ЛЕКЦИЯ 14

ИДЕАЛЫ В КОЛЬЦЕ МАТРИЦ

ФАКТОР-КОЛЬЦА

ИДЕАЛЫ В КОЛЬЦЕ МАТРИЦ

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 $\mathbf{M}_n(R)$.

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.

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 корректность 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. □

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

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

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

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