**МЕХАНИКО-МАТЕМАТИЧЕСКИЙ И ХИМИЧЕСКИЙ ФАКУЛЬТЕТЫ МГУ ИМ. М.В.ЛОМОНОСОВА**

# ГРУППЫ, КОЛЬЦА, ПОЛЯ

**(для студентов химических специальностей)**

**А.И.КОЗКО, Л.М.ЛУЖИНА, А.А.ЛУЖИН, В.Г.ЧИРСКИЙ**

**2026**

Рекомендовано методической комиссией химического факультета и кафедрой математического анализа механико-математического факультета МГУ им. М.В. Ломоносова в качестве учебного пособия для студентов

*В современном мире компьютерные технологии внедрены практически во все научные и прикладные исследования. В свою очередь, это вызывает бурное развитие математических дисциплин, поскольку многие из математических дисциплин имеют важное прикладное значение и являются основой компьютерных технологий.*

*Для правильного и эффективного использования многих математических программ требуется умение сформулировать задачи, возникающие в процессе исследования математической модели изучаемого явления, выбрать подходящий алгоритм решения, осмыслить полученный результат. Для этого требуется достаточный уровень математической подготовки.*

*В серии методических разработок «математика для современной химии» рассматриваются вопросы, усвоение которых способствует повышению математической культуры учащихся, развитию их профессиональных компетенций.*

*Предлагаемая Вашему вниманию серия пособий содержит описание курса лекций по линейной алгебре, многие годы читавшегося на химическом факультете МГУ им. М.В. Ломоносова и образцы решения типовых задач.*

*Важная цель этих разработок – облегчить самостоятельную работу студентов и способствовать успешной сдаче ими экзаменов и зачётов.*

Элементы теории групп

Поле. Кольцо. Подполе. Подкольцо

Гомоморфизм и изоморфизм групп, колец и полей (Гомоморфизм и изоморфизм групп. Образ. Ядро. Нормальная подгруппа. Фактор-группа. Теорема о гомоморфизме для групп. Гомоморфизм колец, изоморфизм колец и полей. Образ. Ядро. Идеал. Фактор-кольцо. Теорема о гомоморфизмах для колец)

# 7. Элементы теории групп

## 7.1. Определение группы. Примеры

**Определение.** Пусть $G$ – множество и пусть каждой паре элементов множества $x \in G, y \in G$ сопоставлен элемент $z \in G$, что будем записывать так:

$$x \circ y = z$$

и будем говорить, что на множестве $G$ задана ***бинарная операция.*** Множество $G$ называется ***группой,*** если определенная выше операция обладает свойствами (аксиомами группы):

1. ассоциативности, то есть $(x \circ y) \circ z = x \circ (y \circ z)$, для любых $x, y, z \in G$;
2. существует нейтральный элемент, обозначаемый $e \in G$ такой, что для любого $x \in G$ выполняются равенства $x \circ e = e \circ x = x$;
3. Для любого $x \in G$ существует обратный элемент, обозначаемый $x^{-1}$, такой, что $x \circ x^{-1} = x^{-1} \circ x = e$.

Если кроме этих свойств, для любых $x, y \in G$ выполняется условие $x \circ y = y \circ x$, то ***группа*** называется ***коммутативной*** или ***абелевой.***

Легко доказать, что нейтральный элемент группы единственный, и что обратный элемент группы также определен однозначно.

Рассмотрим примеры групп. Отметим, что в них мы указываем как множество, так и бинарную операцию $\circ$, поскольку одно и то же множество, снабженное различными бинарными операциями, может дать различные группы.

**Примеры групп**

1. Группа целых чисел $\mathbb{Z}$ с операцией сложения $a + b$. Выполнение аксиом групп очевидно. Нейтральным элементом является число $0$. Обратимый элемент по сложению для числа $a$ равен $-a$. Группа является коммутативной. Также являются группами по сложению рациональные числа, действительные числа, комплексные числа.
   «Группы, операцию в которых называют сложением», часто называют

***аддитивными*** группами.

Отметим, что натуральные числа $\mathbb{N}$ не являются группой по сложению, так как $0$, не является натуральным числом и, разумеется, для $a \in \mathbb{N}$ число $-a$ не принадлежит $\mathbb{N}$.

2. Группа $\mathbb{R}^*$, состоящая из отличных от $0$ действительных чисел, с операцией умножения. Нейтральный элемент в ней – число 1, обратный элемент по умножению для числа $a \neq 0$ равен $\frac{1}{a}$. Группа также абелева. Точно так же образуют группу по умножению все отличные от $0$ рациональные числа, все отличные от $0$ комплексные числа. Отличные от $0$ целые числа не образуют группу по умножению, так как обратное к целому числу не равному 1, не является целым числом. «Группы, операцию в которых называют умножением», часто называют ***мультипликативными*** группами.

3. Любое векторное множество представляет собой абелеву группу по сложению. Например, матрицы размера $m \times n$ с обычной операцией сложения, образуют группу.

4. Группа $GL(n, R)$. Её элементами являются все невырожденные матрицы порядка $n$, а операция – обычное умножение матриц. Так как невырожденность матрицы равносильна отличию от $0$ ее определителя, все матрицы из этого множества имеют обратные. Единичная матрица, разумеется, равна $\begin{pmatrix} 1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 1 \end{pmatrix}$ и $GL(n, R)$ дает пример некоммутативной группы.
5. Группа симметрий $C_n$ ориентированного правильного $n$-угольника, (состоящая из поворотов $n$-угольника на углы $\frac{2\pi k}{n}$, $k = 0,1, \dots, n-1$). Групповая операция состоит в последовательном выполнении поворотов. Эти повороты можно изобразить матрицами

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} \cos\frac{2\pi}{n} & -\sin\frac{2\pi}{n} \\ \sin\frac{2\pi}{n} & \cos\frac{2\pi}{n} \end{pmatrix}, \dots, \begin{pmatrix} \cos\frac{2\pi k}{n} & -\sin\frac{2\pi k}{n} \\ \sin\frac{2\pi k}{n} & \cos\frac{2\pi k}{n} \end{pmatrix}, \dots,$$
$$\begin{pmatrix} \cos\frac{2\pi(n-1)}{n} & -\sin\frac{2\pi(n-1)}{n} \\ \sin\frac{2\pi(n-1)}{n} & \cos\frac{2\pi(n-1)}{n} \end{pmatrix}$$

Групповой операции соответствует произведение матриц. Единичная матрица – нейтральный элемент группы. Обратной для матрицы $\begin{pmatrix} \cos\frac{2\pi k}{n} & -\sin\frac{2\pi k}{n} \\ \sin\frac{2\pi k}{n} & \cos\frac{2\pi k}{n} \end{pmatrix}$, задающей поворот на угол $\frac{2\pi k}{n}$ является матрица $\begin{pmatrix} \cos\frac{2\pi k}{n} & \sin\frac{2\pi k}{n} \\ -\sin\frac{2\pi k}{n} & \cos\frac{2\pi k}{n} \end{pmatrix}$,

соответствующая обратному повороту, то есть на повороту на угол $-\frac{2\pi k}{n}$.

Легко видеть, что:

$$\begin{pmatrix} \cos\frac{2\pi k}{n} & -\sin\frac{2\pi k}{n} \\ \sin\frac{2\pi k}{n} & \cos\frac{2\pi k}{n} \end{pmatrix}\begin{pmatrix} \cos\frac{2\pi}{n} & -\sin\frac{2\pi}{n} \\ \sin\frac{2\pi}{n} & \cos\frac{2\pi}{n} \end{pmatrix} =$$
$$= \begin{pmatrix} \cos\frac{2\pi(k+1)}{n} & -\sin\frac{2\pi(k+1)}{n} \\ \sin\frac{2\pi(k+1)}{n} & \cos\frac{2\pi(k+1)}{n} \end{pmatrix}$$

и, значит,

$$\begin{pmatrix} \cos\frac{2\pi k}{n} & -\sin\frac{2\pi k}{n} \\ \sin\frac{2\pi k}{n} & \cos\frac{2\pi k}{n} \end{pmatrix} = \begin{pmatrix} \cos\frac{2\pi}{n} & -\sin\frac{2\pi}{n} \\ \sin\frac{2\pi}{n} & \cos\frac{2\pi}{n} \end{pmatrix}^{\mathrm{k}}.$$

Это означает, что все элементы группы $C_n$ – это $1, a, a^2, \dots, a^{n-1}$, где $a$ – это поворот на угол $\frac{2\pi k}{n}$. Такая группа называется ***циклической.***

6. Группа симметрий $D_n$ правильного $n$-угольника состоит из матриц группы $C_n$, к которым добавлены матрицы

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} \cos\frac{2\pi}{n} & -\sin\frac{2\pi}{n} \\ -\sin\frac{2\pi}{n} & -\cos\frac{2\pi}{n} \end{pmatrix}, \dots, \begin{pmatrix} \cos\frac{2\pi k}{n} & -\sin\frac{2\pi k}{n} \\ -\sin\frac{2\pi k}{n} & -\cos\frac{2\pi k}{n} \end{pmatrix}, \dots,$$
$$\begin{pmatrix} \cos\frac{2\pi(n-1)}{n} & -\sin\frac{2\pi(n-1)}{n} \\ -\sin\frac{2\pi(n-1)}{n} & -\cos\frac{2\pi(n-1)}{n} \end{pmatrix}.$$

Например, $D_3$ совпадает с группой симметрии молекулы $C_2H_6$.

7. Группа симметрий тетраэдра $T$ состоит из вращений вокруг каждой из верхних осей вращения, перпендикулярной плоскости основания и из

вращений вокруг осей, соединяющих середины противоположных ребер. $T$ – группа симметрии молекулы $CH_4$.

Необходимо отметить замечательную книгу: В.А. Артамонов, Ю.Л. Словохотов. Группы и их применение в физике, химии, кристаллографии. Москва, «Академия», 2005. На 500 страницах этой книги изложены основы теории групп, теория кристаллографических групп, элементы теории представлений групп, основы теории групп Ли и рассказано о приложениях теории групп в физике и химии.

## 7.2. Конечные группы

Группы с конечным числом элементов называются ***конечными группами*** или ***группами конечного порядка.***

**Определение.** ***Порядком группы $G$*** называется количество ее элементов. Порядок обозначается$|G|$.

Примеры 1–4 предыдущего параграфа – бесконечные группы, примеры 5–7 – конечные группы.

**Определение.** Подмножество $H \subset G$ называется ***подгруппой группы $G$***, если оно само является группой относительно операции, имеющейся в группе $G$.

**Примеры**

1. Группа $\mathbb{Z}$ целых чисел по сложению – подгруппа $\mathbb{Q}$ группы рациональных чисел по сложению; $\mathbb{Q}$ – подгруппа группы $\mathbb{R}$ действительных чисел по сложению.
2. Любое подпространство векторного пространства – его подгруппа по сложению.

**Теорема 7.1 (Теорема Лагранжа).** Если $H$ – подгруппа конечной группы $G$, то число $|H|$ делит число $|G|$, то есть порядок подгруппы конечной группы делит порядок этой конечной группы.

Доказательство.

Обозначим, для краткости, групповую операцию группы $G$ символом $gh$, где $g, h \in G$. Назовем ***левым смежным классом $gH$ по подгруппе $H$*** множество элементов группы $G$, имеющих вид $gh,\ h \in H$. (Аналогично, ***правый смежный класс $Hg$*** представляет собой множество элементов группы $G$, имеющих вид $hg,\ h \in H$.)

Докажем, что если смежные классы $g_1H$ и $g_2H$ пересекаются, то есть имеют общие элементы, то они совпадают.

Пусть $g \in g_1H$ и $g \in g_2H$. Это означает, что существуют $h_1, h_2 \in H$, такие, что $g = g_1h_1$ и $g = g_2h_2$, то есть $g_1h_1 = g_2h_2$, откуда $g_1 = g_2h_2h_1^{-1}$, то есть $g_1$ имеет вид $g_1 = g_2h$, где $h = h_2h_1^{-1}$ и, следовательно, $g_1 \in g_2H$. Аналогично, $g_2 = g_1h_1h_2^{-1} \in g_1H$.

