МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ
БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

В.В. Картак, А.В. Зеркина

ОСНОВНЫЕ АЛГЕБРАИЧЕСКИЕ СТРУКТУРЫ: ГРУППЫ, КОЛЬЦА, ПОЛЯ, АЛГЕБРЫ

Учебное пособие

Уфа
РИЦ БашГУ
2012

.

УДК 512.5
ББК 22.1
К45

Издание осуществлено при финансовой поддержке РФФИ (проект 12-01-06819-моб-г), при поддержке гранта правительства РФ по договору №11.G34.31.0042 и за счет внебюджетных средств БашГУ

Картак В.В., Зеркина А.В.

К45 Основные алгебраические структуры: группы, кольца, поля, алгебры: учебное пособие / – Уфа: РИЦ БашГУ 2012. – 51 с.

ISBN

В основу издания лег курс лекций, прочитанных в рамках Международной уфимской школы-конференции по математике, физике и химии для студентов, аспирантов и молодых ученых. Пособие предназначено для студентов 2 курса специальности "Математика"и соответствует программе 3 семестра курса "Алгебра". Полезно будет также всем, интересующимися основами группового анализа.

УДК 512.5
ББК 22.1
ISBN

Содержание

1 Бинарные операции. Полугруппы

Пусть X - некоторое множество. *Бинарной алгебраической операцией* (или законом композиции) на X называется произвольное (фиксированное) отображение $\varphi : X \times X \to X$. Таким образом, любой упорядоченной паре элементов $a, b \in X$ ставится в соответствие однозначно определенный элемент $\varphi(a, b)$ **того же множества** X. Бинарную операцию на X обозначают каким-нибудь символом: $*$, $\circ$, $\diamond$, $\star$, $\cdot$, $+$.

На X можно задать много различных операций. Выделять одну из них будем так: $(X, *)$. При этом говорят, что операция $*$ определяет на X *алгебраическую структуру*.

Например, на множестве $\mathbb{Z}$ целых чисел, помимо операций сложения и умножения, можно указать другие операции: $n \circ m = n + m - nm$, $n * m = -n - m$ и т. д. Мы получаем различные алгебраические структуры $(\mathbb{Z}, +)$, $(\mathbb{Z}, \cdot)$, $(\mathbb{Z}, \circ)$, $(\mathbb{Z}, *)$.

Бинарная операция $*$ называется *ассоциативной*, если

$$(a * b) * c = a * (b * c) \qquad \forall\ a,\ b,\ c \in X.$$

Эта операция называется *коммутативной*, если

$$a * b = b * a \qquad \forall\ a,\ b \in X.$$

Требования ассоциативности и коммутативности независимы. Рассмотрим операцию $*$ на $\mathbb{Z}$, заданную правилом $n * m = -n - m$. Эта операция коммутативна, так как $n * m = m * n$, но эта операция не ассоциативная. Докажем это.

Рассмотрим $(n * m) * k = (-n - m) * k = -(-n - m) - k = n + m - k$, с другой стороны $n * (m * k) = -n - (m * k) = -n + m + k$, сравнивая левые и правые части, видим, что $(n * m) * k \neq n * (m * k)$.

Возьмем множество $M_n(\mathbb{R})$ всех квадратных матриц порядка $n > 1$. На этом множестве определена операция умножения, которая подчиняется ассоциативному закону и не подчиняется коммутативному закону.

Непустое множество X с заданной на нем бинарной ассоциативной операцией $*$ называется *полугруппой* $(X, *)$. Таким образом верны два условия:
G1. $\forall\ \ a,\ b \in X \quad a * b \in X$ замкнутость;

G2. $(a * b) * c = a * (b * c) \quad \forall\ a,\ b,\ c \in X$ ассоциативность.

Пример 1. *1. Множество целых чисел с операцией деления* $(\mathbb{Z}, :)$ *не является полугруппой, так как* $a : b$ *вообще говоря не целое число.* (Не выполняется аксиома замкнутости).

2. *Множество действительных чисел $\mathbb{R}$ с операцией сложения будет полугруппой, так как заданная операция подчиняется ассоциативному закону.*

3. *Это же множество $\mathbb{R}$ по операции умножения тоже является полугруппой.*

4. *Множество целых чисел $\mathbb{Z}$ по операции вычитания не является полугруппой, так как эта операция не подчиняется ассоциативному закону*

$$((a-b)-c \neq a-(b-c)) \Rightarrow (a-b-c \neq a-b+c)$$

5. *Множество квадратных матриц над полем $\mathbb{R}$ по операции вычитания есть полугруппа. Аналогично, это множество по умножению тоже полугруппа, так как операции сложения и умножения матриц подчиняются ассоциативному закону.*

Упражнение 1. *Исследовать свойства алгебраических операций. Операцию будем обозначать* $\circ$.

1. $(\mathbb{Z}, \circ)$, *где* $n \circ m = -n - m$.

2. $(\mathbb{Z}, \circ)$, *где* $n \circ m = n + m + nm$.

3. $(\mathbb{Z}, \circ)$, *где* $a \circ b = \begin{cases} a+b, & \text{если } a \text{ — четное,} \\ a-b, & \text{если } a \text{ — нечетное.} \end{cases}$

4. $(\mathbb{R}, \circ)$, *где* $x \circ y = x^2 y$.

Исследуем операцию в пункте 2. Итак, в множестве целых чисел операция задана следующим образом:

$$n \circ m = n + m + nm$$

Проверим подчиняется ли эта операция ассоциативному закону, т. е. $(n \circ m) \circ k = n \circ (m \circ k)$?

Найдем левую часть

$$\begin{aligned}(n \circ m) \circ k = (n+m+nm) \circ k = n+m+nm+k+(n+m+nm)k = \\ = n+m+nm+k+nk+mk+nmk\ .\end{aligned}$$

Найдем правую часть

$$\begin{aligned}(n \circ (m \circ k)) = n \circ (m+k+mk) = n+m+k+mk+n(m+k+mk) \\ = n+m+k+mk+nm+nk+nmk\end{aligned}$$

Сравнивая левые и правые части мы видим, что они равны, следовательно операция подчиняется ассоциативному закону и множество $\mathbb{Z}$ с этой операцией образует полугруппу. Решите остальные пункты самостоятельно.

Упражнение 2. *Доказать, что для любого элемента a полугруппы A имеют место соотношения*

$$(a^m)^m = a^{mn}, \qquad a^n a^m = a^{m+n}$$

при любых натуральных m и n.

2 Группы

Полугруппа называется *моноидом*, если она содержит единичный элемент
G3. $\exists\, e \in X: \quad \forall\, a \in X \quad a * e = e * a = a.$

Если для каждого элемента моноида существует обратный элемент, то моноид называется *группой.*

G4. $\forall\, a \in X \quad \exists\, a^{-1} \in X: \quad a * a^{-1} = a^{-1} * a = e.$

Итак, если на множестве $(X, *)$ выполнены

- аксиомы $G1$, $G2$, то это полугруппа;
- аксиомы $G1$, $G2$, $G3$, то это моноид;
- аксиомы $G1$, $G2$, $G3$, $G4$, то это группа.

Группы бывают конечные и бесконечные. Если группа содержит конечное число элементов, то эта группа называется *конечной.* Число элементов в конечной группе называется *порядком группы.* Группы, содержащие бесконечное число элементов, называются *бесконечными группами.*

Пример 2. *Рассмотрим множество целых чисел $\mathbb{Z}$. Под бинарной операцией на этом множестве будем понимать обычное сложение. Тогда мы получим группу $(\mathbb{Z}, +)$.*

Действительно, роль единичного элемента в этом случае будет играть 0, так как $0 + a = a + 0 = a$ для любого $a \in \mathbb{Z}$. (0 еще называют нейтральным элементом). Кроме того, для каждого a существует обратный элемент $-a$, (называемый в случае сложения противоположным элементом), так как $a + (-a) = (-a) + a = 0$. Ассоциативность в этом случае следует из законов арифметики. Полученная группа называется *аддитивной группой целых чисел* $(\mathbb{Z}, +)$. Эта группа бесконечная.

Пример 3. *Множество целых чисел* $\mathbb{Z}$ *с операцией умножения есть мультипликативная группа целых чисел* $(\mathbb{Z}, \cdot)$.

Пример 4. *Группа вращений правильного треугольника.*

Пусть A, B и C вершины равностороннего треугольника ABC. Повернем треугольник вокруг его центра O на $120°$ против часовой стрелки. Тогда вершина A перейдет в вершину B, $B \to C$ и $C \to A$. Таким образом, треугольник совместится со своим первоначальным положением (если не учитывать названия вершин), т. е. поворот на $120°$ вокруг точки является преобразованием, переводящим данный треугольник в себя. Обозначим это преобразование через.

$$a = \begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix},$$

где в верхней строчке перечислены все вершины треугольника, а нижняя строчка показывает, куда каждая вершина переходит. Поворот на $240°$ в том же направлении вокруг точки O также является преобразованием, переводящим треугольник в себя. Обозначим это преобразование через b, тогда

$$b = \begin{pmatrix} A & B & C \\ C & A & B \end{pmatrix}$$

Имеется еще одно вращение, переводящее треугольник в себя, отличное от a и b - это поворот на $0°$. Обозначим это преобразование через

$$e = \begin{pmatrix} A & B & C \\ A & B & C \end{pmatrix},$$

Легко видеть, что существуют только три различных вращения плоскости, переводящих равносторонний треугольник в себя, а именно: e, a, b. Рассмотрим теперь множество $G = \{e, a, b\}$. Составим таблицу умножения, где каждая строка, а также каждый столбец соответствует некоторому вращению, переводящему треугольник ABC в себя.

	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Таблица 1.

Преобразование $a \circ b$ получится, если сначала повернуть треугольник на $240°$ а затем еще на $120°$. Следовательно, $a \circ b$ - поворот на $360°$, т.е. не совпадает с e. Нетрудно доказать, что введенная операция в G подчиняется ассоциативному закону, существует единица, это поворот на $0°$. Для каждого элемента существует обратный. Элементы a и b взаимно обратны, т.к. $ab = ba = e$. Итак, G - группа, причем конечная группа. Эта группа называется группой вращения треугольника.

Пример 5. *Группа симметрий правильного треугольника.*

Кроме вращений у равностороннего треугольника имеются еще три симметрии, а именно: отражения относительно осей симметрии l_1, l_2 и l_3, проходящих через вершину треугольника и середину противолежащей стороны.

$$c = \begin{pmatrix} A & B & C \\ A & C & B \end{pmatrix}, \quad d = \begin{pmatrix} A & B & C \\ C & B & A \end{pmatrix}, \quad f = \begin{pmatrix} A & B & C \\ B & A & C \end{pmatrix}.$$

Рассмотрим множество $G = \{e, a, b, c, d, f\}$. Таблица умножения.

	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	b	e	f	c	d
b	b	e	a	d	f	c
c	c	d	f	e	a	b
d	d	f	c	b	e	a
f	f	c	d	a	b	e

Таблица 2.

По таблице 2 видно, что множество G замкнуто относительно введенной операции, операция подчиняется ассоциативному закону, существует единица e - поворот на $0°$. Каждый элемент имеет обратный. Для элемента $a^{-1} = b$, $b^{-1} = a$, $c^{-c} = c$ (сам себе обратный элемент), $d^{-1} = d$, $f^{-1} = f$. Значит, G и в этом случае группа. Она называется *группой симметрии правильного треугольника.*

При рассмотрении конечных групп удобно пользоваться таблицами умножения, которые называются *таблицами Кэли.* В нашем случае это таблицы 1 и 2.

Если все элементы группы коммутируют между собой, то такая группа называется *коммутативной* или *абелевой группой.* Группы из примеров 1 -3 абелевы, а в примере 4 группа G абелевой не является, это сразу видно из таблицы Кэли. Например, $cb = d$, $bc = f$.

Еще несколько примеров групп содержатся в Таблице 3.

Пример 6. $(\mathbb{Z}, \circ)$, *где* $n \circ m = n + m + nm$ *группу не образует.*

Мы уже доказали, что $(\mathbb{Z}, \circ)$ есть полугруппа. Найдем единичный (нейтральный) элемент. Этим элементом является 0, то есть $n \circ 0 = n + 0 + n \cdot 0 = 0$. Теперь нужно для элемента n найти обратный, то есть такой элемент, что $n \circ k = 0$, $n \circ k = n + k + nk = 0$. Следовательно, $k = -\frac{n}{1+n}$, но элемент $-\frac{n}{1+n} \notin \mathbb{Z}$. Таким образом, это множество по данной операции группу не образует.

№	множ.	операция	асс-ть	ком-ть	единица	обр. элемент	группа
1	$\mathbb{R}$	$+$	да	да	0	-a	абел.
2	$\mathbb{R}$	$\cdot$	да	да	1	a^{-1}, $a \neq 0$; у 0 нет	нет
3	$\mathbb{R} \setminus 0$	$\cdot$	да	да	1	a^{-1}	абел.
4	$\mathbb{Z}$	$+$	да	да	0	-a	абел.
5	$\mathbb{Z}$	-	нет	нет	нет	$-$	нет
6	$\mathbb{Z}^+$	$+$	да	да	0	только у 0	нет
7	квадр. матр. поряд. $n \geq 2$	$\cdot$	да	нет	E	только у невыр. матр.	нет
8	матр. $m \times n$	$+$	да	да	0	-A	абел.
9	невыр. матр. поряд. $n \geq 2$	$\cdot$	да	нет	E	A^{-1}	да
10	все отобр. множ. в себя	$\cdot$	да	нет	id	есть только у биект. отобр.	нет
11	биект. отобр. множ. в себя	$\cdot$	да	нет	id	обратн. отобр.	да

Таблица 3.

