектор-столбец $v \in K^n$ в вектор-столбец $Av \in K^m$. Система $Ax = b$ разрешима тогда и только тогда, когда $b \in \operatorname{im} \mu_A$, что равносильно тому, что столбец b лежит в линейной оболочке столбцов матрицы A (если $K = k$ – поле, то последнее означает, что *ранг расширенной матрицы системы равен рангу матрицы* A).

Если $b \in \operatorname{im} \mu_A$, то множество решений есть *полный прообраз* вектора b относительно μ_A, и стало быть, представляет собой смежный класс по подмодулю $\ker \mu_A$, т. е. имеет вид

$$\{ x = c + w \} ,$$

где c – произвольное фиксированное решение системы $Ax = b$, а w пробегает множество решений однородной системы $Ax = 0$. Если модуль $\ker \mu_A$ свободен (например, если $K = k$ – поле), то выбирая в нём базис $(e_1, e_2, \dots, e_d)$, мы получаем для каждого решения единственное представление в виде $x = c + \lambda_1 e_1 + \lambda_2 e_2 + \dots + \lambda_d e_d$, где c – какое-либо одно фиксированное решение системы $Ax = b$, а λ_i – произвольные постоянные.

1.3.3. Пример: сизигии. Всякий конечно порождённый K-модуль V является фактором свободного модуля. В самом деле, пусть V порождается набором векторов $(v_1, v_2, \dots, v_{n_0})$. Тогда отображение, переводящее стандартный базисный вектор $e_i \in K^{n_0}$ в вектор v_i можно продолжить по линейности до гомоморфизма модулей $K^{n_0} \xrightarrow{\varphi_0} V$. Поскольку v_i порождают V, получаем, что $V = K^{n_0} / \ker(\varphi_0)$. Подмодуль $\ker \varphi_o \subset K^{n_0}$ называется *модулем соотношений* или 0-*сизигий* между образующими v_i. Название связано с тем, что всякий элемент $\sum x_i e_i \in \ker \varphi_0$ соответствует линейной зависимости $\sum x_i v_i = 0$ в модуле V, и это соответствие, очевидно, биективно.

Если модуль соотношений $\ker \varphi_0$ также конечно порождён, то его тоже можно представить как образ сюрьективного гомоморфизма $K^{n_1} \xrightarrow{\varphi_1} \ker \varphi_0$ из свободного модуля, базисные векторы которого соответствуют *образующим соотношениям* между $v_i \in V$ (т. е. соотношениям, из которых вытекают все остальные соотношения). Ядро $\ker \varphi_1$ называется *модулем 1-сизигий* между образующими v_i. Интуитивно, 1-сизигии это “соотношения между соотношениями”.

Процедуру можно итерировать и далее, построив последовательность гомоморфизмов

$$\dots \xrightarrow{\varphi_{k+1}} K^{n_k} \xrightarrow{\varphi_k} K^{n_{k-1}} \xrightarrow{\varphi_{k-1}} \dots \xrightarrow{\varphi_2} K^{n_1} \xrightarrow{\varphi_1} K^{n_0} \xrightarrow{\varphi_0} V \to 0 ,$$

в которой каждый раз $\ker(\varphi_k) = \operatorname{im}(\varphi_{k+1})$. Этот модуль называется модулем k-сизигий. Если процесс оборвётся на m-том шагу, т. е. очередной гомоморфизм $K^{n_m} \xrightarrow{\varphi_m} \ker(\varphi_{m-1})$ окажется изоморфизмом (что ознаачает, что модуль $(n-1)$-сизигий свободен), то говорят что исходный модуль V имел *когомологическую размерность* $\le m$. Когомологическая размерность измеряет, таким образом, насколько данный модуль V далёк от свободного модуля.

1.4. Факторизация прямых сумм. Факторизация согласована с взятием прямых сумм в следующем смысле.