Из $g_1 \in g_2H$ следует, что $g_1H \subset g_2H$, из $g_2 \in g_1H$ следует, что $g_2H \subset g_1H$, поэтому $g_1H = g_2H$.

Это означает, что вся группа $G$ представляет собой объединение конечного числа непересекающихся смежных классов, в каждом из которых $|H|$ элементов, то есть $|G|$ кратно $|H|$, что и утверждалось.

Обозначим $X_n$ множество чисел $1, \dots, n$ , то есть $X_n = \{1, \dots, n\}$. При изучении определителей мы рассматривали перестановки (также называемые подстановками) этих чисел, которые можно рассматривать, как взаимно-однозначные отображения $X_n$ на себя. Множество всех перестановок обозначается $S_n$.

Введём ***операцию умножения перестановок***, понимая под произведением перестановок их последовательное выполнение.

Умножение ассоциативно, нейтральный элемент – тождественная перестановка, оставляющая все числа на своих местах. Обратный элемент – обратная подстановка. Ранее мы записывали перестановку в виде:

$$\sigma = \begin{pmatrix} 1 & 2 & n \\ \sigma(1) & \sigma(2) & \sigma(n) \end{pmatrix}, \qquad (7.2)$$

понимая под $\sigma(1), \sigma(2), \dots, \sigma(n)$ соответствующим образом расположенные числа $1, \dots, n$.

Удобнее не ограничивать себя перестановками вида (7.2), а допускать запись $\sigma$ в виде

$$\sigma = \begin{pmatrix} i_n & i_n \\ \sigma(i_n) & \sigma(i_n) \end{pmatrix}, \qquad (7.3)$$

то есть допускать любой порядок столбцов в матрице перестановки (7.3).

Если $\tau = \begin{pmatrix} 1 & 2 & n \\ \tau(1) & \tau(2) & \tau(n) \end{pmatrix}$, (7.4)

то для любого $k$ существует такое $j_k$, что

$$\tau(j_k) = i_k \qquad (7.5)$$

($i_k$ – числа первой строки (7.3)).

Тогда перестановка $\sigma\tau$ – результат последовательного применения перестановки $\tau$, затем $\sigma$ выражается следующим образом, ввиду (7.3)–(7.5):

$$\sigma\tau = \begin{pmatrix} j_1 & \dots & j_n \\ \tau(j_1) & \dots & \tau(j_n) \end{pmatrix}\begin{pmatrix} i_1 & \dots & i_n \\ \sigma(i_1) & \dots & \sigma(i_n) \end{pmatrix} =$$
$$\begin{pmatrix} j_1 & \dots & j_n \\ i_1 & \dots & i_n \end{pmatrix}\begin{pmatrix} i_1 & \dots & i_n \\ \sigma(i_1) & \dots & \sigma(i_n) \end{pmatrix} = \begin{pmatrix} j_1 & \dots & j_n \\ \sigma(i_1) & \dots & \sigma(i_n) \end{pmatrix} =$$
$$\begin{pmatrix} j_1 & \dots & j_n \\ \sigma(\tau(j_1)) & \dots & \sigma(\tau(j_n)) \end{pmatrix} = \begin{pmatrix} j_1 & \dots & j_n \\ \sigma\tau(j_1) & \dots & \sigma\tau(j_n) \end{pmatrix}.$$

Обратную для перестановки (7.3) $\sigma^{-1}$ перестановку получим по правилу

$$\sigma^{-1} = \begin{pmatrix} \sigma(i_n) & \sigma(i_n) \\ i_n & i_n \end{pmatrix}.$$

Итак, $S_n$ – группа. При $n \geq 3$ эта группа не является коммутативной.

Действительно,

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$
$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

Будем называть транспозицией перестановку вида

$$\sigma^{-1} = \begin{pmatrix} 1 & 2 & i & j & n \\ 1 & 2 & i & j & n \end{pmatrix}, i \leq j \qquad (7.6)$$

и равные ей перестановки вида (7.3).

Без доказательства сформулируем теорему.

**Теорема 7.2.** Любая группа $G$ конечного порядка является подгруппой некоторой группы перестановок.

Рассмотрим примеры. Отметим, что в них мы указываем как множество, так и бинарную операцию, поскольку одно и то же множество, снабжённое различными бинарными операциями, может дать различные группы, или не образовывать группы. Жирным шрифтом дан ответ на вопрос, является ли рассматриваемое множество с заданной операцией группой.

1. Целые числа относительно сложения.
   **Да**
2. Чётные числа относительно сложения.
   **Да**

3. Целые числа, кратные данному натуральному числу $n$, относительно сложения.
   **Да**
4. Степени одного и того же действительного числа $a, a \neq 0, \pm 1$ относительно умножения.
   **Да**
5. Неотрицательные целые числа относительно сложения.
   **Нет** (обратный элемент не принадлежит множеству)
6. Нечётные числа относительно сложения.
   **Нет** (сумма элементов не принадлежит множеству)
7. Целые числа относительно вычитания.
   **Нет** (не выполняется аксиома ассоциативности
   $a - (b - c) \neq (a - b) - c$)
8. Рациональные числа относительно сложения.
   **Да**
9. Рациональные числа относительно умножения.
   **Нет** (0 не имеет обратного элемента)
10. Рациональные числа, отличные от 0, относительно умножения.
    **Да.**
11. Положительные рациональные числа относительно умножения.
    **Да.**
12. Положительные рациональные числа относительно деления.
    **Нет** (не выполняется аксиома ассоциативности
    $a: (b: c) \neq (a: b): c$)
13. Рациональные числа, знаменатели которых – неотрицательные степени числа 2 относительно сложения.
    **Да**
14. Матрицы размера $m \times n$ с действительными элементами относительно сложения.
    **Да**
15. Матрицы размера $m \times n$ с действительными элементами относительно умножения.
    **В общем случае – нет.** Умножение таких матриц возможно только при $m = n$.
16. Квадратные матрицы порядка $n$ с действительными элементами относительно умножения.
    **Нет** (обратный элемент имеют только невырожденные матрицы)
17. Невырожденные квадратные матрицы порядка $n$ с действительными элементами относительно умножения.

**Да.**

18. Невырожденные квадратные матрицы порядка $n$ с целыми элементами относительно умножения.
    **Нет** (обратная матрица может иметь не целые, а рациональные элементы).
19. Невырожденные квадратные матрицы порядка $n$ с целыми элементами и определителем, равным $\pm 1$,относительно умножения.
    **Да.**
20. Остатки от деления целых чисел, на данное натуральное число $n$ относительно сложения. При этом, если сумма остатков превзошла число $n$, то мы, в качестве результата операции, берем остаток полученной суммы от деления на число $n$.
    **Да.** Например, для $n = 3$ группа состоит из элементов 0,1,2 и операция сложения в ней определена равенствами $0 + 0 = 0$, $0 + 1 = 1,\ 0 + 2 = 2,\ 1 + 1 = 2,\ 1 + 2 = 0,\ 2 + 2 = 1$ и условием коммутативности.

# Приложение

## 1. ПОЛЕ. КОЛЬЦО. ПОДПОЛЕ. ПОДКОЛЬЦО

### Поля и кольца

Понятие поля ближе всего к привычным для нас действительным числам. Разумеется, слово «поле» здесь употребляется не в сельскохозяйственном смысле…

**Определение.** ***Полем*** называется непустое множество $K$, в котором определены две операции, называемые ***сложением*** и ***умножением***, которые сопоставляют любым двум элементам $a, b$ множества $K$ элементы, называемые их ***суммой*** и ***произведением*** и обозначаемые $a + b$ и $ab$, соответственно. Эти операции должны обладать следующими свойствами.

1. Коммутативность: $a + b = b + a$ и $ab = ba$ для любых $a, b$.
2. Ассоциативность: $a + (b + c) = (a + b) + c,\ a(bc) = (ab)c$ для любых $a, b, c$.
3. Существование нейтральных элементов, называемых ***нулём*** 0 для операции сложения и ***единицей*** 1 для операции умножения: для любого $a$ выполнено равенство $a + 0 = a,\ a \cdot 1 = a$. Можно доказать единственность нейтральных элементов по сложению и по умножению. Предполагается, что поле содержит не только элемент 0, иными словами, $0 \neq 1$.

4. Существование противоположного элемента по сложению: для любого $a$ существует элемент $-a$, такой, что $a + (-a) = 0$.
5. Существование обратного элемента по умножению: для любого $a \neq 0$ существует элемент $a^{-1}$, такой, что $aa^{-1} = 1$. Противоположный и обратный элементы для заданного $a$ единственны.
6. Дистрибутивность: $a(b + c) = ab + ac$ для любых $a, b, c$.

Совокупность всех этих условий называется аксиомами поля. Примерами полей служат множество рациональных чисел, множество действительных чисел и множество комплексных чисел с обычными операциями. Выполнение для них аксиом поля известно из школьного курса математики.

**Определение**. Подмножество $L \subset K$ поля $K$ называется ***подполем*** поля $K$, если оно является полем относительно введенных в поле $K$ операций. Это означает, что если $a, b \in L$, то $a + b \in L$, $ab \in L$. В свою очередь, при этом поле $K$ называется ***расширением*** поля $L$.

Например, поле рациональных чисел – подполе поля действительных чисел, поскольку сумма и произведение рациональных чисел – рациональные числа. Точно так же – поле действительных чисел – подполе поля комплексных чисел.

Рассмотрим важный пример поля, имеющего конечное число элементов. Для этого рассмотрим множество, состоящее из чисел 0,1,2, и определим на этом множестве операции сложения и умножения с помощью таблиц. В первой строке и первом столбце стоят слагаемые (сомножители), на пересечении строк и столбцов стоят их суммы (произведения).

| сумма | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | 1 | 2 |
| 1 | 1 | 2 | 0 |
| 2 | 2 | 0 | 1 |

| произведение | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 |
| 2 | 0 | 2 | 1 |

Иными словами, результатом операции является остаток от деления суммы (произведения) на число 3.

Проверка того, что это множество с введёнными операциями образует поле, не представляет труда и будет полезна для читателя. В качестве примера

найдём для числа 2 обратные по сложению и умножению. Так как $2 + 1 = 0$, то обратным элементом по сложению является 1. Так как $2 \cdot 2 = 1$, то обратным по умножению для числа 2 служит само это число. Это поле принято обозначать $\mathbb{Z}_3$.

**Кольца (коммутативные)**

**Определение.** ***Коммутативным кольцом с единицей*** называется непустое множество $A$, в котором определены две операции, называемые ***сложением*** и ***умножением***, которые сопоставляют любым двум элементам $a, b$ множества $A$ элементы, называемые их ***суммой*** и ***произведением*** и обозначаемые $a + b$ и $ab$, соответственно. Эти операции должны обладать следующими свойствами.

1. Коммутативность: $a + b = b + a$ и $ab = ba$ для любых $a, b$.
2. Ассоциативность: $a + (b + c) = (a + b) + c$, $a(bc) = (ab)c$ для любых $a, b, c$.
3. Существование нейтральных элементов, называемых нулём 0 для операции сложения и единицей 1 для операции умножения: для любого $a$ выполнено равенство $a + 0 = a$, $a \cdot 1 = a$. Можно доказать единственность нейтральных элементов по сложению и по умножению.
4. Существование противоположного элемента по сложению: для любого $a$ существует элемент $-a$, такой, что $a + (-a) = 0$.
5. Дистрибутивность: $a(b + c) = ab + ac$ для любых $a, b, c$.

Таким образом, аксиомы коммутативного кольца с единицей совпадают с аксиомами поля, за исключением существования обратного элемента по умножению и требования $0 \neq 1$. Иными словами, множество, состоящее только из нуля, с операциями $0 + 0 = 0$, $0 \cdot 0 = 0$ относится к коммутативным кольцам.

Следовательно, всякое поле представляет собой и коммутативное кольцо с единицей относительно тех же операций. Обратное утверждение неверно.