Упражнение 3. 1. *Составить таблицу умножения для вращений квадрата (поворот на $0°$, на $180°$, на $90°$ и $270°$ против часовой стрелки, вокруг точки пересечения диагоналей). Доказать, что это множество относительно умножения есть группа. Эта группа называется группой вращения квадрата.*

2. *Составить таблицу умножения для всех симметрий квадрата. Это множество из 8 элементов: 4 поворота и 4 оси симметрии. Докажите, что это будет группа которая называется группой симметрии квадрата.*

3. *Найти все симметрии ромба и составить для них таблицу умножения. Доказать, что это множество дает группу, которая называется группой симметрии ромба.*

4. *Образуют ли натуральные числа группу а) по сложению б) по умножению.*

5. *Являются ли абелевыми следующие группы: группа вращений треугольника, группа вращений квадрата, группа симметрий квадрата, группа симметрий ромба.*

6. *Доказать, что в любой группе существует единственный единичный элемент.*

7. *Доказать, что в любой группе существует единственный обратный элемент.*

8. *Доказать, что в произвольной группе: а)* $(ab)^{-1} = b^{-1}a^{-1}$, *б)* $(a_1 \cdot a_2 \cdot \ldots \cdot a_n)^{-1} = a_1^{-1}a_2^{-1}\ldots a_n^{-1}$.

Замечание. Пиджак надевают после рубашки, а снимают раньше. Докажем 8 пункт а) Надо доказать, что $(ab)^{-1} = b^{-1}a^{-1}$ т.е. для элемента (ab) - обратный ему будет $b^{-1}a^{-1}$. Рассмотрим произведение

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

С другой стороны

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

Таким образом, $(ab)(b^{-1}a^{-1}) = (b^{-1}a^{-1})(ab) = e.$

Значит $b^{-1}a^{-1}$ обратный элемент для ab т. е.

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

б) Докажем теперь

$$(a_1 \cdot a_2 \cdot ... \cdot a_n)^{-1} = a_n^{-1} a_{n-1}^{-1} ... a_1^{-1}$$

Доказательство проведем индукцией по n: если для $n-1$ уже доказано, то $(a_1 \cdot a_2 \cdot ... \cdot a_n)^{-1}$ (по пункту (а)) $a_n^{-1}(a_1 \cdot ... \cdot a_{n-1})^{-1} = a_n^{-1} \cdot a_{n-1}^{-1} \cdot ... \cdot a_1^{-1}$ что и требовалось доказать.

Порядок элемента a группы G есть наименьшее натуральное число k такое, что $a^k = e$. Если такого k не существует, то говорят, что a - элемент бесконечного порядка. Порядок элемента будем обозначать через $O(a) = k$.

Порядок конечной группы G – это число ее элементов. Обозначается $O(G)$ или $|G|$.

Упражнение 4. 1. *Найдем порядки всех элементов группе симметрий правильного треугольника. Используя таблицу 2, получим, что* $O(a) = O(b) = 3$, *так как* $a^3 = b^3 = e$, $O(c) = O(d) = O(f) = 2$, *так как* $c^2 = d^2 = f^2 = e$.

2. *Найдите порядки всех элементов в группе симметрий квадрата и ромба.*

3. *В мультипликативной группе всех невырожденных комплексных матриц второго порядка, найдите порядки следующих элементов:*

$$a = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \qquad b = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \qquad c = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix},$$

$$d = \begin{pmatrix} -2+3i & -2+2i \\ 1-i & 3-2i \end{pmatrix}, \qquad f = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}.$$

$O(a) = 2$, так как 2 - наименьшее натуральное число, удовлетворяющее

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

$O(c) = 4$, $O(b) = O(d) = O(f) = \infty$, т. к. не существует такого k, что $b^k = e$, аналогично для d и f. Проверьте.

4. *Доказать, что для любых элементов* a *и* b *группы* G *элементы* ab *и* ba *имеют одинаковые порядки.*

Доказательство: Нам надо доказать, что $O(ab) = O(ba)$, для любых $a, b \in G$. Пусть $O(ab) = n$, $O(ba) = m$. 1) Так как $O(ab) = n$, то

$(ab)^n = e$ и $(ab)^{n+1} = ab\,\underbrace{(ab)(ab)\cdot\ldots\cdot(ab)}_{n+1} = a\,\underbrace{(ba)(ba)\cdot\ldots\cdot(ba)}_{n}\,b = ab$

или $a(ba)^n b = ab$, отсюда следует, что $(ba)^n = e$ и $n \vdots m$ так как $O(ba) = m$ где m - наименьшее натуральное число

2) $O(ba) = m$ и $(ba)^{m+1} = ba$, т. е.

$$\underbrace{(ba)(ba)\cdot\ldots\cdot(ba)}_{m+1} = b\,\underbrace{(ab)(ab)\cdot\ldots\cdot(ab)}_{m}\,a = ba$$

или $b(ab)^m a = ba$. Отсюда следует, что $(ab)^m = m$ и $m \vdots n$. Получим, что $n = m$, т. к. $n \vdots m$ и $m \vdots n$. Таким образом $O(ab) = O(ba)$.

5. *Докажите, что для любых элементов a, b, c группы G*

$$O(abc) = O(bca) = O(cab)$$

6. *Пусть элемент a имеет порядок n. Доказать, что $a^m = e$ тогда и только тогда, когда $m = nd$, где d - произвольное число.*

   Доказательство. Пусть $m = nd + r$, где $0 \leqslant r \leqslant n-1$, тогда $a^m = a^{nd+r} = (a^n)^d a^r = a^r$, т. к. $a^n = e$, но $a^r = e$ в том и только том случае, если $r = 0$, отсюда $a^m = e$ тогда и только тогда, когда $m = nd$.

7. *Пусть a имеет простой порядок p и m - произвольное целое число. Доказать, что либо $a^m = e$, либо элемент a^m имеет порядок p.*

   Указание. Используйте предыдущий пример.

3 Подгруппы

Подмножество A группы G называется *подгруппой*, если оно само является группой относительно той же бинарной операции, которая задана на G.

Многие из групп, указанных ранее, являются подгруппами других групп.

Пример 7. *Аддитивная группа четных чисел является подгруппой аддитивной группы всех целых чисел, а последняя в свою очередь есть подгруппа аддитивной группы рациональных чисел. Все аддитивные группы чисел являются подгруппами аддитивной группы комплексных чисел.*

Пример 8. *Множество всех подстановок n степени по операции умножения дает нам группу, которая называется симметрической группой S_n. Если рассматривать подмножество группы S_n всех четных подстановок, то это подмножество тоже есть группа, эта группа называется знакопеременной группой A_n, и эта группа A_n есть подгруппа группы G_n.*

Пример 9. *Множество всех квадратных невырожденных матриц по операции умножения - группа, которая называется общей линейной группой $GL(n,\mathbb{R})$. Если рассмотреть подмножество $GL(n,\mathbb{R})$ всех матриц с определителем равным единице, то это подмножество даст нам группу, которая называется специальной группой и обозначается $SL(n,\mathbb{R})$. Эта группа будет подгруппой группы $GL(n,\mathbb{R})$.*

Пример 10. *Подмножество группы G, состоящее из одного элемента e, будет тоже подгруппой группы G, эта подгруппа называется единичной подгруппой группы G. С другой стороны, сама группа G является одной из своих подгрупп.*

Центр группы G - это максимальное множество элементов группы G, коммутирующих с каждым элементом группы $Z_G = \{a \in G \quad : \quad \forall b \in G \quad ab = ba\}$.

Упражнение 5. *Докажите, что Z_G есть подгруппа G.*

Доказательство. Пусть g – произвольный элемент группы G. Так как $eg = ge$, то e входит в центр Z_G. Если a входит в центр, то $ag = ga$. Умножив обе части этого равенства слева и справа на a^{-1}, получим $ga^{-1} = a^{-1}g$. Поэтому a^{-1} также входит в центр. Если a и b входят в центр, то $ag = ga$ и $bg = gb$. Поэтому $g(ab) = (ga)b = a(gb) = (ab)g$ и, следовательно, ab входит в центр. Мы получили, что центр – подгруппа.

Интересным примером подгрупп служат так называемые *циклические подгруппы*. Обозначим через $< a >$ подмножество группы G, составленное из всех степеней элемента a; в него входит и сам элемент a, являющийся своей первой степенью. Подмножество $< a >$ будет подгруппой группы G, так как произведение элементов из $< a >$ лежит в $< a >$ ввиду того, что $a^n a^m = a^{n+m}$. В $< a >$ входит и единичный элемент, так как $a^0 = 1$ и $< a >$ вместе со всяким своим элементом содержит и его обратный элемент, так как из $(a^n)^m = a^{nm}$ следует равенство $(a^n)^{-1} = a^{-n}$.

Подгруппа $< a >$ называется *циклической подгруппой* группы G, порожденной элементом a.

Мы знаем, что группа G называется *циклической группой*, если она состоит из степеней одного из своих элементов a, то есть совпадает с одной из своих циклических подгрупп подгрупп $< a >$. Элемент a называется в этом случае *образующим элементом* группы G.

Пример 11. *Примером бесконечной циклической группы служит аддитивная группа целых чисел.*

Докажем это. Так как рассматривается группа по сложению, то под a^m понимается сумма $a + a + ... + a$ из m слагаемых и под a^{-1} понимается $-a$. Всякое целое число кратно 1, то есть это число служит образующим элементом рассматриваемой группы, в качестве образующего элемента можно было бы взять и -1.

Пример 12. *Примером конечной циклической группы порядка n служит мультипликативная группа корней степени n из 1.*

Как известно все, эти корни является степенями одного из них, а именно *первообразного корня*. Если ε - первообразный корень, то $G = \{1, \varepsilon, \varepsilon^2, ..., \varepsilon^{n-1}\}$.

Упражнение 6. 1. *Найдите центр в группе $GL(n, \mathbb{R})$.*

2. *Найти все образуюшие элементы в группах вращений треугольника и квадрата.*

3. *Пусть H – подгруппа группы G. Доказать, что единичный элемент H совпадает с единичным элементом G.*

4. *Доказать, что конечное множество G, в котором определена ассоциативная алгебраическая операция и каждое из уравнений $ax = b$, $ya = b$ для любых a и b из G имеет в G не более одного решения, будет группой.*

5. *Доказать, что если $a^2 = e$ для любого элемента a группы G, то эта группа абелева.*

6. *Доказать, что если e - единица и a - элемент порядка n группы G, то $a^k = e$ тогда и только тогда, когда k делится на n.*

7. *Найти все подгруппы:*

   а) циклической группы порядка 6;

   б) циклической группы порядка 24;

   в) симметрической группы S_3.

   г) Какие из подгрупп группы S_3 являются нормальными делителями?

   д) Доказать, что знакопеременная группа четвертой степени A_4 не имеет подгруппы шестого порядка. Таким образом, группа G порядка n для некоторых k, делящих n, может не иметь подгрупп порядка k.

8. *Найти все подгруппы группы G порядка 8, все элементы которой, кроме единицы e, имеют порядок 2.*

9. *Пусть* $G = a$ *- конечная циклическая группа порядка* n. *Доказать утверждения: а) порядок любой подгруппы группы* G *делит порядок* n *этой группы;*

   б) для любого делителя d *числа* n *существует единственная подгруппа* H *группы* G, *имеющая порядок* d;

   в) подгруппа H *порядка* d *содержит в качестве образующих все элементы порядка* d *группы* G. *В частности,* $H = \left\{a^{\frac{n}{a}}\right\}$

10. *Доказать, что: а) центр* Z *группы* G *порядка* p^n, *где* p *- простое число, содержит более одного элемента;*

    б) любая группа порядка p^2, *где* p *- простое число, коммутативна.*

    в) Привести пример некоммутативной группы порядка n^2, *где* n *- составное число.*

    г) Привести пример некоммутативной группы порядка p^3, *где* p *- простое число.*

11. *Доказать, что если порядок конечной группы* G *делится на простое число* p, *то* G *содержит элемент порядка* p *(теорема Коши).*

4 Гомоморфизм и изоморфизм групп

Гомоморфизмом группы G в группу F называется отображение $\varphi : (G, \circ) \to (F, \star)$, сохраняющее операцию:

$$\varphi(a \circ b) = \varphi(a) \star \varphi(b) \quad \forall\ a,\, b \in G.$$

Заметим, что $a,\, b \in G$, а $\varphi(a)$ и $\varphi(b)$ принадлежат F.

Ядром гомоморфизма φ называется множество элементов из G, отображающихся в e_F:

$$Ker\varphi = \{a \in G\ :\ \varphi(a) = e_F\}.$$

Упражнение 7. 1. *При гомоморфизме единица группы* G *переходит в единицу группы* F *и обратный элемент группы* G *переходит в обратный элемент группы* F.

2. *Доказать, что ядро гомоморфизма есть подгруппа группы* G.

3. *Пусть* $\varphi_1 : G_1 \to G_2$ *и* $\varphi_2 : G_2 \to G_3$ *- гомоморфизмы. Доказать, что* $\varphi_2 \cdot \varphi_1 : G_1 \to G_3$ *- гомоморфизм.*

4. *Пусть* $\varphi : G \to F$ *гомоморфизм группы* G *на группу* F. *Если группа* G *коммутативна, то и* F *- коммутативна.*

Решим эти задачи.