1.4.1. Предложение. *Пусть в каждом из модулей $(V_1, V_2, \dots, V_m)$ задано по подмодулю $W_i \subset V_i$, $i = 1, 2, \dots, m$. Тогда $W = \bigoplus\limits_i W_i$ — подмодуль в $V = \bigoplus\limits_i V_i$ и $V/W = \bigoplus\limits_i (V_i/W_i)$.*

Доказательство. То, что наборы вида $(w_1, w_2, \ldots, w_m)$ составляют подмодуль в V, — очевидно. Легко видеть, что отображение $\alpha\colon V/W \longrightarrow \bigoplus_i (V_i/W_i)$:

$$(v_1, v_2, \ldots, v_m) \bmod W \longmapsto \Big(v_1(\bmod W_1),\ v_2(\bmod W_2),\ \ldots,\ v_m(\bmod W_m)\Big)\,.$$

является корректно определённым эпиморфизмом с нулевым ядром.

Задача 7.9. Проверьте это.

□

1.4.2. Следствие. *Свободные модули K^m и K^n над произвольным коммутативным кольцом K изоморфны только при $k = m$.*

Доказательство. Пусть $V = K^n$, $W = K^m$, и пусть $\alpha\colon V \longrightarrow W$ — изоморфизм. Рассмотрим какой-нибудь максимальный идеал $\mathfrak{m} \subset K$, так что фактор-кольцо $k = K/\mathfrak{m}$ является полем. Ясно, что α отождествляет подмодуль $\mathfrak{m}V = \{\, w = \lambda v \mid \lambda \in \mathfrak{m}, v \in V \,\} \subset V$ с аналогичным подмодулем $\mathfrak{m}W \subset W$, и стало быть, индуцирует изоморфизм фактор-модулей $V/\mathfrak{m}V \xrightarrow{\sim} W/\mathfrak{m}W$.

Задача 7.10. Пусть V – произвольный K-модуль и $\mathfrak{q} \subset K$ – любой идеал. Убедитесь, что $\mathfrak{q}V$ является подмодулем в V и что правило

$$\lambda \bmod (q) \cdot v \bmod (qV) \stackrel{\text{def}}{=} \lambda v \bmod (qV)$$

корректно задаёт на $V/\mathfrak{q}V$ структуру модуля над кольцом $K/\mathfrak{q}$.

Поскольку $V = \underbrace{K \oplus K \oplus \cdots \oplus K}_{n}$, имеем $\mathfrak{m}V = \mathfrak{m}K \oplus \mathfrak{m}K \oplus \cdots \oplus \mathfrak{m}K = \mathfrak{m} \oplus \mathfrak{m} \oplus \cdots \oplus \mathfrak{m}$, и по предыдущему предложению $V/\mathfrak{m}V = \underbrace{K/\mathfrak{m}K \oplus K/\mathfrak{m}K \oplus \cdots \oplus K/\mathfrak{m}K}_{n} = k^n$ является n-мерным векторным пространством над полем k. Аналогично, $W/\mathfrak{m}W = k^m$. Поскольку α индуцирует отождествление этих пространств, должно выполняться равенство $n = m$.

□

Задача 7.11. Пусть U — подмодуль в V, а W — подмодуль в U. Убедитесь, что W является подмодулем в V и что U/W можно рассматривать как подмодуль в V/W. Постройте изоморфизм $\big(V/W\big)/\big(U/W\big) \xrightarrow{\sim} V/U$.

§2. Конечно порождённые модули над кольцом главных идеалов

2.1. Некоторые напоминания. Всюду в этом параграфе мы будем предполагать, что K — это кольцо главных идеалов, т. е. целостное коммутативное кольцо с единицей, каждый идеал $I \subset K$ в котором имеем вид $I = (d) = dK$ для некоторого $d \in K$. Основными модельными примерами для нас будут случаи $K = \mathbb{Z}$ и $K = k[x]$, где k – поле. Читателю настоятельно рекомендуется отдельно проговаривать все формулировки и доказательства в конкретных терминах этих колец.