Примерами колец служат все поля, как отмечено выше. Важными примерами, также, являются множество целых чисел и множество многочленов от одной или нескольких переменных.

По аналогии с приведённым выше примером конечного (то есть состоящего из конечного числа элементов) поля, рассмотрим множество чисел 0,1,2,3 с операциями сложения и умножения этих чисел, определёнными как остатки от деления на 4 результатов обычных операций над этими числами. В

первой строке и первом столбце стоят слагаемы (сомножители), на пересечении строк и столбцов стоят их суммы (произведения).

| сумма | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 |
| 1 | 1 | 2 | 3 | 0 |
| 2 | 2 | 3 | 0 | 1 |
| 3 | 3 | 0 | 1 | 2 |

| произведение | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 |
| 2 | 0 | 2 | 0 | 2 |
| 3 | 0 | 3 | 2 | 1 |

Легко проверить, что это множество, обозначаемое $\mathbb{Z}_4$, является коммутативным кольцом с единицей. Однако оно не является полем, так как число 2 не имеет обратного элемента по умножению (в строке, перечисляющей результаты умножения числа 2 на все элементы кольца, нет числа 1). Можно доказать, что аналогично определяемое множество $\mathbb{Z}_n$, состоящее из остатков от деления на число $n$, то есть из чисел $0,1 \ldots, n-1$ с операциями, аналогичными приведённым в примерах выше, является коммутативным кольцом с единицей, и это кольцо является полем тогда и только тогда, когда число $n$ – простое.

Довольно часто в определении кольца опускают требование коммутативности умножения и требование существования единицы. Ниже мы будем упоминать об этом при необходимости.

## ГОМОМОРФИЗМ И ИЗОМОРФИЗМ ГРУПП, КОЛЕЦ И ПОЛЕЙ

## Гомоморфизм и изоморфизм групп. Образ. Ядро. Нормальная подгруппа. Фактор-группа. Теорема о гомоморфизме для групп

**Определение.** Подгруппа $H$ группы $G$ называется нормальной подгруппой группы $G$, если для любого $g \in G$ выполнено условие $gH = Hg$.

**Определение.** Отображение $f: G \to F$ группы $G$ с операцией $x \circ y$ в группу $F$ с операцией $a * b$ называется ***гомоморфизмом*** групп, если для любых $x, y \in G$ имеем: $f(x \circ y) = f(x) * f(y)$. Подмножество группы $F$, состоящее из образов элементов $G$ при этом отображении, называется образом

этого гомоморфизма и обозначается $Im\, f$. Элементы группы $G$, которые при этом отображении переходят в нейтральный элемент группы $F$, называется ядром $Kerf$ этого гомоморфизма. Если это отображение взаимно-однозначное, то гомоморфизм называется изоморфизмом.

**Теорема.** ***Образ гомоморфизма*** $\boldsymbol{f: G \to F}$ ***групп является подгруппой группы*** $\boldsymbol{F}$***, а ядро этот гомоморфизма является нормальной подгруппой группы*** $\boldsymbol{G}$***.***

**Доказательство.**

Если $b_1 = f(a_1)$ и $b_2 = f(a_2)$, то $f(a_1) * f(a_2) = f(a_1 \circ a_2) \in Imf$. Это доказывает первое утверждение.

Пусть $a_1 \in Kerf$ и $a_2 \in Kerf$. Тогда $f(a_1 \circ a_2) = f(a_1) * f(a_2) = e_F * e_F = e_F$. Это означает, что $a_1 \circ a_2 \in Kerf$. Пусть $a \in Kerf$. Тогда $a^{-1} \circ a = e_G$. Так как $f(a) = e_F$ и $f(e_G) = e_F$, получаем, что $e_F = f(e_G) = f(a^{-1} \circ a) = f(a^{-1}) * f(a) = f(a^{-1}) * e_F = f(a^{-1})$. Осталось проверить условие, что для любого $g \in G$ выполнено условие $g \circ H = H \circ g$, где обозначено $H = Kerf$. Это условие равносильно тому, что для любого $g \in G$ множество $g \circ H \circ g^{-1}$, состоящее из элементов вида $g \circ h \circ g^{-1},\ h \in H$ совпадает с множеством $H$. Для этого достаточно проверить, что $f(g \circ h \circ g^{-1}) = f(g) * f(h) * f(g^{-1}) = f(g) * e_F * f(g^{-1}) = f(g) * f(g^{-1}) = f(g \circ g^{-1}) = f(e_G) = e_F$.

**Теорема.** *Множество смежных классов* $g \circ H$ *группы* $G$ *по ее нормальной подгруппе* $H$ *является группой относительно операции* $(g_1 \circ H) \circ (g_2 \circ H) = (g_1 \circ g_2) \circ H$*. Эта подгруппа называется* ***факторгруппой группы*** $\boldsymbol{G}$ *по её* ***нормальной подгруппе*** $\boldsymbol{H}$ *и обозначается* $G/H$.

Доказательство.

Ассоциативность операции:

$((g_1 \circ H) \circ (g_2 \circ H)) \circ (g_3 \circ H) = ((g_1 \circ g_2) \circ H) \circ (g_3 \circ H) = (g_1 \circ g_2 \circ g_3) \circ H = \big(g_1 \circ (g_2 \circ g_3)\big) \circ H = (g_1 \circ H) \circ (g_2 \circ g_3) \circ H) = (g_1 \circ H) \circ ((g_2 \circ H) \circ (g_3 \circ H))$.

Нейтральный элемент: $e_G \circ H$. Действительно, $g \circ H \circ e_G \circ H = (g \circ e_G) \circ H = g \circ H$ и $(e_G \circ H) \circ (g \circ H) = (e_G \circ g) \circ H = g \circ H$ для любого $g \in G$.

Обратный элемент: $g^{-1} \circ H$. Действительно,

$(g \circ H) \circ (g^{-1} \circ H) = (g \circ g^{-1}) \circ H = e_G \circ H$ и
$(g^{-1} \circ H) \circ (g \circ H) = (g^{-1} \circ g) \circ H = e_G$

для любого $g \in G$.

**Теорема.** *Образ* $Imf$ *гомоморфизма* $f: G \to F$ *групп изоморфен факторгруппе* $G$ *по ядру* $Kerf$ *этого гомоморфизма.*

Доказательство.

Изоморфизм задаётся сопоставлением образу $f(a)$ элемента $a \in G$ смежного класса $a \circ Kerf$. Действительно, для любого $h \in Kerf$ имеем $f(a \circ h) = f(a) * f(h) = f(a) * e_F = f(a)$.

Рассмотрим примеры подгрупп.

1. В группе целых чисел по сложению множество чисел, делящихся на одно и то же число $n$, образует подгруппу (обозначим это множество $(n)$). Действительно, если $a = kn$ и $b = ln$, то и $a + b = kn + ln = (k + l)n$, то есть делится на число $n$.
2. Рассмотрим группу по сложению, состоящую из многочленов с действительными коэффициентами, Множество многочленов, делящихся без остатка на многочлен $p(x)$, обозначаемое далее $(p(x))$, является подгруппой. Действительно, если $a(x) = k(x)p(x)$ и $b(x) = l(x)p(x)$, то и $a(x) + b(x) = k(x)p(x) + l(x)p(x) = \big(k(x) + l(x)\big)p(x)$, то есть делится на многочлен $p(x)$.
3. В группе по сложению $\mathbb{Z}_4$ элементы 0 и 2 образуют подгруппу, обозначаемую $(2)$. Действительно, $0 + 0 = 0$, $0 + 2 = 2$, $2 + 2 = 0$, то есть операция сложения не выводит за границы рассматриваемого множества.
4. В группе по сложению $\mathbb{Z}_5$ подгруппами являются лишь сама группа и нулевая подгруппа, состоящая из нулевого элемента. Действительно, по теореме Лагранжа порядок подгруппы является делителем порядка конечной группы, а число 5 – простое.

Рассмотрим примеры смежных классов по подгруппе и соответствующих факторгрупп.

1. Для подгруппы $(n)$ группы целых чисел по сложению смежными классами являются множества вида $a + (n)$, состоящие из всех чисел вида $a + kn$, $k \in \mathbb{Z}$. Иными словами, все числа из одного смежного класса имеют одинаковые остатки при делении на число $n$. Так как различные остатки от деления на число $n$ – это числа $0,1, \dots, n-1$, все различные смежные классы по подгруппе $(n)$ группы целых чисел по сложению имеют вид: $0 + (n)$, $1 + (n)$, …,$n - 1 + (n)$.Они и образуют факторгруппу. Часто используют также обозначения $\mathbb{Z}$, $n\mathbb{Z}$, $\mathbb{Z}_n$ для группы целых чисел по сложению, подгруппы целых чисел, кратных числу $n$, и множества остатков от деления целых чисел на $n$. Факторгруппой

группы $\mathbb{Z}$ по подгруппе $n\mathbb{Z}$ является множество смежных классов и эта группа изоморфна группе $\mathbb{Z}_n$.

2. Так как остатками от деления многочленов $a(x)$ на многочлен $p(x)$ являются все многочлены $b(x)$ степени меньшей, чем степень многочлена $p(x)$, множеством смежных классов по подгруппе $(p(x))$ является множество всех многочленов вида $b(x) + k(x)p(x)$. Это множество образует факторгруппу.
3. В группе по сложению $\mathbb{Z}_4$ смежными классами по подгруппе $(2)$ являются $0 + (2)$, $1 + (2)$, так как класс $2 + (2)$ равен классу $0 + (2)$, а класс $3 + (2)$ равен классу $1 + (2)$. Эти смежные классы и образуют факторгруппу.

Рассмотрим примеры сложения в факторгруппах.

1. Сумма смежных классов $3 + (6)$ и $4 + (6)$ по подгруппе $(6)$ группы целых чисел по сложению представляет собой смежный класс $7 + (6) = 1 + (6)$, так как число 7 даёт при делении на 6 остаток 1.
2. Суммой смежных классов $2x + 3 + (x^2 + 1)$ и $x + 2 + (x^2 + 1)$ по подгруппе $(x^2 + 1)$ является смежный класс $3x + 5 + (x^2 + 1)$.
3. В группе $\mathbb{Z}_4$ сумма смежных классов $0 + (2), 1 + (2)$ по подгруппе $(2)$ равна $1 + (2)$.

## Гомоморфизм колец, изоморфизм колец и полей. Образ. Ядро. Идеал. Фактор-кольцо. Теорема о гомоморфизмах для колец

Пусть кроме поля $K$ (коммутативного кольца $A$) с введёнными в нём операциями рассматривается поле $K^*$ (коммутативное кольцо $B$) с операциями сложения и умножения элементов $a^*, b^*$, обозначаемыми, соответственно, $\oplus$, $\times$, то есть $a^* \oplus b^*$, $a^* \times b^*$. Сложение и умножение в поле $K$ (кольце $A$) обозначены $a_1 + a_2$ и $a_1 a_2$. Символы $0_K$ и $0_{K^*}$ обозначают, соответственно, нулевые элементы полей $K$ и $K^*$, $0_A$ и $0_B$ обозначают, соответственно, нулевые элементы колец $A$ и $B$.

Символы $1_K$ и $1_{K^*}$ обозначают, соответственно, единицы полей $K$ и $K^*$, $1_A$ и $1_B$ обозначают, соответственно, единицы колец $A$ и $B$. Часто мы будем $0_K$ и $0_A$ обозначать просто 0, а $1_K$ и $1_A$ – просто 1.

**Определение.** Если существует взаимно-однозначное отображение $\varphi$ множества $K$ на множество $K^*$, при котором $\varphi(a + b) = \varphi(a) \oplus \varphi(b)$, $\varphi(ab) = \varphi(a) \times \varphi(b)$, то поля $K$ и $K^*$ называются изоморфными, а отображение $\varphi$ называется ***изоморфизмом*** полей. Для изоморфных полей $K$, $K^*$ используется обозначение $K \cong K^*$.

**Определение.** Отображение $f: A \to B$ коммутативного кольца $A$ в коммутативное кольцо $B$ называется ***гомоморфизмом*** колец, если для любых $a_1, a_2 \in A$ выполняются равенства $f(a_1 + a_2) = f(a_1) \oplus f(a_2)$, $f(a_1 a_2) = f(a_1) \times f(a_2)$, $f(1_A) = 1_B$.

