

ЛЕКЦИЯ 15

ТИПЫ КОЛЕЦ

ПОЛЯ

ХАРАКТЕРИСТИКА ПОЛЯ

ТИПЫ КОЛЕЦ

ОПРЕДЕЛЕНИЕ 1. Если $ab = 0$ при $a \neq 0$ и $b \neq 0$ в кольце R , то a называется *левым*, а b — *правым делителем нуля* (в коммутативных кольцах говорят просто о делителях нуля).

Сам ноль — это тривиальный делитель нуля. Если в кольце нет нетривиальных делителей нуля, то R называется *кольцом без делителей нуля*.

Коммутативное кольцо с единицей $1 \neq 0$ без делителей нуля называют *целостным кольцом* (или *областью целостности*).

Теорема 1. *Нетривиальное коммутативное кольцо R с единицей является целостным тогда и только тогда, когда в нем выполнен закон сокращения*

$$ab = ac, \quad a \neq 0 \implies b = c$$

для всех $a, b, c \in R$.

Доказательство. В самом деле, если в R имеет место закон сокращения, то из $ab = 0 = a \cdot 0$ следует $a = 0$ или $b = 0$.

Обратно, если R — область целостности, то

$$ab = ac, \quad a \neq 0 \implies a(b - c) = 0 \implies b - c = 0 \implies b = c.$$

□

В кольце R с единицей естественно рассматривать множество обратимых элементов.

Элемент a называется *обратимым*, если существует элемент a^{-1} , для которого $a^{-1}a = aa^{-1} = 1$.

Точнее, следовало бы говорить об элементах, обратимых справа или слева ($ab = 1$ или $ba = 1$), но в коммутативных кольцах, а также в кольцах без делителей нуля эти понятия совпадают.

Действительно, из

$$ab = 1$$

следует

$$aba = a,$$

откуда

$$a(ba - 1) = 0 \implies ba = 1,$$

если $a \neq 0$. Но мы знаем, что $a \neq 0$, так как $ab = 1$.

Нам известно, например, что в кольце матриц $M_n(\mathbb{R})$ обратимые элементы — это в точности матрицы с отличным от нуля определителем.

Обратимый элемент a не может быть делителем нуля:

$$ab = 0 \implies a^{-1}(ab) = 0 \implies b = 0.$$

Имеет место

Теорема 2. *Все обратимые элементы кольца R с единицей составляют группу $U(R) = R^*$ по умножению.*

Доказательство. В самом деле, так как множество $U(R)$ содержит единицу, из $a \in U(R)$ следует $a^{-1} \in U(R)$, ассоциативность по умножению выполнена автоматически, то нам нужно только убедиться в замкнутости множества $U(R)$ по умножению, то есть проверить, что произведение ab двух обратимых элементов обратимо.

Но это очевидно, так как

$$(ab)^{-1} = b^{-1}a^{-1}.$$

□

ПРИМЕР 1. В кольце целых чисел \mathbb{Z} обратимы только ± 1 .

В кольцах многочленов обратимыми могут быть только константы, так как у многочленов при умножении складываются степени. Соответственно, обратимыми элементами являются обратимые константы кольца R .

В кольце вычетов \mathbb{Z}_n обратимыми являются все остатки, взаимно простые с n . Таким образом, в данном кольце каждый элемент либо обратим, либо является делителем нуля.

Доказательство. Действительно, пусть имеется $k \in \{0, 1, \dots, n-1\}$ и мы хотим найти к нему обратный элемент. Это означает, что мы хотим найти такое $m \in \{0, 1, \dots, n-1\}$, что $km \equiv 1 \pmod{n}$, а более подробно — найти такие два числа m и $q \in \mathbb{Z}$, что

$$km + nq = 1.$$

Как мы уже замечали в первых лекциях, это возможно тогда и только тогда, когда числа k и n взаимно просты. □

В кольце рядов $R[[x]]$ обратимыми являются те и только те ряды, у которых обратим коэффициент при нулевой степени.

