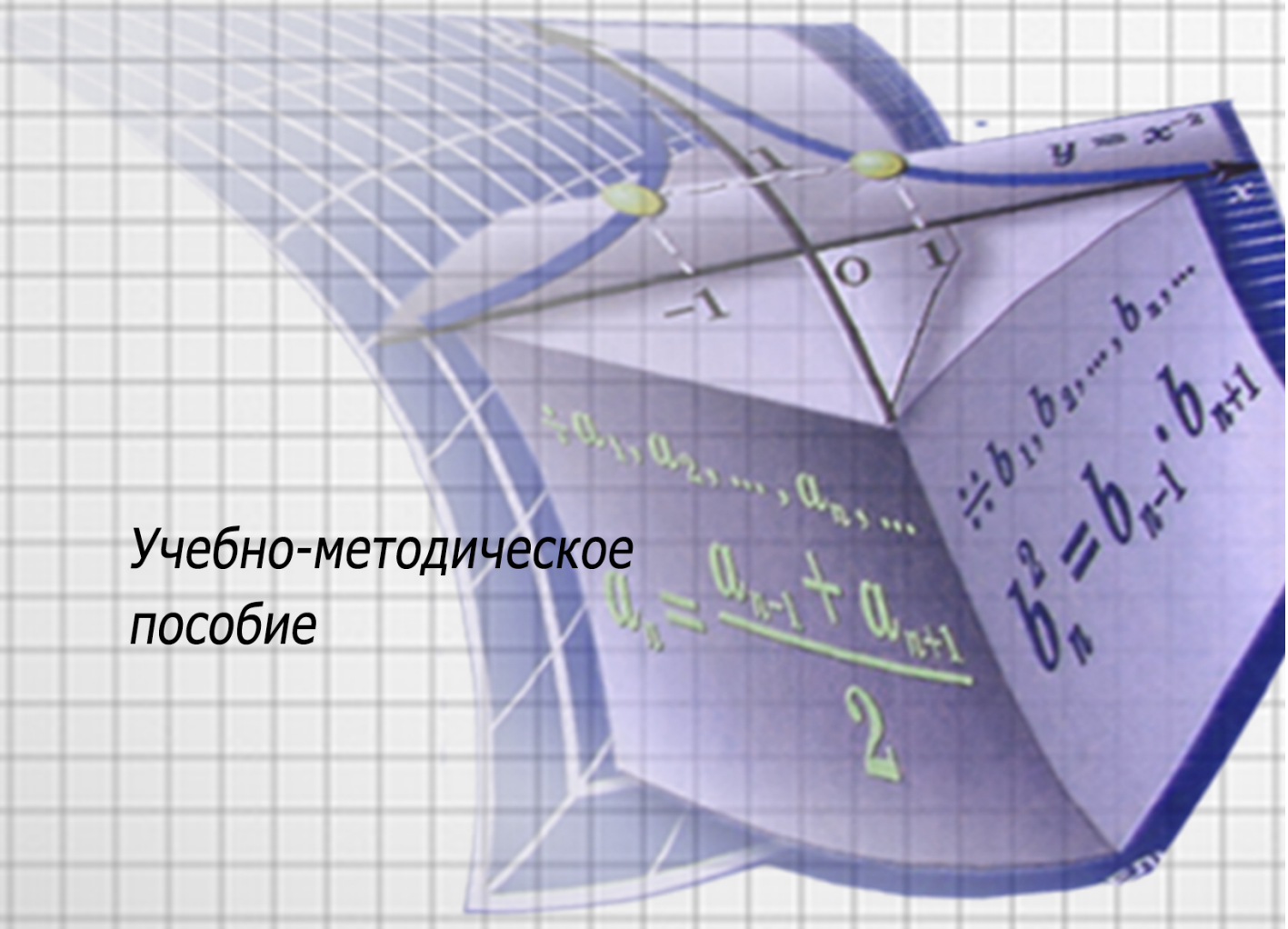
ГОУ ВПО «Донецкий национальный университет»

Л.И.Селякова

АЛГЕБРАИЧЕСКИЕ СТРУКТУРЫ В СИСТЕМЕ ФУНДАМЕНТАЛЬНОЙ ПОДГОТОВКИ БУДУЩЕГО УЧИТЕЛЯ



Учебно-методическое пособие

Донецк, 2016

Государственное образовательное учреждение
высшего профессионального образования
«Донецкий национальный университет»

Л.И. Селякова

АЛГЕБРАИЧЕСКИЕ СТРУКТУРЫ В СИСТЕМЕ ФУНДАМЕНТАЛЬНОЙ ПОДГОТОВКИ БУДУЩЕГО УЧИТЕЛЯ

учебно-методическое пособие

Донецк 2016

УДК 378.011.3-057.175:512 (07)
ББК В152.7р30
С 299

Рекомендовано к изданию Ученым советом
ГОУ ВПО «Донецкий национальный университет»
(протокол № 1 от 29.01.2016 г.)

Селякова Л.И.

Алгебраические структуры в системе фундаментальной подготовки будущего учителя: учебно-методическое пособие / Л.И. Селякова. – Донецк: ДонНУ, 2016. – 69 с.

Рецензенты:

Вит.В.Волчков доктор физико-математических наук, профессор,
ГОУ ВПО «Донецкий национальный университет»;

Т.Б.Волобуева кандидат педагогических наук, доцент,
Донецкий республиканский институт дополнительного педагогического образования

Пособие предназначено для организации самостоятельной работы студентов, изучающих алгебраические структуры. Перечень понятий и фактов дает представление о содержании рассматриваемых тем. Опорный конспект знакомит студентов с основными определениями и теоремами. Примеры решения задач содействуют успешному усвоению материала. Приведенные в каждом разделе контрольные вопросы и упражнения нацеливают на глубокое понимание изучаемых объектов, на отыскание нестандартных путей решения поставленных проблем.

Для преподавателей и студентов учреждений высшего профессионального образования, будущих учителей математики.

УДК 378.011.3-057.175:512 (07)
ББК В152.7р30

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Теория алгебраических структур составляет основу современного фундаментального математического образования учителя математики. С одной стороны, она естественно продолжает школьную математическую подготовку, усиливая и, даже, завершая на определенном уровне содержательную линию, связанную с числами, многочленами, геометрическими векторами и так далее. С другой – вводит студентов в мир современной математики, знакомит их с основами теории групп, колец и полей, связующей и обобщающей математическое знание как таковое. Теория алгебраических структур имеет незаурядное прикладное значение, составляя математический аппарат многих современных теорий. Значительна роль алгебраических структур и с позиции методологии науки, так как здесь четко и в полной мере реализуется построение аксиоматической теории, пропагандируется идея отыскания общей точки зрения на разные (на первый взгляд) понятия, факты и явления.

Учебно-методическое пособие предназначено для организации самостоятельной работы студентов, изучающих алгебраические структуры. На странице 5 перечислены основные обозначения, необходимые для понимания содержания любой учебной литературы по алгебраическим структурам. Далее предлагаются вопросы для аттестации по дисциплине. Пособие содержит материалы для изучения шести тем, каждая из которых представлена четырьмя блоками.

Методический блок содержит перечень понятий, фактов, формулировок теорем и умений, необходимых при изучении темы.

Информационный блок представляет собой краткий опорный конспект и примеры решения задач по теме. Конспект не является достаточным для изучения темы. Для полноценного изучения необходима дополнительная учебная литература.

Список рекомендуемых для этих целей учебников дан в конце пособия.

Практический блок включает индивидуальные задания для домашней работы в двенадцати вариантах. Этот блок содержит задания реконструктивно-вариативного уровня, которые можно выполнять по образцу.

