Лекция 8

Кольца и поля

Определение 1. Кольцом $K =< M, +, \times >$ называется непустое множество $M \neq \emptyset$ с заданными на нем бинарными операциями сложение и умножение, причем выполняется:

1) по сложению кольцо – коммутативная группа;

2) по умножению – полугруппа;

3) дистрибутивность:

$$a \times (b + c) = (a \times b) + (a \times c)$$

$$(b + c) \times a = (b \times a) + (c \times a).$$

Кольцо с единицей – если существует единичный элемент по умножению $(e_{\times})$.

Если операция умножения коммутативна, то и кольцо называется коммутативным. В этом случае достаточно проверить выполнение одного закона дистрибутивности.

Подкольцом называется подмножество $K' \subseteq K$, являющееся подгруппой по сложению и замкнутое по умножению.

Определение 3. Подкольцо J кольца K называется **идеалом**, если $\forall j \in J$ и $\forall k \in K$ выполняется $jk \in J$ и $kj \in J$

$$JK \subseteq J, \ KJ \subseteq J.$$

Пример 1. $< \mathbb{Z}, +, \times >$ – коммутативное кольцо с $e_{\times} = 1$.

Подкольцо – $K' = \{3k\}, k \in \mathbb{Z}$. Подкольцо является идеалом.

Пример 2. $< M_{n \times n}, +, \times >$ кольцо матриц с элементами действительными числами – некоммутативное кольцо с единицей. Обратная матрица по умножению существует не всегда.

Для кольца матриц второго порядка

– подкольцо матриц второго порядка вида $\begin{pmatrix} a & b \\ 2b & a \end{pmatrix}$ идеалом не является, так как, например,

$$\begin{pmatrix} a & b \\ 2b & a \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}=\begin{pmatrix} a+b & a+b \\ 2b+a & 2b+a \end{pmatrix}: \; 2b+a \neq 2(a+b)$$

– подкольцо матриц вида $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$ – левый идеал, но правым идеалом не является. Под определение идеала не подходит.

Пример 3. $< F, +, \times >$ – кольцо функций одной переменной с операциями поэлементного сложения и умножения

$$f: X \to Y \qquad (f+g)(x) = f(x) + g(x) \qquad (f \cdot g)(x) = f(x) \cdot g(x)$$

Пример 4. $< C, +, \times >$ – кольцо классов вычетов по $mod\ 4$.

Напомним как определяются операции для классов вычетов по $mod\ n$.

$$C_k + C_l = C_{k+l} = C_r \qquad r = (k+l) mod\ n$$

$$C_k \cdot C_l = C_{kl} = C_r \qquad r = (kl) mod\ n$$

Рассмотрим кольцо классов вычетов по $mod\ 4$.

Для $n = 4 \Rightarrow\ 4$ класса:

$$C_0 = \{0; \pm 4; \pm 8; \dots\}$$

$$C_1 = \{1; 5; -3; 9; -7; \dots\}$$

$$C_2 = \{2; 6; -2; 10; -6; \dots\}$$

$$C_3 = \{3; 7; -1; 11; -5; \dots\}$$

1. По сложению получим коммутативную группу. $C_0 = e_+, {C_1}^{-1} = C_3, \; {C_2}^{-1} = C_2$

+	C_0	C_1	C_2	C_3
C_0	C_0	C_1	C_2	C_3
C_1	C_1	C_2	C_3	C_0
C_2	C_2	C_3	C_0	C_1
C_3	C_3	C_0	C_1	C_2

2. По умножению получим коммутативный моноид. $C_1 = e_{\times}$, $\nexists C_2^{-1}$.

$\times$	C_0	C_1	C_2	C_3
C_0	C_0	C_0	C_0	C_0
C_1	C_0	C_1	C_2	C_3
C_2	C_0	C_2	C_0	C_2
C_3	C_0	C_3	C_2	C_1

3. Дистрибутивность выполняется.

Вывод. Коммутативное кольцо с единицей.

Легко убедиться, что $J = \{C_0, C_2\} -$ подкольцо (без единицы). Подгруппа по сложению и замкнуто по умножению.

Является ли данное подкольцо идеалом?

В силу коммутативности умножения достаточно проверить одно включение: $JK \subseteq J$.

$$C_0 \times C_i = C_0, i = 1,2,3,4;$$

$$C_2 \times C_1 = C_2, \qquad C_2 \times C_2 = C_0, \qquad C_2 \times C_3 = C_2.$$

Подкольцо $J = \{C_0, C_2\}$ является идеалом.

Кольцо с делителями нуля.

Определение 4. Пусть в кольце $K \quad a \neq 0$ и $b \neq 0$, а $ab = 0$, тогда a – левый делитель нуля, b – правый делитель нуля, K – кольцо с делителями нуля.

Проанализируем, существуют ли делители нуля для колец, рассмотренных в примерах выше.

Пример 1. $K_{\mathbb{Z}} =< \mathbb{Z}, +, \times >$ – кольцо без делителей нуля.

Пример 2. Кольцо квадратных матриц порядка $n \geq 2$, $a_i \in \mathbb{R}$ – с делителями нуля.

