ЛЕКЦИЯ 15

ТЕОРЕМА О ГОМОМОРФИЗМЕ ДЛЯ КОЛЕЦ

МАКСИМАЛЬНЫЕ ИДЕАЛЫ В КОЛЬЦАХ

КОЛЬЦА ГЛАВНЫХ ИДЕАЛОВ

ОПРЕДЕЛЕНИЕ И ПРИМЕРЫ МОДУЛЕЙ

ФАКТОР-МОДУЛИ И ТЕОРЕМА О ГОМОМОРФИЗМЕ ДЛЯ МОДУЛЕЙ

ТЕОРЕМА О ГОМОМОРФИЗМЕ ДЛЯ КОЛЕЦ

Отображение f кольца R в кольцо S называется *гомоморфизмом*, если оно сохраняет операции, т.е.

$$f(x+y) = f(x) + f(y),$$
$$f(xy) = f(x)f(y)$$

для любых $x, y \in R$. Образ $\operatorname{Im} f$ гомоморфизма f является подкольцом кольца S, а ядро

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

— идеалом кольца R.

Согласно определению фактор-кольца R/I отображение

$$\pi : R \to R/I, \quad r \mapsto r + I,$$

является гомоморфизмом. Оно называется *каноническим гомоморфизмом* кольца R на фактор-кольцо R/I. Его ядром, очевидно, является идеал I.

Имеет место следующая *теорема о гомоморфизме для колец*, аналогичная теореме о гомоморфизме для групп.

Теорема 1. *Пусть $f : R \to S$ гомоморфизм колец. Тогда*

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

Более точно, имеется изоморфизм

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

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

Доказательство. Благодаря теореме о гомоморфизме для групп мы уже знаем, что отображение φ является изоморфизмом аддитивных групп.

Остается только проверить, что оно сохраняет операцию умножения. Пусть $f(x) = u$, $f(y) = v$. Тогда $f(xy) = uv$ и

$$\varphi(uv) = \pi(xy) = \pi(x)\pi(y) = \varphi(u)\varphi(v).$$

□

МАКСИМАЛЬНЫЕ ИДЕАЛЫ В КОЛЬЦАХ

Для того, чтобы доказывать существование максимального идеала в кольце (определение — ниже), нам потребуется принять в качестве аксиомы так называемую *аксиому выбора*, а точнее, *лемму Цорна*, которая ей эквивалентна.

АКСИОМА ВЫБОРА. *Если X_i — непустое множество для каждого $i \in I$, то декартово произведение $\prod_{i\in I} X_i$ непусто.*

Эквивалентной формулировкой аксиомы выбора является следующая:

ЛЕММА ЦОРНА. Пусть X — непустая совокупность множеств, замкнутая относительно объединений непустых цепей *(*т.е. если $0 \neq Y \subset X$ и Y — цепь, то $\cup Y \in X$*);* тогда X обладает максимальным элементом, т.е. таким элементом $x \in X$, что из $x \subset y \in X$ следует $x = y$.

Еще одной эквивалентной формулировкой аксиомы выбора является следующий

Принцип вполне-упорядоченности Каждое множество может быть вполне упорядочено.

Упражнение 1. Докажите, что у любого линейного пространства есть базис.

Теперь мы можем ввести понятие максимального идеала.

Определение 1. Идеал I кольца R называется *максимальным*, если он является максимальным по включению среди всех собственных идеалов кольца R.

Теорема 2. *В любом ассоциативном кольце R с единицей существует (возможно, не единственный), максимальный идеал I.*

Доказательство. Для доказательства теоремы нам понадобится следующее (очевидное) утверждение:

Идеал I кольца R тогда и только тогда является собственным, когда он не содержит единицы.

Теперь перейдем к доказательству теоремы.

Рассмотрим множество всех собственных идеалов кольца R (оно непусто, так как содержит нулевой идеал) с отношением порядка по включению.

Если в этом множестве есть некоторая линейно упорядоченная цепь идеалов, то она состоит из вложенных друг в друга идеалов. Взяв ее объединение, мы снова получим собственный идеал, так как объединение не содержит единицы.

Значит, множество собственных идеалов удовлетворяет условию леммы Цорна, т.е. обладает некоторым максимальным элементом — максимальным идеалом I. □

Упражнение 2. Будет ли верно условие теоремы, если кольцо R было кольцом без единицы?

Теорема 3. *Для коммутативного кольца R с единицей фактор-кольцо R/I тогда и только является полем, когда идеал I — максимальный.*

Доказательство. Сначала пусть идеал I — максимальный. Рассмотрим некоторый ненулевой элемент фактор-кольца R/I — $r + I$, $r \notin I$.