Образующая d идеала $\mathfrak{I}$ называется *наибольшим общим делителем* элементов этого идеала и обозначается *НОД* $(\mathfrak{I})$. Напомню (см. лекции 2, 3), *НОД* $(\mathfrak{I})$ определяется идналом $\mathfrak{I}$

однозначно с точностью до умножения на обратимые элементы кольца[2]. В лекции 3 мы видели, что всякое кольцо главных идеалов нётерово и факториально. Из первого вытекает, в частности

2.1.1. Следствие. *Псякое множество идеалов в кольце главных идеалов содержит по меньшей мере один идеал, не содержащийся (строго) ни в каком другом идеале из этого множества.*

□

Второе же означает, что в кольце главных идеалов каждый элемент m допускает разложение на простые множители

$$m = p_1^{d_1} p_2^{d_2} \cdots p_s^{d_s} \ ,$$

в котором $p_1, p_2, \ldots, p_s$ – попарно неассоциированные простые (= неприводимые) элементы кольца и неупорядоченная совокупность степеней $p_\nu^{d_\nu}$ определяются по m однозначно с точностью до умножения любого p_i на обратимый элемент кольца K.

2.2. Теорема. (Теорема о взаимных базисах) *Пусть $U \subset V$ — произвольный подмодуль в свободном K-модуле $V \simeq K^n$. Тогда U тоже свободен, и существуют такие базисыв $(u_1, u_2, \ldots, u_r)$ в U и $(v_1, v_2, \ldots, v_n)$ в V, что $u_i = m_i v_i$, $1 \le i \le r$, для некоторых $m_i \in K$, таких что m_i делит m_j при $i < j$.*

Терминологическое замечание. Базисы, о которых идёт речь в теореме, называются *взаимными базисами* модуля V и подмодуля U, а числа m_i называются *инвариантными множителями* подмодуля U.

Доказательство. Индукция по n. При $n = 1$ теорема в утверждает в точности то, что K является кольцом главных идеалов.

Пусть $n \ge 2$ и $e = (e_1, e_2, \ldots, e_n)$ – какой-либо базис в V. Подмножество $I(e) \subset K$, состоящее из первых координат всевозможных векторов $u \in U$ в базисе e является идеалом в K (проверьте!). Пусть $f = (f_1, f_2, \ldots, f_n)$ – такой базис в V, что идеал $I(f)$ не содержится в качестве собственного подмножества ни в одном из идеалов семейства $I(e)$, где e пробегает все базисы V (существование f гарантировано предыдущим следствием). Пусть m_1 — образующая идеала $I(f)$, и пусть это m_1 служит первой координатой вектора $u_1 \in U$.

Заметим, что все координаты вектора u_1 в базисе f делятся на m_1. В самом деле, если, скажем, вторая координата x вектора $u_1 = m_1 f_1 + x f_2 + \cdots$ не лежит в идеале $(m_1) = I(f)$, то идеал $I(f')$, построенный по базису

$$f' = (f_2, (f_1 + f_2), f_3, f_4, \ldots, f_n) \ ,$$

будет (вопреки выбору f) строго содержать $I(f)$, поскольку первая координата вектора $x f_2 - u_1$ будет равна m_1, а первая координата вектора u_1 будет равна $x - m_1 \notin (m_1)$ (обязательно проверьте!).

Таким образом, $u_1 = m_1 v_1$ для некоторого $v_1 \in V$. Подчеркнём, что первая координата вектора v в базисе f равна 1, и обозначим через V' свободный подмодуль ранга $(k-1)$, порождённый векторами $f_2, f_3, \ldots, f_n$, а через U' – пересечение $V' \cap U$. Я утверждаю, что $V = K v_1 \oplus V'$ и $U = K u_1 \oplus U'$.

Первое следует из того, что подмодули $K v_1$ и V' пересекаются только по нулю (ибо вектор вида $x v_1$ в разложении по базису f содержит $x f_1$, а стало быть лежит в V' лишь при $x = 0$) и порождают V (ибо всякий $v = \sum x_i f_i = x_1 v_1 + v'$ с $v' \in V'$).

[2] в $\mathbb{Z}$ и $k[x]$ этот произвол можно устранить требуя чтобы *НОД* был неотрицательным числом или соответственно приведённым многочленом.

Второе устанавливается аналогично: очевидно, что $Ku_1 \cap U' = 0$, а u_1 и U' порождают U потому, что первая координата всякого $u \in U$ в базисе f делится на первую координату вектора u_1 (по определению $I(f)$, f и u_1), и значит, может быть обнулена вычитанием из u подходящего кратного u_1.