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

$$\begin{pmatrix} a_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 0 \end{pmatrix}\begin{pmatrix} 0 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & a_n \end{pmatrix} = \begin{pmatrix} 0 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 0 \end{pmatrix}, \qquad a_1 \neq 0, a_n \neq 0.$$

Пример 3. Кольцо функций одной переменной с операциями поэлементного сложения и умножения имеет делители нуля.

$f_1(x) = |x| + x \quad f_2(x) = |x| - x$

$$f_1(x) = \begin{cases} 2x, & \text{если } x \geq 0 \\ 0, & \text{если } x < 0 \end{cases}$$

$$f_2(x) = \begin{cases} -2x, & \text{если } x < 0 \\ 0, & \text{если } x \geq 0 \end{cases}$$

$f_1(x) \cdot f_2(x) = 0$, но $f_1(x) \neq 0,\ f_2(x) \neq 0.$

Пример 4. Кольцо классов вычетов $mod\ n$

$\times$	C_0	C_1	C_2	C_3
C_0	C_0	C_0	C_0	C_0
C_1	C_0	C_1	C_2	C_3
C_2	C_0	C_2	C_0	C_2
C_3	C_0	C_3	C_2	C_1

$C_2 \cdot C_2 = C_0$, следовательно C_2 – правый и левый делители нуля. $e_+ = C_0$.

Таким образом, структура, определенная в примере 4 – коммутативное кольцо с единицей и делителями 0.

Определение 5. Если в кольце K $a \in K$ и $\exists a^{-1}: a^{-1}a = aa^{-1} = e_\times$, то a – обратимый элемент кольца, a^{-1} – обратный элемент.

Утверждение 1. Обратимые элементы не могут быть делителями нуля.

Доказательство. От противного.

Пусть $ab = 0$, но $a \neq 0$ и $b \neq 0$. И пусть a^{-1} обратный элемент для элемента a. Домножим равенство на a^{-1}, получим: $a^{-1}ab = a^{-1}0$. Откуда $b = 0$, что противоречит предположению $b \neq 0$.

Утверждение 2. Все обратимые элементы кольца образуют группу по умножению.

Доказательство.

1) ассоциативность следует из того, что кольцо – полугруппа по умножению;
2) $e \in G, e^{-1} = e$;
3) $a, a^{-1} \in G$, т. к. все элементы обратимы;
4) замкнутость: обратимы $a, a^{-1} \in G$ и $b, b^{-1} \in G$

   Следовательно, обратим $ab, (ab)^{-1} \in G$.

   Покажем, что $(ab)^{-1} = b^{-1}a^{-1}$

   $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aa^{-1} = e$

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

Определение 6. Поле – коммутативное кольцо с единицей (по умножению), в котором каждый элемент, кроме нуля, обратим.

Поле и по сложению, и по умножению (без нулевого элемента) – коммутативная группа.

Поскольку обратимые элементы не могут быть делителями нуля, поле не может содержать делителей нуля.

	Кольцо	**Поле**
1. По сложению	Коммутативная группа	Коммутативная группа
2. По умножению	Полугруппа или моноид. Коммутативные или нет	Коммутативная группа без e_+
3. Дистрибутивность	Два закона, т.к. умножение может быть некоммутативным	Один закон
4. Делители нуля	Могут быть	Отсутствуют

Примеры поля. $P =< \mathbb{R}, +, \times >$ – поле.

$P =< \mathbb{Q}, +, \times >$ – поле.

$P =< \mathbb{C}, +, \times >$ – поле.

Пример 5. Какую алгебраическую структуру получим для классов вычетов по $mod\ 3$.

1. По сложению коммутативная группа. $C_0 = e_+, {C_1}^{-1} = C_2$.

+	C_0	C_1	C_2
C_0	C_0	C_1	C_2
C_1	C_1	C_2	C_3
C_2	C_2	C_3	C_0

2. По умножению без класса C_0 (нуль) – коммутативная группа.

   $C_1 = e_\times, \qquad {C_2}^{-1} = C_2.$

×	C_1	C_2
C_1	C_1	C_2
C_2	C_2	C_1

3. Дистрибутивность выполняется.

Вывод. Поле.

Пример 6. Рассмотрим подробно комплексные числа.

Образуют ли поле комплексные числа $\mathbb{C}$ $(c = a + bi)$?

Решение.

1. **По сложению – коммутативная группа.**

   1.1. Коммутативность очевидна.

   1.2. Ассоциативность очевидна.

   1.3. $\exists\ e_+$: $\qquad c + e_+ = c \ \Rightarrow\ e_+ = 0$

   1.4. Обратные элементы. Для любого комплексного числа c:

   $$c + c^{-1} = 0 \ \Rightarrow\ c^{-1} = -c$$

2. **По умножению (без $e_+ = 0$) – коммутативная группа.**

2.1. Коммутативность очевидна.

2.2. Ассоциативность очевидна.

2.3. $\exists\, e_{\times}$: $\quad c \times e_{\times} = c \Rightarrow e_{\times} = 1.$

2.4. Обратные элементы существуют (кроме $c = 0$, но мы этот элемент не рассматриваем)

$$c \times c^{-1} = 1 \Rightarrow$$

$$c^{-1} = \frac{1}{a+bi} \cdot \frac{(a-bi)}{(a-bi)} = \frac{a-bi}{a^2+b^2} = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2} i$$

3. **Дистрибутивность очевидна.**

Вывод: комплексные числа с операциями сложения и умножения образуют поле.