Если это отображение взаимно-однозначное, то гомоморфизм называется изоморфизмом. Для изоморфных колец $A$ и $B$ используется обозначение $A \cong B$.

**Определение.** Подмножество кольца $B$, состоящее из образов $f(a)$ элементов $a$ кольца $A$ при гомоморфизме $f: A \to B$, называется ***образом*** этого гомоморфизма и обозначается $Imf$.

**Определение.** Подмножество кольца $A$, состоящее из тех элементов $a$, образом которых при гомоморфизме $f: A \to B$ является нулевой элемент $0_B$ кольца $B$, называется ***ядром*** этого гомоморфизма и обозначается $Kerf$.

**Определение.** Подмножество $A \subset B$ кольца $B$ называется ***подкольцом*** кольца $B$, если оно являлется кольцом относительно введённых на кольце $B$ операций. Это означает, что если $a, b \in A$, то $a + b \in A$, $ab \in A$.

Например, кольцо целых чисел является подкольцом поля рациональных чисел (напомним, что всякое поле является кольцом).

**Определение.** Подмножество $I \subset A$ кольца $A$ называется ***идеалом*** этого кольца, если выполнены следующие свойства:
для любых $a, b \in I$ также $a + b \in I$, для любого $a \in I$ и любого $b \in A$ элемент $ab \in I$.

Примеры.

1. Идеалом в кольце целых чисел является множество чисел, делящихся на одно и то же число $n$, обозначим это множество $(n)$ и проверим выполнение свойств идеала. Действительно, если $a = kn$ и $b = ln$, то и $a + b = kn + ln = (k + l)n$, то есть делится на число $n$. Если $a = kn$, то для любого целого числа $b$ имеем $ab = knb = kb \cdot n$, то есть $ab$ делится на число $n$.
2. Рассмотрим кольцо многочленов с действительными коэффициентами, обозначаемое $\mathbb{R}[x]$. Множество многочленов, делящихся без остатка на многочлен $p(x)$, обозначаемое далее $(p(x))$, является идеалом кольца $\mathbb{R}[x]$. Действительно, если
$a(x) = k(x)p(x)$ и $b(x) = l(x)p(x)$, то и
$a(x) + b(x) = k(x)p(x) + l(x)p(x) = \big(k(x) + l(x)\big)p(x)$,
то есть делится на многочлен $p(x)$. Если $a(x) = k(x)p(x)$, то для

любого многочлена $b(x)$ имеем
$a(x)b(x) = k(x)p(x)b(x) = (k(x)b(x))p$, то есть $a(x)b(x)$ делится на многочлен $p(x)$.

3. В кольце $\mathbb{Z}_4$ идеал образуют элементы 0 и 2. Действительно, $0 + 0 = 0,\ 0 + 2 = 2, 2 + 2 = 0$, то есть операция сложения не выводит за границы рассматриваемого множества. Таблица умножения для этого кольца, приведённая выше, показывает, что при умножении любого элемента кольца $\mathbb{Z}_4$ на числа 0 и 2 мы снова получаем те же числа 0 и 2. Обозначим этот идеал $(2)$.
4. Стоит отметить, что в поле – частном случае кольца – существуют только два идеала. Один из них состоит из нулевого элемента. Если же в идеале есть отличные от нуля элемент $a$, то при умножении его на обратный элемент $a^{-1}$ мы получим, что этому идеалу принадлежит единица поля, а вместе с ней и остальные элементы поля.

**Теорема.** *Образ гомоморфизма $f: A \to B$ является подкольцом кольца $B$, а ядро этого гомоморфизма – идеалом кольца $A$.*

Доказательство.

Для доказательства первого утверждения достаточно проверить, что если $b_1 \in Imf,\ \ b_2 \in Imf$, то $b_1 \oplus b_2 \in Imf$ и $b_1 \times b_2 \in Imf$. Так как $b_1 \in Imf$, $b_2 \in Imf$, существуют $a_1,\ a_2 \in A$, такие, что $b_1 = f(a_1),\ b_2 = f(a_2)$. Тогда, по определению гомоморфизма $b_1 \oplus b_2 = f(a_1) \oplus f(a_2) = f(a_1 + a_2) \in Imf$ и $b_1 \times b_2 = f(a_1) \times f(a_2) = f(a_1 a_2) \in Imf$.

Докажем второе утверждение. Для этого заметим, что если $a_1 \in Kerf$ и $a_2 \in Kerf$, т.е. $f(a_1) = 0_B$ и $f(a_2) = 0_B$, то $f(a_1 + a_2) = f(a_1) \oplus f(a_2) = 0_B$, т.е. $a_1 + a_2 \in Kerf$. Кроме того, для любого $a \in Kerf$ и любого $b \in A$ выполняется равенство $f(ab) = f(a) \times f(b) = 0_B \times f(b) = 0_B$, т.е. элемент $ab \in Kerf$.

**Следствие.** *При гомоморфизме полей образом поля является поле, изоморфное исходному полю, так как ядром, согласно примеру 4 выше, будет нулевой идеал. Ядро не может совпасть с исходным полем, иначе в образе не содержится $1_B \neq 0_B$ . Следовательно, гомоморфное отображение полей – взаимно-однозначное и, следовательно, гомоморфизм является изоморфизмом исходного поля и его образа.*

**Определение.** ***Смежным классом*** $a + I$ по идеалу $I$ кольца $A$ называется подмножество кольца $A$, состоящее из элементов вида $a + b$, где $b \in I$.

**Определение.** Смежные классы $a + I$ и $c + I$ называются ***равными***, если $c - a \in I$.

Примеры. (Обратите внимание на соответствующие примеры вопроса 3)

1. Для идеалов $(n)$ кольца целых чисел смежными классами являются множества вида $a+(n)$, состоящие из всех чисел вида $a+kn,\ k\in\mathbb{Z}$. Иными словами, все числа из одного смежного класса имеют одинаковые остатки при делении на число $n$. Так как различные остатки от деления на число $n$ – это числа $0,1,\dots,n-1$, все различные смежные классы по идеалу $(n)$ кольца целых чисел имеют вид: $0+(n)$, $1+(n)$, $\dots$, $n-1+(n)$.
2. Так как остатками от деления многочленов $a(x)$ на многочлен $p(x)$ являются все многочлены $b(x)$ степени меньшей, чем степень многочлена $p(x)$, множеством смежных классов по идеалу $(p(x))$ является множество всех многочленов вида $b(x)+k(x)p(x)$.
3. В кольце $\mathbb{Z}_4$ смежными классами по идеалу $(2)$ являются $0+(2)$, $1+(2)$, так как класс $2+(2)$ равен классу $0+(2)$, а класс $3+(2)$ равен классу $1+(2)$.

**Определение.** Суммой смежных классов $a+I$ и $c+I$ называется смежный класс $(a+c)+I$, а произведением этих смежных классов называется смежный класс $(ac)+I$.

Проверим корректность этого определения. Это означает, что требует проверки следующее утверждение:

*Если* $a+I=b+I$ *и* $c+I=d+I$, *то* $(a+c)+I=(b+d)+I$ *и* $(ac)+I=(bd)+I$.

Доказательство.

Равенства $a+I=b+I$ и $c+I=d+I$ по определению означают, что $a-b\in I$ и $c-d\in I$. При этом $(a+c)-(b+d)=(a-b)+(c-d)\in I$. Первое утверждение доказано.

Из $a-b\in I$ следует, что $a=b+k, k\in I$, из $(c-d)\in I$ следует, что $c=d+l,\ l\in I$. Поэтому
$ac-bd=(b+k)(d+l)-bd=bd+kd+bl+kl-bd=kd+bl+kl\in I$.

Таким образом, $(ac)+I=(bd)+I$.

**Примеры.**

1. Сумма смежных классов $3+(6)$ и $4+(6)$ по идеалу $(6)$ кольца $\mathbb{Z}$ целых чисел представляет собой смежный класс $7+(6)=1+(6)$, так как число 7 даёт при делении на 6 остаток 1. Произведение этих смежных классов равно $12+(6)=(6)$, так как 12 делится на 6 без остатка.

2. Суммой смежных классов $2x+3+(x^2+1)$ и $x+2+(x^2+1)$ по идеалу $(x^2+1)$ кольца многочленов $\mathbb{R}[x]$ является смежный класс $3x+5+(x^2+1)$. Произведением этих смежных классов является смежный класс $2x^2+7x+6+(x^2+1)=7x+4+(x^2+1)$, так как остаток от деления многочлена $2x^2+7x+6$ на многочлен $x^2+1$ равен $7x+4$.
3. В кольце $\mathbb{Z}_4$ сумма смежных классов $0+(2), 1+(2)$ по идеалу $(2)$ равна $1+(2)$, а произведение этих смежных классов равно $0+(2)$.

**Теорема.** *Множество смежных классов по идеалу $I$ коммутативного кольца с единицей $A$ образует коммутативное кольцо с единицей относительно операций, заданных на множестве смежных классов.*

Доказательство.

Проверим коммутативность операций:

$a+I+b+I=(a+b)+I=(b+a)+I=b+I+a+I,$

$(a+I)(b+I)=(ab)+I=(ba)+I=(b+I)(a+I)$ для любых $a,b\in A$.

Ассоциативность:

$a+I+(b+c)+I=\big(a+(b+c)\big)+I=\big((a+b)+c\big)+I=(a+b)+I+c+I,$

$(a+I)\big((b+I)(c+I)\big)=(a+I)\big((bc)+I\big)=a(bc)+I=(ab)c+I=(ab+I)(c+I)=\big((a+I)(b+I)\big)(c+I)$ для любых $a,b,c\in A$.

Нейтральным элементом по сложению является сам идеал $I$, нейтральным элементом по умножению является $1+I$, где 1 обозначает единицу кольца $A$. Обратным элементом по сложению для класса $a+I$ является класс $-a+I$.

**Определение.** Множество смежных классов по идеалу $I$ кольца $A$ называется ***факторкольцом кольца A по идеалу I***. Оно обозначается $A/I$.

**Теорема.** *Пусть $f: A\to B$ – гомоморфизм колец. Тогда $A/Kerf\cong Imf$.*

*Словами: при гомоморфизме $f$ колец образ $Imf$ гомоморфизма изоморфен факторкольцу кольца $A$ по идеалу $Kerf$, являющемуся ядром этого гомоморфизма.*

Доказательство.

Требуется установить взаимно-однозначное соответствие между смежными классами и образами элементов кольца, являющееся гомоморфизмом. Сопо-

ставим смежному классу $a + Kerf$ элемент $f(a)$ из кольца $Imf$. Это – взаимно-однозначное соответствие между смежными классами и образами элементов кольца, так как для всех элементов $a + Kerf$, имеющих вид $a + k$, $k \in Kerf$, имеем:

$f(a + k) = f(a) \oplus f(k) = f(a) \oplus 0_B = f(a)$.

При этом сумме смежных классов $a + Kerf$ и $b + Kerf$, то есть смежному классу $a + b + Kerf$, сопоставляется элемент $f(a + b) = f(a) \oplus f(b)$ кольца $Imf$, а произведению смежных классов $a + Kerf$ и $b + Kerf$, то есть смежному классу $ab + Kerf$, сопоставляется элемент $f(ab) = f(a) \times f(b)$ кольца $Imf$.◀

Проиллюстрируем это доказательство примером. Пусть рассматривается гомоморфизм кольца целых чисел в кольцо $\mathbb{Z}_n$, состоящее из чисел $0,1, \dots, n-1$ – остатков от деления на число $n$, с операциями сложения и умножения, результаты которых равны остаткам от деления на $n$ обычных сумм и произведений этих чисел. Ядром этого гомоморфизма является идеал $(n)$, состоящий из всех целых чисел, делящихся на $n$. Смежные классы по этому идеалу равны $0 + (n)$, $1 + (n)$, …, $n - 1 + (n)$ и изоморфизм, как и в доказательстве теоремы, состоит в сопоставлении этим смежным классам чисел $0,1, \dots, n-1$, то есть $a \leftrightarrow a + (n)$.