Блок самоконтроля содержит контрольные вопросы, дополнительные упражнения и задачи повышенной сложности, которые предназначены не только для самостоятельного контроля знаний по теме, но и для организации самостоятельной работы, которая носит эвристический характер. Решение задач этого блока связано с научным поиском, отысканием нестандартных путей мышления и предполагает уровень умственной деятельности, на котором осуществляется более глубокое понимание явлений, процессов и начинается творческая деятельность.

ЛИТЕРАТУРА содержит список учебников**,** достаточный для полноценного изучения рассматриваемых тем.

ОБОЗНАЧЕНИЯ

N, Z, Q, R, C – соответственно множества всех натуральных, целых, рациональных, действительных, комплексных чисел;

$M_n(K)$ – множество $(n \times n)$-матриц над кольцом K;

$K[x]$ – кольцо всех многочленов от x над кольцом K;

$K[x_1,...,x_n]$ – кольцо всех многочленов от $x_1,...,x_n$ над кольцом K;

S_m – симметрическая группа степени m;

A_m – знакопеременная группа степени m;

$GL(n,K)$ – мультипликативная группа невырожденных $(n \times n)$-матриц над кольцом K;

Z_m – кольцо классов вычетов по модулю m;

(a)– циклическая группа с образующим элементом a;

$(a_1,...,a_n)$ – группа с образующими элементами $a_1,...,a_n$;

(a)– главный идеал кольца с образующим элементом a;

$(a_1,...,a_n)$ – идеал кольца с образующими $a_1,...,a_n$;

G/H – факторгруппа группы G по нормальной подгруппе H;

K/I – факторкольцо кольца K по идеалу I;

$Ker\ \varphi$ – ядро гомоморфизма φ;

$A \times B$ – прямое произведение групп A и B.

ВОПРОСЫ ДЛЯ АТТЕСТАЦИИ

1. Алгебраические операции и алгебры, бинарные операции и их свойства, группы, полугруппы, моноиды (определения и примеры).
2. Следствия из аксиом группы (единственность нейтрального и обратного элементов, теорема о расстановке скобок при последовательном применении ассоциативной операции к n элементам, $n>3$).
3. Изоморфизмы групп, теорема Кэли.
4. Подгруппы, системы образующих (определения и примеры).
5. Критерий подгруппы. Критерий конечной подгруппы.
6. Циклические подгруппы (конечные и бесконечные) и их описание с точностью до изоморфизма.
7. Смежные классы, определение и свойства. Теорема Лагранжа.
8. Нормальные подгруппы, критерий нормальной подгруппы.
9. Факторгруппа, определение и свойства.
10. Критерий принадлежности элементов группы одному смежному классу.
11. Гомоморфизмы групп (определение, примеры и свойства).
12. Ядро гомоморфизма, определение и свойства.
13. Теорема о гомоморфизмах групп.
14. Прямые суммы и прямые произведения групп (определения и критерии).
15. Разложение циклических групп в прямую сумму подгрупп.
16. Разложение конечных абелевых групп в прямую сумму p-групп. Разложение p-групп в прямую сумму примарных циклических подгрупп.
17. Основная теорема о конечных абелевых группах.
18. Кольца и поля (определения и примеры), простейшие свойства.
19. Гомоморфизмы колец.

20. Идеалы колец, кольца главных идеалов, конгруэнции по модулю идеала.

21. Теорема о гомоморфизмах колец.

22. Прямые суммы колец.

23. Факторкольцо по простому идеалу.

24. Характеристика полей, простые поля. Поля Галуа.

25. Алгебраические и трансцендентные расширения. Строение простых расширений.

ТЕМА 1.
ГРУППЫ И ИХ ПРОСТЕЙШИЕ СВОЙСТВА

Методический блок

В результате изучения темы студент должен знать определения и уметь приводить примеры следующих понятий: алгебраическая операция, группоид, полугруппа, моноид, группа, абелева группа, порядок группы, конечная и бесконечная группы, изоморфизм и автоморфизм групп, система образующих группы, симметрическая группа.

В результате изучения темы студент должен знать формулировки и уметь доказывать следующие факты: следствия из аксиом группы (простейшие свойства группы), свойства изоморфизмов групп, теорема Кэли.

В результате изучения темы студент должен уметь: распознавать группы, абелевы группы, моноиды, полугруппы, группоиды, изоморфизмы и автоморфизмы групп; строить группы по системе образующих; строить группу подстановок, изоморфную данной; определять изоморфные и не изоморфные группы.

Информационный блок

Будем говорить что *на множестве G определена бинарная операция* $*$, если любой упорядоченной паре (a,b) элементов $a,b \in G$ ставится в соответствие однозначно определённый элемент $c \in G$, что записывается в виде $c=a*b$.

В учебной литературе понятие группы вводится различными способами. Начинающим рекомендуем использовать следующее

***Определение* 1.** Множество $(G, *)$ называется *группой* относительно бинарной операции $*$, если выполнены следующие условия:

1) операция $*$ определена на множестве G

2) операция $*$ ассоциативна: $(a*b)*c = a*(b*c)$ для любых $a,b,c \in G$;

3) в G существует нейтральный элемент, т.е. такой элемент e что $e*a=a*e=a$ для всех $a \in G$;

4) для каждого элемента $a \in G$ существует обратный элемент $a^{-1} \in G$, такой, что $a^{-1}*a=a*a^{-1}=e$.

Множество A называется моноидом, если выполняются первые три указанные условия; полугруппой, если выполняются первые два условия; группоидом, если выполняется первое условие.

Обратим внимание на то, что операция в группе не обязательно является коммутативной.

***Определение* 2.** Группа называется *коммутативной* (или *абелевой* – в честь выдающегося математика Абеля), если операция в этой группе коммутативна, то есть $a*b = b*a$ для любых $a,b \in G$.

Определенность операции на множестве A означает, что для каждой пары элементов из A результат операции, во-первых, существует, а во-вторых – также принадлежит A. Так, операция деления не определена на множестве всех целых чисел, потому что, например, не существует элемента 1/0; операция деления не определена на множестве всех натуральных чисел, так как, например, число 2/3 хотя и существует, но оно не является

натуральным; операция деления определена на множестве всех положительных рациональных чисел, так как для любых положительных рациональных чисел a и b результат операции $a : b$ существует и также является положительным рациональным числом.

Вместо фразы «операция определена на множестве A» употребляют также фразу «множество A замкнуто относительно данной операции» или «операция является алгебраической на множестве A». Говорить о замкнутости множества A относительно данной операции особенно целесообразно тогда, когда относительно существования результата операции нет сомнения.

Если операция в группе – сложение, то такая группа называется аддитивной; если же операция – умножение, то такая группа называется мультипликативной.

Ассоциативный закон имеет вид $a+(b+c)=(a+b)+c$ в аддитивной записи и $a\cdot(b\cdot c)=(a\cdot b)\cdot c$ – в мультипликативной записи.

Нейтральный элемент аддитивной группы называется нулем и обозначается 0: $0+a=a$, $a+0=a$. Нейтральный элемент мультипликативной группы называется единицей и обозначается 1: $1\cdot a=a$, $a\cdot 1=a$.

Если элемент e удовлетворяет условию $e*a=a$ для каждого a группоида, то e называется левым нейтральным элементом. Аналогично определяется правый нейтральный элемент. Если в группоиде существуют левый и правый нейтральные элементы, то они совпадают, и можно говорить о нейтральном элементе.

