ЛЕКЦИЯ 14

ЦИКЛИЧЕСКИЕ И СВОБОДНЫЕ МОДУЛИ

КОЛЬЦА ГЛАВНЫХ ИДЕАЛОВ

ТЕОРЕМА О СОГЛАСОВАННЫХ БАЗИСАХ

ТЕОРЕМА О СТРОЕНИИ

ЖОРДАНОВА ФОРМА

ЦИКЛИЧЕСКИЕ И СВОБОДНЫЕ МОДУЛИ

Пусть M — некоторый R-модуль.

Для любого подмножества $S \subset M$ множество линейных комбинаций

$$a_1 x_{i_1} + \dots a_m x_{i_m}, \quad a_1, \dots, a_m \in R, x_{i_1}, \dots, x_{i_m} \in S,$$

— это наименьший подмодуль в M, содержащий подмножество S.

Он называется *подмодулем, порожденным множеством* S, и обозначается через $\langle S \rangle$.

Если $\langle S \rangle = M$, то говорят, что модуль M порождается множеством S. Если множество S можно выбрать конечным, то говорят, что M *конечно порожден.*

Модуль, порожденный одинм элементом, называется *циклическим.*

Идеал

$$\operatorname{Ann} M = \{r \in R \mid rM = 0\}$$

называется *аннулятором* модуля M. Если $\operatorname{Ann} M \neq 0$, то модуль M называется *периодическим.*

Теорема 1. *Всякий циклический R-модуль M изоморфен модулю вида R/I, где I — левый идеал кольца R. Если кольцо R коммутативно, то идеал I совпадает с $\operatorname{Ann} M$ и тем самым определен модулем M однозначно.*

Доказательство. Пусть $M = \langle x \rangle$ — циклический R-модуль. Отображение

$$f : R \to M, \quad a \mapsto ax,$$

является гомомоорфизмом модулей, причем $\operatorname{Im} f = M$. По теореме о гомоморфизме $M \cong A/I$, где $I = \ker f$. Второе утверждение теоремы очевидно. □

Система $\{x_1, \ldots, x_n\}$ элементов модуля M называется *линейно независимой*, если $r_1x_1 + \cdots + r_nx_n = 0$ ($r_i \in R$) только при $r_1 = \cdots = r_n = 0$. Линейно независимая система порождающих называется *базисом*.

Конечно порожденный модуль, обладающий базисом, называется *свободным*. Свободный циклический модуль изоморфен R (как R-модуль).

Для конечно порожденных модулей над кольцами главных идеалов (коммутативными, без делителей нуля) можно построить теорию, вполне аналогичную теории конечно порожденных абелевых групп.

Начиная с этого момента мы будем считать, что R — кольцо главных идеалов.

КОЛЬЦА ГЛАВНЫХ ИДЕАЛОВ

Определение 1. Коммутативное кольцо без делителей нуля, в котором каждый идеал является главным, мы будем далее называть *кольцом главных идеалов* (КГИ).

Определение 2. Коммутативное кольцо R без делителей нуля (целостное кольцо), не являющееся полем, называется *евклидовым кольцом*, если существует функция

$$\Phi : R \setminus \{0\} \to \mathbb{Z}_+,$$

(называемая *нормой*), удовлетворяющая следующим условиям:

1) $\Phi(ab) \geq \Phi(a)$, причем равенство имеет место только тогда, когда элемент b обратим;

2) для любых $a, b \in R$, $b \neq 0$, существуют такие $q, r \in R$, что $a = bq + r$, и либо $r = 0$, либо $\Phi(r) < \Phi(b)$.

Условие 2) ознчает возможность “делить с остатком”. Однозначности не требуется.

Основными примерами евклидовых колец являются кольцо целых чисел $\mathbb{Z}$ и кольца многочленов над полями.

Существуют и другие евклидовы кольца.

Пример 1. Комплексные числа вида $c = a + b\mathbf{i}$, $a, b \in \mathbb{Z}$, называются *целыми гауссовыми числами*. Они образуют подкольцо в $\mathbb{C}$, обозначаемое через $\mathbb{Z}[\mathbf{i}]$. Кольцо $\mathbb{Z}[\mathbf{i}]$ является евклидовым относительно нормы

$$\Phi(c) = |c|^2 = a^2 + b^2.$$

В самом деле, очевидно, что $\Phi(cd) = \Phi(c)\Phi(d)$, при этом обратимые элементы кольца $\mathbb{Z}[\mathbf{i}]$ — это элементы с нормой 1, и только они. Отсюда следует выполнение условия 1).