Применяя к $U' \subset V'$ предположение индукции, мы можем построить для этих модулей взаимные базисы $(u_2, \dots, u_r)$ и $(v_2, \dots, v_n)$ с $u_i = m_i v_i$ при $i = 2, \dots, r$, где $r' \leq (n-1)$ и целые числа m_i таковы, что m_i делит m_j при $i < j$. Добавляя к этим базисам построенные выше v_1 и $u_1 = m_1 v_1$ мы получим базисы в исходных модулях U и V и для проверки того, что они будут взаимными нам остаётся только показать, что все m_i с $i \geq 2$ делятся на m_1.

Для этого покажем сначала, что *все* координаты *всех* векторов $u' \in U'$ в базисе f делятся на m_1. Действительно, пусть, к примеру, координата x вектора $u' = xf_2 + \cdots$ не лежит в идеале $(m_1) = I(f)$ и пусть $u_1 = m_1 f_1 + yf_2 + \cdots$. Тогда идеал $I(f'')$, построенный по базису

$$f'' = (f_2, (f_1 + f_2), f_3, f_4, \dots, f_n) ,$$

опять-таки, будет строго содержать $I(f)$, поскольку первая координата вектора $yf_2 - u_1$ будет равна m_1, а первая координата вектора u' будет равна $x \notin (m_1)$ (обязятельно проверьте!).

Заметим теперь, что каждое m_i есть координата вектора u_i в базисе $(v_1, v_2, \dots, v_n)$, а потому является k-линейной комбинацией координат вектора u_i в базисе f (при замене базиса столбец координат умножается на матрицу перехода). Так как последние делятся на m_1, мы получаем, что m_i также делится на m_1.

□

Задача 7.12. Убедитесь, что приведённое только что рассуждение по-существу дублирует доказательство теоремы о приведении матрицы к строгому ступенчатому виду.

Задача 7.13. Докажите такой вариант теоремы о ранге матрицы: пусть A – матрица размера $m \times n$ над кольцом главных идеалов K; тогда ее столбцы порождают свободный подмодуль в K^m, а строки — свободный подмодуль в K^n, причём ранги этих подмодулей совпадают и равны числу ненулевых диагональных элементов, возникающих в результате приведения матрицы A к строгому диагональному виду элементарными преобразованиями строк и столбцов.

2.3. Теорема. (Теорема об инвариантных множителях.) *Каждый из инвариантных множителей $m_i \in K$ в предыдущей теореме однозначно с точностью до умножения на обратимый элемент кольца K определяется самими модулями U и V, и не зависит от выбора взаимных базисов.*

Доказательство. Пусть $\{v_1, v_2, \dots, v_n\} \subset K^n$ и $\{u_1, u_2, \dots, u_r\} \subset U \subset K^n$ — какая-то пара взаимных базисов, так что $u_i = m_i v_i$, $m_i \in K$. Мы дадим независящее от выбора взаимных базисов описание для каждого из произведений

$$M_i = m_1 m_2 \dots m_i \quad , \qquad 1 \leq i \leq r$$

(тем самым, $m_i = M_i / M_{i-1}$ тоже будут описаны инвариантно).

Для каждого набора $w = \{w_1, w_2, \dots, w_i\} \subset U$ из i векторов и каждого базиса $e = (e_1, e_2, \dots, e_n)$ модуля V обозначим через $C_i(e, w) \in Mat_i(K)$ матрицу, j-тый столбец которой сотоит из первых i координат вектора w_j в базисе e, и положим $D_i(e, w) = \det(C_i(e, w)) \in K$ (при $i = 1$ $C_1(e, w) = D_1(e, w)$ — это в точности первая координата вектора $w = w_1$ в базисе

e). Матрица $C_i(e,w)$ есть подматрица, составленная из верхних i строк матрицы перехода C_{ew}, которая, напомню, имеет размер $(n \times i)$ и однозначно определяется равенством

$$(w_1, w_2, \ldots, w_i) = (e_1, e_2, \ldots, e_n) C_{ew} \, .$$

Отметим, что $M_i = D_i(v,u)$, где $(v,u) = \Big((v_1, v_2, \ldots, v_n) ,\ (u_1, u_2, \ldots, u_i) \Big)$ происходит из зафиксированных выше взаимных базисов. Инвариантная характеризация M_i состоит в том, что *M_i является наибольшим общим делителем всех чисел $D_i(e,w)$ по всем w, e.* Чтобы доказать это, нам остаётся проверить, что M_i делит каждое из чисел $D_i(e,w)$.

