# КОЛЬЦА.ПОЛЯ

*Кольцом* называется множество $K$ с операциями сложения и умножения, обладающими следующими свойствами:

1) относительно сложения $K$ есть абелева группа (называемая аддитивной группой кольца $K$):

$a + b = b + a$ для любых $a, b \in K$ (коммутативность);

$(a + b) + c = a + (b + c)$ для любых $a, b, c \in K$ (ассоциативность);

в $K$ существует такой элемент $0$ (нуль), что $a + 0 = 0 + a$ для любого $a \in K$;

для любого элемента $a \in K$ существует такой элемент $-a \in K$ (противоположный), что $a + (-a) = 0$;

2) $a(b + c) = ab + ac$ и $(a + b)c = ac + bc$ для любых $a, b, c \in K$ (дистрибутивность умножения относительно сложения).

Кольцо $K$ называется *коммутативным*, если умножение в нем коммутативно, т.е. $ab = ba$ для любых $a, b \in K$.

Кольцо $K$ называется *ассоциативным*, если умножение в нем ассоциативно, т.е. $(ab)c = a(bc)$ для любых $a, b, c \in K$.

Элемент $1$ кольца называется *единицей*, если $1 \cdot a = a \cdot 1 = a$.

Элемент $a^{-1}$ кольца с единицей называется обратным к элементу $a$, если $aa^{-1} = a^{-1}a = 1$.

Элемент, имеющий обратный, называется *обратимым.*

*Полем* называется коммутативное ассоциативное кольцо с единицей, в котором всякий ненулевой элемент обратим.

Кольцо, состоящее из одного нуля, не считается полем.

Любое поле обладает следующим важным свойством: $ab = 0 \Rightarrow a = 0$ или $b = 0$.

Ненулевые элементы $a, b$ кольца $K$ называются *делителями нуля*, если $ab = 0$.

Пусть $K$ - поле. Наименьшее натуральное $n$, для которого в $K$ выполняется

$$\underbrace{1 + 1 + ... + 1}_{n} = 0$$

называется *характеристикой* этого поля. Если такого $n$ не существует, то $K$

- поле нулевой характеристики. Характеристика поля $K$ обозначается через $\mathrm{char}K$.

Если $\mathrm{char}K = n$, для любого элемента $a \in K$

$$\underbrace{a + a + ... + a}_{n} = \underbrace{1 + 1 + ... + 1}_{n} a = 0 \cdot a = 0.$$

Подмножество $L$ кольца $K$ называется *подкольцом*, если

1) $L$ является подгруппой аддитивной группы кольца $K$;

2) $L$ замкнуто относительно умножения.

Очевидно, что всякое подкольцо само является кольцом относительно тех же операций. При этом оно наследует такие свойства, как коммутативность и ассоциативность.

Подмножество $L$ поля $K$ называется *подполем*, если

1) $L$ является подкольцом кольца $K$;

2) $a \in L, a \neq 0 \Rightarrow a^{-1} \in L$;

3) $1 \in L$.

Отображение $f$ кольца $K_1$ в кольцо $K_2$ называется *гомоморфизмом*, если

$$f(a + b) = f(a) + f(b), \quad f(ab) = f(a)f(b)$$

$a, b \in K_1$.

Если гомоморфизм $f$ является биекцией, то он называется *изоморфизмом*.

Изоморфизм кольца на себя называется *автоморфизмом*.

Аналогично определяется гомоморфизм, изоморфизм, автоморфизм для полей.

Если $f : K_1 \to K_2$ - гомоморфизм, то множество

$$\mathrm{Ker}f = \{a \in K_1 | f(a) = 0\}$$

называется *ядром* гомоморфизма $f$.

Множество

$$\mathrm{Im}f = \{a_2 \in K_2 | a_2 = f(a_1), a_1 \in K_1\}$$

называется *образом* гомоморфизма $f$.

Пусть $n$ - фиксированное натуральное число. Рассмотрим в множестве $\mathbb{Z}$ целых чисел следующее *отношение сравнимости по модулю* $n$: $a$ сравнимо с $b$ по модулю $n$ (обозначение: $a \equiv b \pmod{n}$), если $a - b$ делится на $n$ или, что равносильно, если $a$ и $b$ дают одинаковые остатки при делении на $n$.

