ЛЕКЦИЯ 15

ОПРЕДЕЛЕНИЕ И ПРИМЕРЫ МОДУЛЕЙ

ЦИКЛИЧЕСКИЕ И СВОБОДНЫЕ МОДУЛИ

КОЛЬЦА ГЛАВНЫХ ИДЕАЛОВ

ОПРЕДЕЛЕНИЕ И ПРИМЕРЫ МОДУЛЕЙ

На абелевы группы можно смотреть как на “ векторные пространства над $\mathbb{Z}$”. Аналогично можно определить и векторные пространства над более общими кольцами. Они называются *модулями*.

Пусть R — ассоциативное кольцо с единицей.

Определение 1. (Левым) R-модулем (или модулем над R) называется аддитивная абелева группа M с операцией умножения (слева) на элементы кольца R, обладающая следующими свойствами:

1) $a(x+y) = ax+ay$ для любых $a \in R$ и $x, y \in M$;
2) $(a+b)x = ax+bx$ для любых $a, b \in R$ и $x \in M$;
3) $(ab)x = a(bx)$ для любых $a, b \in R$ и $x \in M$;
4) $1x = x$ для любого $x \in M$.

В частности, модули над полем — это векторные пространства, модули над кольцом целых чисел — это в точности абелевы группы.

Приведем другие важные примеры модулей.

Пример 1. Модули над кольцом многочленов $\mathbb{F}[x]$ — это векторные пространства с линейным оператором, играющим роль умножения на x.

Пример 2. Кольцо R всегда является модулем над самим собой (просто умножение кольца на элементы этого же кольца).

Пример 3. Всякое линейное пространство V является модулем над кольцом своих линейных операторов $\operatorname{End} V$.

ПОДМОДУЛИ И ФАКТОР-МОДУЛИ

Подмножество N модуля M называется *подмодулем*, если оно замкнуто относительно сложения и умножения на элементы кольца R. Всякий подмодуль является модулем относительно тех же операций.

Пример 4. Подмодуль абелевой группы — это просто любая ее подгруппа.

Пример 5. Подмодуль $\mathbb{F}[x]$-модуля из первого примеры — это подпространство, инвариантное относительно оператора умножения на x.

Пример 6. Подмодуль кольца R, рассматирваемого как модуль над самим собой, — это любой его левый идеал.

Внутренняя и внешняя прямые суммы модулей определяются точно так же, как и для абелевых групп (просто групп, векторных пространств).

Перейдем теперь к понятию фактор-модуля.

Пусть M — модуль, N — его подмодуль. Будем считать два элемента $m_1, m_2 \in M$ сравнимыми по модулю N, если $m_1 - m_2 \in N$. Ясно, что в этом случае отношение сравнимости является отношением эквивалентности и модуль M разбивается на смежные классы по подмодулю N вида $m + N$.

Ясно также, что M/N — абелева группа.

Операцию умножения на элементы кольца введем естественным образом:

$$a(m + N) = am + N.$$

Очевидно проверяется, что операция корректна и превращает фактор-группу M/N в R-модуль.

Этот модуль мы будем просто обозначать через M/N и называть *фактор-модулем* M по N.

В частности, таким образом определялось в прошлом семестре фактор-пространство V/U. Фактор-модули $\mathbb{Z}$-модулей — это то же, что и фактор-группы абелевых групп.

ТЕОРЕМА О ГОМОМОРФИЗМЕ ДЛЯ МОДУЛЕЙ

Отображение f модуля M в модуль N (над тем же кольцом) называется гомоморфизмом модулей, если

$$f(x+y) = f(x) + f(y),$$
$$f(ax) = af(x).$$

Обратимый гомоморфизм называет изоморфизмом.

Если $f : M \to N$ — какой-либо гомоморфизм модулей, то его образ

$$\operatorname{Im} f = \{f(x) \mid x \in M\} \subset N$$

— подмодуль модуля N, а его ядро

$$\ker f = \{x \in M \mid f(x) = 0\} \subset M$$

— подмодуль модуля M.

Для любого подмодуля $N \subset M$ определяется *канонический гомоморфизм*

$$\pi : M \to M/N, \quad x \mapsto x + N,$$

ядром которого является N.

Теорема 1 (о гомоморфизме для модулей). *Пусть* $f : M \to N$ — *гомоморфизм* R*-модулей. Тогда*

$$\operatorname{Im} f \cong M/\ker f.$$

Более точно, имеется изоморфизм

$$\varphi : \operatorname{Im} f \to M/\ker f,$$

ставящий в соответствие каждому элементу $y = f(x) \in \operatorname{Im} f$ *смежный класс* $\pi(x) = x + \ker f$.

Доказательство. Ясно, что отображение φ является изоморфизмом аддитивных групп. Остается только проверить, что оно перестановочно с умножением на элементы кольца R.

Пусть $f(x) = y$. Тогда $f(ax) = ay$ при $a \in R$ и

$$\varphi(ay) = \pi(ax) = a\pi(x) = a\varphi(x).$$

□

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 одним 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 2. *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 2. Коммутативное кольцо без делителей нуля, в котором каждый идеал является главным, мы будем далее называть *кольцом главных идеалов* (КГИ).

Определение 3. 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) $\Phi(ab) \geqslant \Phi(a)$, 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 7. 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

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

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

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

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

Теорема 3. *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 (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 4. *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 5. *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 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. $\square$