Далее задачи из задачника И.В.Проскурякова «Сборник задач по линейной алгебре».

**Задача 1**. Выяснить, образует ли группу множество целых чисел относительно сложения.

Ответ: да (коммутативна).

1) Сумма двух целых чисел – целое число.
2) На множестве целых чисел выполняется ассоциативность по сложению, так как $\mathbb{Z}$ является подмножеством действительных чисел.
3) $\exists e = 0$ (единичный элемент равен 0), $0 \in \mathbb{Z}$, причем, $a + 0 = 0 + a = a$.
4) $\exists a^{-1} = -a$. Действительно, если $a \in \mathbb{Z}$, то $-a \in \mathbb{Z}$ и $a + (-a) = (-a) + a = 0$.
5) Группа коммутативна (как подмножество действительных чисел).

**Задача 2**. Выяснить, образует ли группу множество четных чисел относительно сложения.

Ответ: да (коммутативна).

1) Сумма двух четных чисел – четное число.
2) На множестве четных чисел выполняется ассоциативность по сложению, так как оно является подмножеством действительных чисел.
3) $\exists\, e = 0$ (единичный элемент равен 0), 0 – четное число, причем, $a + 0 = 0 + a = a$.
4) $\exists\, a^{-1} = -a$. Действительно, если $a$ – четное число, то $-a$ – тоже четное число, и $a + (-a) = (-a) + a = 0$.
5) Группа коммутативна (как подмножество действительных чисел).

**Задача 3**. Выяснить, образуют ли группу целые числа, кратные данному натуральному числу $n$ относительно сложения.

Ответ: да (коммутативна).

Заметим, что любое целое число, кратное данному натуральному числу $n$, можно записать в виде $a = n \cdot k,\ k \in \mathbb{Z}$.

1) $a + b = n \cdot k_1 + n \cdot k_2 = n \cdot (k_1 + k_2) \in G$, так как $k_1 + k_2$ – целое число.
2) $a + b + c = n \cdot k_1 + n \cdot k_2 + n \cdot k_3 = n \cdot (k_1 + k_2 + k_3) = n \cdot \big(k_1 + (k_2 + k_3)\big) = n \cdot k_1 + (n \cdot k_2 + n \cdot k_3)$ (или проще: так как ассоциативность выполнена на множестве действительных чисел).
3) $\exists\, e = n \cdot 0 = 0$: $n \cdot k + 0 = n \cdot k + n \cdot 0 = n \cdot (k + 0) = n \cdot k,\ 0 + n \cdot k = n \cdot 0 + n \cdot k = n \cdot (0 + k) = n \cdot k$.
4) $\exists\, a^{-1} = n \cdot (-k) = -nk$: $a + a^{-1} = n \cdot k + n \cdot (-k) = n \cdot \big(k + (-k)\big) = n \cdot \big((-k) + k\big) = a^{-1} + a = n \cdot 0 = 0$.
5) Группа коммутативна (как подмножество действительных чисел).

**Задача 4**. Выяснить, образуют ли группу степени данного действительного числа $b$, $b \neq 0, \pm 1$, с целыми показателями относительно умножения.

Ответ: да (коммутативна).

Заметим, что $G = \{a = b^m, \forall \mathrm{m} \in \mathbb{Z}\}$, $b \neq 0, \pm 1$.

1) $b^{m_1} \cdot b^{m_2} = b^{m_1 + m_2} = b^m \in \mathbb{Z}$, так как сумма двух целых чисел – целое число.
2) $b^{m_1} \cdot b^{m_2} \cdot b^{m_3} = b^{m_1} \cdot (b^{m_2} \cdot b^{m_3})$.
3) $\exists\, e = b^0 = 1$: $b^m \cdot 1 = b^m \cdot b^0 = b^{m+0} = b^{0+m} = 1 \cdot b^m = b^m$.

4) $\exists\, a^{-1} = b^{-m}$ – обратный элемент для $a = b^m$: $a \cdot a^{-1} = b^m \cdot b^{-m} = b^{m-m} = b^{-m} \cdot b^m = a^{-1} \cdot a = b^0 = 1 = e$.

5) Группа коммутативна ($G \subset \mathbb{R}$).

**Задача 5.** Выяснить, образуют ли группу неотрицательные целые числа относительно сложения.

Ответ: нет.

**Замечание 3.** Для того, чтобы доказать, что множество с определенной на нем операцией образует группу, необходимо проверить выполнение всех условий. Для того, чтобы доказать, что множество с определенной на нем операцией не образует группу, достаточно доказать, что не выполняется хотя бы одно условие.

Покажем, что не выполняется условие 4).

Действительно, нейтральным элементом может быть только $e = 0$. Но тогда обратный элемент $a^{-1} = -m \notin G$, так как, если $m$ – положительное число, то $-m$ – отрицательное число, а значит оно не принадлежит нашему множеству.

**Задача 6.** Выяснить, образуют ли группу нечетные целые числа относительно сложения.

Ответ: нет.

Действительно, нечетные числа – это числа вида $a = 2n + 1,\ \forall \mathrm{n} \in \mathbb{Z}$, четные числа – это числа вида $b = 2n,\ \forall \mathrm{n} \in \mathbb{Z}$. Но тогда $a_1 + a_2 = (2n_1 + 1) + (2n_2 + 1) = 2(n_1 + n_2 + 1) \notin G$, так как последнее число является четным.

**Задача 7.** Выяснить, образуют ли группу целые числа относительно вычитания.

Ответ: нет.

Докажем, что не выполняется ассоциативность. Действительно, $(m - n) - k = m - n - k = m - (n + k) \neq m - (n - k)$.

**Задача 8**. Выяснить, образуют ли группу рациональные числа относительно сложения.

Ответ: да (коммутативна).

1) Сумма двух рациональных чисел – рациональное число. Действительно, рациональные числа – это числа вида $\frac{p}{q}$, где $\forall p \in \mathbb{Z},\ \forall q \in \mathbb{N}$, поэтому $\frac{p_1}{q_1} + \frac{p_2}{q_2} = \frac{p_1 q_2 + q_1 p_2}{q_1 q_2} \in G$, так как $p_1 q_2 + q_1 p_2 \in \mathbb{Z},\ q_1 q_2 \in \mathbb{N}$.

2) Ассоциативность выполнена, так как рациональные числа – подмножество действительных чисел. Но можно это и доказать: $\frac{p_1}{q_1}+\frac{p_2}{q_2}+\frac{p_3}{q_3}=\frac{p_1q_2+q_1p_2}{q_1q_2}+\frac{p_3}{q_3}=\frac{p_1q_2q_3+p_2q_1q_3+p_3q_1q_2}{q_1q_2q_3}=\frac{p_1q_2q_3+(p_2q_1q_3+p_3q_1q_2)}{q_1q_2q_3}=\frac{p_1q_2q_3}{q_1q_2q_3}+\frac{(p_2q_1q_3+p_3q_1q_2)}{q_1q_2q_3}=\frac{p_1}{q_1}+\frac{p_2q_3+p_3q_2}{q_2q_3}=\frac{p_1}{q_1}+\left(\frac{p_2}{q_2}+\frac{p_3}{q_3}\right)$.

3) $\exists\, e=0=\frac{0}{q}\in G,\ \forall q\in\mathbb{N}$: $\frac{p}{q}+0=\frac{p}{q}+\frac{0}{q}=\frac{0}{q}+\frac{p}{q}=\frac{p}{q}$.

4) $\exists\, a^{-1}=\frac{-p}{q}\in G$ (так как $p\in\mathbb{Z}$, то $-p\in\mathbb{Z}$): $\frac{p}{q}+\frac{-p}{q}=\frac{0}{q}=\frac{-p}{q}+\frac{p}{q}=0$.

5) Группа коммутативна (так как $G\subset\mathbb{R}$).

**Задача 9.** Выяснить, образуют ли группу рациональные числа относительно умножения.

Ответ: нет.

Заметим, что единичным элементом может быть только $e=1=\frac{1}{1}$. Но тогда, очевидно, не существует обратного элемента по умножению для рационального числа $0=\frac{0}{q}$.

**Задача 10**. Выяснить, образуют ли группу рациональные числа, отличные от нуля, относительно умножения.

Ответ: да (коммутативна).

1) $\frac{p_1}{q_1}\cdot\frac{p_2}{q_2}=\frac{p_1p_2}{q_1q_2}\in G$, так как произведение целых чисел – целое число и произведение натуральных чисел – натуральное число.

2) Ассоциативность выполнена ($\mathbb{Q}\subset\mathbb{R}$).

3) Как уже отмечалось выше, $\exists e=1=\frac{1}{1}\in G$.

4) Обратный элемент будет существовать для всех $a=\frac{p}{q}\neq 0$. Действительно, если $p>0$, то $a^{-1}=\frac{q}{p}$ ($q\in\mathbb{Z}, p\in\mathbb{N}$), если же $p<0$, то $-p>0$ и тогда $a^{-1}=\frac{-q}{-p}$ ($-q\in\mathbb{Z}, -p\in\mathbb{N}$).

5) Группа коммутативна (так как $G\subset\mathbb{R}$).

**Задача 11.** Выяснить, образуют ли группу положительные рациональные числа относительно умножения.

Ответ: да (коммутативна).

Заметим, что положительные рациональные числа имеют вид $a = \frac{p}{q}$, $p, q \in \mathbb{N}$. Но тогда условия 1)–5) выполнены (см. решения предыдущих задач).

**Задача 12.** Выяснить, образуют ли группу положительные рациональные числа относительно деления.

Ответ: нет.

Не выполняется пункт 2). Действительно, $\left(\frac{p_1}{q_1} : \frac{p_2}{q_2}\right) : \frac{p_3}{q_3} = \frac{p_1 q_2 q_3}{q_1 p_2 p_3}$. В то время, как $\frac{p_1}{q_1} : \left(\frac{p_2}{q_2} : \frac{p_3}{q_3}\right) = \frac{p_1}{q_1} : \frac{p_2 q_3}{q_2 p_3} = \frac{p_1 q_2 p_3}{q_1 p_2 q_3}$. Результаты не одинаковы. Ассоциативность не выполняется.

**Задача 13.** Выяснить, образуют ли группу двоично-рациональные числа, то есть дроби, у которых в числителе стоит целое число, а в знаменателе – степень числа 2 с целым неотрицательным показателем, относительно сложения.

Ответ: да (коммутативна).

Итак, рассматриваются числа вида $a = \frac{p}{2^n}$, $p \in \mathbb{Z}$, $n \in \mathbb{Z}, n \geq 0$.

1) $\frac{p_1}{2^{n_1}} + \frac{p_2}{2^{n_2}} = \frac{p_1 2^{n_2} + p_2 2^{n_1}}{2^{n_1+n_2}} = \frac{p}{2^n} \in G$ (так как $p_1 2^{n_2} + p_2 2^{n_1} \in \mathbb{Z}$).

2) Ассоциативность выполнена, так как рассматривается подмножество действительных чисел.

3) $\exists e = 0 = \frac{0}{2^n} \in G$: $\frac{p}{2^n} + 0 = \frac{p}{2^n} + \frac{0}{2^n} = \frac{0}{2^n} + \frac{p}{2^n} = \frac{p}{2^n}$.

4) $\exists a^{-1} = \frac{-p}{2^n} \in G$: $a + a^{-1} = \frac{p}{2^n} + \frac{-p}{2^n} = \frac{-p}{2^n} + \frac{p}{2^n} = a^{-1} + a = \frac{0}{2^n} = 0$.

5) Группа коммутативна (так как $G \subset \mathbb{R}$).

**Задача 14.** Выяснить, образуют ли группу все рациональные числа, числители которых – целые числа, а знаменатели равны произведениям простых чисел из данного множества $M$ (конечного или бесконечного) с целыми неотрицательными степенями (лишь конечное число которых может быть отлично от нуля), относительно сложения.

Ответ: да (коммутативна).