Доказательство. Пусть у ряда

$$z = \sum_{i=0}^{\infty} r_i x^i$$

r_0 необратим, но у него существует обратный ряд

$$z' = \sum_{j=0}^{\infty} s_j x^j.$$

Тогда, с одной стороны, и произведение должно быть равно ряду 1, с другой стороны, у произведения таких рядов коэффициент при нулевой степени x равен $r_0 s_0$, т.е. r_0 обратим.

Напротив, пусть у ряда

$$z = \sum_{i=0}^{\infty} r_i x^i$$

коэффициент r_0 обратим. Будем искать обратный ряд в общем виде

$$z' = \sum_{j=0}^{\infty} s_j x^j.$$

Тогда мы получим систему уравнений:

$$\left\{ \begin{array}{l} 1 = r_0 s_0, \\ 0 = r_0 s_1 + r_1 s_0, \\ 0 = r_0 s_2 + r_1 s_1 + r_2 s_0, \\ \dots = \dots, \\ 0 = r_0 s_n + r_1 s_{n-1} + \dots + r_{n-1} s_1 + r_n s_0, \\ \dots = \dots \end{array} \right.$$

Мы видим, что $s_0 = r_0^{-1}$ (существует и однозначно определено),
 $s_1 = (-r_1 s_0) r_0^{-1}$ (также существует и однозначно определено),
 $s_2 = (-r_1 s_1 - r_2 s_0) r_0^{-1}, \dots, s_n = (-r_1 s_{n-1} - \dots - r_n s_0) r_0^{-1}, \dots$

Таким образом, каждый коэффициент s_i однозначно определяется по коэффициентам r_j и предыдущим коэффициентам s_0, \dots, s_{i-1} .
Значит, ряд z был обратим. \square

В кольце функций обратимыми являются функциями, у которых все значения обратимы.

ПОЛЯ

ОПРЕДЕЛЕНИЕ 2. Ассоциативное кольцо с единицей называется *кольцом с делением* или *телом*, если любой ненулевой элемент в нем обратим.

Тело с коммутативным умножением называется *полем*.

Выражение ab^{-1} в случае поля записывают просто: $\frac{a}{b}$ или a/b .

Можно легко вывести из аксиом, что действия с дробями подчиняются следующим правилам:

$$\frac{a}{b} = \frac{c}{d} \iff ad = bc, \quad b, d \neq 0,$$

$$\frac{a}{b} + \frac{c}{d} = \frac{ac + bd}{bd}, \quad b, d \neq 0,$$

$$-\frac{a}{b} = \frac{-a}{b} = \frac{a}{-b}, \quad b \neq 0,$$

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}, \quad b, d \neq 0,$$

$$\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}, \quad a, b \neq 0.$$

Подполем F поля K называется подмножество $F \subset K$, которое само является полем (то есть замкнутое относительно сложения и умножения из K , содержащее 0 и 1, а также замкнутое относительно взятия противоположных и обратных элементов).

Например, поле рациональных чисел \mathbb{Q} — подполе поля действительных чисел \mathbb{R} .

Рассмотрим несколько примеров полей, помимо полей \mathbb{Q} и \mathbb{R} .

ПРИМЕР 2. Рассмотрим кольцо вычетов \mathbb{Z}_n и поймем, при каких условиях на число n оно является полем.

Мы уже доказывали, что элемент $k \in \{0, 1, \dots, n - 1\}$ обратим в кольце \mathbb{Z}_n тогда и только тогда, когда он взаимно прост с числом n .

Таким образом, кольцо \mathbb{Z}_n является полем в том и только том случае, когда все числа $k \in \{1, 2, \dots, n - 1\}$ взаимно просты с числом n .

Это, очевидно, выполняется тогда и только тогда, когда n простое.

Таким образом, для любого простого числа p кольцо вычетов \mathbb{Z}_p является полем.