Проверка того, что множество A относительно операции $*$ образует группу, сводится к проверке выполнения условий (аксиом) (1)-(4) в определении 1. Так, $(Q,:)$ не является группой, поскольку уже первая аксиома не выполняется: результат 1:0 не определен. Для множества всех рациональных чисел без нуля Q^* операция деления определена, но не выполняется ассоциативный закон: $a:(b:c)\neq(a:b):c$.

Хотя для множества четных чисел $2Z$ операция умножения определена (произведением четных чисел является четное число), и она является ассоциативной, но это множество не содержит

нейтрального элемента и группу не образует, а является полугруппой.

Так, например, $(N,\cdot)$ – моноид, т.е. множество всех натуральных чисел относительно умножения удовлетворяют аксиомам (1)-(3), но это не группа, поскольку не выполняется аксиома (4).

Нетрудно убедиться, что группами являются $(Q^*,\cdot)$, $(R,+)$, $(R[x],+)$, $(M_2,+)$, $(C,+)$, $(GL(n,R),\cdot)$.

Пример 1. Выяснить, является ли группой относительно операции $a*b=\dfrac{a+b}{1+ab}$ каждое из следующих множеств: а) R – множество действительных чисел; б) R^+ – множество положительных действительных чисел; в) множество $A = (-1; 1)$.

а) Дробь $\dfrac{a+b}{1+ab}$ существует только при $1+ab\neq 0$. На множестве R, если $a\neq 0$, а $b=-\dfrac{1}{a}$, то $1+ab=0$, и поэтому операция * определена не для всех действительных чисел (например, для пары чисел -1 и 1), значит $(R, *)$ – не является группой.

б) Операция * определена на R^+, т. к. для всех $a>0$ и $b>0$ дробь $\dfrac{a+b}{1+ab}$ существует и положительна. Операция * является ассоциативной:

$$(a*b)*c=\frac{a+b}{1+ab}*c=\frac{\dfrac{a+b}{1+ab}+c}{1+\dfrac{a+b}{1+ab}c}=\frac{a+b+c+abc}{1+ab+ac+bc}=\frac{a+\dfrac{b+c}{1+bc}}{1+a\dfrac{b\_c}{1+bc}}=a*\frac{b+c}{1+bc}=$$

$$=a*(b*c).$$

Нейтральный элемент e определяется из условий $e*a = a*e = a$ для всех $a\in R^+$. Тогда $\dfrac{a+e}{1+ae}=a$, что равносильно $e(1-a^2)=0$, откуда $e = 0$. Но число $0\notin R^+$, поэтому $(R^+, *)$ является полугруппой, но не группой.

в) операция * определена на A, т.к. для всех $|a|<1$ и $|b|<1$ $1+ab\neq 0$, выполняются неравенства $(1-a)(1-b)>0$ и $(1+a)(1+b)>0$

, которые равносильны соответственно $1+ab>a+b$ и $-(1+ab)<a+b$, т. е. $|a+b|<|1+ab|$. Поэтому $\left|\frac{a+b}{1+ab}\right|<1$ и $\frac{a+b}{1+ab}\in A$.

Операция $*$ является ассоциативной (проверено выше), нейтральный элемент $e=0\in A$.

Обратный для a элемент x должен удовлетворять условию

$x*a = a*x = 0$ или $\frac{a+x}{1+ax}=0$, откуда $x = -a$. Если $|a|<1$, то $|x|=|-a|=|a|<1$ и $x\in A$, т. е. Все элементы множества A обратимы.

Следовательно $(A, *)$ – группа. Очевидно, что $a*b = b*a$ для всех $a,b\in A$, поэтому $(A, *)$ – абелева группа.

Пример 2. Пусть $H=\begin{pmatrix}1 & 1\\ 0 & -1\end{pmatrix}$. Образует ли группу относительно операции $A*B=ABH$ множество всех (2×2) матриц над R вида:

а) $\begin{pmatrix}1 & x\\ 0 & 0\end{pmatrix}$; б) $\begin{pmatrix}0 & x\\ 0 & -1\end{pmatrix}$; в) $\begin{pmatrix}0 & x\\ 0 & y\end{pmatrix}$?

а) $A*B=\begin{pmatrix}1 & x\\ 0 & 0\end{pmatrix}*\begin{pmatrix}1 & y\\ 0 & 0\end{pmatrix}=\begin{pmatrix}1 & x\\ 0 & 0\end{pmatrix}\begin{pmatrix}1 & y\\ 0 & 0\end{pmatrix}\begin{pmatrix}1 & 1\\ 0 & -1\end{pmatrix}=\begin{pmatrix}1 & 1-y\\ 0 & 0\end{pmatrix}$.

Операция определена на множестве и ее действие сводится к действиям над над числами: $x*y=1-y$.

Проверка показывает, что в случае а) операция не является ассоциативной: $(x*y)*z=(1-y)*z=1-z;\quad x*(y*z)=x*(1-z)=1-(1-z)=z$.

б) $A*B=\begin{pmatrix}0 & x\\ 0 & -1\end{pmatrix}*\begin{pmatrix}0 & y\\ 0 & -1\end{pmatrix}=\begin{pmatrix}0 & x\\ 0 & -1\end{pmatrix}\begin{pmatrix}0 & y\\ 0 & -1\end{pmatrix}\begin{pmatrix}1 & 1\\ 0 & -1\end{pmatrix}=\begin{pmatrix}0 & x\\ 0 & -1\end{pmatrix}$.

Получилось, что $A*B=A$. Эта операция является ассоциативной, поскольку $(A*B)*C=B*C=C$ и $A*(B*C)=A*C=C$. Очевидно, каждая матрица является правой единицей, в то время, как левых единиц нет вообще. Таким образом, мы имеем полугруппу, но не группу.

в) $A*B=\begin{pmatrix}0 & x\\ 0 & y\end{pmatrix}*\begin{pmatrix}0 & z\\ 0 & t\end{pmatrix}=\begin{pmatrix}0 & x\\ 0 & y\end{pmatrix}\begin{pmatrix}0 & z\\ 0 & t\end{pmatrix}\begin{pmatrix}1 & 1\\ 0 & -1\end{pmatrix}=\begin{pmatrix}0 & -xt\\ 0 & -yt\end{pmatrix}$.

Операция, очевидно, определена на данном множестве, и ее действие сводится к действию над упорядоченными парами чисел: $(x, y)*(z, t)=(-xt, -yt)$.

Операция является ассоциативной, поскольку

$((x, y)*(z, t))*(u, v)=(-xt, -yt)*(u, v)=(xtv, ytv),$

$(x, y)*((z, t)*(u, v))=(x, y)*(-zv, -tv)=(xtv, ytv).$

Все матрицы вида $\begin{pmatrix} 0 & z \\ 0 & -1 \end{pmatrix}$ являются правыми единицами, а левых единиц – нет вообще.

Пример 3. Построить мультипликативную группу (A,B), порожденную матрицами $A=\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$, $B=\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$.

Для решения задачи необходимо найти наименьшее множество, содержащее матрицы A и B, замкнутое относительно операции умножения и обращения матриц, содержащее единичную матрицу. Непосредственной проверкой можно убедиться, что $A^2=B^2=E$, $BAB=ABA$, поэтому всевозможных конечных произведений матриц A, B и обратных к ним будет конечное число. Различными будут только матрицы E, A, B, AB, BA, ABA, которые и составляют искомую группу. Составим для нее таблицу Кэли.