1. Нам надо доказать, что $\varphi(e_G) = e_F$, то есть единица группы G отображается в единицу группы F. Пусть $\varphi(e_G) = x$, где $x \in F$, тогда $x \circ x = \varphi(e_G) \star \varphi(e_G) = \varphi(e_G \circ e_G) = \varphi(e_G) = x$, отсюда $x \circ x = x$ и $x = e_F$, т. е. $\varphi(e_G) = e_F$.

   Теперь докажем, что обратный элемент группы G переходит в обратный F, то есть $\varphi(a^{-1}) = [\varphi(a)^{-1}]$. Действительно, $\varphi(a) \star \varphi(a^{-1}) = \varphi(a \circ a^{-1}) = \varphi(e_G) = e_F$. Отсюда $\varphi(a^{-1}) = [\varphi(a)^{-1}]$.

2. Для решения этой задачи надо воспользоваться определением ядра гомоморфизма. Докажем, что $Ker\,\varphi$ - подгруппа группы G. По 1 задаче, мы уже знаем, что единичный элемент группы G переходит в единичный группы F, а обратный элемент группы G – в обратный группы F. Остается доказать, что если g_1 и g_2 и содержатся в $Ker\varphi$, то $g_1 \circ g_2 \in Ker\,\varphi$. Итак, пусть g_1 и g_2 содержатся в $Ker\,\varphi$, тогда $\varphi(g_1) = e_F$ и $\varphi(g_2) = e_F$, а $\varphi(g_1 \circ g_2) = \varphi(g_1) \star \varphi(g_2) = e_F \star e_F = e_F$ и следовательно, $g_1 \circ g_2 \in Ker\,\varphi$. Таким образом, мы показали, что $Ker\,\varphi$ есть подгруппа группы G.

3. Пусть $\varphi_1 : G_1 \to G_2$ и $\varphi_2 : G_2 \to G_3$ – гомоморфизмы, где $(G_1, *)$, $(G_2, \star)$, $(G_3, \circ)$. Докажем, что $\varphi_1 \cdot \varphi_2 : G_1 \to G_3$ – гомоморфизм.

   Доказательство. Допустим, что a, b - произвольные элементы группы G. Тогда

   $$(\varphi_2 \cdot \varphi_1)(a * b) = \varphi_2(\varphi_1(a * b)) = \varphi_2(\varphi_1(a) \star \varphi_1(b)) =$$

   $$= \varphi_2(\varphi_1(a)) \circ \varphi_2(\varphi_1(b)) = (\varphi_2\varphi_1)(a) \circ (\varphi_2\varphi_1)(b),$$

   что и требовалось доказать.

4. Нам надо доказать, что если $\varphi : G \to F$ - гомоморфизм группы G на группу F и G - коммутативна, то и F - коммутативна.

   Предположим, что f_1 и f_2 – произвольные элементы группы F, так как φ - гомоморфизм (на) $G \to F$, то найдутся g_1 и g_2 такие, что $\varphi(g_1) = f_1$ и $\varphi(g_2) = f_2$, тогда

   $$f_1 \star f_2 = \varphi(g_1) \star \varphi(g_2) = \varphi(g_1 \circ g_2) =$$

   $$= \varphi(g_2 \circ g_1) = \varphi(g_2) \star \varphi(g_1) = f_2 \star f_1.$$

   Значит из коммутативности группы G следует коммутативность группы F. Обратное утверждение неверно.

Обоснуем на примере. Пусть $G = GL(n, \mathbb{R})$, а $F = \mathbb{R} \setminus 0$ – группа действительных чисел без нуля по операции умножения. Установим гомоморфизм следующим образом: каждой матрице $GL(n, \mathbb{R})$ поставим в соответствие ее определитель, то есть число, принадлежащее $\mathbb{R} \setminus 0$. $\varphi : GL(n, \mathbb{R}) \to \mathbb{R} \setminus 0$, при этом $\varphi(A) = \det A$. Ясно, что $\varphi(AB) = \varphi(A)\varphi(B) = \det A \cdot \det B$. В этом случае группа $F = \mathbb{R} \setminus 0$ коммутативна, а $GL(n, \mathbb{R})$ нет.

Задачу 3 решите самостоятельно, кроме того обоснуйте таблицу 4, в ней $\varphi : G \to F$, где φ - гомоморфизм.

№	G	F	φ	$Ker\,\varphi$
1	$(\mathbb{Z}, +)$	{-1,1}	1, при x=2n -1, при x=2n+1	2n
2	$(\mathbb{R}^+, \cdot)$	$(\mathbb{R}, +$	$\ln x$	{1}
3	$GL(n, \mathbb{R})$	$(\mathbb{R} \setminus 0, \cdot)$	$\det A$	$SL(n, \mathbb{R})$
4	$(\mathbb{Z}, +)$	$(\mathbb{Z}_n, +)$	$a \to \bar{a}$	nz
5	множ. всех вект. на плоск., +	множ. всех вект., лежащ. на ОХ, +	$pr_{OX}\mathbf{x}$	множ. тех вект., проекц. к-рых 0
6	$(\mathbb{R} \setminus 0, \cdot)$	{-1,1}	1, при x>0, -1, при x<0	$\mathbb{R}^+$

Таблица 4.

Гомоморфизм $\varphi : G \to F$ называется *изоморфизмом*, если φ биекция, то есть между элементами группы G можно установить взаимно-однозначное соответствие. Группы, между которыми можно установить изоморфизм, называют *изоморфными* и обозначают это так: $G \cong F$.

Изоморфное отображение группы G на себя называется *автоморфизмом*, а гомоморфное отображение в себя - *эндоморфизмом* этой группы.

Упражнение 8. 1. *Пусть $\varphi : G \to F$ - изоморфизм и $\varphi(g) = f$. Доказать, что g и f имеют одинаковые порядки.*

Доказательство. Рассмотрим $\varphi(g^n)$, где $n \in \mathbb{N}$.

$$\varphi(g^n) = \varphi(g \cdot \ldots \cdot g) = \varphi(g)\,\varphi(g) \cdot \ldots \cdot \varphi(g) = f^n$$

Предположим, что $O(g) = n_1$ и $O(f) = n_2$, значит верно $\varphi(g^{n_2}) = f^{n_2} =$

e_F и g^{n_2}, отсюда $n_1 \leqslant n_2$. С другой стороны $f^{n_1} = \varphi(g^{n_1}) = \varphi(e_G) = e_F$, откуда $n_2 \leqslant n_1$. Следовательно, $n_1 = n_2$.

2. *Какие из следующих групп изоморфны между собой:*

   а) группа вращений квадрата;

   б) группа симметрий ромба;

   в) группа симметрий прямоугольника;

   г) $(\mathbb{Z}(4), +)$, *группа классов вычетов по модулю 4.*

3. *Привести пример двух групп с одинаковым числом элементов и неизоморфных. Например, группа вращений квадрата не изоморфна группе симметрий ромба, т.к. в первой группе есть элемент порядка 4, а во второй группе нет.*

4. *Какой гомоморфизм из таблицы 4 является изоморфизмом?*

5. *Докажите, что мультипликативная группа корней n-ой степени из единицы изоморфна аддитивной группе классов вычетов по модулю n* $(\mathbb{Z}_n, +)$.

6. *Пусть $\varphi : G_1 \to G_2$ – изоморфизм. Доказать, что обратное отображение $\varphi^{-1} : G_2 \to G_1$ также изоморфизм.*

7. *Пусть $\varphi_1 : G_1 \to G_2$ и $\varphi_2 : G_2 \to G_3$ – изоморфизмы. Доказать, что $\varphi_2\varphi_1 : G_1 \to G_3$ есть изоморфизм.*

   Из последних двух задач следует, что две группы, изоморфные третьей группе, изоморфны между собой.

8. *Может ли группа быть изоморфна своей подгруппе?*

9. *Доказать, что: а) все бесконечные циклические группы изоморфны между собой; б) все конечные циклические группы данного порядка n изоморфны между собой.*

10. *Доказать, что: а) группа положительных действительных чисел по умножению изоморфна группе всех действительных чисел по сложению; б) группа положительных рациональных чисел по умножению не изоморфна группе всех рациональных чисел по сложению.*

11. *Доказать, что: а) любая конечная группа порядка n изоморфна некоторой группе подстановок n элементов;*

    б) любая группа изоморфна группе некоторых взаимно однозначных отображений множества элементов этой группы на себя.

12. *Доказать, что группа G' тогда и только тогда является гомоморфным образом конечной циклической группы G, когда G' также циклическая и ее порядок делит порядок группы G.*

13. *Найти все гомоморфные отображения:*

    а) циклической группы a порядка n в себя;

    б) циклической группы a порядка 6 в циклическую группу b порядка 18;

    в) циклической группы a порядка 18 в циклическую группу b порядка 6;

    г) циклической группы a порядка 12 в циклическую группу b порядка 15;

    д) циклической группы a порядка 6 в циклическую группу b порядка 25.

14. *Доказать, что аддитивную группу рациональных чисел нельзя гомоморфно отобразить на аддитивную группу целых чисел.*

5 Смежные классы. Нормальные подгруппы.

Левым смежным классом группы G по подгруппе H называется множество элементов $aH = \{ab,\ b \in H\}$, здесь a – фиксированный элемент из G, а b пробегает все элементы подгруппы H. Элемент a называется *представителем* смежного класса aH.

Аналогично *правый смежный класс группы G по подгруппе H* – это множество элементов $Ha = \{ba,\ b \in H\}$.

Отношение $\sim$, заданное на множестве G, есть *отношение эквивалентности*, если выполнены условия:

E1. рефлексивность $\forall\ a \in G$ верно $a \sim a$;

E2. симметричность $\forall\ a, b \in G$ из $a \sim b \quad \Rightarrow \quad b \sim a$;

E3. транзитивность $\forall\ a, b, c \in G$ из $a \sim b, \quad b \sim c \quad \Rightarrow \quad a \sim c$.

Упражнение 9. *Доказать, что разбиение G на левые (правые) смежные классы по H определяет на G отношение эквивалентности.*

Множество всех левых смежных классов G по H обозначается G/H. Его мощность называется *индексом подгруппы H в G.*

Теорема Лагранжа. Порядок конечной группы делится на порядок каждой своей подгруппы.

Упражнение 10. *Проверить, что в знакопеременной группе A_4 порядка 12 нет подгрупп порядка 6.*

№	группа G	подгруппа H	элемент x	смежный класс xH
1	$(\mathbb{R} \setminus 0, \cdot)$	$(\mathbb{R}^+, \cdot)$	-5	$\mathbb{R}^-$
2	$(\mathbb{R} \setminus 0, \cdot)$	{1,-1}	-5	{-5,5}
3	$(\mathbb{Z}, +)$	$(2\mathbb{Z}, +)$	-5	Все нечет. числа
4	$GL(2, \mathbb{R})$	$SL(2, \mathbb{R})$	$\begin{pmatrix} 1 & 2 \\ 2 & 6 \end{pmatrix}$	Матрицы: $\det A = 2$
5	$GL(2, \mathbb{R})$	Матр. вида λE, $\lambda \neq 0$	$\begin{pmatrix} 1 & 3 \\ 3 & 7 \end{pmatrix}$	$\begin{pmatrix} \lambda & 3\lambda \\ 3\lambda & 7\lambda \end{pmatrix}$, $\lambda \neq 0$

Таблица 5.

Упражнение 11. 1. *Доказать, что порядок любого элемента является делителем порядка группы.*

Указание: порядок любого элемента равен порядку порожденной им циклической подгруппы. Далее, воспользуйтесь теоремой Лагранжа.

2. *Группа G содержит 31 элемент. Сколько подгрупп может содержать группа G?*

3. *Построить разложение группы $(\mathbb{Z}, +)$ по подгруппе чисел, делящихся на 3.*

   Так как $(\mathbb{Z}, +)$ абелева группа, то оба разложения совпадают и содержат по 3 смежных класса: 1) все числа вида $3k$; 2) все числа вида $3k + 1$; 3) все числа вида $3k + 2$, где $k \in \mathbb{Z}$. Индекс подгруппы H в группе $\mathbb{Z}$ равен 3.

4. *Построить левое и правое разложение группы симметрий треугольника по подгруппе: а) вращений $\{e, a, b\}$; б) отражений относительно оси $\{e, c\}$.*

   Ответ:

   а) левое и правое разложения совпадают: $\{e, a, b\}$, $\{e, d, f\}$ – два класса.

   б) левое разложение: $\{e, e\}$, $\{a, f\}$, $\{b, d\}$; правое разложение: $\{e, c\}$, $\{a, d\}$, $\{b, f\}$.

5. *Найти смежные классы аддитивной группы векторов плоскости (выходящих из начала координат) по подгруппе векторов, лежащих на оси OX.*

Так как группа абелева, то левостороннее и правостороннее разложения совпадают. Возьмем $\mathbf{x} \in G$ и H, где H – все векторы на оси ОУ. Рассмотрим $\mathbf{x}+\mathbf{h}$, где $\mathbf{h}$ пробегает все H. Мы получим множество векторов, концы которых лежат на прямой, параллельной оси ОХ и проходящих через конец вектора $\mathbf{x}$.