Итак, рассматриваются числа вида $a = \frac{n}{p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}}$, $n \in \mathbb{Z}$, $p_1, p_2, \dots p_k$ – простые числа, степени неотрицательны.

1) $\frac{n_1}{p_1^{\alpha_1}p_2^{\alpha_2}\dots p_k^{\alpha_k}}+\frac{n_2}{q_1^{\beta_1}q_2^{\beta_2}\dots q_k^{\beta_k}}\in G$, так как после приведения к общему знаменателю в числителе будет стоять целое число, а знаменатель является произведением простых чисел из данного множества $M$ с целыми неотрицательными степенями (лишь конечное число которых будет отлично от нуля).

2) Ассоциативность выполнена, так как рассматривается подмножество действительных чисел.

3) $\exists\, e=0=\frac{0}{p_1^{\alpha_1}p_2^{\alpha_2}\dots p_k^{\alpha_k}}\in G$.

4) $\exists\, a^{-1}=\frac{-n}{p_1^{\alpha_1}p_2^{\alpha_2}\dots p_k^{\alpha_k}}\in G$.

5) Группа коммутативна (так как $G\subset\mathbb{R}$).

**Задача 15.** Выяснить, образуют ли группу корни $n$-й степени из единицы (как действительные, так и комплексные) относительно умножения.

Ответ: да (коммутативна).

Существует ровно $n$ различных комплексных чисел $\varepsilon_1,\varepsilon_2,\dots\varepsilon_n$, таких, что $\varepsilon_k^n=1$, $k=1,2,\dots n$. Каждое из них можно записать в тригонометрической форме: $\varepsilon_k=e^{i\frac{2\pi k}{n}}$.

1) Пусть $\varepsilon_1,\varepsilon_2\in G$, то есть $\varepsilon_1^n=1$ и $\varepsilon_2^n=1$. Покажем, что $\varepsilon_1\cdot\varepsilon_2\in G$. Действительно, $(\varepsilon_1\cdot\varepsilon_2)^n=\varepsilon_1^n\cdot\varepsilon_2^n=1\cdot1=1$.

2) Ассоциативность выполнена, так как рассматривается подмножество комплексных чисел.

3) $\exists\, e=1=e^{\frac{2\pi ni}{n}}\in G$. Действительно, $1^n=1$ и $\varepsilon_k\cdot1=1\cdot\varepsilon_k=\varepsilon_k$.

4) Более сложным является вопрос о существовании и виде обратного элемента. Пусть $a=\varepsilon_k=e^{i\frac{2\pi k}{n}}$, тогда $a^{-1}=\varepsilon_k^{-1}=e^{i\frac{2\pi(n-k)}{n}}$. Действительно, $\varepsilon_k\cdot\varepsilon_k^{-1}=e^{i\frac{2\pi k}{n}}\cdot e^{i\frac{2\pi(n-k)}{n}}=e^{i\frac{2\pi(n-k)}{n}}\cdot e^{i\frac{2\pi k}{n}}=\varepsilon_k^{-1}\cdot\varepsilon_k=e^{i\cdot2\pi}=1$ (формула Эйлера).

5) Группа коммутативна (так как $G\subset\mathbb{C}$).

**Задача 17.** Выяснить, образуют ли группу квадратные матрицы порядка $n$ с действительными элементами относительно умножения.

Ответ: нет.

Пусть $A,B,C$ – матрицы порядка $n$.

1) $A \cdot B \in G$.

2) $A \cdot B \cdot C = A \cdot (B \cdot C)$ (ассоциативность по умножению на множестве квадратных матриц).

3) $\exists\, e = E \in G$.

4) Если $detA = 0$, то $A^{-1}$ не существует.

**Замечание 4.** Обратным элементом может быть только обратная матрица, если она существует, и тогда $A \cdot A^{-1} = A^{-1} \cdot A = E$.

**Задача 18.** Выяснить, образуют ли группу невырожденные квадратные матрицы порядка $n$ с действительными элементами относительно умножения.

Ответ: да (некоммутативна).

1)–4) выполняется (см. предыдущую задачу).

5) Произведение матриц (даже квадратных), как известно, в общем случае не коммутативно.

**Задача 19.** Выяснить, образуют ли группу невырожденные матрицы порядка $n$ с целыми элементами относительно умножения.

Ответ: нет.

1)–3) выполняются (см. предыдущие задачи).

1) Нет. Если $detA = 0$, то $A^{-1}$ не существует. Но если и существует, то в качестве элементов может содержать рациональные числа, например, $A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \Rightarrow A^{-1} \begin{pmatrix} -2 & 1 \\ \frac{3}{2} & -\frac{1}{2} \end{pmatrix}$.

**Задача 20.** Выяснить, образуют ли группу квадратные матрицы порядка $n$ с целыми элементами и определителем, равным 1, относительно умножения.

Ответ: да (некоммутативна).

1) $det(AB) = det\mathrm{A} \cdot det\mathrm{B} = 1 \cdot 1 = 1 \Rightarrow AB \in G$.

2) $A \cdot B \cdot C = A \cdot (B \cdot C)$ (ассоциативность по умножению на множестве квадратных матриц).

3) $\exists\, e = E \in G$, так как $detE = 1$.

4) $\exists\ a^{-1} = A^{-1} \in G$, так как $A^{-1} = \frac{1}{detA}\begin{pmatrix} A_{11} & \cdots & A_{1n} \\ \vdots & \ddots & \vdots \\ A_{n1} & \cdots & A_{nn} \end{pmatrix}$, где $detA = 1$, а все числа $A_{ij}$ – целые числа (алгебраические дополнения элементов $a_{ij}$ – определители квадратных матриц порядка $n-1$ с целыми элементами.

5) Произведение матриц некоммутативно.

**Задача 21.** Выяснить, образуют ли группу квадратные матрицы порядка $n$ с целыми элементами и определителем, равным $\pm 1$, относительно умножения.

Ответ: да (некоммутативна).

См. предыдущую задачу.

**Задача 22.** Выяснить, образуют ли группу матрицы порядка $n$ с действительными элементами относительно сложения.

Ответ: да (коммутативна).

1) $A + B \in G$.

2) $A + B + C = A + (B + C)$ (ассоциативность по сложению на множестве квадратных матриц).

3) $\exists\ e = \begin{pmatrix} 0 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 0 \end{pmatrix}$ – нулевая матрица.

4) $\exists\ a^{-1} = -A = \begin{pmatrix} -a_{11} & \cdots & -a_{1n} \\ \vdots & \ddots & \vdots \\ -a_{n1} & \cdots & -a_{nn} \end{pmatrix}$, очевидно, что $a + a^{-1} = A + (-A) = (-A) + A = a^{-1} + a = e$.

5) $A + B = B + A$, так как сложение матриц коммутативно.

**Задача 23.** Выяснить, образуют ли группу векторы $n$-мерного линейного пространства $\mathbb{R}^n$ относительно сложения.

Ответ: да (коммутативна).

1) $\bar{b} + \bar{c} \in G$, так как $\bar{b} + \bar{c} \in \mathbb{R}^n$.

2) $\bar{b} + \bar{c} + \bar{d} = \bar{b} + (\bar{c} + \bar{d})$ (так как выполняется ассоциативность по координатам).

3) $\exists\ e = \bar{0}$ – нулевой вектор.

4) Если $a = \bar{b}\ \exists\ a^{-1} = -\bar{b} = (-b_1, \ldots, -b_n)$.

5) $\bar{b}+\bar{c}=(b_1+c_1,\dots,b_n+c_n)=(c_1+b_1,\dots,c_n+b_n)=\bar{c}+\bar{b}\Rightarrow$ группа коммутативна.

**Задача 24.** Выяснить, образуют ли группу параллельные переносы трехмерного пространства $\mathbb{R}^3$, если за произведение переносов $s$ и $t$ принято их последовательное выполнение.

Ответ: да (коммутативна).

Пусть $s(\bar{x})=\bar{x}+\bar{s_0},\ \mathrm{t}(\bar{x})=\bar{x}+\bar{t_0},\ r(\bar{x})=\bar{x}+\bar{r_0}$.

1) $s(\bar{x})\cdot\mathrm{t}(\bar{x})=(\bar{x}+\bar{s_0})+\bar{t_0}=\bar{x}+\bar{s_0}+\bar{t_0}=\bar{x}+(\bar{s_0}+\bar{t_0})\in G$ – перенос на вектор $(\bar{s_0}+\bar{t_0})$.

2) $(s(\bar{x})\cdot\mathrm{t}(\bar{x}))\cdot r(\bar{x})=(\bar{x}+\bar{s_0}+\bar{t_0})+\bar{r_0}=\bar{x}+\bar{s_0}+\bar{t_0}+\bar{r_0}=$
$=(\bar{x}+\bar{s_0})+(\bar{t_0}+\bar{r_0})=s(\bar{x})\cdot(\mathrm{t}(\bar{x})\cdot r(\bar{x}))\Rightarrow$ ассоциативность.

3) $\exists\, e$ – перенос на нулевой вектор, то есть $e(\bar{x})=\bar{x}+\bar{0}$. Действительно,
$s(\bar{x})\cdot e(\bar{x})=(\bar{x}+\bar{s_0})+\bar{0}=\bar{x}+\bar{s_0}=s(\bar{x})$ и
$e(\bar{x})\cdot s(\bar{x})=(\bar{x}+\bar{0})+\bar{s_0}=\bar{x}+\bar{s_0}=s(\bar{x})$.

4) Если $a=s(\bar{x})=\bar{x}+\bar{s_0}$, то $\exists\, a^{-1}=\bar{x}+(-\bar{s_0})$ – перенос на вектор $(-\bar{s_0})$. Действительно, $a\cdot a^{-1}=(\bar{x}+\bar{s_0})+(-\bar{s_0})=\bar{x}+\bar{0}=\bar{x}=e(\bar{x})$.
Аналогично,
$a^{-1}\cdot a=\big(\bar{x}+(-\bar{s_0})\big)+\bar{s_0}=\bar{x}+\bar{s_0}+(-\bar{s_0})=\bar{x}+\bar{0}=e(\bar{x})$.

5) $s(\bar{x})\cdot\mathrm{t}(\bar{x})=(\bar{x}+\bar{s_0})+\bar{t_0}=\bar{x}+\bar{s_0}+\bar{t_0}=\bar{x}+\bar{t_0}+\bar{s_0}=$
$=(\bar{x}+\bar{t_0})+\bar{s_0}=\mathrm{t}(\bar{x})\cdot s(\bar{x})\Rightarrow$ группа коммутативна.

**Задача 25.** Выяснить, образуют ли группу положительные действительные числа, если операция определена так: $a*b=a^b$.

Ответ: нет.

Ассоциативность не выполняется, так как $(a*b)*c=(a^b)^c=a^{bc}$, в то время, как $a*(b*c)=a^{b^c}$. Эти величины, вообще говоря, не равны, например, $(2^2)^3=2^6\neq 2^{2^3}=2^8$.

**Задача 26.** Выяснить, образуют ли группу положительные действительные числа, если операция определена так: $a*b=a^2b^2$.

Ответ: нет.

Ассоциативность не выполняется, так как

$(a*b)*c=(a^2b^2)*c=(a^2b^2)^2c^2=a^4b^4c^2$,
в то время, как $a*(b*c)=a*(b^2c^2)=a^2(b^2c^2)^2=a^2b^4c^4$.

**Задача 27.** Выяснить, образуют ли группу действительные многочлены степени $\leq n$ от неизвестного $x$, включая $P(x) \equiv 0$, относительно сложения.

Ответ: да (коммутативна).

1) $P_n(x) + P_m(x) \in G$.

2) $\big(P_n(x) + P_m(x)\big) + P_l(x) = P_n(x) + (P_m(x) + P_l(x))$.

3) $\exists\, e$ – многочлен, тождественно равный нулю.

4) $\exists\, a^{-1}$. Для многочлена $a = P_n(x)$ обратным элементом будет $a^{-1} = -P_n(x)$.

5) $P_n(x) + P_m(x) = P_m(x) + P_n(x) \Rightarrow$ группа коммутативна.