ПРИМЕР 3. Мы, таким образом, научились сразу строить поля из двух и трех элементов.

Попробуем построить поле из четырех элементов.

Для этого надо построить таблицы сложения и умножения в этом поле и доказать все аксиомы.

Для начала мы знаем, что в нашем поле \mathbb{F}_4 (если оно существует) должны быть 0 и 1, поэтому остаются элементы a и b . Заметим, что $a + 1 \neq 1$ и $a + 1 \neq a$, поэтому либо $a + 1 = 0$, либо $a + 1 = b$.

Рассмотрим сначала случай, когда $a + 1 = 0$. Тогда

- $b + a = 0 \implies b = 1$, что невозможно;
- $b + a = b$ или $b + a = a$ также невозможно.

Значит, $b + a = 1$, то есть $b = 1 + 1$, $b + 1 = a$, так как никаких других вариантов не остается. Отсюда получается, что таблица сложения (и умножения) в данном поле совпадает с таблицей для кольца вычетов \mathbb{Z}_4 , которое полем не является.

Таким образом, должен выполняться второй вариант

$$a + 1 = b.$$

Значит, мы имеем дело с четырьмя элементами

$$0, 1, a, a + 1.$$

Если $1 + 1 = a$, то мы снова придем к кольцу \mathbb{Z}_4 , поэтому (так как другие суммы невозможны)

$$1 + 1 = 0.$$

Это означает, что

$$a + a = a(1 + 1) = 0,$$

то есть все элементы, сложенные с собой, дают ноль.

Таким образом, таблица сложения построена:

+	0	1	a	$a + 1$
0	0	1	a	$a + 1$
1	1	0	$a + 1$	a
a	a	$a + 1$	0	1
$a + 1$	$a + 1$	a	1	0

Построим теперь таблицу умножения, исходя из того, что знаем, как умножать 0 и 1 на все остальные элементы.

Остается узнать, как возвести в квадрат элементы a и $a + 1$ и как перемножить a и $a + 1$.

Ясно, что нам достаточно определить a^2 , так как остальные произведения посчитаются благодаря дистрибутивности.

Может быть либо $a^2 = 1$, либо $a^2 = a + 1$.

Если $a^2 = 1$, то $(a + 1)^2 = a^2 + a + a + 1 = 1 + 1 = 0$, что невозможно, поэтому $a^2 = a + 1$.

Вот таблица умножения:

\times	0	1	a	$a + 1$
0	0	0	0	0
1	0	1	a	$a + 1$
a	0	a	$a + 1$	1
$a + 1$	0	$a + 1$	1	a

Остается доказать, что полученная структура является полем.

Законы коммутативности сложения и умножения очевидны из симметричности таблички.

Наличие нуля и единицы тоже видно из таблицы.

По сложению все элементы противоположны сами себе, по умножению — 1 обратная сама себе, а a и $a + 1$ взаимно обратны.

Требуют проверки ассоциативность сложения и умножения и дистрибутивность.

Проверяются непосредственно.

ПРИМЕР 4. Рассмотрим подмножество в поле \mathbb{R} , состоящее из чисел вида

$$a + b\sqrt{2}, \quad a, b \in \mathbb{Q}.$$

Обозначим такое подмножество через $\mathbb{Q}[\sqrt{2}]$ и докажем, что оно является полем.

Действительно, если мы сложим два элемента описанного вида, то получим также элемент описанного вида:

$$(a_1 + b_1\sqrt{2}) + (a_2 + b_2\sqrt{2}) = (a_1 + a_2) + (b_1 + b_2)\sqrt{2}.$$

Понятно, что 0 представляется как $0 + 0\sqrt{2}$, противоположный к $a + b\sqrt{2}$ элемент имеет вид $(-a) + (-b)\sqrt{2}$.