Докажем возможность деления с остатком.

Пусть $c, d \in \mathbb{Z}[\mathbf{i}]$, $d \neq 0$. Рассмотрим целое гауссово число q, ближайшее (по расстоянию на комплексной плоскости) к c/d. Ясно, что

$$\left|\frac{c}{d} - q\right| \leq \frac{1}{\sqrt{2}}.$$

Положим $r = c - qd$. Тогда $c = qd + r$ и

$$\Phi(r) = |c - qd|^2 = |c/d - q|^2|d|^2 \leq 1/2\Phi(d) < \Phi(d).$$

Упражнение 1. Докажите, что кольцо рациональных чисел вида $2^{-n}m$ ($m \in \mathbb{Z}$, $n \in \mathbb{Z}_+$) является евклидовым.

Теорема 2. *Всякое евклидово кольцо является кольцом главных идеалов.*

Доказательство. Очевидно, что нулевой идеал является главным. Пусть I — ненулевой идеал кольца R, и пусть u — наименьший по норме ненулевой элемент идеала I. Остаток при делении на u любого элемента идеала I принадлежит идеалу I, следовательно, может быть только нулем. Это означает, что $I = (u)$. □

Упражнение 2. Существуют кольца главных идеалов, которые не являются ни полями, не евклидовыми кольцами. Докажите, что таковым является кольцо чисел вида $a + b\sqrt{-19}$, где $a, b \in \mathbb{Z}$ или $a, b \in \mathbb{Z} + 1/2$.

В кольце главных идеалов можно определить понятие наибольшего общего делителя двух (или более) элементов этого кольца.

Будем говорить, что a делит b, если $a \in \langle b \rangle$ (довольно естественное определение). Делители можно "сравнивать": будем говорить, что делитель d_1 больше делителя d_2, если идеал $\langle d_1 \rangle$ содержится в идеале $\langle d_2 \rangle$.

Очевидным образом тогда можно ввести понятие *наибольшего общего делителя*: это такой делитель элементов $a, b \in R$, который больше любого другого их общего делителя.

Теорема 3. *В кольце главных идеалов R для любых двух элементов x, y существует их наибольший общий делитель d, и он может быть представлен в виде $d = ax + by$, $a, b \in R$.*

Доказательство. Рассмотрим идеал

$$(x, y) = \{ax + by \mid a, b \in R\},$$

порожденный элементами x и y. Существует такой элемент $d \in R$, что $(x, y) = (d)$. Это и будет наибольший общий делитель элементов x и y. По самому построению он представляется в виде $d = ax + by$. □

Теорема 4. *В кольце главных идеалов R каждый элемент $a \in R$ можно разложить в произведение $a = p_1 \dots p_n$ простых сомножителей.*

Доказательство. Ясно, что если a не является простым, то его можно разложить в произведение $a = a_1 a_2$ двух необратимых сомножителей, а далее пытаться продолжить процесс, пока все сомножители на станут простыми.

Это не будет возможно, если процесс можно продолжать бесконечно, т.е. существуют такие последовательности $a_1, a_2, \dots$ и $b_1, b_2, \dots$, что

$$a = a_1 a_2 \dots a_i \cdot b_i$$

для всех $i = 1, 2, \dots$, причем все сомножители a_i необратимы, а все сомножители b_i не просты.

Значит, в последовательности (b_n) каждый b_i делится на b_{i+1}, но при этом b_{i+1} не делится на b_i. Это в точности означает, что идеал (b_{i+1}) строго содержит идеал (b_i) для любого $i \in \mathbb{N}$, т.е. мы имеем беконечную цепочку строго расширяющихся идеалов, все они являются собственными.

Рассмотрев объединение этой цепочки, мы получим (собственный) идеал B, содержащий все идеалы (b_i). Так как R — кольцо главных идеалов, то этот идеал B также является главным. Пусть он порожден элементом d. Но тогда элемент d лежит в почти всех идеалах (b_i), т.е. они должны все совпадать с B, начиная с какого-то момента.

Противоречие с предположением. □

Можно также доказать и единственность разложения на простые множители в кольце главных идеалов.