Очевидно, что это отношение эквивалентности, причем классы эквивалентности могут быть занумерованы числами $0, 1, ..., n-1$ таким образом, что $r$-й класс состоит из всех целых чисел, дающих при делении на $n$ остаток $r$.

Класс эквивалентности, содержащий целое число $a$, называется вычетом числа $a$ по модулю $n$ и обозначается через $[a]_n$ или просто через $[a]$, если ясно, какое $n$ имеется в виду.

Фактормножество множества $\mathbb{Z}$ по отношению сравнимости по модулю $n$ обозначается через $\mathbb{Z}_n$. Мы можем написать, что

$$\mathbb{Z}_n = \left\{[0]_n, [1]_n, ..., [n-1]_n\right\}.$$

Каждый элемент множества можно обозначать по-разному. Так, элемент $[1]_n$ может быть обозначен через $[2n+1]_n, [-(n-1)]_n$ и т.д.

Отношение сравнимости по модулю $n$ согласовано с операциями сложения и умножения в $\mathbb{Z}$:

Пусть $a \equiv a' \pmod{n}$, $b \equiv b' \pmod{n}$. Тогда

$$a + b \equiv a' + b \equiv a' + b' \pmod{n}$$

и, аналогично,

$$ab \equiv a'b \equiv a'b' \pmod{n}.$$

Таким образом, может определить в множестве $\mathbb{Z}_n$ операции сложения и умножения по формулам

$$[a]_n + [b]_n = [a+b]_n \quad [a]_n[b]_n = [ab]_n$$

(справедливым для любых $a, b \in \mathbb{Z}$). Тем самым $\mathbb{Z}_n$ превращается в коммутативное ассоциативное кольцо с единицей. Оно называется *кольцом вычетов по модулю $n$*.

Кольцо $\mathbb{Z}_n$ является полем тогда и только тогда, когда $n$ - простое число.

Таблицы сложения и умножения в кольце $\mathbb{Z}_5$ :

$$\begin{array}{c|ccccc} + & 0 & 1 & 2 & 3 & 4 \\ \hline 0 & 0 & 1 & 2 & 3 & 4 \\ 1 & 1 & 2 & 3 & 4 & 0 \\ 2 & 2 & 3 & 4 & 0 & 1 \\ 3 & 3 & 4 & 0 & 1 & 2 \\ 4 & 4 & 0 & 1 & 2 & 3 \end{array} \qquad \begin{array}{c|ccccc} \times & 0 & 1 & 2 & 3 & 4 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 2 & 3 & 4 \\ 2 & 0 & 2 & 4 & 1 & 3 \\ 3 & 0 & 3 & 1 & 4 & 2 \\ 4 & 0 & 4 & 3 & 2 & 1 \end{array}$$

## Примеры

**1.** Докажите, что множество $M$ матриц вида $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, где $a$ и $b$ - действительные числа, является полем относительно матричного сложения и умножения. Найдите характеристику этого поля.

`Решение.`

1. Пусть $A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, $B = \begin{pmatrix} c & d \\ -d & c \end{pmatrix}$, - матрицы данного множества.

$$A + B = \begin{pmatrix} a+c & -(b+d) \\ -(b+d) & a+c \end{pmatrix}, \quad A + B \in M$$

$$AB = \begin{pmatrix} ac - bd & ad + bc \\ -(ad+bc) & ac - bd \end{pmatrix}, \quad AB \in M$$

т.е. множество $M$ замкнуто относительно матричного сложения и умножения.

Из теории матриц известно, что на множестве квадратных матриц одного и того же порядка, а значит, и на множестве $M$, сложение коммутативно и ассоциативно, умножение дистрибутивно относительно сложения:

2. $A + B = B + A$ (коммутативность сложения)

3. $(A + B) + C = A + (B + C)$ (ассоциативность сложения)

4. $A+O = O+A$, где $O$ - нулевая матрица второго порядка (существование нулевого элемента)

5. $A + (-A) = O$, $-A = \begin{pmatrix} -a & -b \\ b & -a \end{pmatrix}$ (существование противоположного элемента)

6. $A(B + C) = AB + AC$, $(A + B)C = AC + BC$.

Значит, $M$ - кольцо.

Из теории матриц известно, что на множестве квадратных матриц одного и того же порядка умножение ассоциативно:

7. $A(BC) = A(BC)$ (ассоциативность умножения)

$M$ - ассоциативное кольцо.

