ЛЕКЦИЯ 13

ИДЕАЛЫ В КОЛЬЦАХ, ФАКТОР-КОЛЬЦА

ТЕОРЕМА О ГОМОМОРФИЗМЕ ДЛЯ КОЛЕЦ

МАКСИМАЛЬНЫЕ ИДЕАЛЫ

ОПРЕДЕЛЕНИЕ И ПРИМЕРЫ МОДУЛЕЙ

ПРИМЕРЫ ИДЕАЛОВ

3. Кольцо многочленов от одной переменной над полем является кольцом главных идеалов (доказательство полностью аналогично доказательству для целых чисел). Кольцо многочленов над кольцом уже не обязательно является кольцом главных идеалов: в кольце $\mathbb{Z}[x]$ можно взять идеал, состоящих из многочленов с четным совободным членом. Докажите, что он не является главным.

Докажите также, что кольцо многочленов над полем от нескольких переменных тоже не является кольцом главным идеалов.

4. В кольце $\mathbb{Z}_n$ также все идеалы главные, так как вместе с любыми элементами m, k идеал всегда содержит их НОД.

5. Кольцо матриц $\mathbf{M}_n(R)$ — некоммутативное кольцо, поэтому в нем нужно различать односторонние и двухсторонние (настоящие) идеалы.

Примерами правых идеалов могут служить множества матриц, у которых некоторый набор строк — нулевой (для получения левого идеала строки нужно заменить на столбцы).

Если $R = \mathbb{K}$ — поле, то в кольце матриц над ним нет нетривиальных идеалов (кольцо $\mathbf{M}_n(\mathbb{K})$ *просто*).

Доказательство. Пусть $0 \neq A \in I$. Тогда в матрице A есть ненулевой элемент a_{ij}. Домножим матрицу A слева на $a_{ij}^{-1}E_{ii}$ и справа — на E_{jj}. В результате получим, что матрица E_{ij} также содержится в идеале I. Значит, любая матричная единица $E_{kl} = E_{ki}E_{ij}E_{jl}$ содержится в идеале I, откуда следует, что $I = \mathbf{M}_n(\mathbb{K})$. □

Упражнение 1. Пусть нам дан набор всех двухсторонних идеалов кольца R. Найдите тогда все идеалы кольца $\mathbf{M}_n(R)$.

6. Каждый идеал кольца рядов $\mathbb{K}[[x]]$ ($\mathbb{K}$ — поле) является главным идеалом, порожденным рядом x^n. Доказывается это очевидным образом, благодаря описанию обратимых элементов в данном кольце.

7. Если I_1 — идеал кольца R_1, I_2 — идеал кольца R_2, то $I_1 \oplus I_2$ — идеал кольца $R_1 \oplus R_2$.

Упражнение 2. Пусть R_1 и R_2 — кольца с единицами. Докажите обратное утверждение, т.е. что если I — идеал кольца $R_1 \oplus R_2$, то он имеет вид $I_1 \oplus I_2$, где $I_1 \lhd R_1$, $I_2 \lhd R_2$. Верно ли это утверждение для колец без единицы?

ФАКТОР-КОЛЬЦА

Определение 1. *Фактор-кольцом кольца R по его идеалу I* называется множество смежных классов $\{r + I \mid r \in R\}$ аддитивной группы кольца R по идеалу I с операциями

$$(r + I) + (s + I) = (r + s) + I \text{ и } (r + I)(s + I) = rs + I.$$

Докажем корретность этого определения. Действительно, корректность сложения очевидна. Для доказательства корректности умножения рассмотрим произведение $(r + I)(s + I) = rs + rI + Is + I^2$. По определению идеала $rI, Is, I^2 \subseteq I$, поэтому умножение не зависит от выбора представителей смежных классов.

То, что в результате получается кольцо, очевидно.

Ясно, что из кольца с единицей при факторизации получается кольцо с единицей (если только мы не рассматриваем фактор R/R); из коммутативного кольца при факторизации получается коммутативное кольцо.

1. Ясно, что фактор кольца $\mathbb{Z}$ по идеалу $n\mathbb{Z}$ — это кольцо $\mathbb{Z}_n$.

2. Факторкольцо $\mathbb{R}[x]$ по идеалу $\langle x^2+1\rangle$ изоморфно полю $\mathbb{C}$.

Вообще, факторкольцо кольца многочленов $\mathbb{K}[x]$ от одной переменной над полем является полем тогда и только тогда, когда соответствующий идеал порожден неприводимым многочленом.

Покажем это.

Действительно, пусть многочлен $f(x) \in \mathbb{K}[x]$ приводим. Тогда $f(x) = g(x)h(x)$. Значит, в факторкольце $\mathbb{K}[x]/\langle f(x)\rangle$ содержатся делители нуля — класс $g(x)$ и класс $h(x)$, поэтому данное фактор-кольцо не может являться полем.