Если взять вектор $\mathbf{y} \neq \mathbf{x}$, то получим другой смежный класс, концы которого тоже лежат на прямой, параллельной оси ОХ, но прямая проходит через конец вектора $\mathbf{y}$.

6. *Найти смежные классы мультипликативной группы комплексных чисел, отличных от нуля, по подгруппе чисел, равных по модулю единице* $G = (\mathbb{C} \setminus 0, \cdot)$,
$H = \{a + bi | \sqrt{a^2 + b^2} = 1\}$.

   Так как G – абелева группа, то левостороннее и правостороннее разложения совпадут. Пусть $\mathbb{Z} \in G$, рассмотрим zh, где h пробегает все H. $|zh| = |z||h| = |z|$, так как. $|h| = 1$. Итак, в один смежный класс попадут все комплексные числа с одинаковыми модулями. Таких смежных классов будет бесконечное множество.

7. *Найдите смежные классы*

   а) аддитивной группы чисел по подгруппе чисел, кратных данному натуральному числу k;

   б) аддитивной группы действительных чисел по подгруппе целых чисел.

   Ответ: в один смежный класс попадают все действительные числа с одной и той же дробной частью.

   в) мультипликативной группы комплексных чисел, отличных от нуля, по подгруппе положительных действительных чисел.

   Ответ: в один смежный класс попадают все комплексные числа с одним и тем же аргументом.

   Подгруппа $H \subset G$ называется *нормальной* в G, если

$$aHa^{-1} = H \qquad \forall\, a \in G.$$

Упражнение 12. *Доказать, что ядро гомоморфизма $Ker\varphi$ есть нормальная подгруппа в G.*

Доказательство. Пусть a – произвольный элемент из ядра $Ker\ \varphi$ и g – произвольный элемент группы G, тогда $\varphi(a) = e_F$ и

$$\varphi(gag^{-1}) = \varphi(g)\varphi(a)\varphi(g^{-1}) = \varphi(g)[\varphi(g)]^{-1} = e_F.$$

Поэтому элемент $gag^{-1} \in Ker\ \varphi$ и, следовательно, $Ker\ \varphi$ – нормальная подгруппа группы G.

Пример 13. *В группе S_3 (перестановок трех элементов) циклическая подгруппа $A_3 =<(123)>$ есть нормальная подгруппа, а подгруппа $<(12)>=\{e, (12)\}$ – нет.*

Упражнение 13. *Доказать, что если H – нормальная подгруппа, то $aH = Ha$, левые и правые смежные классы совпадают $\forall\ a \in G$.*

Пример 14. *Примером нормальной подгруппы может служить подгруппа матриц с определителем, равным 1, в группе $GL(n, \mathbb{R})$.*

Действительно, когда $\det A = 1$ и $A \in H$, то смежным классом по подгруппе H, одновременно левым и правым, порожденным матрицей $B \in GL(n, \mathbb{R})$, является класс всех матриц, определитель которых равен определителю матрицы B, так как

$$\det(BA) = \det(AB) = \det A \det B = \det B.$$

Упражнение 14. *Докажем, что подгруппа H диагональных матриц в группе невырожденных матриц второго порядка не является нормальной.*

Подгруппа H группы G тогда и только тогда является нормальным делителем в G, когда для любых $h \in G$ и $g \in G$ элемент $ghg^{-1} \in H$. Возьмем

$$g = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in GL(2, \mathbb{R}), \qquad h = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \in H.$$

Рассмотрим

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} =$$

$$= \begin{pmatrix} 1 & 2 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix}.$$

Получившаяся в результате матрица не является диагональной, значит H не является нормальным делителем.

Упражнение 15. 1. *Докажите, что подгруппа вращений является нормальной подгруппой в группе симметрий треугольника, а подгруппа отображений относительно высоты, опущенной из вершины A на сторону BC (состоящая из двух элементов), нормальной подгруппой группы симметрии треугольника не является.*

2. *Пусть n – порядок группы G, m – порядок подгруппы H и $m = n/2$. Доказать, что H является нормальной подгруппой группы G.*

3. *Доказать, что пересечение любого числа нормальных подгрупп некоторой группы G является нормальной подгруппой группы G.*

4. *Доказать, что центр группы G есть нормальная подгруппа группы G.*

   Доказательство. Пусть a – произвольный элемент из центра и g – произвольный элемент группы G. Тогда элемент $gag^{-1} = agg^{-1} = a$ также принадлежит центру. Поэтому центр – нормальная подгруппа группы G.

5. *Найдите нормальные подгруппы в S_3.*

6 Фактор-группа

Пусть дана группа G и H ее нормальная подгруппа, в этом случае левые и правые смежные классы совпадают. Можно построить новую группу G/H, которая называется *фактор-группой*. Элементами в этой группе являются смежные классы (всякий смежный класс порождается любым своим элементом). Групповая операция наследуется: $xH + yH = (x + y)H$. Роль единицы играет сама нормальная подгруппа H, и для смежного класса xH, обратным будет $x^{-1}H$ класс.

Упражнение 16. *1. Проверить корректность определения групповой операции. 2. Проверить, что G/H действительно есть группа.*

Со всякой группой G связывается целый набор новых групп – ее фактор-групп по различным нормальным делителям этой группы. Очевидно, что $G/\{e\} \cong G$, $G/G \cong \{e\}$.

Упражнение 17. *Докажите, что порядок любой фактор-группы G/H конечной группы G является делителем порядка самой этой группы.*

Действительно, порядок G/H равен индексу нормального делителя в группе G, а дальше см. теорему Лагранжа.

Пример 15. *Два целых числа n и n' называются сравнимыми по модулю m, если их остатки при делении на m равны: $n \equiv n'(mod\, m)$. При фиксированном m все множество целых чисел разбивается на m непересекающихся классов - классов вычетов: $\bar{0}$, $\bar{1}$, ..., $\overline{m-1}$. Заметим, что $\bar{0} = m\mathbb{Z}$.*

$\bar{0}$	$\bar{1}$	$\dots$	$\overline{m-1}$
.	.	$\dots$	.
.	.	$\dots$	.
-m	-m+1	$\dots$	-1
0	1	$\dots$	m-1
m	m+1	$\dots$	2m-1
2m	2m+1	$\dots$	3m-1
.	.	$\dots$	.
.	.	$\dots$	.

Упражнение 18. *Проверьте, что $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$ с операцией сложения есть аддитивная фактор-группа.*

Пример 16. *Фактор-группа S_n/A_n есть группа второго порядка, один элемент этой группы есть сама A_n, а другой элемент – все нечетные подстановки.*

Упражнение 19. 1. *Докажите, что всякая фактор-группа G/H абелевой группы сама является абелевой.*

2. *Докажите, что всякая фактор-группа G/H циклической группы сама циклическая.*

3. *Найти фактор-группы:*

   1) аддитивной группы целых чисел по подгруппе чисел, кратных данному натуральному числу n;

   2) аддитивной группы целых чисел, кратных 3, по подгруппе чисел, кратных 15;

   3) мультипликативной группы действительных чисел, отличных от нуля по подгруппе положительных чисел.

4. *Доказать, что фактор-группа группы действительных матриц по подгруппе матриц с определителем, равным 1, изоморфна мультипликативной группе действительных чисел, отличных от нуля.*

   Рассмотрим $GL(n,\mathbb{R})/SL(n,\mathbb{R})$. В один смежный класс попадают все матрицы с одним и тем же определителем. Каждому смежному классу A_i, где $i \in I$ поставим в соответствие $|A_i| = r \in \mathbb{R} \setminus 0$. Таким образом устанавливается биективное соответствие между элементами $GL(n,\mathbb{R})/SL(n,\mathbb{R})$ и $\mathbb{R} \setminus 0$. $A_j \cdot A_k \to |A_j||A_k|$,

$$A_jA_k \in GL(n,\mathbb{R})/SL(n,\mathbb{R}), \qquad |A_j||A_k| \in \mathbb{R} \setminus 0.$$

   Таким образом, $GL(n,\mathbb{R})/SL(n,\mathbb{R}) \cong \mathbb{R} \setminus 0$.

5. *Доказать, что $GL(n,\mathbb{R})$ по подгруппе матриц с положительным определителями является циклической группой второго порядка.*

   Доказательство. $GL(n,\mathbb{R})/H = \{H, B\}$, где $H =$
   $\{A|\det A = r \in \mathbb{R}^+\}$, $B = \{B|\det B = -r, r \in \mathbb{R}^+\}$, то есть в B попадают все матрицы с отрицательными определителями. В $GL(n,\mathbb{R})/H$ два элемента, следовательно $GL(n,\mathbb{R})/H \cong \{-1, 1\}$ или группе S_n/A_n. Значит, данная фактор-группа есть циклическая группа.

6. *Доказать, что $GL(n,\mathbb{C})$ по подгруппе матриц с определителями, по модулю равными единице, изоморфна мультипликативной группе положительных чисел.*

$$GL(n,\mathbb{C})/H = \left\{\bigcup_{i=1}^{\infty}, \, |A_i| = z, \, z \in \mathbb{C}, \, |z| = z \in \mathbb{R}^+\right\}.$$

$$H = \left\{A, \, |A| = a + bi, \, |a + bi| = \sqrt{a^2 + b^2} = 1\right\}.$$

   В один смежный класс попадают все матрицы, у которых $mod|A_i| = r, \, r \in \mathbb{R}^+, \, A_i \to mod|A_i|$. Биективное соответствие установлено.

   $\varphi(A_iA_j) = \varphi(A_i)\varphi(A_j) = = mod|A_i|mod|A_j| = r_1r_2 \in \mathbb{R}^+$, таким образом $GL(n,\mathbb{C})/H \cong \mathbb{R}^+$.

7. *Доказать, что фактор-группа $GL(n,\mathbb{C})$ подгруппе матриц с положительными определителями изоморфна мультипликативной группе комплексных*
   чисел, по модулю равных единице.

   В один смежный класс попадают все матрицы, такие, что $|A_i| = z$, $z \in \mathbb{C}$ и у всех этих z одинаковые аргументы. Как известно, каждому комплексному числу соответствует точка на плоскости. Множеству комплексных чисел с одним аргументом соответствует луч. Множеству комплексных чисел с модулем, равным 1, соответствует окружность с центром в начале координат и радиусом, равным 1. Можно установить биективное соответствие следующим образом: каждому смежному классу поставим в соответствие такое комплексное число, которому соответствует точка пересечения луча и окружности.

$$\varphi(A_iA_j) = \varphi(A_i)\varphi(A_j) \in B,$$

   где B – мультипликативная группа комплексных чисел, по модулю равных единице. Таким образом,
   $GL(n,\mathbb{C})/H \cong B$.

8. *Найти смежные классы:*

   а) аддитивной группы целых чисел по подгруппе чисел, кратных данному натуральному числу n;

   б) аддитивной группы действительных чисел по подгруппе целых чисел;

   в) аддитивной группы комплексных чисел по подгруппе целых гауссовых чисел, т. е. чисел $a + bi$ с целыми a и b;

   г) аддитивной группы векторов плоскости (выходящих из начала координат) по подгруппе векторов, лежащих на оси абсцисс Ox;

   д) мультипликативной группы комплексных чисел, отличных от нуля, по подгруппе чисел, равных по модулю единице;

   е) мультипликативной группы комплексных чисел, отличных от нуля, по подгруппе положительных действительных чисел;

   ж) мультипликативной группы комплексных чисел, отличных от нуля, по подгруппе действительных чисел;

   з) симметрической группы Sn по подгруппе подстановок, оставляющих число n на месте.

9. *Доказать, что любая подгруппа индекса два является нормальным делителем.*

10. *Элемент $aba^{-1}b^{-1}$ называется коммутатором элементов a и b группы G. Доказать, что все коммутаторы и их произведения (с любым конечным числом сомножителей) образуют нормальный делитель K группы G (коммутант данной группы).*

11. *Доказать, что если пересечение двух нормальных делителей H_1 и H_2 группы G содержит лишь единицу e, то любой элемент $h_1 \in H_1$ перестановочен с любым элементом $h_2 \in H_2$.*

12. *Доказать, что:*

    а) элементы группы G, перестановочные с данным элементом a, образуют подгруппу $N(a)$ группы G (нормализатор a в G), содержащую циклическую подгруппу a в качестве нормального делителя;

    б) число элементов группы G, сопряженных с a, равно индексу нормализатора $N(a)$ в G.

13. *Доказать, что:*

а) элементы группы G, перестановочные с данной подгруппой H (но не обязательно с элементами из H), образуют подгруппу $N(H)$ группы G (нормализатор подгруппы H в G), содержащую подгруппу H в качестве нормального делителя;

б) число подгрупп группы G, сопряженных с H, равно индексу нормализатора $N(H)$ в G.

14. *Доказать, что любой нормальный делитель H знакопеременной группы A_n степени $n \geqslant 5$, содержащий хотя бы один тройной цикл, совпадает с A_n.*

15. *Доказать, что факторгруппа симметрической группы S_n по знакопеременной группе A_n изоморфна факторгруппе аддитивной группы целых чисел по погруппе четных чисел.*

16. *Найти факторгруппы:*

а) аддитивной группы целых чисел по подгруппе чисел, кратных данному натуральному числу n;

б) аддитивной группы целых чисел, кратных 3, по подгруппе чисел, кратных 15;

в) аддитивной группы целых чисел, кратных 4, по подгруппе чисел, кратных 24;

г) мультипликативной группы действительных чисел, отличных от нуля, по подгруппе положительных чисел.