**Задача 28.** Выяснить, образуют ли группу действительные многочлены степени $n \geq 1$ от неизвестного $x$ относительно сложения.

Ответ: нет.

1) Если $P_n(x)$ – многочлен степени $n$, то $-P_n(x)$ – тоже многочлен степени $n$. Но сумма этих многочленов является многочленом нулевой степени, то есть $P_n(x) + (-P_n(x)) \notin G$. Множество не замкнуто относительно операции, следовательно, группой не является.

Выяснить, какие из следующих множеств являются кольцами (но не полями) и какие полями относительно указанных операций (если операции не указаны, то подразумеваются сложение и умножение чисел).

**Задача 1.** Целые числа.

Ответ: Коммутативное кольцо с единицей, но не поле.

Пусть $a, b, c \in \mathbb{Z}$. Множество замкнуто относительно операций сложения и умножения.

1) $a + b = b + a,\ ab = ba$ (подмножество $\mathbb{R}$).

2) $a + b + c = a + (b + c),\ abc = a(bc)$ (подмножество $\mathbb{R}$).

3) $\exists\, 0,\ \exists\, 1$.

4) $\exists$ противоположный элемент $-a$ для любого целого числа $a$. Но если $a \neq \pm 1$, то $a^{-1} = \frac{1}{a}$ не будет целым числом, а это значит, что на множестве целых чисел обратный элемент существует не всегда.

5) Дистрибутивность выполняется (подмножество $\mathbb{R}$).

Поэтому множество целых чисел с определенными на нем сложением и умножением является коммутативным кольцом с единицей, но не полем.

**Задача 2.** Четные числа.

Ответ: Коммутативное кольцо без единицы.

Множество четных чисел замкнуто относительно сложения и умножения, на нем выполняются коммутативность и ассоциативность по сложению и умножению.

1) $\exists\ 0$, но нет 1, так как 1 не является четным числом.

2) $\exists\ -a$ – противоположный элемент (это число также является четным).

**Задача 3.** Целые числа, кратные данному числу $n$. Рассмотреть случаи: а) $n = 0$, б) $n \neq 0$.

Ответ: а) Кольцо, но не поле; б) кольцо, но не поле.

а) Если $n = 0$, то $M$ состоит только из числа 0. Коммутативность и ассоциативность выполнены (сумма нулей и произведение нулей равно нулю). $\exists\ 0 = 1$ (в этом случае нейтральный элемент по сложению и нейтральный элемент по умножению совпадают (поэтому $M$ полем быть уже не может): $0 + 0 = 0$ и $0 \cdot 0 = 0$. Кроме того, $\exists\ -a = 0$. Поэтому $M$ – коммутативное кольцо с единицей.

б) Если $n \neq 0$. Тогда элементы множества $M$ имеют вид $a = pn,\ b = qn,$ $c = mn,\ p, q, m \in \mathbb{Z}$. Это множество замкнуто относительно сложения и умножения:
$a + b = pn + qn = (p + q)n \in M,\ a \cdot b = pn \cdot qn = (p \cdot q)n \in M.$
Коммутативность и ассоциативность по сложению и умножению выполняются, так как $M \subset \mathbb{R}$. Дистрибутивность выполняется, так как $M \subset \mathbb{R}$.

Заметим, что нейтральный элемент по сложению $0 \in M$ при любом $n$, и для любого $a = pn$ существует противоположный элемент $-a = (-p)n$ при любом $n$. Если $n = 1$, то нейтральный элемент по умножению $1 \in M$ (обратный элемент $a^{-1} = \frac{1}{a} \notin M$, если $a \neq \pm 1$), и поэтому $M$ – коммутативное кольцо с единицей. Если же $n \neq 1$, то среди элементов вида $pn$ нет 1, и тогда $M$ – коммутативное кольцо без единицы.

**Задача 4.** Рациональные числа.

Ответ: Поле.

1) Коммутативность по сложению и умножению выполняется, так как $\mathbb{Q} \subset \mathbb{R}$.

2) Ассоциативность по сложению и умножению выполняется, так как $\mathbb{Q} \subset \mathbb{R}$.

3) $\exists\, 0 \in \mathbb{Q}$ и $\exists\, 1 \in \mathbb{Q}$.

4) Для любого $a = \frac{p}{q} \in \mathbb{Q}$ $\exists\, -a = \frac{-p}{q} \in \mathbb{Q}$, и при условии $a = \frac{p}{q} \neq 0$ $\exists\, a^{-1} \in \mathbb{Q}$ (подробно об этом см. в части «Группы»).

5) $1 \neq 0$.

6) $a(b + c) = ab + ac$, так как $\mathbb{Q} \subset \mathbb{R}$.

**Задача 5.** Действительные числа.

Ответ: Поле.

Рассуждения аналогичны проведенным в задаче 4.

**Задача 6.** Комплексные числа.

Ответ: Поле.

Рассуждения аналогичны проведенным в задаче 4.

**Задача 7.** Числа вида $a + b\sqrt{2}$, где $a, b \in \mathbb{Z}$.

Ответ: Кольцо, но не поле.

Множество $M$ замкнуто относительно сложения и умножения:
$\left(a_1 + b_1\sqrt{2}\right) + \left(a_2 + b_2\sqrt{2}\right) = (a_1 + a_2) + (b_1 + b_2)\sqrt{2} \in M$ и
$\left(a_1 + b_1\sqrt{2}\right)\left(a_2 + b_2\sqrt{2}\right) = (a_1a_2 + 2b_1b_2) + (b_1a_2 + a_1b_2)\sqrt{2} \in M$.

1) Коммутативность по сложению и умножению выполняется, так как $M \subset \mathbb{R}$.

2) Ассоциативность по сложению и умножению выполняется, так как $M \subset \mathbb{R}$.

3) $\exists\, 0 = 0 + 0\sqrt{2} \in M$ и $\exists\, 1 = 1 + 0\sqrt{2} \in M$, причем, $1 \neq 0$.

4) Для любого $\alpha = a + b\sqrt{2}$ существует противоположный элемент $(-a) + (-b)\sqrt{2} \in M$. А вот обратный элемент существует не для всех отличных от нуля чисел множества $M$. Например, для числа $\alpha = 2 + \sqrt{2}$ обратным будет $\alpha^{-1} = \frac{1}{2+\sqrt{2}} = \frac{2-\sqrt{2}}{(2+\sqrt{2})(2-\sqrt{2})} = \frac{2-\sqrt{2}}{4-2} = 1 + \left(-\frac{1}{2}\right)\sqrt{2} \notin M$, так как не все коэффициенты являются целыми числами.

5) Дистрибутивность выполняется, так как $M \subset \mathbb{R}$.

Поэтому $M$ – коммутативное кольцо с единицей.

**Задача 8.** Числа вида $a + b\sqrt{3}$, где $a, b \in \mathbb{Q}$ (рациональные числа).

Ответ: Поле.

Множество $M$ замкнуто относительно сложения и умножения:
$\left(a_1 + b_1\sqrt{3}\right) + \left(a_2 + b_2\sqrt{3}\right) = (a_1 + a_2) + (b_1 + b_2)\sqrt{3} \in M$ и
$\left(a_1 + b_1\sqrt{3}\right)\left(a_2 + b_2\sqrt{3}\right) = (a_1a_2 + 3b_1b_2) + (b_1a_2 + a_1b_2)\sqrt{3} \in M.$

1) Коммутативность по сложению и умножению выполняется, так как $M \subset \mathbb{R}$.

2) Ассоциативность по сложению и умножению выполняется, так как $M \subset \mathbb{R}$.

3) $\exists\ 0 = 0 + 0\sqrt{3} \in M$ и $\exists\ 1 = 1 + 0\sqrt{3} \in M$.

4) $\exists$ противоположный элемент $(-a) + (-b)\sqrt{3} \in M$. Для любого не равного нулю числа $\alpha = a + b\sqrt{3}$ существует обратный элемент: $\alpha^{-1} = \frac{1}{a+b\sqrt{3}} = \frac{a-b\sqrt{3}}{(a+b\sqrt{3})(a-b\sqrt{3})} = \frac{a-b\sqrt{3}}{a^2-3b^2} \in M$, так как $a^2 - 3b^2$ не может быть равно 0 ни при каких $a, b \in \mathbb{Q}$.

5) $1 = 1 + 0\sqrt{3} \neq 0 + 0\sqrt{3} = 0$.

6) $a(b + c) = ab + ac$, так как $M \subset \mathbb{R}$.

**Задача 9.** Комплексные числа вида $a + bi$, где $a, b \in \mathbb{Z}$.

Ответ: Кольцо, но не поле.

Множество $M$ замкнуто относительно сложения и умножения:
$(a_1 + b_1i) + (a_2 + b_2i) = (a_1 + a_2) + (b_1 + b_2)i \in M$ и
$(a_1 + b_1i)(a_2 + b_2i) = (a_1a_2 - b_1b_2) + (b_1a_2 + a_1b_2)i \in M.$

1) Коммутативность по сложению и умножению выполняется, так как $M \subset \mathbb{C}$.

2) Ассоциативность по сложению и умножению выполняется, так как $M \subset \mathbb{C}$.

3) $\exists\ 0 = 0 + 0 \cdot i \in M$ и $\exists\ 1 = 1 + 0 \cdot i \in M$, причем, $1 = 1 + 0 \cdot i \neq 0 + 0 \cdot i = 0$.

4) Для любого $\alpha = a + bi$ существует противоположный элемент $(-a) + (-b)i \in M$. А вот обратный элемент существует не для всех отличных от нуля чисел множества $M$. Например, для числа $\alpha = 1 + i$

обратным будет $\alpha^{-1} = \frac{1}{1+i} = \frac{1-i}{(1+i)(1-i)} = \frac{1-i}{1+1} = \frac{1}{2} + \left(-\frac{1}{2}\right) i \notin M$, так как не все коэффициенты являются целыми числами.

5) Дистрибутивность выполняется, так как $M \subset \mathbb{R}$.

Поэтому $M$ – коммутативное кольцо с единицей.

**Задача 10.** Комплексные числа вида $a + bi$, где $a, b \in \mathbb{Q}$.

Ответ: Поле.

Множество $M$ замкнуто относительно сложения и умножения:
$(a_1 + b_1 i) + (a_2 + b_2 i) = (a_1 + a_2) + (b_1 + b_2) i \in M$ и
$(a_1 + b_1 i)(a_2 + b_2 i) = (a_1 a_2 - b_1 b_2) + (b_1 a_2 + a_1 b_2) i \in M$.

1) Коммутативность по сложению и умножению выполняется, так как $M \subset \mathbb{C}$.

2) Ассоциативность по сложению и умножению выполняется, так как $M \subset \mathbb{C}$.

3) $\exists\ 0 = 0 + 0 \cdot i \in M$ и $\exists\ 1 = 1 + 0 \cdot i \in M$, причем, $1 = 1 + 0 \cdot i \neq 0 + 0 \cdot i = 0$.

4) Для любого $\alpha = a + bi$ существует противоположный элемент $(-a) + (-b) i \in M$. И для любого не равного нулю $\alpha = a + bi$ существует обратный элемент
$\alpha^{-1} = \frac{1}{a+bi} = \frac{a-bi}{(a+bi)(a-bi)} = \frac{a-bi}{a^2+b^2} = \frac{a}{a^2+b^2} + \frac{-b}{a^2+b^2} i \in M$,
так как все коэффициенты являются рациональными числами и по условию $a$ и $b$ не равны нулю одновременно.

5) $1 = 1 + 0 \cdot i \neq 0 + 0 \cdot i = 0$.

6) $a(b + c) = ab + ac$, так как $M \subset \mathbb{C}$.

**Задача 11.** Квадратные матрицы порядка $n$ с целыми элементами относительно сложения и умножения матриц.

Ответ: Некоммутативное кольцо с единицей.

Множество $M$ замкнуто относительно сложения и умножения.

1) Коммутативность по сложению выполняется, а коммутативность по умножению не выполняется.

2) Ассоциативность по сложению и умножению выполняется.