Если перемножить два элемента из $\mathbb{Q}[\sqrt{2}]$, то получим

$$(a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2}) = (a_1a_2 + 2b_1b_2) + (a_1b_2 + a_2b_1)\sqrt{2},$$

то есть произведение элементов из множества $\mathbb{Q}[\sqrt{2}]$ лежит там же.

Самое основное — это для каждого ненулевого элемента

$$x = a + b\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$$

найти обратный элемент.

Рассмотрим

$$y = \frac{a - b\sqrt{2}}{a^2 - 2b^2}.$$

Посчитаем

$$(a + b\sqrt{2}) \cdot \frac{a - b\sqrt{2}}{a^2 - 2b^2} = \frac{a^2 - b^2\sqrt{2}^2}{a^2 - 2b^2} = 1,$$

в случае, когда элемент y определен. Нам необходимо, чтобы

$$a^2 - 2b^2 \neq 0,$$

однако существование таких $a, b \neq 0$, что $a^2 - 2b^2 = 0$, означало бы, что число 2 являлось бы полным квадратом рационального числа, что не так.

Таким образом, $\mathbb{Q}[\sqrt{2}]$ — поле, строго содержащее поле рациональных чисел.

ОПРЕДЕЛЕНИЕ 3. Поле K , строго содержащее подполе F , называется *расширением* поля F .

Поля K и K' называются *изоморфными*, если они между ними существует изоморфизм как между кольцами, то есть существует биективное отображение $\varphi : K \rightarrow K'$ такое, что

$$\forall a, b \in K \varphi(a + b) = \varphi(a) + \varphi(b) \text{ и } \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b).$$

ХАРАКТЕРИСТИКА ПОЛЯ

В поле всегда есть единица, не равная нулю. В аддитивной группе поля единица порождает циклическую подгруппу $\langle 1 \rangle = \{1, 1 + 1, 1 + 1 + 1, \dots\}$. Если данная группа конечна и содержит n элементов, то говорят, что характеристика поля равна n . Если циклическая группа $\langle 1 \rangle$ бесконечна, то говорят, что характеристика поля — нулевая.

ЗАМЕЧАНИЕ 1. Если у поля \mathbb{F} характеристика равна $n > 0$, то n — простое число.

Доказательство. Действительно, если $n = tk$, то в поле \mathbb{F} сумма t единиц (не равная нулю), умноженная на сумму k единиц (не равную нулю) равна нулю. Значит, в поле имеются делители нуля, что невозможно. Таким образом, положительная характеристика всегда является простым числом. \square

Если единица в поле имеет порядок p или бесконечный порядок, то такой же порядок имеет и любой ненулевой элемент:

$$a + a + \dots + a + a = a \cdot 1 + a \cdot 1 + \dots + a \cdot 1 = a(1 + 1 + \dots + 1).$$

Лемма 1. Если поле \mathbb{F} имеет характеристику 0, то в него естественно вложено подполе \mathbb{Q} рациональных чисел. Если поле \mathbb{F} имеет характеристику p , то в него естественно вложено подполе \mathbb{Z}_p .

Доказательство. Действительно, пусть характеристика поля \mathbb{F} равна нулю. Тогда целые числа можно вложить в поле \mathbb{F} следующим образом: если $n > 0$, то $n = 1 + 1 + \dots + 1$ (сумма n единиц), отображаем ее в сумму того же числа единиц; ноль отображаем в ноль, а противоположное к n — в противоположное к его образу.

Такое отображение, очевидно, будет гомоморфизмом. Если бы какой-то ненулевой элемент принадлежал ядру этого гомоморфизма, то сумма конечного числа единиц была бы равно нулю в поле \mathbb{F} , что невозможно. Значит, это вложение.

Таким образом, можно считать, что целые числа лежат в поле \mathbb{F} . Рациональные числа тогда лежат в нем как отношения целых к натуральным.

Если у поля \mathbb{F} характеристика равна p , то то же самое отображение имеет ядро — все целые числа, кратные p . Таким образом, образ \mathbb{Z} — это \mathbb{Z}_p , которое является полем. \square