17. *Пусть G_n – аддитивная группа векторов n-мерного линейного пространства и H_k – подгруппа векторов k-мерного подпространства, $0 \leq k \leq n$. Доказать, что факторгруппа G_n/H_k изоморфна G_{n-k}.*

18. *ПустьG – мультипликативная группа всех комплексных чисел, отличных от нуля, и H - множество всех чисел из G, лежащих на действительной и мнимой осях.*

а) Доказать, что H - подгруппа группы G.

б) Найти смежные классы группы G по подгруппе H.

в) Доказать, что факторгруппа G/H изоморфна мультипликативной группе U всех комплексных чисел, равных по модулю 1.

19. *Пусть G – мультипликативная группа комплексных чисел, отличных от нуля, H – множество чисел из G, лежащих на n лучах, выходящих*

из нуля под равными углами, причем один из этих лучей совпадает с положительной действительной полуосью, K – аддитивная группа всех действительных чисел, Z – аддитивная группа целых чисел, D – мультипликативная группа положительных чисел, U – мультипликативная группа комплексных чисел, равных по модулю единице, U_n – мультипликативная группа корней n-й степени из единицы. Доказать, что:

а) K/Z изоморфна U; б) G/D изоморфна U; в) G/U изоморфна D; г) U/U_n изоморфна U; д) G/U_n изоморфна G; е) H есть подгруппа группы G и G/H изоморфна U; ж) H/D изоморфна U_n; з) H/U_n изоморфна D.

20. *Для мультипликативных групп невырожденных квадратных матриц порядка n доказать утверждения:*

    а) факторгруппа группы действительных матриц по подгруппе матриц с определителем, равным 1, изоморфна мультипликативной группе действительных чисел, отличных от нуля;

    б) факторгруппа группы действительных матриц по подгруппе матриц с определителем, равным ± 1, изоморфна мультипликативной группе положительных чисел;

    в) факторгруппа группы действительных матриц по подгруппе матриц с положительными определителями является циклической группой второго порядка;

    г) факторгруппа группы комплексных матриц по подгруппе матриц с определителями, по модулю равными единице, изоморфна мультипликативной группе положительных чисел;

    д) факторгруппа группы комплексных матриц по подгруппе матриц с положительными определителями изоморфна мультипликативной группе комплексных чисел, по модулю равных единице.

21. *Пусть G – группа всех движений трехмерного пространства, H – подгруппа параллельных переносов, K – подгруппа вращений вокруг данной точки O. Доказать, что:*

    а) H является нормальным делителем группы G, а K – нет;

    б) факторгруппа $G/$ изоморфна .

22. *Доказать, что факторгруппа некоммутативной группы G по ее центру не может быть циклической.*

7 Кольца. Поля

Кольца и поля - алгебраические структуры с двумя бинарными операциями: „сложение“ и „умножение“.

Кольцо $(K, +, \cdot)$ – это множество K с заданными на нем операциями сложения $+$ и умножения $\cdot$, обладающими следующими свойствами:

К1. $(K, +)$ есть абелева группа;

К2. $(K, \cdot)$ есть полугруппа;

К3. $\forall\ a,\ b,\ c\ \in K$ верно $a \cdot (b + c) = a \cdot b + a \cdot c$, $(a + b) \cdot c = a \cdot c + b \cdot c$ дистрибутивность умножения относительно сложения.

Структура $(K, +)$ называется *аддитивной группой кольца*, $(K, \cdot)$ – его *мультипликативной полугруппой.* Если $(K, \cdot)$ моноид, то говорят, что $(K, +, \cdot)$ *кольцо с единицей,* элемент e кольца называется *единицей*, если $a \cdot e = e \cdot a = a\ \forall\, a \in K$.

Если аксиома $K2$ не выполняется, то кольцо называется *неассоциативным.*

Если умножение в кольце K коммутативно, $a \cdot b = b \cdot a\ \forall\, a,\ b \in K$, то кольцо называется *коммутативным.*

Подмножество L кольца K называется *подкольцом,* если

$$\forall\ a,\ b \in L\ \Rightarrow\ a - b \in L,\ a \cdot b \in L.$$

(Если L подгруппа аддитивной группы и подполугруппа мультипликативной полугруппы кольца).

Упражнение 20. *Доказать, что* $\forall\, a,\ b,\ c \in K$

1. $a \cdot 0 = 0 \cdot a = 0.$

2. $a \cdot (-b) = (-a) \cdot b = -a \cdot b.$

3. $a \cdot (b - c) = a \cdot b - a \cdot c$ *и* $(a - b) \cdot c = a \cdot c - b \cdot c.$

1. Пусть $a \cdot 0 = b$, тогда $b + b = a \cdot 0 + a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 = b$. Значит $b = b - b = 0$. Проделать для $0 \cdot a = b$!!!

2. Действительно, $a \cdot b + a \cdot (-b) = a \cdot (b + (-b)) = a \cdot 0 = 0$. Проделать для $a \cdot b + (-a) \cdot b$!!!

3. В самом деле, $a \cdot (b - c) + a \cdot c = a \cdot (b - c + c) = a \cdot b$. Проделать для $(a - b) \cdot c + b \cdot c$!!!

Упражнение 21. *Доказать, что в кольце не может быть двух различных единиц. (Но может быть ни одной!)*

Пример 17. *1. Числовые множества $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ – это коммутативные ассоциативные кольца с единицей.*

2. *Множество четных чисел $2\mathbb{Z}$ – коммутативное ассоциативное кольцо без единицы.*

3. *Множество $m\mathbb{Z}$ целых чисел, делящихся на m, будет подкольцом в $\mathbb{Z}$ (без единицы при $m > 1$).*

4. *Множество E^3 векторов пространства с операциями сложения и векторного умножения – это некоммутативное и неассоциативное кольцо. Однако в нем выполнены следующие тождества:*

$$a \times b + b \times a = 0 \quad \text{антикоммутативность,}$$
$$(a \times b) \times c + (b \times c) \times a + (c \times a) \times b = 0, \text{ тождество Якоби.}$$

5. *Множество квадратных матриц размеров $n \times n$ – ассоциативное кольцо с единицей.*

6. *Множество многочленов степени не выше n – коммутативное ассоциативное кольцо с единицей.*

7. *Кольцо функций: множество всех функций, заданных на некотором множестве X с операциями поточечной суммой и поточечным произведением. Кольцо всех непрерывных функций, определенных на отрезке $[0, 1]$ является подкольцом.*

Элемент a^{-1} кольца с единицей называется *обратным* к элементу a, если $a{\cdot}a^{-1} = a^{-1}{\cdot}a = 1$. Элемент a, имеющий обратный, называется *обратимым.*

Гомоморфизмом колец называется отображение $\varphi: \ (K, +, \cdot) \ \to (K', \oplus, \odot)$, сохраняющее обе операции:

1. $\varphi(a + b) = \varphi(a) \oplus \varphi(b)$,

2. $\varphi(a \cdot b) = \varphi(a) \odot \varphi(b), \quad \forall\, a, b \in K.$

Ядром гомоморфизма колец называется множество элементов $Ker\,\varphi = \{a \in K : \quad \varphi(a) = 0'\} \subset K$.

Упражнение 22. *Доказать, что ядро гомоморфизма колец $Ker\,\varphi$ есть подкольцо кольца K.*

(Двусторонним) идеалом кольца K называется подкольцо J, такое, что $JK \subset J$ и $KJ \subset J$.

Упражнение 23. *Доказать, что ядро гомоморфизма колец* $Ker\,\varphi$ *есть идеал кольца* K.

Упражнение 24. *Доказать, что в кольце многочленов* $K[x]$ *совокупность многочленов, делящихся на многочлен* $f(x)$, *является идеалом. Он называется главным идеалом, порожденным* $f(x)$.

Пример 18. *Подкольцо* $J = (2\mathbb{Z}, +, \cdot)$ *является идеалом кольца* $K = (\mathbb{Z}, +, \cdot)$, *так как для любых целых чисел* $n \in \mathbb{Z}$ *и четных чисел* $p = 2q \in 2\mathbb{Z}$ *их произведение четно:* $n \cdot p = n \cdot 2q = 2nq \in 2\mathbb{Z}$.

Упражнение 25. *Доказать, если* K *и* K' – *кольца с единицей, то*

$$\varphi(e) = e', \quad \varphi - \text{гомоморфизм.}$$

Пусть $K = (S, +, \cdot)$ кольцо и $J = (T, +, \cdot)$ его идеал. Так как J – подкольцо K, то $H = (T, +)$ – нормальная подгруппа аддитивной абелевой группы $G = (S, +)$ (проверить!!!) Возьмем $a \in K$. *Классом вычетов по модулю идеала* J *кольца* K называется смежный класс аддитивной группы G кольца K по ее нормальной подгруппе H:

$$[a]_J = a + J = \{a + h \ : \ h \in J\}.$$

Определим операции сложения и умножения:

$$[a]_J + [b]_J = [a + b]_J, \quad [a]_J \cdot [b]_J = [a \cdot b]_j, \quad a,\, b \in K.$$

Упражнение 26. *1. Доказать корректность введенных операций. 2. Доказать, что множество классов вычетов с этими операциями есть кольцо.*

Кольцо вычетов по модулю идеала J кольца K называется *фактор-кольцом* кольца K по модулю идеала J и обозначается K/J.

Рассмотрим кольцо целых чисел $\mathbb{Z}$ и его подкольцо $m\mathbb{Z}$. С их помощью построим ненулевое кольцо, состоящее из конечного числа элементов. *Кольцом классов вычетов* называется фактор-кольцо: $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$.

Пример 19. *Таблицы сложения и умножения для* $\mathbb{Z}_2$:

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

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

Пример 20. *1. Полями являются $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.*

2. $\mathbb{Z}$ не является полем, так как в нем обратимы только элементы ± 1.

Упражнение 27. *Доказать, что любое поле обладает свойством $ab = 0 \quad \Rightarrow \quad \{a = 0$ или $b = 0\}$.*

Действительно, если $a \neq 0$, тогда существует a^{-1}. Умножим обе части равенства $ab = 0$ на a^{-1}, получим $a^{-1}ab = a^{-1}0$, откуда $b = 0$. Кольца, обладающие этим свойством, называются *кольцами без делителей нуля.*

Пример 21. *1. Кольцо $\mathbb{Z}$ – кольцо без делителей нуля.*

2. Множество квадратных матриц размеров $n \times n$ имеет делители нуля. Действительно, выберем $n = 2$, тогда нулевая матрица имеет делители:

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

В кольце без делителей нуля возможно сокращение:

$$\{\ ac = bc \ \text{ и } \ c \neq 0\} \quad \Rightarrow \quad a = b.$$

в самом деле, $ac = bc$ перепишем $(a - b)c = 0$. Так как $c \neq 0$, значит $a - b = 0$, т.е. $a = b$.

Упражнение 28. *Проверить, что ненулевые элементы поля K образуют абелеву группу относительно умножения.*

Подмножество L поля K является *подполем*, если оно является полем относительно тех же операций.

Пример 22. *1. Цепочка подколец: $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$.*

2. При любом $n \in \mathbb{Z}_+$ множество $n\mathbb{Z}$ является подкольцом кольца $\mathbb{Z}$.

3. Цепочка подполей: $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.

Поля называются изоморфными, если они изоморфны как кольца. При этом $\varphi(0) = 0'$, $\varphi(e) = e'$.

Наименьшее натуральное n, для которого в поле K выполнено равенство

$$\underbrace{e + e + \cdots + e}_{n} = 0$$

называется *характеристикой* поля и обозначается $charK$. Если такого n не существует, то говорят, что K - *поле нулевой характеристики.*

Пример 23. *1. $char\mathbb{Z} = 0$;*

2. $char\mathbb{Z}_p = p$, если p простое число.

Упражнение 29. *1. Доказать, что кольцо $\mathbb{Z}_n$ является полем тогда и только тогда, когда $n-$ простое число.*

2. Построить таблицы умножения и сложения для колец $\mathbb{Z}_3$ и $\mathbb{Z}_4$.

3. Доказать, что кольцо K, состоящее из 5 элементов, либо изоморфно $\mathbb{Z}_5$, либо является кольцом с нулевым умножением.

4. Показать, что матрицы $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, где $b \in \mathbb{Z}_3$, образуют поле из девяти элементов.

8 Линейные пространства. Алгебры

Линейным пространством над полем P называется множество V с заданными на нем операциями сложения и умножения на элементы поля P, обладающими свойствами:

P1. V есть абелева группа по сложению;

P2. $\lambda(a + b) = \lambda a + \lambda b$, $\forall\, \lambda \in P$, $\forall\, a$, $b \in V$;

P3. $(\lambda + \mu)a = \lambda a + \mu a$, $\forall\, \lambda$, $\mu \in P$, $\forall\, a \in V$;

P4. $(\lambda\mu)a = \lambda(\mu a)$, $\forall\, \lambda$, $\mu \in P$, $\forall\, a \in V$;

P5. $1a = a$, $\forall\, a \in V$.

Алгеброй над полем P называется множество A с заданными на нем операциями сложения, умножения и умножения на элементы поля P, обладающими следующими свойствами:

A1. относительно сложения и умножения на элементы поля P множество A есть линейное пространство;

A2. относительно сложения и умножения A есть кольцо;

A3. $(\lambda a)b = a(\lambda b) = \lambda(a \cdot b)$, $\forall\, \lambda \in P$, $\forall\, a$, $b \in A$.