3) Существует нейтральный элемент по сложению $O = \begin{pmatrix} 0 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 0 \end{pmatrix}$ – нулевая матрица и нейтральный элемент по умножению $E = \begin{pmatrix} 1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 1 \end{pmatrix}$ – единичная матрица, причем $O \neq E$.

4) Всегда существует противоположный элемент, равный $-A = \begin{pmatrix} -a_{11} & \cdots & -a_{1n} \\ \vdots & \ddots & \vdots \\ -a_{n1} & \cdots & -a_{nn} \end{pmatrix}$ – противоположная матрица. А вот обратный элемент существует не всегда (см. «Группы»).

5) Дистрибутивность выполняется, так как $M \subset \mathbb{R}$.

Поскольку произведение матриц некоммутативно, то получаем некоммутативное кольцо с единицей.

**Задача 12.** Квадратные матрицы порядка $n$ с действительными элементами относительно сложения и умножения матриц.

Ответ: Некоммутативное кольцо с единицей.

Множество $M$ замкнуто относительно сложения и умножения.

1) Коммутативность по сложению выполняется, а коммутативность по умножению не выполняется.

2) Ассоциативность по сложению и умножению выполняется.

3) Существует нейтральный элемент по сложению $O = \begin{pmatrix} 0 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 0 \end{pmatrix}$ – нулевая матрица и нейтральный элемент по умножению $E = \begin{pmatrix} 1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 1 \end{pmatrix}$ – единичная матрица, причем $O \neq E$.

4) Всегда существует противоположный элемент, равный $-A = \begin{pmatrix} -a_{11} & \cdots & -a_{1n} \\ \vdots & \ddots & \vdots \\ -a_{n1} & \cdots & -a_{nn} \end{pmatrix}$ – противоположная матрица. А вот обратный элемент существует не всегда, например, если $detA = 0$, то обратная матрица не существует.

5) Дистрибутивность выполняется.

Поскольку произведение матриц некоммутативно, то получаем некоммутативное кольцо с единицей.

**Задача 13.** Функции с действительными значениями, непрерывные на отрезке$[-1;1]$, относительно обычных сложения и умножения функций: $(f+g)(x)=f(x)+g(x),\ (fg)(x)=f(x)g(x)$.

Ответ: Коммутативное кольцо с единицей.

Множество $M$ замкнуто относительно так определенных сложения и умножения.

1) Коммутативность по сложению и умножению выполняется, так как выполняется для чисел.
2) Ассоциативность по сложению и умножению выполняется, так как выполняется для чисел.
3) Существует нейтральный элемент по сложению $\varphi(x)\equiv 0,\ \varphi(x)\in M$ и нейтральный элемент по умножению $\phi(x)\equiv 1,\ \phi(x)\in M$.
4) Для любой $f(x)$ существует противоположный элемент $(-f)(x)\equiv -f(x)$. А вот обратный элемент существует не для любой функции, тождественно не равной нулю ($\varphi(x)\equiv 0$ – нулевой элемент!). Действительно, $f(x)=x\in M$, но обратный элемент $\frac{1}{f(x)}=\frac{1}{x}\notin M$, так не является непрерывной на отрезке$[-1;1]$ функцией.
5) Дистрибутивность выполняется.

   Поэтому $M$ – коммутативное кольцо с единицей.

**Задача 14.** Все многочлены от одного неизвестного $x$ с целыми коэффициентами относительно обычных операций сложения и умножения.

Ответ: Коммутативное кольцо с единицей.

Множество $M$ замкнуто относительно так определенных сложения и умножения.

1) Коммутативность по сложению и умножению выполняется, так как выполняется для целых чисел.
2) Ассоциативность по сложению и умножению выполняется, так как выполняется для целых чисел.
3) Существует нейтральный элемент по сложению $P_0(x)\equiv 0,\ P_0(x)\in M$ и нейтральный элемент по умножению $P_1(x)\equiv 1,\ P_1(x)\in M$.
4) Для любого $P_n(x)$ существует противоположный элемент $(-P_n)(x)\equiv -P_n(x)$. А вот обратный элемент существует не всегда.

Если степень многочлена $\geq 1$, то есть многочлен не является константой, то функция $\frac{1}{P_n(x)}$ не является многочленом.

5) Дистрибутивность выполняется, так как так как выполняется для целых чисел.

Поэтому $M$ – коммутативное кольцо с единицей.

**Задача 15.** Матрицы вида $\begin{pmatrix} a & b \\ 2b & a \end{pmatrix}$ с рациональными $a$ и $b$ относительно обычных сложения и умножения матриц.

Ответ: Поле.

Покажем, что множество замкнуто относительно сложения и умножения.

$$\begin{pmatrix} a & b \\ 2b & a \end{pmatrix} + \begin{pmatrix} c & d \\ 2d & c \end{pmatrix} = \begin{pmatrix} a+c & b+d \\ 2(b+d) & a+c \end{pmatrix} \in M,$$

$$\begin{pmatrix} a & b \\ 2b & a \end{pmatrix}\begin{pmatrix} c & d \\ 2d & c \end{pmatrix} = \begin{pmatrix} ac+2bd & ad+bc \\ 2bc+2ad & ac+2bd \end{pmatrix} =$$
$$= \begin{pmatrix} ac+2bd & ad+bc \\ 2(ad+bc) & ac+2bd \end{pmatrix} \in M.$$

Получили, что сумма и произведение матриц являются матрицами того же вида.

1) Сложение матриц такого вида коммутативно, так как коммутативно сложение любых матриц, причем, это будут матрицы того же вида. А вот будет ли коммутативно произведение?

$$\begin{pmatrix} a & b \\ 2b & a \end{pmatrix}\begin{pmatrix} c & d \\ 2d & c \end{pmatrix} = \begin{pmatrix} ac+2bd & ad+bc \\ 2(ad+bc) & ac+2bd \end{pmatrix},$$

$$\begin{pmatrix} c & d \\ 2d & c \end{pmatrix}\begin{pmatrix} a & b \\ 2b & a \end{pmatrix} = \begin{pmatrix} ac+2bd & ad+bc \\ 2(ad+bc) & ac+2bd \end{pmatrix}.$$

Следовательно, для матриц такого вида выполняется и коммутативность по умножению.

2) Ассоциативность по сложению и умножению выполняется для всех матриц (а замечание в начале решения говорит о том, что это будут матрицы того же вида).

3) Существует нейтральный элемент по сложению $O = \begin{pmatrix} 0 & 0 \\ 2\cdot 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in M$ – нулевая матрица, и нейтральный элемент по умножению $E = \begin{pmatrix} 1 & 0 \\ 2\cdot 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}) \in M$ – единичная матрица.

4) Для любой матрицы $A = \begin{pmatrix} a & b \\ 2b & a \end{pmatrix}$ существует противоположный элемент $-A = \begin{pmatrix} -a & -b \\ 2(-b) & -a \end{pmatrix} \in M$.

Существует ли обратный элемент? Заметим, что для любых $a, b \in \mathbb{Q}$ будет выполняться $detA = a^2 - 2b^2 \neq 0$, если $A \neq O$, так как иначе $a^2 = 2b^2 \Leftrightarrow a = \pm\sqrt{2}b$, что невозможно, так как $a$ и $b$ рациональные числа. Это означает, что обратная матрица существует. Но это не означает, что обратная матрица будет иметь такой же вид, то есть будет принадлежать множеству $M$. Посчитаем обратную матрицу.

Итак, $A = \begin{pmatrix} a & b \\ 2b & a \end{pmatrix}$, $detA = a^2 - 2b^2 \neq 0$, $\tilde{A} = \begin{pmatrix} a & -2b \\ -b & a \end{pmatrix}$, $\tilde{A}^t = \begin{pmatrix} a & -b \\ -2b & a \end{pmatrix} \Rightarrow A^{-1} = \frac{1}{a^2-2b^2}\begin{pmatrix} a & -b \\ 2(-b) & a \end{pmatrix} \in M$, то есть имеет такой же вид, что и матрица $A$.

5) $E \neq O$.

6) Рассмотрим

$$\begin{pmatrix} a & b \\ 2b & a \end{pmatrix}\left(\begin{pmatrix} c & d \\ 2d & c \end{pmatrix} + \begin{pmatrix} p & q \\ 2q & p \end{pmatrix}\right) = \begin{pmatrix} a & b \\ 2b & a \end{pmatrix}\begin{pmatrix} c+p & d+q \\ 2(d+q) & c+p \end{pmatrix} = \begin{pmatrix} a(c+p)+2b(d+q) & a(d+q)+b(c+p) \\ 2b(c+p)+2a(d+q) & 2b(d+q)+a(c+p) \end{pmatrix},$$

$$\begin{pmatrix} a & b \\ 2b & a \end{pmatrix}\begin{pmatrix} c & d \\ 2d & c \end{pmatrix} + \begin{pmatrix} a & b \\ 2b & a \end{pmatrix}\begin{pmatrix} p & q \\ 2q & p \end{pmatrix} = \begin{pmatrix} ac+2bd & ad+bc \\ 2bc+2ad & 2bd+ac \end{pmatrix} + \begin{pmatrix} ap+2bq & aq+bp \\ 2bp+2aq & 2bq+ap \end{pmatrix} =$$

$$\begin{pmatrix} a(c+p)+2b(d+q) & a(d+q)+b(c+p) \\ 2b(c+p)+2a(d+q) & 2b(d+q)+a(c+p) \end{pmatrix}$$ ⇒ дистрибутивность выполняется.

**Задача 16.** Матрицы вида $\begin{pmatrix} a & b \\ 2b & a \end{pmatrix}$ с действительными $a$ и $b$ относительно обычных сложения и умножения матриц.

Ответ: Коммутативное кольцо с единицей.

Решение задачи аналогично предыдущей с той лишь разницей, что даже если $A \neq O$, тем не менее, на множестве действительных чисел возможно, что $detA = a^2 - 2b^2 = 0$, а это означает, что обратная матрица (обратный элемент по умножению) не существует.

**Задача 17.** $P_n(x) = a_0 + \sum_{k=1}^{n} a_k \cos kx + b_k \sin kx$ – тригонометрические многочлены произвольной степени $n$.

Ответ: Коммутативное кольцо с единицей.

Множество замкнуто относительно операций сложения и умножения многочленов. Для суммы это очевидно. При умножении будут возникать попарные произведения синусов и косинусов различных аргументов. Но, например, $2\cos kx \sin mx = \sin(k+m)x + \sin(m-k)x$ – тоже тригонометрический многочлен. Аналогично рассматриваются произведения синусов и произведения косинусов.

1) Коммутативность по сложению и умножению выполняется, так как выполняется для действительных чисел.
2) Ассоциативность по сложению и умножению выполняется, так как выполняется для действительных чисел.
3) Существует нейтральный элемент по сложению $P_0(x) \equiv 0,\ P_0(x) \in M$ и нейтральный элемент по умножению $P_1(x) \equiv 1,\ P_1(x) \in M$.
4) Для любого $P_n(x)$ существует противоположный элемент $(-P_n)(x) \equiv -P_n(x)$. А вот обратный элемент существует не всегда. Если степень многочлена $\geq 1$, то есть тригонометрический многочлен не является константой, то функция $\frac{1}{P_n(x)}$ не является тригонометрическим многочленом.
5) Дистрибутивность выполняется, так как выполняется для действительных чисел.

**Замечание.** Если рассмотреть только многочлены произвольной степени вида $P_{\boldsymbol{n}}(x) = a_0 + \sum_{k=1}^{n} a_k \cos kx$, то это тоже будет коммутативное кольцо с единицей, так как оно замкнуто относительно умножения:
$2\cos kx \cos mx = \cos(m+k)x + \cos(m-k)x$ (остальные свойства проверяются аналогично). Но если рассмотреть только многочлены произвольной степени вида $P_{\boldsymbol{n}}(x) = \sum_{k=1}^{n} b_k \sin kx$, то это множество уже не будет кольцом, так как оно не замкнуто относительно умножения. Действительно,
$2\sin kx \sin mx = \cos(m-k)x - \cos(m+k)x$ не является многочленом нужного вида.