	E	A	B	AB	BA	ABA
E	E	A	B	AB	BA	ABA
A	A	E	AB	B	ABA	BA
B	B	BA	E	ABA	A	AB
AB	AB	ABA	A	BA	E	B
BA	BA	B	ABA	E	AB	A
ABA	ABA	AB	BA	A	B	E

Анализируя таблицу, убеждаемся, что построенное множество замкнуто относительно операции умножения матриц, единичная матрица принадлежит множеству, а так же, вместе с каждой из шести матриц множество содержит обратную:

$$E^{-1}=E;\ A^{-1}=A;\ B^{-1}=B;\ (AB)^{-1}=BA;\ (BA)^{-1}=AB;\ (ABA)^{-1}=ABA.$$

Нужно заметить, что речь идет об обычной операции умножения матриц, ассоциативность которой известна и доказана. Таким образом, нами построена именно группа. Обратим внимание на то, что построенная группа не является абелевой, так как в ней, например, $AB \neq BA$.

***Определение* 3.** Отображение φ группы $(A,*)$ на группу $(B,\circ)$ называется изоморфизмом, если оно:

1) взаимно однозначно (биективно);

2) сохраняет операцию, т.е. $\varphi(x*y)=\varphi(x)\circ\varphi(y)$ для всех $x,y\in A$.

В этом случае группы A и B называют изоморфными и обозначают $A\cong B$. Такое же определение изоморфизма вводят и для произвольных группоидов.

Чтобы установить изоморфизм двух групп, следует отыскать функцию φ, которая удовлетворяет условиям определения 3.

Для доказательства того, что две группы не изоморфны, следует указать какое-либо алгебраическое свойство, которое сохраняется при изоморфизме и которым обладает одна из групп, а другая – нет. Такими свойствами могут быть цикличность, коммутативность группы или наличие элементов определенных конечных порядков. На основании этого свойства методом «от противного» доказать, что группы не могут быть изоморфными.

Пример 4. Доказать, что аддитивная группа $(R, +)$ изоморфна группе $(iR^+,*)$, где $u*v = -iuv$ для любых $u,v\in iR^+$.

Отображение $\varphi: R\to iR^+$, заданное формулой $\phi(x)=ie^x$, $x\in R$, является биекцией и

$\phi(x+y)=ie^{x+y}=-i(ie^x ie^y)=-i(\varphi(x)\varphi(y))=\varphi(x)*\varphi(y)$ для любых $x,y\in R$.

Следовательно, $(R,+)\cong(iR_+,*)$.

Симметрической группой степени n называется множество S_n всех биективных отображений множества {1, 2, …, n} (или любого конечного множества) на себя с бинарной операцией, являющейся композицией отображений. Элементы S_n называются подстановками.

Теорема Кэли. Всякая конечная группа изоморфна некоторой группе подстановок.

При доказательстве этой теоремы каждому элементу a данной группы $A=\{e,a_2,...,a_n\}$ ставится в соответствие подстановка

$$\pi_a=\begin{pmatrix} e & a_2....a_n \\ a & aa_2....aa_n \end{pmatrix}.$$

Здесь мы использовали мультипликативное обозначение групповой операции. Оно наиболее экономное, а потому наиболее употребляемое. Мы и далее будем им пользоваться, причем группу $(A,\cdot)$ обозначим просто через A.

Пример 5. Построить таблицы Кэли мультипликативных групп S_3 и Z_{14}^*. Выяснить, изоморфны ли эти группы между собой?

Мультипликативная группа Z_{14}^* содержит все классы вычетов по модулю 14, взаимно простых с числом 14. Её элементами являются классы $\bar{1},\bar{3},\bar{5},\bar{9},\overline{11},\overline{13}$. Группа S_3 содержит все подстановки третьей степени: e – тождественную, $\alpha=(123)$, $\beta=(132)$, $\gamma=(12)$, $\delta=(13)$, $\zeta=(23)$. Как видим, обе группы S_3 и Z_{14}^* состоят из 6 элементов. Построим для них таблицы Кэли:

	e	α	β	γ	δ	ζ
e	e	α	β	γ	δ	ζ
α	α	β	e	δ	ζ	γ
β	β	e	α	ζ	γ	δ
γ	γ	ζ	δ	e	β	α
δ	δ	γ	ζ	α	e	β
ζ	ζ	δ	γ	β	α	e

	$\bar{1}$	$\bar{3}$	$\bar{5}$	$\bar{9}$	$\overline{11}$	$\overline{13}$
$\bar{1}$	$\bar{1}$	$\bar{3}$	$\bar{5}$	$\bar{9}$	$\overline{11}$	$\overline{13}$
$\bar{3}$	$\bar{3}$	$\bar{9}$	$\bar{1}$	$\overline{13}$	$\bar{5}$	$\overline{11}$
$\bar{5}$	$\bar{5}$	$\bar{1}$	$\overline{11}$	$\bar{3}$	$\overline{13}$	$\bar{9}$
$\bar{9}$	$\bar{9}$	$\overline{11}$	$\bar{3}$	$\overline{13}$	$\bar{1}$	$\bar{5}$
$\overline{11}$	$\overline{11}$	$\bar{5}$	$\overline{13}$	$\bar{1}$	$\bar{9}$	$\bar{3}$
$\overline{13}$	$\overline{13}$	$\overline{11}$	$\bar{9}$	$\bar{5}$	$\bar{3}$	$\bar{1}$

Группа Z_{14}^* абелева, ибо её таблица Кэли симметрична относительно главной диагонали, а группа S_3 абелевой не является. Следовательно, эти группы не изоморфны. Предлагаем самостоятельно доказать, что если некоторая группа – абелева, то изоморфная ей группа – также абелева.

Пример 6. Построить группу подстановок, изоморфную группе из примера 3.

Подстановка π_A, соответствующая матрице A, переводит элементы E, A, B, AB, BA, ABA соответственно в элементы $AE=A$, $A\cdot A=E$, $A\cdot B=AB$, $A\cdot AB=B$, $A\cdot BA=ABA$, $A\cdot ABA=BA$, получаем:

$$\pi_A=\begin{pmatrix} E & A & B & AB & BA & ABA \\ A & E & AB & B & ABA & BA \end{pmatrix}.$$

Аналогично $\pi_B=\begin{pmatrix} E & A & B & AB & BA & ABA \\ B & BA & E & ABA & A & AB \end{pmatrix}$. Остальные подстановки получаем таким же образом. Если обозначить элементы *E, A, B, AB, BA, ABA* соответственно числами 1, 2, 3, 4, 5, 6, то подстановки π_A, π_B примут вид $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 4 & 3 & 6 & 5 \end{pmatrix}$, $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 1 & 6 & 2 & 4 \end{pmatrix}$, или, в виде произведения циклов, (12)(34)(56), (13)(25)(46). Остальным элементам группы *AB, BA, ABA, E* будут соответствовать подстановки (145)(263), (154)(236), (16)(24)(35), *e* – тождественная подстановка.