Пусть произвольный набор $(w_1, w_2, \ldots, w_i)$ векторов подмудуля U раскладывается по векторам из зафиксированных выше взаимных базисов по формулам

$$w_j = \sum_{\alpha=1}^{r} c_{\alpha j} u_\alpha = \sum_{\alpha=1}^{r} m_\alpha c_{\alpha j} v_\alpha \, .$$

Если для любого вектора $g \in V$ обозначить через $g^{(i)} \in K^i$ вектор-столбец высоты i, состоящий из первых i координат вектора g относительно произвольно выбранного базиса $(e_1, e_2, \ldots, e_n)$ в V, то согласно предыдущей формуле, j-тый столбец матрицы $C_i(e,w)$ можно представить в виде линейной комбинации $w_j^{(i)} = \sum\limits_{\alpha=1}^{r} m_\alpha c_{\alpha j} v_\alpha^{(i)}$, откуда пользуясь полилинейностью и кососимметричностью определителя получаем

$$D_i(e,w) = \det(w_1^{(i)}, w_2^{(i)}, \ldots, w_i^{(i)}) =$$

$$\sum_{1 \le \alpha_1 < \alpha_2 < \cdots < \alpha_i \le r} \; \sum_{\sigma \in \mathfrak{S}_i} sgn\,(\sigma) m_{\alpha_{\sigma(1)}} m_{\alpha_{\sigma(2)}} \cdots m_{\alpha_{\sigma(i)}} \cdot c_{\alpha_{\sigma(1)} j} c_{\alpha_{\sigma(2)} j} \cdots c_{\alpha_{\sigma(i)} j} \cdot \det\Big(v_{\alpha_1}^{(i)}, v_{\alpha_2}^{(i)}, \ldots, v_{\alpha_i}^{(i)} \Big) \, .$$

Так как m_α делит m_β при $\alpha < \beta$, каждое слагаемое суммы делится на $M_i = m_1 m_2 \cdots m_i$, что и требовалось.

□

Задача 7.14. Докажите, что две прямоугольные матрицы одинакового размера над кольцом главных идеалов тогда и только тогда приводятся к одинаковому строгому диагональному виду элементарными преобразованиями строк и столбцов, когда при всех k у этих матриц совпадает наибольший общий делитель всех миноров k-того порядка.

2.4. Элементарные делители. Пусть теперь $(m_1, m_2, \ldots, m_r)$ – упорядоченная последовательность элементов кольца, в которой m_i делит m_j при $i < j$. Если разложить каждый из них на простые множители

$$m_i = p_{i_1}^{d_{i_1}} p_{i_2}^{d_{i_2}} \cdots p_{i_{s_i}}^{d_{i_{s_i}}} \, ,$$

то исходная упорядоченная последовательность $(m_1, m_2, \ldots, m_r)$ будет однозначно восстанавливаться по неупорядоченному набору, полученному *дизъюнктным объединением* всех степеней p^d из всех этих разложений (дизъюнктность означает, что каждая степень присутствует в итоговом неупорядоченном наборе столько раз, сколько она появляется во всевозможных разложениях). В самом деле, все степени одного и того же простого элемента p из итогового набора можно выстроить в ряд так, чтобы показатели монотонно невозрастали слева направо. Тогда первый слева элемент этого ряда входит в разложение числа m_r, второй – в разложение m_{r-1} и т. д. пока ряд не кончится. В результате мы однозначно восстанавливаем разложение каждого m_i в отдельности. Нами доказана

2.4.1. Лемма. *Произвольный набор (возможно повторяющихся) степеней p^d простых элементов возникает из единственной последовательности $(m_1, m_2, \dots, m_r)$, в которой m_i делит m_j при $i < j$, как дизъюнктное объединение всех степеней простых элементов, входящих в разложения m_i на простые множители.*

□

В ситуации, когда набор $(m_1, m_2, \dots, m_r)$ является набором инвариантных множителей подмодуля U в свободном модуле V, соответствующее ему дизъюнктное объединение степеней простых сомножителей p^d, входящих в разложения m_i, называется *набором элементарных делителей* подмодуля U в свободном модуле V.

