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

МЕЖДИСЦИПЛИНАРНЫЕ НАУЧНО-ОБРАЗОВАТЕЛЬНЫЕ ШКОЛЫ МГУ

ГРУППЫ, ПОЛЯ, КОЛЬЦА

В.Г.ЧИРСКИЙ

2023

УДК 512.5

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» в рамках проекта «Междисциплинарные научно-образовательные школы МГУ» рассматриваются вопросы, усвоение которых способствует повышению математической культуры учащихся, развитию их профессиональных компетенций. Выбор тем разработок не случаен. Он основан на методических исследованиях кафедры математического анализа, на учёте мнений кафедр химического факультета, на анализе результатов экзаменов.

Важная цель этих разработок – облегчить самостоятельную работу студентов и способствовать успешной сдаче экзаменов и зачётов. В этом пособии содержится материал, дополняющий курс линейной алгебры, читаемый студентам первого курса химического факультета МГУ.

Элементы теории групп

§1.Определение группы. Примеры

Определение: Пусть G – множество и пусть каждой паре элементов $x \in G, y \in G$ 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, т.е. $(x \circ y) \circ z = x \circ (y \circ z)$, 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, выполняется также: для любых $x, y \in G \quad x \circ y = y \circ x$, 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, т.к. 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 также 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, т.к. 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, т.е. 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 ггрупп, элементы теории представлений групп, основы теории групп Ли и рассказано о приложениях теории групп в физике и химии.

§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 1 (Теорема Лагранжа)

Если H – подгруппа конечной группы G, то число $|H|$ делит число $|G|$, т.е. 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, т.е. 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 $g = g_2h_2$, т.е. $g_1h_1 = g_2h_2$, откуда $g_1 = g_2h_2h_1^{-1}$, т.е. 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, т.е. $|G|$ кратно $|H|$, что и утверждалось.◄

Обозначим X_n множество чисел $1, \dots, n$, т.е. $X_n = \{1, \dots, n\}$. 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 (7.8) , а допускать запись σ в виде

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

т.е. 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 τ, затем σ 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) σ^{-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 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 $\boldsymbol{a - (b - c) \neq (a - b) - c}$)**
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 $\boldsymbol{a : (b : c) \neq (a : b) : c}$)**
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 $\boldsymbol{m = n}$.**
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 ± 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.

§3. 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 $a + (-a) = 0$.

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 (т.е. 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 на 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, т.е. 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.

§4. 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 $f: G \to F$ групп является подгруппой группы F, а ядро этот гомоморфизма является нормальной подгруппой группы 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 $(g_1 \circ$***

$\boldsymbol{H}) \circ (\boldsymbol{g_2} \circ \boldsymbol{H}) = (\boldsymbol{g_1} \circ \boldsymbol{g_2}) \circ \boldsymbol{H}$. ***Эта подгруппа называется факторгруппой группы*** $\boldsymbol{G}$ ***по её нормальной подгруппе*** $\boldsymbol{H}$ ***и обозначается*** $\boldsymbol{G/H}$.

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*** $\boldsymbol{Imf}$ ***гомоморфизма*** $\boldsymbol{f: G \to F}$ ***групп изоморфен факторгруппе*** $\boldsymbol{G}$ ***по ядру*** $\boldsymbol{Kerf}$ ***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 $a + b = kn + ln = (k + l)n$, т.е. 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 $a(x) + b(x) = k(x)p(x) + l(x)p(x) = \big(k(x) + l(x)\big)p(x)$, т.е. делится на многочлен $p(x)$.
3. В группе по сложению $\mathbb{Z}_4$ элементы 0 и 2 образуют подгруппу, обозначаемую (2). Действительно, $0 + 0 = 0,\ 0 + 2 = 2, 2 + 2 = 0$, т.е. 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 $a + kn, \quad k \in \mathbb{Z}$. 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: $0 + (n), \quad 1 + (n), \ \dots \ , \quad n - 1 + (n)$.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. 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, $\oplus$, $\times$, т.е. $a^* \oplus b^*$, $a^* \times b^*$. 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 φ 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 φ 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 $a + b = kn + ln = (k + l)n$, т.е. делится на число n. Если $a = kn$, то для любого целого числа b имеем $ab = knb = kb \cdot n$, т.е. 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 $a(x) + b(x) = k(x)p(x) + l(x)p(x) = \big(k(x) + l(x)\big)p(x)$, т.е. делится на многочлен $p(x)$. Если $a(x) = k(x)p(x)$, то для любого многочлена $b(x)$ имеем $a(x)b(x) = k(x)p(x)b(x) = (k(x)b(x))p$, т.е. $a(x)b(x)$ делится на многочлен $p(x)$.
3. В кольце $\mathbb{Z}_4$ идеал образуют элементы 0 и 2. Действительно, $0 + 0 = 0$, $0 + 2 = 2$, $2 + 2 = 0$, т.е. 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 $\boldsymbol{a+I=b+I}$ ***и*** $\boldsymbol{c+I=d+I}$***, то*** $\boldsymbol{(a+c)+I=(b+d)+I}$ ***и*** $\boldsymbol{(ac)+I=(bd)+I}$**.**

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 $c=d+l,\quad l\in I$. 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*** $\boldsymbol{f: A \to B}$ ***– гомоморфизм колец. Тогда*** $\boldsymbol{A/Kerf \cong Imf}$.

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. Сопоставим 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 $b + Kerf$, т.е. смежному классу $a + b + Kerf$, сопоставляется элемент $f(a + b) = f(a) \oplus f(b)$ кольца Imf, а произведению смежных классов $a + Kerf$ и $b + Kerf$, т.е. 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 $0,1, \dots, n - 1$, т.е. $a \leftrightarrow a + (n)$.