Лемма 1. *В кольце главных идеалов R если элемент a не делится на простой элемент p, то они взаимно просты (т.е. $(a, p) = 1$).*

Доказательство. Идеал (p) является максимальным, поэтому любое его расширение (которым является идеал (a, p)) совпадает со всем кольцом R и содержит единицу. □

Лемма 2. *Если в кольце главных идеалов R произведение ab делится на простой элемент $p \in R$, то либо a делится на p, либо b делится на p.*

Доказательство. Пусть ab делится на p, но a не делится на p. Тогда $(a, p) = 1$ и

$$1 = ax + py, \quad x, y \in R.$$

Домножим это равенство на b:

$$b = abx + pby.$$

Правая часть этого равенства делится на p, так как ab делится на p.

Значит, b делится на p. □

Отсюда очевидным образом следует теорема о единственности разложения на простые множители в кольцах главных идеалов:

Теорема 5. *В кольце главных идеалов R разложение элемента на простые множители единственно в следующем смысле.*

Если

$$a = p_1 \dots p_m = q_1 \dots q_n$$

разложение элемента a на простые множители двумя способами, то $m = n$ и элементы $q_1, \dots, q_n$ можно так перенумеровать, чтобы $p_1 = \alpha_1 q_1$, $\dots$, $p_n = \alpha_n q_n$, где $\alpha_1, \dots, \alpha_n$ — обратимые элементы кольца R.

Теорема 6. *Все базисы свободного R-модуля L содержат одно и то же число элементов.*

Доказательство. Пусть p — какой-либо простой элемент кольца R (т.е. такой элемент, который нельзя разложить на два необратимых множителя). Тогда идеал (p) максимален, так как если он строго содержится в идеале (q) (а ведь каждый идеал является главным), то $p = qr$, r также необратим (иначе идеалы (p) и (q) совпадали бы).

Значит, $R/(p)$ — поле, а L/pl — векторное пространство над этим полем. Если $\{e_!, \ldots, e_n\}$ — базис модуля L, то $\{[e_1], \ldots, [e_n]\}$ (где $[x]$ означает класс $x + pL$) — базис этого векторного пространства. Следовательно, $n = \dim L/pL$, а для векторного пространства это число определяется однозначно.

□

Число элементов базиса свободного модуля L называется его рангом и обозначается через $\operatorname{rk} L$.

Теорема 7. *Пусть u и v — взаимно простые элементы кольца главных идеалов R. Тогда*

$$R/(uv) \cong R/(u) \oplus R/(v).$$

Доказательство. Отображение

$$f : R \to R/(u) \oplus R/(v), \qquad a \mapsto (a + (v), a + (u)),$$

является гомоморфизмом колец. Пусть a и b — такие элементы кольца R, что $au + bv = 1$. Тогда

$$f(bv) = (1 + (u), 0 + (v)), \quad f(au) = (0 + (u), 1 + (v)),$$

откуда следует, что гомоморфизм f сюръективен. Очевидно, что $\ker f = (uv)$. Это и дает нужным нам изоморфизм. □

ТЕОРЕМА О СОГЛАСОВАННЫХ БАЗИСАХ

Теорема 8. *Всякий подмодуль N свободного R-модуля L ранга n является свободным R-модулем ранга $m \le n$, причем существует такой базис $\{e_1, \dots, e_n\}$ модуля L и такие (ненулевые) элементы $u_1, \dots, u_m \in R$, что $\{u_1 e_1, \dots, u_m e_m\}$ — базис подмодуля N и $u_1 | u_{i+1}$ при $i = 1, \dots, m-1$.*

Доказательство. Первое утверждение теоремы при $n = 1$ — это определение кольца главных идеалов (Всякий подмодуль кольца R, т.е. всякий идеал кольца R является свободным ранга не выше одного, т.е. порожден одним элементом, т.е. главным).

При $n > 1$ утверждение доказывается точно так же, как и для $R = \mathbb{Z}$.

Напомним доказательство для удобства.

Пусть $n > 1$ и $\{e_1, \dots, e_n\}$ — базис модуля L. Рассмотрим подмодуль $L_1 = \langle e_1, \dots e_{n-1} \rangle \subset L$. Это свободный R-модуль ранга $n - 1$.

По предположению индукции модуль $N_1 = N \cap L_1$ является свободным R-модулем ранга $m \le n - 1$. Пусть $\{f_1, \dots, f_m\}$ — его базис.