Пример 24. *1. $\mathbb{C}$ есть алгебра над $\mathbb{R}$. Оно задается следующей таблицей умножения базисных векторов:*

$\cdot$	1	i
1	1	i
i	i	-1

2. Множество E^3 векторов пространства есть алгебра относительно векторного умножения. В ортонормированном базисе таблица векторного умножения имеет следующий вид:

$\times$	i	j	k
i	0	k	-j
j	-k	0	i
k	j	-i	0

Размерность алгебры – это размерность соответствующего векторного пространства.

Подмножество называется *подалгеброй*, если оно одновременно является подпространством и подкольцом. Отображение алгебр называется *изоморфизмом*, если оно одновременно является изоморфизмом векторных пространств и колец. Напомним, что два линейных пространства V и W изоморфны, если существует взаимно-однозначное соответствие
$\varphi: V \to W$, такое что:

$$\varphi(x+y) = \varphi(x) + \varphi(y), \quad \varphi(\lambda x) = \lambda\varphi(x), \quad \forall\, x\,, y \in V,\ \lambda \in P.$$

Упражнение 30. *Проверить, что множество квадратных матриц образует ассоциативную алгебру с единицей M_n. Убедиться, что эта алгебра не коммутативна и имеет делители нуля.*

Упражнение 31. *1. Показать, что в алгебре $M_2(\mathbb{R})$ матрицы вида $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ образуют подалгебру, изоморфную алгебре комплексных чисел.*

2. Матрица E_{ij}, у которой на (i,j)-м месте стоит 1, а на остальных - нули, называется матричной единицей. Доказать, что матричные единицы E_{ij} образуют базис векторного пространства M_n. Выписать таблицу умножения алгебры M_n в этом базисе.

Алгебры, как и кольца, не обязательно должны быть ассоциативными.

Очень важный пример неассоциативной алгебры – *алгебра Ли*. В ней операция умножения $*$ удовлетворяет аксиомам:

1. x*y=-y*x *антикоммутативность,*

2. (x*y)*z+(y*z)*x+(z*x)*y=0 *тождество Якоби.*

Операцию $*$ чаще обозначают символом $[\cdot,\cdot]$ и называют *операцией коммутирования.*

Упражнение 32. *Проверить, что аксиома 1 равносильна равенству $x*x=0$.*

Действительно, $(x+y)*(x+y)=0 \Leftrightarrow x*x+y*x+x*y+y*y=0 \Leftrightarrow x*y=-y*x$.

Пример 25. *1. Векторное пространство $\mathbb{R}^3$ с операцией векторное произведение есть трехмерная алгебра Ли. (Проверить!)*

2. Пусть $L(V)$ есть множество линейных операторов над линейным пространством V. Определим на этом множестве новую операцию коммутирования $[A,B]=AB-BA$. Тогда $L(V)$ с операцией коммутирования есть алгебра Ли.

9 Локальная группа Ли однопараметрических преобразований $\mathbb{R}^n$

Теория групп Ли объединяет в себе алгебру, анализ и геометрию. Группа Ли G есть дифференцируемое многообразие, наделенное структурой группы с гладкими отображениями:

$$\text{умножение:}\quad G\times G\to G,\qquad (x,y)\mapsto xy,$$
$$\text{взятие обратного элемента:}\quad G\to G,\qquad x\mapsto x^{-1}.$$

Гомоморфизм групп Ли также является гладким отображением. Подгруппа Ли $H\subset G$ группы Ли G есть подмногообразие, которое, в свою очередь является группой Ли.

Пример 26. *Группами Ли являются:*

1. $GL(n,\mathbb{K})$;

2. $SL(n,\mathbb{K})$;

3. $O(n)$;

4. $SO(n)$;

5. $U(n)$;

6. $SU(n)$.

Теория групп Ли достаточно сложна, поэтому ограничимся здесь рассмотрением полезного частного случая: однопараметрической группы Ли преобразований $\mathbb{R}^n$.

Множество однопараметрических преобразований евклидова пространства $\mathbb{R}^n$ на себя

$$\mathbf{x}' = f(\mathbf{x}, a), \qquad \mathbf{x},\ \mathbf{x}' \in \ \mathbb{R}^n,$$

где a – непрерывный параметр ($a \in \mathbb{R}$), образует *локальную группу Ли* G, если выполнены аксиомы:

1. *аксиома замыкания*: любые два последовательно проведенные преобразования

   $$\mathbf{x}' = f(\mathbf{x}, a), \qquad \mathbf{x}'' = f(\mathbf{x}', b),$$

   могут быть заменены одним преобразованием

   $$\mathbf{x}'' = f(\mathbf{x}, c), \qquad c = \varphi(a, b).$$

2. *аксиома тождественности*: существует единственное значение $a_0 \in \mathbb{R}$, при котором любая точка $\mathbf{x}$ остается на месте, то есть выполняется условие

   $$\mathbf{x} = f(\mathbf{x}, a_0),$$

   При этом $\varphi(a, a_0) = a$, $\varphi(a_0,\ b) = b$.

3. *аксиома инверсии*: существует единственное значение параметра $a_{-1} \in \mathbb{R}$, которое соответствует возвращению точки $\mathbf{x}'$ в точку $\mathbf{x}$:

   $$\mathbf{x} = f(\mathbf{x}', a_{-1}).$$

   Последовательное выполнение преобразований $f(\mathbf{x}, a)$ и $f(\mathbf{x}', a_{-1})$ в любом порядке эквивалентно тождественному преобразованию.

Упражнение 33. *Найдите сходства и отличия в определениях локальной группы Ли однопараметрических преобразований евклидова пространства G и определения группы Гл.2.*

Пример 27. *1. Преобразование трансляции $x' = x + a$ есть преобразование локальной группы Ли G.*

Действительно, аксиома 1: $x'' = x' + b = x + a + b = x + c$, где $c = \varphi(a, b) = a + b$. Аксиома 2: $x = x + a_0$, $a_0 = 0$. Аксиома 3: $x = x' + a_{-1} = x + a + a_{-1} = x$, $a_{-1} = -a$.

2. *Преобразование отражения $x' = a - x$ не образует локальную группу Ли G.*

   Действительно, $x'' = b - x' = b - a + x = c + x$, $c \neq \varphi(a, b)$. Не существует закона преобразования параметра, не содержащего x.

3. *Преобразование растяжения $x' = ax$ есть преобразование локальной группы Ли G.*

   Действительно: $x'' = bx' = bax = cx$, $c = \varphi(a, b) = ab$, $a_0 = 1$, $a_{-1} = 1/a$.

Параметр a, удовлетворяющий условиям

$$c = \varphi(a, b) = a + b, \quad a_0 = 0, \quad a_{-1} = -a$$

называют *каноническим.* Закон преобразования параметра $\varphi(a,\, b)$ может быть приведен к канонической форме.

Для примера 27.3 параметр приводится к каноническому виду заменой:

$$\bar{a} = \int_{a_0}^{a} A(a)\, da, \qquad \frac{1}{A(a)} = \left.\frac{\partial \varphi(a, b)}{\partial b}\right|_{b=a}.$$

Упражнение 34. *Проверить, образуют ли следующие преобразования локальные группы G:*

1. $x' = x/(1 - ax)$, $y' = y/(1 - x)$;
2. $x' = x + a + a^2$, $y' = y$;
3. $x' = ax$, $y' = (1 - a)y$;
4. $x' = x/(1 - ay)$, $y' = y/(1 - ay)$;
5. $x' = a/(1 - ax)$, $y' = 2a/(1 - ay)$;
6. $x' = x \cos a + y \sin a$, $y' = -x \sin a + y \cos a$;
7. $x' = e^a x$, $y' = e^{5a} y$, $z = e^{-2a} z$;
8. $x' = x + ay$, $y' = y$;
9. $x' = x \operatorname{ch} a + y \operatorname{sh} a$, $y' = y \operatorname{ch} a + x \operatorname{sh} a$;

Инфинитезимальный оператор однопараметрического преобразования – это дифференциальный оператор вида

$$X = \xi_1 \frac{\partial}{\partial x_1} + \xi_2 \frac{\partial}{\partial x_2} + \cdots + \xi_n \frac{\partial}{\partial x_n}, \quad \xi_i = \left.\frac{\partial f_i(\mathbf{x}, a)}{\partial a}\right|_{a=a_0}$$

Пример 28. *1. Преобразованию трансляции $x' = x+a$, $y' = y$ соответствует оператор $X = \frac{\partial}{\partial x}$.*

2. Преобразованию растяжения $x' = e^a x$, $y' = e^{2a}y$ соответствует оператор $X = x\frac{\partial}{\partial x} + 2y\frac{\partial}{\partial y}$.

Упражнение 35. *Найти операторы для тех преобразований упражнения 34, которые представляют собой локальную группу Ли.*

Однопараметрические преобразования могут быть восстановлены в виде рядов по степеням a в малой окрестности тождественного преобразования (ему соответстует значение $a = a_0$) с использованием оператора X:

$$\mathbf{x}' = \mathbf{x} + aX\mathbf{x} + \frac{a^2}{2!}X^2\mathbf{x} + \frac{a^3}{3!}X^3\mathbf{x} + \dots = e^{aX}\mathbf{x}.$$

Пример 29. *По оператору $X = y\frac{\partial}{\partial x} - x\frac{\partial}{\partial y}$ локальное преобразование строится в виде рядов:*

$$x' = x + ya - x\frac{a^2}{2!} - y\frac{a^3}{3!} + x\frac{a^4}{4!} - \dots = x\cos a + y\sin a;$$
$$y' = y - xa - y\frac{a^2}{2!} + x\frac{a^3}{3!} + y\frac{a^4}{4!} - \dots = -x\sin a + y\cos a.$$

Упражнение 36. *Найти локальное преобразование в виде рядов для следующих операторов:*

1. $X = \frac{y}{x}\frac{\partial}{\partial x}$;
2. $X = \left(x + \frac{y^2}{x}\right)\frac{\partial}{\partial x}$;
3. $X = y\frac{\partial}{\partial x} - xy\frac{\partial}{\partial y}$;
4. $X = 3xy^6\frac{\partial}{\partial x} + y^7\frac{\partial}{\partial y}$;
5. $X = r\ln r\frac{\partial}{\partial r} + \varphi\frac{\partial}{\partial \varphi} - 2(1+\ln r)\frac{\partial}{\partial u}$;
6. $X = xy\frac{\partial}{\partial x} + y^2\frac{\partial}{\partial y}$;
7. $X = x^2\frac{\partial}{\partial x} - y^2\frac{\partial}{\partial y}$.

Введем на множестве операторов операцию *коммутирования* по следующему правилу: $[X_1, X_2] = X_1X_2 - X_2X_1$.

Если $X_1 = \xi_1\frac{\partial}{\partial x_1} + \dots + \xi_n\frac{\partial}{\partial x_n}$, $X_2 = \eta_1\frac{\partial}{\partial x_1} + \dots + \eta_n\frac{\partial}{\partial x_n}$, то

$$[X_1, X_2] = (X_1\eta_1 - X_2\xi_1)\frac{\partial}{\partial x_1} + \dots + (X_1\eta_n - X_2\xi_n)\frac{\partial}{\partial x_n}.$$

Упражнение 37. *Проверить, что эта операция коммутирования линейна по каждому аргументу (то есть билинейна), кососимметрична и удовлетворяет тождеству Якоби.*

Таким образом, мы построили *алгебру Ли локальной многопараметрической группы Ли*. Пусть X_1, X_2, ..., X_r – базис в соответствующем линейном пространстве L_r.

Упражнение 38. *Проверить, что* $[X_i, X_j] = c_{ij}^k X_k$. *По повторяющемуся индексу подразумевается суммирование.*

Числа $c_{ij} \in \mathbb{R}$ называются *структурными константами.*

Упражнение 39. *Доказать свойства:*

$$c_{ij}^k = -c_{ji}^k, \qquad c_{ij}^k c_{kl}^m + c_{jl}^k c_{ki}^m + c_{li}^k c_{kj}^m = 0.$$

Пример 30. *Таблица Кэли для алгебры* L_6 *с операторами*

$$\begin{aligned}
&X_1 = \frac{\partial}{\partial x}, \qquad X_2 = \frac{\partial}{\partial t}, \qquad X_3 = u\frac{\partial}{\partial u},\\
&X_4 = x\frac{\partial}{\partial x} + 2t\frac{\partial}{\partial t}, \qquad X_5 = 2t\frac{\partial}{\partial x} - xu\frac{\partial}{\partial u},\\
&X_6 = 4tx\frac{\partial}{\partial x} + 4t^2\frac{\partial}{\partial t} - (x^2 + 2t)\frac{\partial}{\partial u} \qquad \textit{имеет вид}
\end{aligned}$$

	X_1	X_2	X_3	X_4	X_5	X_6
X_1	0	0	0	X_1	$-X_3$	$2X_5$
X_2	0	0	0	$2X_2$	$2X_1$	$4X_4 - 2X_3$
X_3	0	0	0	0	0	0
X_4	$-X_1$	$-2X_2$	0	0	X_5	$2X_6$
X_5	X_3	$-2X_1$	0	$-X_5$	0	0
X_6	$-2X_5$	$2X_3 - 4X_4$	0	$-2X_6$	0	0

Упражнение 40. *Выписать таблицы Кэли для следующих операторов:*

1. $X_1 = \frac{\partial}{\partial x}$, $X_2 = \frac{\partial}{\partial y}$, $X_3 = x\frac{\partial}{\partial x} + ky\frac{\partial}{\partial y}$, $k \neq 1$;
2. $X_1 = \frac{\partial}{\partial x} + \frac{\partial}{\partial y}$, $X_2 = x\frac{\partial}{\partial x} + y\frac{\partial}{\partial y}$, $X_3 = x^2\frac{\partial}{\partial x} + y^2\frac{\partial}{\partial y}$;
3. $X_1 = \frac{\partial}{\partial x}$, $X_2 = \frac{\partial}{\partial y}$, $X_3 = x\frac{\partial}{\partial x} + (x + y)\frac{\partial}{\partial y}$;
4. $X_1 = \frac{\partial}{\partial x}$, $X_2 = \frac{\partial}{\partial y}$, $X_3 = x\frac{\partial}{\partial y}$;
5. $X_1 = \frac{\partial}{\partial x}$, $X_2 = \frac{\partial}{\partial y}$, $X_3 = y\frac{\partial}{\partial y}$, $X_4 = x\frac{\partial}{\partial x}$, $X_5 = y\frac{\partial}{\partial x}$, $X_6 = x\frac{\partial}{\partial y}$, $X_7 = x^2\frac{\partial}{\partial x} + xy\frac{\partial}{\partial y}$, $X_8 = xy\frac{\partial}{\partial x} + y^2\frac{\partial}{\partial y}$.