2.5. Теорема. *Всякий конечно порождённый модуль V над кольцом главных идеалов K допускает конечное разложение вида*

$$V = K^n \oplus \bigoplus_\nu \frac{K}{p_\nu^{d_\nu} K} \tag{7-1}$$

где $p_\nu \in K$ – простые элементы. Число n и совокупность степеней $p_\nu^{s_\nu}$ не зависят (с точностью до умножения p_ν на обратимые элементы кольца) от способа разложения[3] и определяются модулем V однозначно.

Доказательство. Пусть V порождается элементами $e_1, e_2, \dots, e_N$. Тогда $V = K^N / \ker(\varphi)$, где $K^N \xrightarrow{\varphi} V$ — эпиморфизм, переводящий стандартный базис координатного модуля K^N в образующие $e_\imath$. Выберем в $\ker(\varphi) \subset K^N$ взаимные базисы $\{u_1, u_2, \dots, u_r\}$ и $\{v_1, v_2, \dots, v_N\}$, где $u_i = m_i v_i$. В этих базисах

$$V = \underbrace{\frac{K \;\oplus\; K \;\oplus \cdots \oplus\; K \;\oplus K \oplus \cdots \oplus K}{m_1 K \oplus m_2 K \oplus \cdots \oplus m_r K \oplus 0 \oplus \cdots \oplus 0}}_{N} = \frac{K}{(m_1)} \oplus \frac{K}{(m_2)} \oplus \cdots \frac{K}{(m_r)}\,.$$

Раскладывая каждый из инвариантных множителей m_i в произведение степеней простых элементов $m_i = p_{i_1}^{d_{i_1}} p_{i_2}^{d_{i_2}} \cdots p_{i_{s_i}}^{d_{i_{s_i}}}$ по китайской теореме об остатках (см. с Сл.1.6.2 лекции 3), получаем дальнейшее разложение

$$\frac{K}{(m_i)} = \frac{K}{(p_{i_1}^{d_{i_1}})} \oplus \frac{K}{(p_{i_2}^{d_{i_2}})} \oplus \cdots \frac{K}{(p_{i_{s_i}}^{d_{i_{s_i}}})}\,.$$

Это доказывает существование разложения.

Для доказательства единственности отметим прежде всего несколько следствий из факта существования разложения (7-1).

2.5.1. Следствие. *Всякий конечно порождённый модуль над кольцом главных идеалов является прямой суммой свободного модуля и подмодуля кручения[4].*

□

2.5.2. Следствие. *Всякий конечно порождённый модуль без кручения над кольцом главных идеалов свободен.*

□

[3]таких способов, разумеется, много: например способов представить свободный модуль V в виде $V = K^n$ имеется столько же, сколько базисов в V

[4]напомню, что подмодуль кручения $Tors(V) = \{\, v \neq 0 \mid \exists \lambda \neq 0 : \lambda v - 0 \,\}$

Из этого следствия сразу же вытекает, что число n в (7-1) однозначно определяется по модулю V как ранг свободного модуля $V/Tors(V)$.

Если p и q — простые неассоциированные элементы, то p^k взаимно-прост с q^d, а стало быть, обратим в $K/(q^d)$, и значит, гомоморфизм $K/(p^d) \xrightarrow{\mu_{p^k}} K/(p^d)$ умножения на p^k в модуле $K/(p^d)$ является изоморфизмом. Напротив, гомоморфизм μ_{p^k} в модуле $K/(p^d)$ тождественно нулевой, если $k \geq d$, и $\ker \mu_{p^k} = p^{d-k}K/(p^d)$, если $k < d$. Таким образом, прямая сумма всех слагаемых из (7-1) вида $K/(p^s)$ с $s \leq d$ инвариантно характеризуется как множество всех векторов, которые аннулируются умножением на p^d. Но тогда число слагаемых вида $K/(p^s)$ с фиксированным s есть логарифм по модулю p^s от числа элементов в фактор модуле $\dfrac{\ker \mu_{p^s}}{\ker \mu_{p^{s-1}}}$, где через $V \xrightarrow{\mu_\alpha} V$ мы на этот раз обозначаем гомоморфизм умножения на α в модуле V.

Теорема доказана.