Практический блок

Индивидуальные задания для домашней работы

Таблица 1

	K	$x \circ y$	$x \oplus y$	$x * y$
1.	$R^- = \{x \mid x \in R, x < 0\}$	$\frac{x}{y}$	$\frac{x+y}{xy}$	$-xy$
2.	$\{ x \mid x \in R, x > -1\}$	$x + y$	$\lvert x \rvert + \lvert y \rvert$	$x + y + xy$
3.	$U = \{x \mid x \in C, \lvert x \rvert = 1\}$	$\frac{x}{y}$	$x + y$	ixy
4.	$R^+ = \{x \mid x \in R, x > 0\}$	$x - y$	$\sqrt{x^2 + y^2}$	$\frac{xy}{2}$
5.	$Q^- = \{x \mid x \in Q, x < 0\}$	xy	$\frac{xy}{x+y}$	$-2xy$
6.	$\{ x \mid x \in R, x > 1\}$	$\frac{xy}{2}$	$2x + 2y$	$xy - x - y + 2$
7.	$C^* = \{x \mid x \in C, x \neq 0\}$	$\frac{1}{xy}$	$\lvert xy \rvert$	$-ixy$
8.	$2Z = \{ 2p \mid p \in Z \}$	$\frac{xy}{2}$	$\frac{x+y}{2}$	$x + y - 2$
9.	$1+2Z = \{ 2p+1 \mid p \in Z\}$	xy	$1 - x - y$	$1 + x + y$
10.	$\{ x \mid x \in R, x < 1\}$	xy	$\frac{x+y}{2}$	$x + y - xy$
11.	C	$-xy$	$x - y$	$x + y - 1$
12.	$Q^+ = \{x \mid x \in Q, x < 0\}$	$\sqrt{xy}$	$x + y$	$2xy$

Таблица 2

	K_1	K_2	H	T	$A*B$	$A\circ B$
1.	$\begin{pmatrix}1 & x\\ 0 & 0\end{pmatrix}$	$\begin{pmatrix}1 & 0\\ x & 0\end{pmatrix}$	$\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}$	$\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}$	*ABH*	*ABT*
2.	$\begin{pmatrix}0 & 0\\ 0 & x\end{pmatrix}$	$\begin{pmatrix}0 & x\\ 0 & 1\end{pmatrix}$	$\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$	$\begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix}$	*HAB*	*ABT*
3.	$\begin{pmatrix}x & -x\\ 0 & x\end{pmatrix}$	$\begin{pmatrix}0 & x\\ 0 & 0\end{pmatrix}$	$\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$	$\begin{pmatrix}0 & 0\\ 1 & 0\end{pmatrix}$	*ABH*	*TAB*
4.	$\begin{pmatrix}0 & x\\ 0 & 1\end{pmatrix}$	$\begin{pmatrix}0 & 0\\ x & 1\end{pmatrix}$	$\begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix}$	$\begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix}$	*AHB*	*TAB*
5.	$\begin{pmatrix}x & x\\ 1-x & 1-x\end{pmatrix}$	$\begin{pmatrix}x & 1-x\\ x & 1-x\end{pmatrix}$	$\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$	$\begin{pmatrix}1 & 1\\ 1 & 1\end{pmatrix}$	*HAB*	*AB*
6.	$\begin{pmatrix}0 & x\\ 0 & -1\end{pmatrix}$	$\begin{pmatrix}0 & x\\ 0 & -x\end{pmatrix}$	$\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$	$\begin{pmatrix}1 & 1\\ -1 & -1\end{pmatrix}$	*ABH*	*TAB*
7.	$\begin{pmatrix}x & -x\\ -x & x\end{pmatrix}$	$\begin{pmatrix}x & 0\\ x & 0\end{pmatrix}$	$\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$	$\begin{pmatrix}1 & -1\\ 1 & -1\end{pmatrix}$	*AHB*	*TAB*
8.	$\begin{pmatrix}x & -x\\ -x & x\end{pmatrix}$	$\begin{pmatrix}x & -x\\ 1-x & 1-x\end{pmatrix}$	$\begin{pmatrix}0 & -1\\ -1 & 0\end{pmatrix}$	$\begin{pmatrix}1 & -1\\ -1 & 1\end{pmatrix}$	*ABH*	*AB*
9.	$\begin{pmatrix}1 & x\\ 0 & 0\end{pmatrix}$	$\begin{pmatrix}x & x\\ 1-x & 1-x\end{pmatrix}$	$\begin{pmatrix}1 & 1\\ 0 & 0\end{pmatrix}$	$\begin{pmatrix}1 & 1\\ 0 & 0\end{pmatrix}$	*ABH*	*TAB*
10.	$\begin{pmatrix}0 & x\\ 0 & 1\end{pmatrix}$	$\begin{pmatrix}1+x & x\\ 0 & 1\end{pmatrix}$	$\begin{pmatrix}0 & -1\\ 0 & 1\end{pmatrix}$	$\begin{pmatrix}0 & -1\\ 0 & 1\end{pmatrix}$	*ABH*	*ABT*
11.	$\begin{pmatrix}1 & x\\ 0 & 0\end{pmatrix}$	$\begin{pmatrix}1 & x\\ 0 & 1+x\end{pmatrix}$	$\begin{pmatrix}1 & -1\\ 0 & 0\end{pmatrix}$	$\begin{pmatrix}1 & -1\\ 0 & 0\end{pmatrix}$	*AHB*	*AB*
12.	$\begin{pmatrix}x & 1-x\\ x & 1-x\end{pmatrix}$	$\begin{pmatrix}1-x & x\\ 0 & 1\end{pmatrix}$	$\begin{pmatrix}0 & 1\\ 0 & 1\end{pmatrix}$	$\begin{pmatrix}0 & 1\\ 0 & 1\end{pmatrix}$	*HAB*	*AB*

Задача 1. Определить, является ли группой: числовое множество K относительно каждой из операций $\circ$, $\oplus$, $*$ (таблица 1). Найти нейтральные элементы (левые, правые,

двусторонние). Если множество не образует группу, то указать условия из определения группы, которые не выполняются.

Задача 2. Проверить, что отображение φ является изоморфизмом группы $(K, *)$ из задания 1 на некоторую числовую группу (определить, на какую):

1) $\varphi(x)=-x$; 4) $\varphi(x)=\frac{x}{2}$; 7) $\varphi(x)=i\bar{x}$; 10) $\varphi(x)=1-x$;

2) $\varphi(x)=x+1$; 5) $\varphi(x)=-2x$; 8) $\varphi(x)=\frac{x}{2}-1$; 11) $\varphi(x)=1-\bar{x}$;

3) $\varphi(x)= ix$; 6) $\varphi(x)=x-1$ 9) $\varphi(x)=\frac{x+1}{2}$; 12) $\varphi(x)=2x$.

Задача 3. Определить, является ли группой каждое из множеств K_1 и K_2 всех (2×2)-матриц над R из таблицы 2 относительно операций $*$ и $\circ$.

Найти нейтральные элементы (левые, правые, двусторонние). Если множество не является группой, то указать условия из определения группы, которые не выполняются

Задача 4. При помощи таблиц Кэли доказать, что приведенное ниже множество матриц составляют группу относительно умножения (таблица 3). Постройте группу подстановок, изоморфную этой группе.

Задача 5. При помощи таблиц Кэли доказать, что приведенное ниже множество числовых функций (таблица 4) составляет группу относительно композиции (суперпозиции) функций. Постройте группу подстановок, изоморфную этой группе.

Таблица 3

1.	E, A, A^2, A^3, A^4, A^5 ; $A = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$.
2.	E, A, A^2, B, AB, A^2B; $A = \begin{pmatrix} 0 & i \\ i & -1 \end{pmatrix}$, $B = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$.
3.	E, A, A^2, A^3; $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.
4.	E, A, A^2, B, AB, A^2B; $A = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$, $B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.
5.	E, A, B, AB, BA, ABA; $A = \begin{pmatrix} 1 & \sqrt{3} \\ 0 & -1 \end{pmatrix}$, $B = \begin{pmatrix} 1 & 0 \\ -\sqrt{3} & -1 \end{pmatrix}$.
6.	E, A, A^2, B, AB, A^2B; $A = \begin{pmatrix} 0 & i \\ i & -1 \end{pmatrix}$, $B = \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix}$.
7.	E, A, B, AB, BA, ABA; $A = \begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix}$, $B = \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}$.
8.	E, A, A^2, A^3; $A = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$.
9.	E, A, A^2, A^3; $A = \begin{pmatrix} -\sqrt{3} & -2 \\ 2 & \sqrt{3} \end{pmatrix}$.
10.	E, A, A^2, A^3, A^4, A^5 ; $A = \begin{pmatrix} 1 & i \\ i & 0 \end{pmatrix}$.
11.	E, A, A^2, A^3, A^4 ; $A = \begin{pmatrix} 0 & -1 \\ 1 & \omega \end{pmatrix}$, $\omega = \frac{\sqrt{5}-1}{2}$, $(\omega^2 = 1-\omega)$.
12.	E, A, B, AB ; $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $B = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$.