Пусть теперь многочлен $f(x) \in \mathbb{K}[x]$ неприводим. Покажем, что (коммутативное) кольцо $R = \mathbb{K}[x]/\langle f(x)\rangle$ является полем.

Для этого достаточно показать, что любой ненулевой смежный класс обратим (то есть любой смежный класс, не содержащий многчлена $f(x)$, содержит обратный к нему смежный класс). Рассмотрим некоторый ненулевой смежный класс и выберем его представителя $g(x)$. Многочлены $f(x)$ и $g(x)$ взаимно просты, так как многочлен $f(x)$ неприводим. Значит (расширенный алгоритм Евклида), существуют такие многочлены $p(x)$ и $q(x)$, что

$$f(x)p(x) + f(x)g(x) = 1.$$

В фактор-кольце R это ровно и означает, что класс многочлена $p(x)$ обратен к классу многочлена $g(x)$.

Такое утверждение дает нам возможность строить новые поля. Самым прозрачным результатом является построение полей из p^n элементов, где n — некоторое (небольшое) натуральное число.

Например, поле из 9 элементов можно строить как

$$\mathbb{Z}_3[x]/\langle x^2+1\rangle;$$

поле из 8 элементов — как

$$\mathbb{Z}_2[x]/\langle x^3+x+1\rangle.$$

Теорема 1. *Если $\mathbb{F}$ — поле, $f(x)$ — неприводимый многочлен над ним, то $\mathbb{F}[x]/\langle f(x)\rangle$ — это поле, в которое естественно вкладывается поле $\mathbb{F}$, а многочлен $f(x)$ имеет в нем корень. Такое поле называется* простым расширением *поля $\mathbb{F}$.*

Доказательство. Действительно, мы уже выше доказали, что $\overline{\mathbb{F}} = \mathbb{F}[x]/\langle f(x)\rangle$ — поле. Поле $\mathbb{F}$ естественно вкладывается в поле $\overline{\mathbb{F}}$ как подполе из классов констант. Многочлен $f(x)$ имеет корень в $\overline{\mathbb{F}}$ — класс многочлена x. $\square$

3. Если профакторизовать кольцо многочленов от двух переменных $\mathbb{F}[x, y]$ по идеалу, порожденному многочленом x (все многочлены, одночлены которых содержат множитель x), то фактор-кольцо будет изоморфно кольцу многочленов от одной переменной $\mathbb{F}[y]$.

4. Рассмотрим кольцо матриц $\mathbf{M}_n(R)$ над кольцом R. Пусть I — идеал кольца R.

Тогда множество всех матриц

$$\mathbf{M}_n(I) = \{(a_{ij}) \mid a_{ij} \in I \forall i, j = 1, \ldots, n\}$$

является идеалом во всем кольце матриц.

Фактор-кольцо

$$\mathbf{M}_n(R)/\mathbf{M}_n(I)$$

изоморфно кольцу матриц

$$\mathbf{M}_n(R/I)$$

с коэффициентами из фактор-кольца R/I.

5. Факторизация кольца рядов $\mathbb{F}[[x]]$ по его идеалам дает нам:

— поле $\mathbb{F}$ для идеала $\langle x\rangle$;

— если в качестве идеала I взять идеал, порожденный многочленом (рядом) x^n, $n > 1$, то представителями смежных классов будут многочлены степени, меньшей n.

Такие многочлены складываются почленно.

При умножении двух многочленов мы сначала умножаем их нормальным образом, а потом удаляем все степени, не меньшие n.

Таким образом, фактор-кольцо — это то же самое, что и

$$\mathbb{F}[x]/\langle x^n \rangle.$$

Ясно, что в таком фактор-кольце появляются делители нуля.

6. Ясно, что если профакторизовать кольцо $R_1 \oplus R_2$ по прямому слагаемому (например, R_2), то в качестве фактор-кольца мы получим дополнительное прямое слагаемое (например, R_1).

Вообще при факторизации кольца

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

по идеалу вида

$$I_1 \oplus I_2 \oplus \cdots \oplus I_n$$

получается кольцо

$$R_1/I_1 \oplus \cdots \oplus R_n/I_n.$$

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 2. *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 3. Докажите, что у любого линейного пространства есть базис.

Теперь мы можем ввести понятие максимального идеала.

Определение 2. Идеал I кольца R называется *максимальным*, если он является максимальным по включению среди всех собственных идеалов кольца R.

Теорема 3. *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 4. Будет ли верно условие теоремы, если кольцо R было кольцом без единицы?

Теорема 4. *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 5. 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 6. 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.

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 3. (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, рассмативаемого 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 факторгруппу 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 факторпространство V/U. Фактор-модули $\mathbb{Z}$-модулей — это то же, что и факторгруппы 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 5 (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

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

□