8. $E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in M$, $AE = EA = A$ (существование единичного элемента).

$M$ - ассоциативное кольцо с единицей.

9. $BA = \begin{pmatrix} c & d \\ -d & c \end{pmatrix} \begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \begin{pmatrix} ac - bd & ad + bc \\ -(ad + bc) & ac - bd \end{pmatrix} = AB$ (коммутативность умножения)

Значит, $M$ - ассоциативное коммутативное кольцо с единицей.

10. $A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \Rightarrow a \neq 0, b \neq 0$. Тогда $\det A = a^2 + b^2 \neq 0$, т.е. матрица $A$ является невырожденной, а значит, она имеет обратную матрицу $A^{-1}$.

$$A^{-1} = \frac{1}{a^2 + b^2} \begin{pmatrix} a & -b \\ b & a \end{pmatrix} = \begin{pmatrix} \frac{a}{a^2+b^2} & \frac{-b}{a^2+b^2} \\ \frac{b}{a^2+b^2} & \frac{a}{a^2+b^2} \end{pmatrix} \in M$$

(существование обратного элемента)

Вывод, $M$ - поле.

Найдем характеристику поля $M$. По правилу умножения числа на матрицу получим, что при любом натуральном $n$

$$n \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} n & 0 \\ 0 & n \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},$$

т.е. не существует натурального $n$ такого, чтобы $n \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$. Значит, характеристика поля $M$ равна нулю.

**2.** Является ли кольцом множество $L$ чисел вида $a + b\sqrt[3]{2}$, $a, b \in \mathbb{Q}$ относительно обычных операций сложения и умножения?

`Решение`. Проверим замкнуто ли множество $L$ относительно операций сложения и умножения.

$a_1 + b_1\sqrt[3]{2} + a_2 + b_2\sqrt[3]{2} = a_1 + a_2 + (b_1 + b_2)\sqrt[3]{2} \in L \Rightarrow L$ замкнуто относительно сложения.

$(a_1 + b_1\sqrt[3]{2})(a_2 + b_2\sqrt[3]{2}) = a_1a_2 + a_2b_1\sqrt[3]{2} + a_1b_2\sqrt[3]{2} + b_1b_2\sqrt[3]{4} \notin L \Rightarrow L$ не замкнуто относительно умножения.

Вывод, $L$ не является кольцом.

**3.** Множество, состоящее из функций, непрерывных на прямой, является кольцом, если сложение и умножение определить следующим образом:

$$(f+g)(x) = f(x) + g(x), \quad (fg)(x) = f(x)g(x), \quad x \in \mathbb{R}.$$

Функции $f(x) = |x| + x$, $g(x) = |x| - x$ являются делителями нуля в кольце непрерывных функций на прямой.

**4.** Является ли отображение $f : \mathbb{C} \to \mathbb{C}$, $f(z) = \bar{z}$ изоморфизмом?

`Решение.`

1. Очевидно, что отображение $f : \mathbb{C} \to \mathbb{C}$ является биекцией:

$$f(z) = f(a + bi) = a - bi = \bar{z} \quad a, b \in \mathbb{R}.$$

2. Проверим выполнимость свойств:

$$f(z_1 + z_2) = f(z_1) + f(x_2), \quad f(z_1z_2) = f(z_1)f(z_2).$$

$$z_1 = a_1 + b_1i,\ z_2 = a_2 + b_2i, \quad f(z_1) = a_1 - b_1i,\ f(z_2) = a_2 - b_2i,$$

$$f(z_1 + z_2) = f(a_1 + b_1i + a_2 + b_2i) = f(a_1 + a_2 + i(b_1 + b_2)) =$$

$$= a_1 + a_2 - i(b_1 + b_2) = a_1 - b_1i + a_2 - b_2i = \bar{z}_1 + \bar{z}_2 = f(z_1) + f(z_2).$$

Или можно записать иначе, по свойствам комплексно сопряженных чисел:

$$f(z_1 + z_2) = \overline{z_1 + z_2} = \bar{z}_1 + \bar{z}_2 = f(z_1) + f(z_2).$$

$$f(z_1z_2) = \overline{z_1z_2} = \bar{z}_1\bar{z}_2 = f(z_1)f(z_2).$$

Вывод, $f$ - изоморфизм.

