

ЛЕКЦИЯ 16

ЦИКЛИЧЕСКИЕ И СВОБОДНЫЕ МОДУЛИ

СВОЙСТВА КГИ

ОДНОЗНАЧНОСТЬ РАНГА СВОБОДНОГО МОДУЛЯ НАД КГИ

ЦИКЛИЧЕСКИЕ И СВОБОДНЫЕ МОДУЛИ

Пусть M — некоторый R -модуль.

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

$$a_1x_{i_1} + \dots + a_mx_{i_m}, \quad a_1, \dots, a_m \in R, x_{i_1}, \dots, x_{i_m} \in S,$$

— 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 одним элементом, называется *циклическим*.

Идеал

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

называется *аннулятором* модуля M . Если $\text{Ann } M \neq 0$, 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 $\text{Ann } M$ и тем самым определен модулем M однозначно.*

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

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

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

Система $\{x_1, \dots, x_n\}$ элементов модуля M называется *линейно независимой*, если $r_1x_1 + \dots + r_nx_n = 0$ ($r_i \in R$) только при $r_1 = \dots = r_n = 0$. 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 R без делителей нуля (целостное кольцо), не являющееся полем, называется *евклидовым кольцом*, если существует функция

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

(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) означает 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 $I = (u)$. \square

УПРАЖНЕНИЕ 2 (СЛОЖНОЕ). 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 $b \in \langle a \rangle$ (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 $d = ax + by$. \square

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 не 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 бесконечную 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. \square

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 $\{e_1, \dots, e_n\}$ — базис модуля L , то $\{[e_1], \dots, [e_n]\}$ (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 $\text{rk } L$.

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

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

Доказательство. Отображение

$$f : R \rightarrow R/(u) \oplus R/(v), \quad a \mapsto (a + (u), a + (v)),$$

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. \square