10 Зачетные задачи

1. Правым (левым) нулем полугруппы называется такой элемент z, что $az = z$ $(za = z)$ при любом . Доказать, что если в полугруппе имеются как правые, так и левые нули, то все они совпадают, так что существует единственный двусторонний нуль.

2. Правой (левой) единицей полугруппы называется такой элемент u, что $au = a$ $(ua = a)$ при любом a. Доказать, что если в полугруппе имеются как правые так и левые единицы, то все они совпадают, так что существует единственная двусторонняя единица.

3. Может ли элемент полугруппы быть одновременно правым нулем и левой единицей?

4. Перечислить (с точностью до изоморфизма) все полугруппы, состоящие из двух элементов.

5. Перечислить (с точностью до изоморфизма) все пол-группы с одной образующей.

6. Доказать, что конечная полугруппа правыми сокращениями (т. е из $ba = ca$ следует $b = c$) хотя бы с одной левой единицей есть группа.

7. Построить пример конечной полугруппы с правыми сокращениями, не являющейся группой.

8. Построить пример бесконечной коммутативной полугруппы с единицей и с сокращениями, не являющейся группой.

9. Доказать, что квадратные невырожденные матрицы порядка n с элементами из данного поля образуют группу (она называется полной линейной группой степени n над полем и обозначается $GL(n, \mathbb{K})$.

10. Доказать, что квадратные матрицы порядка n с элементами из поля , имеющие определитель, равный 1, образуют группу (она называется специальной линейной группой и обозначается $SL(n, \mathbb{K})$.

11. Доказать, что квадратные матрицы порядка n, в каждой строке и в каждом столбце которых один элемент равен 1, а остальные нули, образуют группу (симметрическая группа S_n).

12. Доказать, что квадратные матрицы порядка n, в каждой строке и в каждом столбце которых имеется не более чем один элемент, равный 1, а остальные нули, образуют полугруппу.

13. Доказать, что для каждого элемента а полугруппы задачи 12 существует единственный элемент a^+ такой, что $aa^+a = a$, $a^+aa^+ = a^+$ (полугруппы с таким свойством называются инверсными).

14. Доказать, что ортогональные матрицы порядка n образуют группу (полная ортогональная группа $GO(n)$), группу же составляют собственно

ортогональные матрицы (специальная ортогональная группа $SO(n)$).

15. Доказать, что целочисленные матрицы с определителями 1 образуют группу.

16. Доказать, что пересечение групп задач 14 и 15 есть конечная группа и найти ее порядок.

17. Доказать, что пары (a, b) элементов поля , $a \neq 0$, составляют группу относительно умножения, определяемого формулой $(a_1, b_1)(a_2, b_2) = (a_1a_2, a_1b_2 + b_1)$.

18. Доказать, что линейные функции $ax + b$, $a \neq 0$, образуют группу относительно суперпозиции, изоморфную группе задачи 17.

19. Доказать, что непрерывные строго возрастающие на отрезке $[0, 1]$ функции φ со значениями $\varphi(0) = 0$, $\varphi(1) = 1$ составляют группу относительно суперпозиции.

20. Доказать, что комплексные числа, изображения которых заполняют логарифмическую спираль $r = e^{k\varphi}$, $k \neq 0$ образуют группу относительно умножения.

21. Доказать, что подстановки n элементов составляют группу, изоморфную группе задачи 20.

22. Установить изоморфизм группы вещественных чисел относительно сложения к группы задачи 20.

23. Установить изоморфизм группы вещественных чисел относительно сложения и группы положительных чисел относительно умножения.

24. Доказать, что группа движений и отражений плоскости, совмещающих с собой равносторонний треугольник, изоморфна группе S_3 подстановок трех элементов.

25. Доказать, что группа движений (без отражений) трехмерного пространства, совмещающих с собой куб, изоморфна группе S_4 подстановок четырех элементов.

26. Доказать, что группа, порожденная движениями и отражениями трехмерного пространства, совмещающими с собой правильный икосаэдр, изоморфна группе S_5, подстановок пяти элементов.

27. Чему равен порядок группы движений, совмещающих с собой плоскую пластину, имеющую вид правильного n-угольника (группа диэдра).

28. Пусть все элементы группы, кроме единицы, имеют порядок 2. Доказать, что группа абелева.

29. Описать правые классы смежности при разложении группы G по подгруппе H:

а) G – циклическая группа Z_8, восьмого порядка, H – ее подгруппа четвертого порядка;

b) $G = S_3$, H – подгруппа, порожденная транспозицией (12);

c) G – группа вращений куба, H – ее подгруппа, совмещающая с собой одну из граней куба;

d) G – группа всех невырожденных вещественных матриц, H - подгруппа матриц с определителем 1.

30. Доказать, что в конечной группе нечетного порядка любой элемент является квадратом другого, однозначно определенного, элемента.

31. Чему равен наибольший порядок элемента симметрической группы S_{12}?

32. Сколько подгрупп имеет группа S_8?

33. Доказать, что если число правых классов смежности в разложении бесконечной группы G по подгруппе H конечно, то и число левых классов смежности конечно и равно числу правых классов.

34. Доказать, что подгруппа H индекса 2 в группе G является ее нормальным делителем.

35. Доказать, что если H – подгруппа конечного индекса в группе G и K – промежуточная подгруппа, т. е. такая, что $H \in K \in G$, то индекс K в G есть делитель индекса H в G.

36. Доказать, что пересечение двух подгрупп H_1 и H_2, конечного индекса в группе G есть подгруппа конечного индекса, не превосходящего произведения индексов H_1 и H_2.

37. Центром группы называется множество всех элементов, коммутирующих со всеми элементами группы. Доказать, что центр есть нормальный делитель.

38. Доказать, что группа, порядок которой есть степень простого числа p, имеет нетривиальный центр.

39. Доказать, что существуют две группы (с точностью до изоморфизма) порядка p^2 где p – простое число, обе абелевы.

40. Перечислить группы восьмого порядка.

41. Показать, что отображение $\varphi \to \cos\varphi + i\sin\varphi$ есть гомоморфное отображение аддитивной группы вещественных чисел на мультипликативную группу комплексных чисел модуля 1. Найти ядро гомоморфизма.

42. Рассмотрим аддитивную труппу в полиномов с вещественными коэффициентами, степени которых не превосходят $n-1$. Каждому полиному $f \in G$ сопоставим строку $(f(x_1), f(x_2), \ldots, f(x_n))$, где $x_1, x_2, \ldots, x_n$ – данные попарно различные числа. Доказать, что это отображение есть изоморфизм.

43. То же отображение применить к аддитивной группе всех полиномов над $\mathbb{R}$, без ограничения степени. Доказать, что это отображение есть

гомоморфизм и найти его ядро.

44. Пусть G-конечная группа, $H = \varphi(G)$ – ее гомоморфный образ. Доказать, что порядок $x \in G$ делится на порядок $\varphi(x) \in H$.

45. Доказать, что если порядок конечной абелевой группы делится на простое число p, то в группе найдется элемент порядка p.

46. Доказать, что для конечной группы число элементов в любом классе сопряженных элементов есть делитель порядка группы.

47. Что представляют собой классы сопряженных элементов в симметрической группе S_n.

48. Пусть H – абелева группа нечетного порядка. Рассмотрим множество $G = H \bigcup Ha$, где а – новый символ, и определим вG умножение по правилам: $x_1 \cdot x_2 = x_1 x_2$, $x_1 \cdot x_2 a = x_1 x_2 a$, $x_1 a \cdot x_2 = x_1 x_2^{-1} a$, $x_1 a \cdot x_2 a = x_1 x_2^{-1}$. Доказать, что G есть группа и все элементы из На сопряжены.

49. Описать конечные группы G порядка $2m$, в которых существует класс сопряженных элементов, содержащий половину элементов G.

50. Найти группы, имеющие три класса сопряженных элементов.

51. Найти группы, имеющие четыре класса сопряженных элементов.

52. Доказать, что если H – подгруппа группы G конечного индекса n, то существует лишь конечное число подгрупп, сопряженных с H, и это число делит n.

53. Доказать, что если группа G содержит подгруппу H конечного индекса, то содержит и нормальный делитель конечного индекса.

54. Доказать, что если подгруппа G содержит группу H индекса n, то она содержит нормальный делитель, индекс которого делит $n!$.

55. Коммутатором элементов a и b группы G называется $aba^{-1}b^{-1}$. Подгруппа, порожденная коммутаторами, называется коммутантом группы G. Доказать, что:

a) коммутатор a и b равен 1 тогда и только тогда, когда a и b коммутируют;

b) конечные произведения коммутаторов составляют коммутант;

c) коммутант является нормальным делителем;

d) факторгруппа по коммутанту абелева;

e) если G/H – абелева группа, то H содержит коммутант G.

56. Доказать, что если A и B – нормальные делители группы G и $a \in A$, $b \in B$, то $aba^{-1}b^{-1} \in A \bigcap B$.

57. Доказать, что если A и B – нормальные делители G и $A \bigcap B = 1$, то элементы из A коммутируют с элементами из B.

58. Доказать, что если порядок конечной группы делится на простое число p, то в ней существует элемент порядка p (теорема Коши).

59. Описать группы порядка $2p$, где p-простое число.

60. Перечислить группы порядка pq, где p и q – простые числа.

61. Пусть группа $G = SL(n, \mathbb{Z})$ есть группа целочисленных матриц порядка n с определителем 1 и m - натуральное число. Переход от кольца $\mathbb{Z}$ к кольцу вычетов $\mathbb{Z}_m$ по модулю m определяет, очевидно, гомоморфизм группы $SL(n, \mathbb{Z})$ в группу $SL(n, \mathbb{Z}_m)$ – группу матриц с определителем 1 над кольцом $\mathbb{Z}_m$. Доказать, что это отображение является эпиморфизмом.

62. Пусть G-конечная группа целочисленных матриц и m-натуральное число, $m \geq 3$. Доказать, что редукция по модулю m осуществляет мономорфное отображение G в $GL(n, \mathbb{Z}_m)$.

63. Что представляют собой классы сопряженных элементов в группе $SO(3)$ вращений трехмерного пространства (или, что то же самое, в группе собственно ортогональных матриц третьего порядка).

64. Доказать, что группа $SO(3)$ простая, т.е. она не содержит нормальных делителей, кроме всей группы и единичной подгруппы.

65. Пусть G-конечная группа. Каждому $x \in G$ сопоставим подстановку $\sigma_x : \ a \to ax$ элементов группы G. Ясно, что произведению элементов групп соответствует произведение сопоставленных им подстановок (если считать первым действующим левый множитель) и группа G изоморфна так построенной группе подстановок. Сопоставление $x \to \ \sigma_x$ называется регулярным представлением конечной группы подстановками.

Доказать, что любая подстановка σ_x регулярного представления разбивается на циклы одинаковой длины, равной порядку элемента x.

66. Для того чтобы среди подстановок регулярного представления конечной группы G нашлась нечетная подстановка, необходимо и достаточно, чтобы порядок n группы G был четным числом и, если $n = 2^k n_1$ при нечетном n_1, чтобы в G существовал элемент порядка 2^k.

11 Тест

1. Какие из данных операций не являются бинарными операциями? (Выбрать все варианты).

a) $\varphi(x, y, z) = x + y + z$; b) $\varphi(x) = |x|$; c) $\varphi(x, y) = xy$; d) $\varphi(x, y) = x + y$.

2. Множество с заданной на нем бинарной ассоциативной операцией это:

a) группа; b) полугруппа; c) подгруппа; d) моноид.

3. Какие из данных операций не являются ассоциативными операциями? (Выбрать все варианты).

a) $\varphi(x, y) = xy$; b) $\varphi(x, y) = xxy$; c) $\varphi(x, y)$=НОД(x,y); d) $\varphi(x, y) = |x| + |y|$.

4. Выберите все подгруппы группы $(\mathbb{Z}, +)$:

a) $(\mathbb{Z}, \times)$; b) $(n\mathbb{Z}, +)$; c) $(\mathbb{Z}_n, +)$; d) $(\mathbb{N}, +)$.