**5.** Решим квадратное уравнение $x^2 + x - 1 = 0$ в поле $\mathbb{Z}_{11}$.

`Решение.` По обычной формуле находим

$$x_{1,2} = \frac{[-1] \pm \sqrt{[5]}}{[2]}.$$

Так как $[5] = [16] = [4]^2$, то можно считать, что $\sqrt{[5]} = [4]$ (одно из значений квадратного корня). Следовательно,

$$x_1 = \frac{[-1] + [4]}{[2]} = \frac{[3]}{[2]} = \frac{[14]}{[2]} = [7], \quad x_2 = \frac{[-1] - [4]}{[2]} = \frac{[-5]}{[2]} = \frac{[6]}{[2]} = [3].$$

## Задачи и упражнения

**1.** Выясните, образует ли кольцо относительно обычных сложения и умножения:

1) множество $\mathbb{N}$
2) множество $\mathbb{Z}$;
3) множество всех четных чисел;
4) множество всех нечетных чисел;
5) $m\mathbb{Z}$ (множество целых чисел, кратных $m$);
6) множество $\mathbb{Q}$;
7) $\left\{a + b\sqrt{3} | a, b \in \mathbb{Z}\right\}$.

**2.** Является ли кольцом множество $L$ чисел вида $a+b\sqrt{3}+c\sqrt{5}$, $a, b, c \in \mathbb{Z}$ относительно обычных операций сложения и умножения?

**3.** Покажите, что множество чисел вида $a + b\sqrt{3} + c\sqrt{5} + d\sqrt{15}$, где $a, b, c, d \in \mathbb{Z}$ является числовым кольцом, т.е. кольцом относительно обычных операций сложения и умножения над числами.

**4.** Выясните, является ли кольцом относительно матричного сложения и умножения:

1) множество всех действительных матриц одного и того же порядка $n > 1$;

2) множество матриц вида $\begin{pmatrix} a & b \\ b & b \end{pmatrix}$ с рациональными компонентами;

3) множество действительных матриц вида $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$.

**5.** Докажите, что множество $M$ матриц вида $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$ составляет коммутативное кольцо относительно матричного сложения и умножения. Выделите мультипликативную группу этого кольца. Выясните, является ли $M$ полем? ($a$ и $b$ - любые действительные числа).

**6.** Докажите, что если $M$ - коммутативная группа относительно операции сложения, такая, что $ab = 0$ для любых $a, b$ и нулевого элемента $0$ группы $M$, то система $M =< M, +, \cdot >$ является кольцом.

**7.** Докажите, что если на $\mathbb{Z}$ задана операция $a \odot b = -ab$, то алгебраическая система $< \mathbb{Z}, +, \odot >$ является коммутативным кольцом с единицей. Каков единичный элемент этого кольца?

**8.** Докажите, что алгебраическая система - множество $\mathbb{Q}$ рациональных чисел с обычной операцией сложения и операцией $a \circ b = \frac{a \cdot b}{2}$, выполняемой по правилу для любых элементов из $\mathbb{Q}$ - является полем. Каков единичный элемент этого поля?

**9.** Докажите, что множество матриц вида $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$, где $a$ - любое рациональное (или действительное) число, является полем относительно матричного сложения и умножения. Будет ли множество матриц данного вида составлять поле, если $a$ - любое целое число?

**10.** На множестве $M = \{a, b\}$ сложение $\oplus$ и умножение $\odot$ определены следующим образом:

$$a \oplus a = a, \quad a \oplus b = b \oplus a = b, \quad b \oplus b = a,$$
$$a \odot b = b \odot a = a, \quad a \odot a = a, \quad b \odot b = b.$$

Выясните, обладает ли это поле множество нулем и единицей и является ли система $< M, \oplus, \odot >$ полем относительно заданных бинарных операций.