Таблица 4

1.	$e(x)=x,\quad \mathrm{f}(x)=-x,\quad g(x)=\dfrac{1}{x},\quad h(x)=-\dfrac{1}{x}\quad (x\neq 0);$
2.	$e(x)=x,\quad \mathrm{f}(x)=1-x,\quad g(x)=\dfrac{x}{2x-1},\quad h(x)=\dfrac{x-1}{2x-1}\quad \left(x\neq \dfrac{1}{2}\right);$
3.	$e(x)=x,\quad \mathrm{f}(x)=\dfrac{1}{1-x},\quad g(x)=\dfrac{x-1}{x},\quad u(x)=1-x,$ $v(x)=\dfrac{1}{x},\quad w(x)=\dfrac{x}{x-1}\quad (x\neq 0;\, x\neq 1);$
4.	$e(x)=x,\quad \mathrm{f}(x)=ix,\quad g(x)=-x,\quad h(x)=-ix;$
5.	$e(x)=x,\quad \mathrm{f}(x)=\dfrac{1}{x-i},\quad g(x)=\dfrac{1+ix}{x}\quad (x\neq 0;\, x\neq i);$
6.	$e(x)=x,\quad \mathrm{f}(x)=-\dfrac{1}{x},\quad g(x)=\dfrac{x+1}{x-1},\quad h(x)=\dfrac{1-x}{1+x}\quad (x\neq 0,\, x\neq 1,\, x\neq -1);$
7.	$e(x)=x,\quad \mathrm{f}(x)=\quad -\dfrac{1}{x+1},\quad g(x)=-\dfrac{x+1}{x}\quad (x\neq 0;\, x\neq -1);$
8.	$e(x)=x,\quad \mathrm{f}(x)=\dfrac{i+x}{1+ix},\quad g(x)=\dfrac{1}{x},\quad h(x)=\dfrac{1+ix}{i+x}\quad (x\neq i;\, -i);$
9.	$e(x)=x,\quad \mathrm{f}(x)=\dfrac{1+ix}{x},\quad g(x)=\dfrac{i}{1+ix},\quad u(x)=i-x,$ $v(x)=-\dfrac{1}{x},\quad w(x)=-\dfrac{x}{1+ix}\quad (x\neq 0;\, x\neq i);$
10.	$e(x)=x,\quad \mathrm{f}(x)=-\dfrac{1}{x+\sqrt{2}},\quad g(x)=-\dfrac{x+\sqrt{2}}{1+x\sqrt{2}},$ $h(x)=-\dfrac{1+x\sqrt{2}}{x}\quad \left(x\neq 0,-\sqrt{2},-\dfrac{\sqrt{2}}{2}\right);$
11.	$e(x)=x,\quad \mathrm{f}(x)=\dfrac{1+x}{1-x},\quad g(x)=-\dfrac{1}{x},\quad h(x)=\dfrac{x-1}{1+x}\quad (x\neq 0,\, x\neq 1,\, x\neq -1);$
12.	$e(x)=x,\quad \mathrm{f}(x)=-2-x,\quad g(x)=\dfrac{3-x}{1+x},\quad h(x)=-\dfrac{x+5}{1+x}\quad (x\neq 1,\, x\neq -1).$

Блок самоконтроля

Контрольные вопросы для самопроверки

1. Сколько бинарных алгебраических операций можно построить на n-элементном множестве?
2. Может ли мультипликативная группа иметь две единицы?
3. Может ли таблица Кэли для группы содержать в столбце одинаковые элементы? А в строке?
4. Существует ли группа произвольного натурального порядка?
5. Для каких групп отображение $\varphi(a) = a^{-1}$ является автоморфизмом (изоморфизмом на эту же группу)?
6. Верно ли, что каждая циклическая группа является абелевой?
7. Верно ли, что две произвольные бесконечные группы изоморфны?
8. Почему аддитивная группа целых чисел и мультипликативная группа рациональных без нуля чисел не изоморфны?

Дополнительные задачи и упражнения

1. Выяснить, какие из следующих подмножеств множества C относительно умножения являются группоидами, полугруппами, моноидами, группами:

а) $\{2^n \mid n \in Z\}$; б) $\{2^n \mid n = -2,-1,0,1,2\}$; в) $\{a + b\sqrt{3} \mid a,b \in Z, a^2 + b^2 \neq 0\}$; г) $\{a + b\sqrt{3} \mid a,b \in Q, a^2 + b^2 \neq 0\}$; д) $\{-1,1\}$; ж) $\{-1,0,1\}$.

2. Доказать, что все матрицы $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$ над R образуют относительно обычного умножения группу, изоморфную аддитивной группе всех действительных чисел.

3. Проверить, что все матрицы $\begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix}$ над R образуют по умножению группу, изоморфную мультипликативной группе U всех комплексных чисел с модулем 1.

4. Даны две мультипликативные группы (A) и (B),

порождённые соответственно матрицами $A=\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$ и $B=\begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}$.

Являются ли отображения $\alpha(X)=X^t$ и $\beta(X)=C^{-1}XC$, где $C=\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$ изоморфизмами группы (A) на группу (B)?

5. Изоморфны ли:

а) аддитивная группа всех комплексных чисел и мультипликативная группа всех отличных от нуля комплексных чисел?

б) аддитивная группа всех действительных чисел и мультипликативная группа всех действительных положительных чисел?

в) аддитивная группа всех рациональных чисел и мультипликативная группа всех рациональных положительных чисел

г) аддитивная группа всех целых чисел и аддитивная группа всех четных чисел?

д) аддитивная и мультипликативная группы, порождённые числом 2?

е) аддитивная и мультипликативная группы, порождённые числом i?

6. Для данных матриц проверить указанные соотношения и, пользуясь ими выписать в каноническом виде все элементы мультипликативной группы, порожденной этими матрицами:

a) $A=\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}$, $B=\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$; $A^4=B^2=E,\quad BA=A^{-1}B;$

b) $A=\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}$, $B=\begin{pmatrix}0 & -i\\ i & 0\end{pmatrix}$; $A^4=B^2=E,\quad BA=AB;$

c) $A=\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}$, $B=\begin{pmatrix}0 & i\\ i & 0\end{pmatrix}$; $A^4=E,\quad B^2=A^2,\quad BA=A^{-1}=B;$

d) $A=\begin{pmatrix}0 & 1\\ i & 0\end{pmatrix}$; $A^8=E;$

e) $A=\begin{pmatrix}0 & -1\\ 1 & \sqrt{2}\end{pmatrix}$, $B=\begin{pmatrix}-\sqrt{2} & -1\\ 1 & 0\end{pmatrix}$; $A^3=B,\quad B^3=A;$

(Указание: вывести отсюда, что $A^8=E$)

f) $A=\begin{pmatrix}i & 0\\ 0 & i\end{pmatrix}$, $B=\begin{pmatrix}-1 & i\\ i & 0\end{pmatrix}$; $A^4=B^3=E,\quad BA=AB;$

g) $A=\begin{pmatrix}1 & 0\\ 0 & i\end{pmatrix}$, $B=\begin{pmatrix}i & 0\\ 0 & 1\end{pmatrix}$; $A^4=B^4=E,\quad BA=AB;$

h) $A=\begin{pmatrix}0 & -1\\ 1 & \omega\end{pmatrix}$; $\omega=\dfrac{\sqrt{5}+1}{2}$; $\quad A^{10}=E.$

(Указание: пользоваться тем, что $\omega^2=\omega+1$).