Рассмотрим главный идеал $\langle r \rangle = rR$. Ясно, что он не содержится целиком в идеале I.

Теперь рассмотрим множество

$$J = \{ra + x \mid a \in R, x \in I\}.$$

Это множество является идеалом (простая проверка), причем сторого содержащим идеал I. Значит, $J = R$, так как идеал I максимален.

В том числе, единица представляется в виде $1 = ra + x$, где $a \in R$, $x \in I$. Получается, что класс элемента a обратен к классу элемента r кольце R/I, то есть это кольцо является полем.

Пусть, напротив, мы знаем, что кольцо R/I является полем, но идеал I — не максимальный. Тогда он содержится в некотором собственном идеале J кольца R. Рассмотрим некоторый $r \in J \setminus I$. Видно, что идеал $\langle r, I \rangle$ содержится в идеале J, то есть не содержит единицу кольца. Это означает, что класс элемента r в фактор-кольце R/I необратим. Противоречие. □

Упражнение 3. Каким свойством обладает фактор-кольцо R/I для максимального идеала I, если R не обязательно коммутативно?

Пример 1. Максимальным идеалом в поле является нулевой идеал.

Максимальными идеалами в кольце целых чисел являются идеалы $p\mathbb{Z}$, где p — простое.

Максимальными идеалами в кольце многочленов $\mathbb{F}[x]$ надо полем являются идеалы, порожденные неприводимыми многочленами.

Максимальными идеалами в кольце $\mathbb{Z}_n$ являются идеалы, порожденные простыми числами, делящими n.

Упражнение 4. Докажите, что максимальными идеалами в кольце матриц $\mathbf{M}_n(R)$ над кольцом R являются кольца матриц $\mathbf{M}_n(I)$ над максимальными идеалами I кольца R.

Пример 2. В кольце рядов над полем $\mathbb{F}[[x]]$ единственным максимальным идеалом является идеал $\langle x \rangle$.

Кольца с единственным максимальным идеалом называются *локальными* (примеры: поля, кольца рядов над полями, кольца $\mathbb{Z}_{p^n}$).

Пример 3. В прямой сумме колец

$$R_1 \oplus R_2 \oplus \cdots \oplus R_n$$

максимальными являются идеалы

$$R_1 \oplus \cdots \oplus R_{i-1} \oplus I_i \oplus R_{i+1} \oplus \cdots \oplus R_n,$$

где I_i — максимальный идеал кольца R_i.

КОЛЬЦА ГЛАВНЫХ ИДЕАЛОВ

Определение 2. Идеал I кольца R называется *главным*, если он порождается одним элементом $a \in R$ (обозначение: $I = (a)$).

Заметим, что для коммутативного кольца R с единицей

$$(a) = aR = \{ar \mid r \in R\},$$

если в кольце нет единицы, то

$$(a) = aR \cup \{a\}.$$

Если кольцо R с единицей некоммутативно, то главный идеал устроен сложнее:

$$(a) = \left\{ \sum_{i=1}^{t} r_i a s_i \mid t \in \mathbb{Z}_+, r_i, s_i \in R \right\}.$$

Определение 3. Коммутативное кольцо без делителей нуля, в котором каждый идеал является главным, мы будем далее называть *кольцом главных идеалов* (КГИ).

Очевидно, что кольцо целых чисел $\mathbb{Z}$ является кольцом главных идеалов, также это очевидно про поля.

Теперь покажем, что кольцо многочленов над полем $R = \mathbb{F}[x]$ также является КГИ.

Действительно, если I — ненулевой идеал в R, то рассмотрим в нем ненулевой многочлен $p(x)$ наименьшей возможной степени. Очевидно, что $(p(x)) \subseteq I$. Пусть вложение строгое. Тогда в идеале I существует многочлен $g(x)$, который не делится на $p(x)$.

Разделим $g(x)$ на $p(x)$ с остатком:

$$g(x) = p(x)q(x)+r(x), \quad \deg r(x) < \deg p(x),\ r(x) \neq 0.$$

Тогда раз $p(x) \in I$, то $p(x)q(x) \in I$, $g(x) \in I$, откуда следует, что

$$r(x) = g(x) - p(x)q(x) \in I,$$

противоречие с выбором $p(x)$.

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

Пример 5. Кольцо R всегда является модулем над самим собой (просто умножение кольца на элементы этого же кольца).

Пример 6. 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 7. Подмодуль абелевой группы — это просто любая ее подгруппа.

Пример 8. Подмодуль $\mathbb{F}[x]$-модуля из первого примеры — это подпространство, инвариантное относительно оператора умножения на x.

Пример 9. 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 4 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

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

□