□

2.6. Пример: конечно порождённые абелевы группы. При $K = \mathbb{Z}$ предыдущая теорема утверждает, что всякая конечно порождённая абелева группа изоморфна

$$\mathbb{Z}^n \oplus \bigoplus_\nu \frac{\mathbb{Z}}{p_\nu^{d_\nu}\mathbb{Z}} \,,$$

где $\mathfrak{p}_\nu$ – простые числа, и две группы такого вида изоморфны, если и только если совпадают числа n и наборы степеней $p_\nu^{d_\nu}$.

Если абелева группа задана в терминах образующих и соотношений, т. е. в виде K^N/R, где модуль соотношений $R \subset K^N$ также задан образующими соотношениями $(r_1, r_2, \ldots, r_k)$, то для определения её канонического разложения в прямую сумму циклических фактор-групп можно воспользоваться явными процедурами из доказательств предыдущих теорем, а именно, составить из вектор-столбцов r_i прямоугольную матрицу, элементарными преобразованиями строк и столбцов привести её к строгому диагональному виду, тогда числа $(m_1, m_2, \ldots, m_r)$, стоящие на диагонали, будут не чем иным как инвариантными множителями подмодуля соотношений R, и набор их элементарных делителей будет совпадать с набором знаменателей, участвующих в каноническом разложении (а n будет равно $N - r$),

Разумеется, на практике часто удаётся избежать полномасштабного вычисления по только что описанному алгоритму и найти базис $\mathbb{Z}$-модуля используя специфику его изначального определения.

2.6.1. Пример: базис в модуле целозначных многочленов. Целозначными называются такие многочлены из $\mathbb{Q}[x]$, которые принимают целые значения при целых значениях x. Поскольку сумма двух целозначных многочленов и целое кратное целозначного многочлена также будут целозначными, эти многочлены образуют $\mathbb{Z}$-модуль. Отметим, что коэффициенты целозначного многочлена вовсе не обязаны быть целыми, как показывает пример многочлена $T(x) = x(x+1)/2$, задающего треугольные числа. Мы собираемся доказать, что *многочлены*

$$b_i(x) = \frac{1}{i!}x(x-1)\ldots(x-i+1) \quad , \qquad i = 0, 1, 2, \ldots$$

(при $i = 0$ мы считаем $b_i(x) \equiv 1$) составляют базис модуля целозначных многочленов над $\mathbb{Z}$.

Для этого заметим прежде всего, что многочлены $b_i(x)$ составляют базис векторного пространства $\mathbb{Q}[x]$ над полем $\mathbb{Q}$.

Задача 7.15. Докажите это (ср. с зад.5.21).
Стало быть, любой многочлен g степени $\le n$ допускает разложение

$$g(x) = \sum_{i=0}^{n} \lambda_i b_i(x)$$

с рациональными коэффициентами λ_i. Покажем, что если $g(x)$ – целозначен, то эти коэффициенты обязаны быть целыми.

Для этого рассмотрим линейный гомоморфизм

$$\nabla \,:\, f(x) \longmapsto \nabla f(x) \stackrel{\text{def}}{=} f(x) - f(x-1)\ .$$

Он переводит целозначные многочлены в целозначные и действует на базисные многочлены $b_i(x) = \binom{x+i}{i}$ по правилу

$$\nabla b_i(x) = \binom{x+i}{i} - \binom{x+i-1}{i} = \binom{x+i-1}{i-1} = b_{i-1}(x)\ .$$

Поскольку $b_i(0) = \begin{cases} 1\ , & \text{при} \quad i=0 \\ 0\ , & \text{при} \quad i>0 \end{cases}$, мы заключам, что

$$\lambda_i = \underbrace{\nabla\nabla\cdots\nabla}_{i}\, g\,(0) \,\in\, \mathbb{Z}\ ,$$

что и требовалось.

Задача 7.16. Докажите, что многочлены

$$c_i^n(x) \stackrel{\text{def}}{=} \binom{x+i+n}{n} = \frac{1}{n!}(x+i)(x+i+11)...(x+i+n)\ ,$$

с $i = 0,\, 1,\, \dots,\, n$ составляют базис модуля целозначных многочленов степени $\le n$ над $\mathbb{Z}$.