**11.** Выясните, является ли система $< \mathbb{Z}, \oplus, \cdot >$ кольцом относительно обычного умножения и операции сложения $\oplus$, выполняемой по правилу:

$$a \oplus b = \begin{cases} a + b, \text{ если } a - \text{четное число}, b - \text{любое целое число}, \\ a - b, \text{ если } a - \text{нечетное число}, b - \text{любое целое число}. \end{cases}$$

**12.** На множестве $A = \mathbb{Q}^2$ упорядоченных пар $(a; b)$ рациональных чисел сложение $\oplus$ и умножение $\odot$ определены следующими правилами:

$$(a; b) \oplus (c; d) = (a + c; b + d), \quad (a; b) \odot (c; d) = (ac; bd).$$

Покажите, что система $< A, \oplus, \odot >$ является коммутативным кольцом с единицей и с делителями нуля.

**13.** Установите, что матрицы вида $\begin{pmatrix} a + bi & c + di \\ -c + di & a - bi \end{pmatrix}$ при действительных $a, b, c, d$ образуют кольцо, не имеющее делителей нуля.

**14.** Докажите, что множество $L$ матриц вида $\begin{pmatrix} a & b \\ 5b & a \end{pmatrix}$, $a, b \in \mathbb{Q}$ является подкольцом кольца $M$ всех веществених матриц порядка 2.

**15.** Докажите, что множество $\mathbb{Z}[\sqrt{5}]$ чисел вида $a + b\sqrt{5}$, где $a, b$ - любые целые числа, является числовым кольцом. Разрешимы ли в этом кольце уравнения

$$(1+2\sqrt{5})x = -8+3\sqrt{5}, \quad (-8+3\sqrt{5})x = 1+2\sqrt{5}, \quad (3+2\sqrt{5})x = 2-3\sqrt{5}?$$

Будет ли $\mathbb{Z}[\sqrt{5}]$ числовым полем?

**16.** Докажите, что множество $A$ чисел вида $2a + 2b\sqrt{3}$, где $a, b$ - любые целые числа, является числовым кольцом.

**17.** Решите систему уравнений:

$$\begin{cases} x + 2z = 1, \\ y + 2z = 2, \\ 2x + z = 1 \end{cases}$$

над полями: 1) $\mathbb{Z}_3$, 2) $\mathbb{Z}_5$, 3) $\mathbb{Z}_7$.

**18.** Докажите, что множество $B = \mathbb{Q}[\sqrt{5}]$ чисел вида $a + b\sqrt{5}$, где $a, b$ - любые рациональные числа, является числовым полем.

**19.** Покажите, что числа вида $a + b\sqrt[3]{2} + c\sqrt[3]{4}$ с рациональными $a, b, c$ образует поле. Найдите в этом поле элемент, обратный числу $\gamma = 1 + \sqrt[3]{2} + 2\sqrt[3]{4}$.

**20.** Пусть $A = \left\{ \begin{Vmatrix} a & b \\ b & a \end{Vmatrix} | a,\, b \in \mathbb{Z} \right\}$. Докажите, что отображение $\varphi : A \to \mathbb{Z} : \varphi\left( \begin{Vmatrix} a & b \\ b & a \end{Vmatrix} \right) = a - b$ - гомоморфизм. Укажите его ядро.

**21.** Докажите, что кольцо чисел вида $a + b\sqrt{5}$ изоморфно кольцу матриц вида $\begin{pmatrix} a & b \\ 5b & a \end{pmatrix}$ ($a$ и $b$ рациональные числа). Почему второе кольцо будет являться полем?

**22.** Покажите, что кольцо $\mathbb{Z}$ можно изоморфно отобразить на кольцо $M$ матриц вида $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$, где $a$ -любое целое число, а поле $\mathbb{R}$ - на поле матриц вида $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$, где $a \in \mathbb{R}$.

**23.** Установите изоморфизм поля комплексных чисел и множества матриц вида $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, где $a, b \in \mathbb{R}$.

**24.** В поле вычетов по модулю 11 решить уравнения:
1) $x^2 + 3x + 7 = 0$;
2) $x^2 + 5x + 1 = 0$;
3) $x^2 + 2x + 3 = 0$.

## Список литературы

1. Проскуряков И.В. Сборник задач по линейной алгебре. - Москва: Лань, 2010. - 475 с.

2. Сборник задач по алгебре / Под ред. А.И. Кострикина: Учебник для вузов. Изд. 3-е, испр. и доп. - М.: ФИЗМАТЛИТ, 2001. - 464 с.

3. Шнеперман Л.Б. Сборник задач по алгебре и теории чисел: учеб. пособие / Л.Б. Шнеперман. - Минск : Выш. шк., 1982. - 223 с.