7. Доказать, что группа, порожденная относительно композиции функциями $f(u)=iu, g(u)=\bar{u}\ (u\in C),$ изоморфна группе (A,B) из задачи 6(а).

8. Доказать, что группа $(C^*,\cdot)$ изоморфна мультипликативной группе всех невырожденных матриц вида $\begin{pmatrix}\alpha & \beta\\ -\beta & \alpha\end{pmatrix}$.

Задачи повышенной сложности

9. Доказать, что композиция любых отображений множеств ассоциативна, если она определена.

10. Доказать, что если в полугруппе имеются левые и правые единицы, то каждая левая единица совпадает с каждой правой единицей.

11. Доказать, что множество с определенной на нем ассоциативной операцией тогда и только тогда является группой, когда для любых $a\ \ u\ \ b$ в этом множестве разрешимы уравнения $xa=b\ \ u\ \ ay=b.$

12. Доказать, что в любой группе $(a*b)^{-1}=b^{-1}*a^{-1}$.

13. Доказать, что если квадрат каждого элемента группы равен единице, то группа абелева.

14. Доказать, что всякая группа 4-го порядка абелева.

Указание: сначала рассмотреть случай, когда в группе имеется элемент 4-го порядка; затем случай, когда все отличные от единицы элементы имеют порядок 2, в последнем случае воспользоваться задачей 11.

15. Доказать, что если отображение $\varphi: A\to A,$ заданное формулой $\varphi(x)=x^{-1},$ является изоморфизмом группы A на себя, то группа A абелева.

16. Пусть отображение $\varphi: A\to A$ циклической группы A в себя задано формулой $\varphi(x)=x^2.$ В каких случаях это отображение

является изоморфизмом?

ТЕМА 2.
ПОДГРУППЫ, НОРМАЛЬНЫЕ ПОДГРУППЫ

Методический блок

В результате изучения темы студент должен знать определения и уметь приводить примеры следующих понятий: подгруппа, циклическая подгруппа, порядок элемента, смежные классы, индекс подгруппы, нормальная подгруппа.

В результате изучения темы студент должен знать формулировки и уметь доказывать следующие факты: критерии подгруппы; теорема о пересечении подгрупп группы; строение элементов группы с данной системой образующих; строение циклических групп; цикличность подгрупп циклических групп; изоморфизмы циклических групп; критерий того, что подгруппа – нормальна; свойства смежных классов, теорема Лагранжа.

В результате изучения темы студент должен уметь: распознавать подгруппы, находить порядок элемента, строить циклические подгруппы; проверять нормальность подгрупп.

Информационный блок

***Определение* 4.** Подмножество H группы A называется ее *подгруппой*, если H также является группой относительно операции, определенной в A.

Важно то, что H является группой именно относительно операции, определенной в группе A. Так, мультипликативная группа невырожденных квадратных матриц порядка n является подмножеством аддитивной группы всех квадратных матриц этого же порядка, но не является ее подгруппой.

Приведем некоторые ***критерии подгруппы***.

1. Непустое подмножество H данной группы A является ее подгруппой тогда и только тогда, когда подмножество H замкнуто относительно операции, определенной в A, и вместе с каждым элементом x подмножество H содержит обратный элемент x^{-1}.

2. Непустое подмножество H данной группы A является ее подгруппой тогда и только тогда, когда для произвольных элементов x, y из подмножества H элемент xy^{-1} также принадлежит H.

Если *подмножество H конечно*, то в этом случае используют наиболее простой критерий:

3. Непустое конечное подмножество H данной группы A является ее подгруппой тогда и только тогда, когда подмножество H замкнуто относительно групповой операции.

Теорема. Пересечение произвольного конечного числа подгрупп группы A является подгруппой группы A.

Если X - некоторое подмножество группы A, то пересечение всех подгрупп группы A, каждая из которых содержит подмножество X, является подгруппой (X), порожденной множеством X, для которой множество X называется *множеством образующих*. Подгруппа (X) является наименьшей (т. е. включенной во все подгруппы, содержащие X) подгруппой группы A среди тех, которые содержат множество X.

Нетрудно получить и комбинаторное описание группы (X). Она состоит из всех конечных произведений элементов множества X и обратных к ним.

Подгруппа (x) с одним образующим элементом x называется *циклической*. Она состоит из всех степеней x^n, $n \in Z$ (в мультипликативной записи). Если для всех целых k, p из того, что $k \neq p$ обязательно следует $x^k \neq x^P$, то (x) – *бесконечная циклическая группа*.

Теорема. Всякая бесконечная циклическая группа изоморфна аддитивной группе целых чисел $(Z,+)$.

Если существуют целые k, p $(k \neq p)$ такие, что в циклической группе (x) верно $x^k = x^p$, то существует наименьшее натуральное число n, такое, что $x^n = e$. В этом случае число n называется *порядком* элемента x. Тогда группу (x) составляют все различные

неотрицательные степени образующего: $x^0=e$, x^1, x^2,...,x^{n-1}. Т.е. порядок группы (x) (иначе – количество ее элементов) равен порядку образующего элемента.

Теорема. Конечная циклическая группа порядка n изоморфна мультипликативной группе всех корней n-ой степени из единицы.

Определение 5. Если H – подгруппа группы A, то множества xH и Hx ($x \in A$) называются, соответственно, *левым и правым смежными классами* группы A по подгруппе H, а элемент x – *представителем этих классов*.

Среди свойств левых (или правых) смежных классов следует отметить такие:

1. если $y \in xH$, то $xH = yH$;
2. произвольные левые смежные классы или не пересекаются, или совпадают.

Индексом подгруппы H в группе A называется количество левых (или правых) смежных классов.

Теорема Лагранжа. *В конечной группе индекс и порядок подгруппы являются делителями порядка группы.*

Определение 6. Подгруппа H группы A называется *нормальной (инвариантной),* если $xH=Hx$ для каждого $x \in A$ (обозначают $H \triangleleft A$).

Определение 7. Элементы x и y называются *сопряженными*, если $y = p^{-1}xp$ для некоторого $p \in A$.

Для проверки нормальности подгруппы можно пользоваться ***критерием***: подгруппа H группы A нормальна тогда и только тогда, когда вместе с каждым элементом эта подгруппа содержит и все его сопряженные.

Пример 7. Разложить группу A_4 в объединение правых и в объединение левых смежных классов по подгруппе H={1,(12)(34),(13)(24),(14)(23)} и по подгруппе K={1,(123),(132)}. Выяснить, нормальны ли эти подгруппы?

Знакопеременная группа A_4 содержит все четные подстановки четвертой степени: 1 (тождественная подстановка), (123), (132), (124), (142), (134), (143), (234), (243), (12)(34), (13)(24); (14)(23). Левые смежные классы по подгруппе H имеют вид xH, например, $(123)\cdot H$ = {(123), (134), (243), (142)}. Еще

одним левым смежным классом является подгруппа H. Осталось еще 4 подстановки, которые составляют третий левый смежный класс {(123), (143), (243), (124)}. Правые смежные классы Hx можно найти аналогично, или используя то, что элементы правого смежного класса являются обратными к элементам некоторого левого смежного класса. В нашем случае *разбиение* группы A_4 на правые смежные классы по группе H совпадает с разбиением на левые смежные классы, поэтому $H \triangleleft A$.