Рассмотрим последние координаты всех элементов из N в базисе $\{e_1, \dots, e_n\}$ модуля L.

Они образуют идеал в кольце R, который по определению кольца главных идеалов имеет вид Ra, $a \in R$. Если $a = 0$, то $N = N_1$ и все доказано.

Если $a \neq 0$, то пусть f_{m+1} — какой-нибудь элемент из N, последняя координата которого равна a. Тогда $\{f_1, \dots, f_m, f_{m+1}$ — базис модуля N, и также все доказано.

Таким образом, первая часть теоремы (подмодуль свободного модуля свободен) доказана.

Доказательство второго утверждения, как и для $R = \mathbb{Z}$, основано на приведении матрицы C перехода от базиса модуля L к базису модуля N к диагональному виду с помощью элементарных преобразований этих базисов.

В случае, когда R — евклидово кольцо, элементарными преобразованиями системы элементов R-модуля называются:

1) прибавление к одному элементу другого, умноженного на элемент кольца R;

2) перестановка двух элементов;

3) умножение одного элемента на обратимый элемент кольца R.

Приведение матрицы C к диагональному виду в этом случае может быть осуществлено так же, как и для абелевых групп, с той оговоркой, что минимизировать надо не сам элемент c_{11} (что не имеет смысла), а его норму.

В общем случае понятие элементарного преобразования следует расширить. Назовем *квазиэлементарным преобразованием* системы элементов $\{x_1, \ldots, x_p\}$ какого-либо R-модуля замену двух элементов x_i и x_j их линейными комбинациями

$$ax_i + bx_j, \qquad cx_i + dx_j,$$

где $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ — обратимая матрица с элементами из кольца R (обратимость матрицы равносильна обратимости ее определителя).

Ясно, что преобразование, обратное к квазиэлементарному, также квазиэлементарно, и что элементарные преобразования являются квазиэлементарными.

Любую пару элементов $\{x, y\}$ самого кольца R с помошью квазиэлементарного преобразования можно привести к виду $\{d, 0\}$, где $d = (x, y)$.

В самом деле, существуют такие $a, b \in R$, что $ax + by = d$.

Рассмотрим матрицу

$$\begin{pmatrix} a & b \\ -y/d & x/d \end{pmatrix}.$$

Она обратима, так как ее определитель равен 1. Соответствующее квазиэлементарное преобразование переводит $\{x, y\}$ в $\{d, 0\}$.

Следовательно, если в каком-то столбце и какой-то строке матрицы C имеются элементы x, y, то с помощью квазиэлементарного преобразования строк или столбцов из них можно получить элементы $d, 0$.

Такого рода преобразований достаточно, чтобы, следуя алгоритмы как в абелевых группах, привести матрицу C к искомому диагональному виду. □

ТЕОРЕМА О СТРОЕНИИ

Изучим теперь строение произвольных конечно порожденных R-модулей.

Всякий нетривиальный циклический R-модуль изоморфен либо R, либо $R/(u)$, где u — необратимый ненулевой элемент.

Если $(u, v) = 1$, то изоморфизм колец

$$R/(uv) \cong R/(u) \oplus R/(v),$$

построенный нами раньше, является, как легко понять и изоморфизмом R-модулей.

Следовательно, если $u = p_1^{k_1} \dots p_s^{k_s}$ — разложение элемента u на простые множители, то имеет место изоморфизм R-модулей

$$R/(u) \cong R/(p_1^{k_1}) \oplus \dots \oplus R/(p_s^{k_s}).$$

Определение 3. Конечно порожденный R-модуль M, аннулятор которого содержит степень простого элемента $p \in R$, называется *примарным* или *p-примарным*.

Таким образом, всякий периодический циклический R-модуль разлагается в прямую сумму примарных циклических подмодулей.

Теорема 9. *Всякий конечно порожденный R-модуль M разлагается в прямую сумму примарных и свободных циклических подмодулей, причем набор аннуляторов этих подмодулей определяется однозначно.*

Доказательство. Пусть $\{x_1, \ldots, x_n\}$ — система порождающих модуля M. Рассмотрим гомоморфизм

$$\varphi : R^n \to M, \qquad (r_1, \ldots, r_n) \mapsto r_1 x_1 + \cdots + r_n x_n.$$

По теореме о гомоморфизме для модулей

$$M \cong R^n / \ker \varphi = R^n / N.$$

Модуль N является подмодулем свободного конечно порожденного модуля M, поэтому по предыдущей теореме он является свободным, при этом существует такой базис $\{e_1, \ldots, e_n\}$ модуля M и такие элементы $r_1, \ldots, r_m$ $(m \leq n)$ кольца R, что $\{r_1 e_1, \ldots, r_m e_m\}$ — базис модуля N, при этом $r_i | r_{i+1}$.