5. Выберите условия, в совокупности определяющие группу: "группа - это множество

a) с заданной ассоциативной бинарной операцией";

b) с заданной коммутативной бинарной операцией";

c) с единичным элементом";

d) с нулевым элементом";

e) все элементы которого обратимы".

6. Выберите все подгруппы мультипликативной группы $(\mathbb{R} \setminus 0, \times)$:

a) $(\mathbb{Q}, \times)$; b) $(\mathbb{Z}, \times)$; c) $(\mathbb{Q} \setminus 0, \times)$; d) $(\mathbb{Z} \setminus 0, \times)$.

7. Выберите все группы мощности 6.

a) S_3 - симметрическая группа из 3 элементов;

b) S_6 - симметрическая группа из 6 элементов;

c) группа симметрий квадрата;

d) $(\mathbb{Z}_6, +)$.

8. Выберите все группы мощности 6.

a) группа корней шестой степени из 1;

b) A_{12} – группа четных перестановок из 12 элементов;

c) группа вращений правильного шестиугольника;

d) циклическая группа $\{e, a, \ldots, a^5\}$.

9. Единица группы $(\mathbb{Z}, +)$ это

a) 1; b) 0; c) -1; d) все целые числа.

10. Сколько независимых циклов, включая циклы длины 1, имеет данная перестановка (82156743)

a) 3; b) 0; c) 2; d) 4.

11. Какие из указанных ниже совокупностей отображений множества $M = \{1, 2, \ldots, n\}$ в себя образуют группу относительно умножения?

a) множество всех отображений;

b) множество всех инъективных отображений;

c) множество всех сюръективных отображений;

d) множество всех биективных отображений.

12. Какие из указанных ниже совокупностей отображений множества $M = \{1, 2, \dots, n\}$ в себя образуют группу относительно умножения?

a) множество всех четных перестановок;

b) множество всех нечетных перестановок;

c) множество транспозиций;

d) множество перестановок, оставляющих неподвижными элементы некоторого подмножества $S \subseteq M$.

13. Какие из указанных множеств квадратных вещественных матриц образуют группу по умножению?

a) множество симметричных матриц;

b) множество косомимметричных матриц;

c) множество невырожденных матриц;

d) множество невырожденных матриц с фиксированным определителем $d \neq 0$.

14. Какие из указанных множеств квадратных вещественных матриц образуют группу по сложению?

a) множество симметричных матриц;

b) множество косомимметричных матриц;

c) множество диагональных матриц;

d) множество невырожденных матриц.

15. Какие из данных отображений являются гомоморфизмами?

a) $\varphi : (\mathbb{C}, +) \to (\mathbb{C}, +)$, такое что $\varphi(z) = |z|$;

b) $\varphi : (\mathbb{C}, \times) \to (\mathbb{C}, \times)$, такое что $\varphi(z) = |z|$;

c) $\varphi : (\mathbb{R}^+, \times) \to (\mathbb{R}, +)$, такое что $\varphi(x) = ln(x)$;

d) $\varphi : GL(n, \mathbb{R}) \to (\mathbb{R} \setminus 0, \times)$, такое что $\varphi(A) = det(A)$.

16. Найдите порядок элемента 4 в группе $(Z_6, +)$

a) 1; b) 2; c) 3; d) 4.

17. Найдите порядок элемента 3 в группе $(Z_6, +)$

a) 1; b) 2; c) 3; 4) 4.

18. Что представляет собой ядро гомоморфизма $\varphi :$ $GL(n, \mathbb{R}) \to (\mathbb{R} \setminus 0, \times)$, такого что $\varphi(A) = det(A)$?

a) $GL(n, \mathbb{R})$; b) $(\mathbb{R} \setminus 0, \times)$; c) $SL(n, \mathbb{R})$; d) 1.

19. Что представляет собой ядро гомоморфизма $\varphi :$ $(\mathbb{R}, \times) \to (1, -1, \times)$, такого что $\varphi(x) = 1$, если x - четное число и $\varphi(x) = -1$, если x - нечетное число?

a) 1; b) -1; c) все четные числа; d) все нечетные числа.

20. Из данных отображений выберите те, какие по вашему мнению являются изоморфизмами

a) $\varphi : (\mathbb{Z}, +) \to (2\mathbb{Z}, +)$, такое что $\varphi(n) = 2n$;

b) $\varphi : (\mathbb{R}, \times) \to (-1,\ 1, \times)$, такое что $\varphi(x) = 1$, если x - четное и $\varphi(x) = -1$, если x - нечетное число;

c) $\varphi : (\mathbb{R}^+, \times) \to (\mathbb{R}, +)$, такое что $\varphi(x) = ln(x)$;

d) $\varphi : GL(n, \mathbb{R}) \to (\mathbb{R} \setminus 0, \times)$, такое что $\varphi(A) = det(A)$.

21. Подгруппы каких порядков может иметь группа S_5?

a) 10; b) 7; c) 11; d) 6.

22. Выберите группы, изоморфные циклической группе с 8 элементами

a) S_8; b) A_8; c) группа корней 8 степени из 1; d) S_3.

23. Среди данных отношений выберите те, какие по вашему мнению являются отношениями эквивалентности

a) $a \sim b$, если $a \equiv b(mod\, p)$, где $a, b, p \in \mathbb{Z}$;

b) $a \sim b$, если |a|=|b|, где $a, b \in \mathbb{C}$;

c) $a \sim b$, если $a = \ln(b)$, где $a, b, p \in \mathbb{R}$;

d) $A \sim B$, если $\det(A) = \det(B)$, где $A, B \in GL(n, \mathbb{R})$.

24. Пусть на C задано отношение эквивалентности $a \sim b$, если |a|=|b|. Тогда фактор-группа $(\mathbb{C}, \times)/\sim$ представляет собой:

a) множество концентрических окружностей с центром в т. 0;

b) множество прямых параллельных оси $Re\mathbb{Z}$;

c) множество прямых параллельных оси $Im\mathbb{Z}$;

d) пучок прямых, проходящих через т.0.

25. Какая из приведенных теорем является теоремой Лагранжа?

a) Порядок конечной группы делится на порядок каждой своей подгруппы.

b) Для каждого делителя порядка группы существует подгруппа данного порядка.

c) Каждая конечная группа порядка n изоморфна группе S_n.

d) Каждая конечная группа порядка n изоморфна какой-либо подгруппе группы S_n.

26. Векторы x и y плоскости назовем эквивалентными, если они отличаются друг от друга на вектор, параллельный оси OX. Тогда соответствующая фактор-группа представляет собой:

a) множество прямых параллельных OX;

b) множество прямых параллельных OY;

c) множество векторов с фиксированным модулем;

d) верхняя полуплоскость.

27. Пусть группа S_7 имеет подгруппу, изоморфную S_4. Тогда порядок фактор-группы S_7/S_4 равен:

a) 210; b) 120; c) 7!; d) 4.

28. Выберите условия, в совокупности определяющие кольцо. "Кольцо K - это непустое множество, на котором заданы две бинарные операции ($+$ и $\times$), такие что:

a) (K,$+$) - группа; b)(K,$+$) - абелева группа; c) (K, $\times$) - полугруппа; d) (K, $\times$) - группа; e) $(a+b)\times c = a\times c + b\times c$, $c\times(a+b) = c\times a + c\times b$.

29. Из приведенных множеств выберите те, какие по вашему мнению являются кольцами:

a) $\mathbb{Q}$; b) множество невырожденных квадратных матриц порядка n; c) $\mathbb{Z}_n$; d) множество квадратных матриц порядка n.

30. Подгруппа H группы G называется нормальной подгруппой если

a) $\forall g \in H$, gH=Hg; b) $\forall g \in G$, gH=Hg;

c) $\forall g \in H$, gG=Gg; d) $\forall g \in G$, $gG \subseteq H$.

31. Множество L называется идеалом кольца K, если:

a) $\forall x \in K\ xK \subseteq K$;

b) $\forall x \in K\ xL \subseteq L$;

c) L - подкольцо и $\forall x \in K\ xL \subseteq L$ и $Lx \subseteq L$;

d) L - подкольцо и $\forall x \in K\ xL \subseteq L$.

32. Решение системы уравнений x+2y=9, y+x=5 на $\mathbb{Z}_3$ это:

a) x=1, y=4; b) x=1, y=1; c) x=4, y=1; d) x=4, y=4.

33. Какие из приведенных колец не содержат делители 0?

a) $\mathbb{Z}$; b) $\mathbb{Q}$; c) $\mathbb{R}$; d) $\mathbb{C}$.

34. Какие из приведенных колец содержат делители 0?

a) кольцо квадратных матриц; b) $\mathbb{Z}_4$; c) кольцо многочленов; d) кольцо непрерывных функций на $\mathbb{R}$.

35. Поле - это

a) коммутативное кольцо;

b) коммутативное кольцо с 1;

c) коммутативное кольцо с 1, в котором каждый элемент $a \neq 0$ обратим;

d) коммутативное кольцо с 1, в котором каждый элемент обратим.

36. Из приведенных множеств выберите те, какие по вашему мнению являются полями

a) $\mathbb{C}$; b) $\mathbb{R}$; c) $\mathbb{Q}$; d) $\mathbb{Z}$.

37. Из приведенных множеств выберите те, какие по вашему мнению являются полями

a) $\mathbb{Z}_3$; b) $\mathbb{Z}_4$; c) $\mathbb{Z}_5$; d) $\mathbb{Z}_6$.

12 Принятые обозначения

$\mathbb{N}$ – множество натуральных чисел $\{1, 2, 3, \dots, \}$.

$\mathbb{Z}$ – множество целых чисел $\{0, \pm 1, \pm 2, \pm 3, \dots, \}$.

$\mathbb{Q}$ – множество рациональных чисел $\{p/q\}$, $p \in \mathbb{Z}$, $q \in \mathbb{N}$.

$\mathbb{R}$ – множество действительных чисел.

$\mathbb{C}$ – множество комплексных чисел.

$\mathbb{N}_0$ – множество натуральных чисел с нулем $\mathbb{N} \cup \{0\}$.

$\mathbb{Z} \setminus 0$ – множество целых чисел без нуля $\{\pm 1, \pm 2, \pm 3, \dots, \}$.

$\mathbb{R} \setminus 0$ – множество действительных чисел без нуля.

$\mathbb{C} \setminus 0$ – множество комплексных чисел без нуля.

$\mathbb{Z}^+$ – множество целых положительных чисел.

$\mathbb{Z}^-$ – множество целых отрицательных чисел.

$\mathbb{Q}^+$ – множество рациональных положительных чисел.

$\mathbb{Q}^-$ – множество рациональных отрицательных чисел.

$\mathbb{R}^+$ – множество действительных положительных чисел.

$\mathbb{R}^-$ – множество действительных отрицательных чисел.

$k\mathbb{Z}$ – множество целых чисел, кратных k.

$\mathbb{Z}_k$ – вычет по модулю k.

S_k – симметрическая группа (группа перестановок) k элементов.

A_k – знакопеременная группа (группа четных перестановок) k элементов.

$GL(n, \mathbb{K})$ – полная линейная группа (группа невырожденных квадратных матриц порядка n над полем $\mathbb{K}$)/

$SL(n, \mathbb{K})$ – специальная линейная группа (группа квадратных матриц порядка n над полем $\mathbb{K}$).

$O(n, \mathbb{K})$ – полная ортогональная группа (группа ортогональных матриц порядка n над полем $\mathbb{K}$).

$SO(n, \mathbb{K})$ – специальная ортогональная группа (группа ортогональных матриц порядка n с определителем равным 1 над полем $\mathbb{K}$).

13 Литература

1. А.И. Кострикин „Введение в алгебру“, Т. 1-3, М.: Физматлит, 2000.

2. А.И. Кострикин „Сборник задач по алгебре“, М.: Факториал, 1995.

3. И.В. Проскуряков „Сборник задач по линейной алгебре“, М.: Наука, 1984.

4. Е.С. Ляпин, А.Я. Айзенштат, М.М. Лесохин „Упражнения по теории групп“, М: Наука, 1967.

5. А.В. Зеркина „Элементы теории групп. Методические рекомендации“, Уфа: БашГУ, 1985.

7. Д.К. Фаддеев, И.С. Соминский „Сборник задач по высшей алгебре“, М.: Наука, 1977.

8. С. В. Дужин, Б. Д. Чеботаревский „От орнаментов до дифференциальных уравнений: Попул. введ. в теорию групп преобразований“, Минск: Высшая школа, 1988.

9. П.С. Александров „Введение в теорию групп“, М: Наука, 1980.

10. В.В. Трофимов „Задачи по теории групп и алгебр Ли“, М: МГУ, 1990.

11. Н.Х. Ибрагимов „Группы преобразований в математической физике“, М: Наука, 1983.

12. Э.Б. Винберг „Курс алгебры“, 2-е издание, испр. и допол. М.: Факториал Пресс, 2001.

13. И.С. Емельянова „Групповой анализ дифференциальных уравнений в примерах и задачах“, Нижний Новгород, 2011.

Учебное издание

Международная школа-конференция для студентов, аспирантов и молодых ученых „Фундаментальная математика и ее приложения в естествознании“

КАРТАК Вера Валерьевна
ЗЕРКИНА Анастасия Васильевна

ОСНОВНЫЕ АЛГЕБРАИЧЕСКИЕ СТРУКТУРЫ: ГРУППЫ, КОЛЬЦА, ПОЛЯ, АЛГЕБРЫ

Учебное пособие