Рассмотрим гомоморфизм

$$\psi : R^n \to R/(u_1) \oplus \cdots \oplus R/(u_m) \oplus R \oplus \cdots \oplus R,$$

при котором

$$u_1 e_1 + \cdots + u_n e_n \mapsto ([u_1]_{r_1}, \ldots, [u_m]_{r_m}, u_{m+1}, \ldots, u_n).$$

Очевидно, что $\ker \psi = N$. Отсюда следует, что

$$M \cong R/(u_1) \oplus \cdots \oplus R/(u_m) \oplus R \oplus \cdots \oplus R.$$

Таким образом, мы разложили модуль M в конечную сумму свободных циклических модулей и периодических циклических модулей. Каждый периодический циклический модуль, как мы показывали выше, раскладывается в сумму примарных циклических модулей.

Таким образом, мы доказали существование, осталась единственность.

Для доказательства единственности рассмотрим подмодуль кручения

$$\operatorname{Tor} M := \{x \in M \mid ax = 0 \text{ для некоторого } a \in R, a \neq 0\}$$

и, для каждого простого элемента $p \in R$, подмодуль p-кручения

$$\operatorname{Tor}_p M := \{x \in M \mid p^k x = 0 \text{ для некоторого } k \in \mathbb{Z}_+\}.$$

Как и для абелевых групп, доказывается, что $M/\operatorname{Tor} M$ — это модуль без кручения, который оказывается свободным (а в этом случае мы знаем, что количество свободных циклических слагаемых определяется однозначно).

Единственность разложения примарного модуля в прямую сумму примарных циклических подмодулей доказывается по индукции, как и для абелевых групп.

Однако соображение, использовавшее порядок группы, тут не работает.

Вместо него можно применить следующее соображение: если модуль M разложен в прямую сумму p-примарных циклических подмодулей, то число слагаемых равно размерности подмодуля $\{x \in M \mid px = 0\}$ как векторного пространства над полем $R/(p)$. □

ЖОРДАНОВА ФОРМА

В случае $R = \mathbb{F}[t]$ ($\mathbb{F}$ — поле) доказанная теорема описывает строение линейных операторов в векторных пространствах над полем $\mathbb{F}$.

Условие конечной порожденности уж точно будет выполнено, если векторное пространство конечномерно. Более того, в этом случае отсутствуют свободные слагаемые, так как свободный циклический модуль над $\mathbb{F}[t]$ имеет бесконечную размерность над $\mathbb{F}$.

Результат выглядит особенно просто, если поле $\mathbb{F}$ алгебраически замкнуто.

Действительно, в этом случае простыми множителями являются одночлены $(t - \lambda)$, примарными множителями — многочлены $(t - \lambda)^m$, а примарные циклические модули имеют вид

$$\mathbb{F}[t]/((t - \lambda)^m), \qquad \lambda \in \mathbb{F}.$$

Такой модуль является m-мерным векторным пространством над $\mathbb{F}$ с базисом

$$\{[(t-\lambda)^{m-1}], \ldots, [t-\lambda], [1]\},$$

где $[f(t)]$ обозначает класс $f(t) + ((t-\lambda)^m)$.

Оператор умножения на t записывается в этом базисе жордановой клеткой

$$J(\lambda) = \begin{pmatrix} \lambda & 1 & 0 & \ldots & 0 \\ 0 & \lambda & 1 & \ldots & 0 \\ & \ddots & \ddots & \ddots & \vdots \\ & & & \lambda & 1 \\ & & & 0 & \lambda \end{pmatrix}.$$

Из всех предыдущих расссуждений вытекает

Теорема 10 (теорема о жордановой нормальной форме). *Всякий линейных оператор в конечномерном векторном пространстве над алгебраически замкнутым полем в некотором базисе записывается жордановой матрицей, причем эта матрица определена однозначно с точностью до перестановки клеток.*

Упражнение 3. Получите канонический вид матрицы линейного оператора над полем вещественных чисел.