Выпишем левые смежные классы группы A_4 по подгруппе K: {1, (123), (132)}, {(12)(34), (243), (143)}, {(13)(24), (142), (234)}, {(14)(23), (134), (124)}. В этом случае правые смежные классы (составлены из обратных подстановок) не совпадают с левыми. Следовательно подгруппа K нормальной не является.

Практический блок

Индивидуальные задания для домашней работы

Задача 6. Пусть n – натуральное число, больше 1. Доказать, что множество Z_n^* всех классов вычетов, взаимно простых с n, является группой относительно умножения. Найти порядок группы $(Z_n^*, \cdot)$ и выписать все ее элементы, если n равно:

1) 20;	2) 36;	3) 15;	4) 11;
5) 24;	6) 13;	7) 22;	8) 21;
9) 16;	10) 28;	11) 30;	12) 25.

Найти порядок элементов этой группы и выписать все ее циклические подгруппы.

Задача 7. Ниже приведены подстановки x, y (или x, y, p), а также соотношения между ними. Проверить эти соотношения и, используя их, выписать все элементы группы A с образующими x, y (или x, y, p).

1) $x = (168)(274)$, $y = (24)(68)$, $p = (17)(28)(35)(46)$,
$x^3 = y^2 = p^2 = 1$, $yx = x^{-1}y$, $xp = px$, $yp = py$; ***(рис. 1);***

2) $x = (15)(24)(36)$, $y = (13)(46)$, $x^2 = y^2 = 1$, $(yx)^3 = (xy)^3$; ***(рис. 3);***

3) $x = (123456)$, $y = (13)(46)$, $x^6 = y^2 = 1$, $yx = x^{-1}y$; ***(рис.4);***

4) $x = (12)(45)$, $y = (16)(25)(34)$, $x^2 = y^2 = 1$, $(yx)^3 = (xy)^3$; ***(рис.2);***

5) $x = (168)(274)$, $y = (12)(35)(46)(78)$, $p = (17)(28)(35)(46)$,

$x^3 = y^2 = p^2 = 1$, $yx = x^{-1}y$, $px = xp$, $py = yp$; ***(рис. 1);***

6) $x = (12)(45)$, $y = (13)(46)$, $p = (14)(25)(36)$;
$x^2 = y^2 = p^2 = 1$, $yxy = xyx$, $px = xp$, $py = yp$; ***(рис.3);***

7) $x = (123)(456)$, $y = (12)(45)$, $p = (14)(25)(36)$,
$x^3 = y^2 = p^2 = 1$, $yx = x^{-1}y$, $px = xp$, $py = yp$; ***(рис. 2);***

8) $x = (14)(28)(35)(67)$, $y = (24)(68)$, $x^2 = y^2 = 1$, $(yx)^3 = (xy)^3$; ***(рис. 1);***

9) $x = (12)(34)(56)(78)$, $y = (14)(23)(58)(67)$, $p = (15)(26)(37)(48)$,
$x^2 = y^2 = p^2 = 1$, $yx = xy$, $px = xp$, $py = yp$; ***(рис.1);***

10) $x = (12)(36)(45)$, $y = (26)(35)$, $x^2 = y^2 = 1$, $(yx)^3 = (xy)^3$; ***(рис.4);***

11) $x = (1234)(5678)$, $y = (1562)(4873)$,
$x^4 = y^4 = 1$, $(yx)^3 = (xy)^3 = 1$; ***(рис. 1);***

12) $x = (24)(68)$, $y = (16)(47)$, $p = (17)(28)(35)(46)$,
$x^2 = y^2 = p^2 = 1$, $yxy = xyx$, $px = xp$, $py = yp$ ***(рис. 1)***.

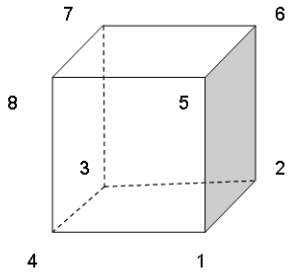


Рис. 1

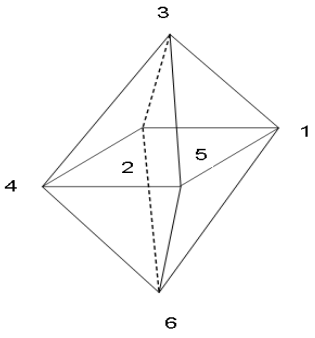


Рис. 2

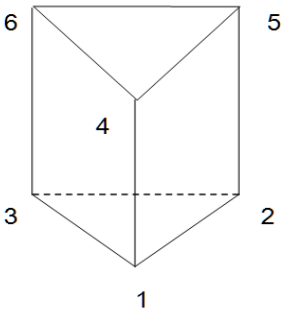


Рис. 3

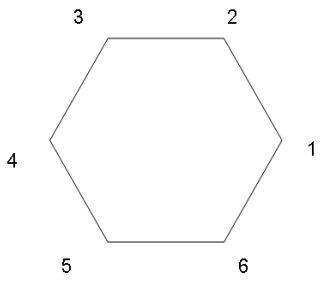


Рис. 4

Задача 8. Проверить, что подмножества H_1, H_2, H_3, H_4 (таблица 5) являются подгруппами группы A из задачи 7. Какие из этих подгрупп нормальны?

Задача 9. Пусть T – матрица из таблицы 2. Выяснить, образует ли группу относительно сложения матриц множество всех (2×2) - матриц A над R, удовлетворяющих условию:

а) $TA = 0$; б) $AT = T$; в) $TA = AT$.

Указание: достаточно проверить, является ли каждое из этих множеств подгруппой аддитивной группы всех (2×2)-матриц над *R*.

Задача 10. Пусть *T* – матрица из таблицы 2. Доказать, что каждое из приведённых далее множеств является группой относительно обычного умножения:

а) множество *H* всех невырожденных (2×2)-матриц над *R*, которые удовлетворяют условию: *AT=T*;

б) множество *K* всех невырожденных (2×2)-матриц над *R*, которые удовлетворяют условию: *TA=AT*.

Доказать, что множество *M* всех невырожденных (2×2)-матриц над *R*, которые удовлетворяют условию *TA=AT=T,* являются подгруппой как в группе *H*, так и в группе *K*. В какой из этих групп подгруппа *M* нормальна?

Таблица 5

N°	H_1	H_2	H_3	H_4
1.	$1, p$	$1, x, x^2$	$1, x, x^2, y, xy, x^2y$	$1, y, p, yp$
2.	$1, (xy)^3$	$1, y$	$1, x, yxy, xyxy, yxyx, xyxyx$	$1, x, yxyxy, xyxyxy$
3.	$1, x^3$	$1, y$	$1, x^2, x^4, y, x^2y, x^4y$	$1, x^3, y, x^3y$
4.	$1, (xy)^3$	$1, x$	$1, y, xyx, xyxy, yxyx, yxyxy$	$1, y, xyxyx, xyxyxy$
5.	$1, p$	$1, x, x^2$	$1, x, x^2, y, xy, x^2y$	$1, y, p, yp$
6.	$1, p$	$1, xy, yx$	$1, x, y, xy, yx, xyx$	$1, x, p, xp$
7.	$1, p$	$1, xy$	$1, x, x^2, y, xy, x^2y$	$1, y, p, yp$
8.	$1, (xy)^3$	$1, y$	$1, x, yxy, xyxy, yxyx, xyxyx$	$1, x, yxyxy, xyxyxy$
9.	$1, p$	$1, x, x^2$	$1, x, x^2, y, xy, x^2y$	$1, y, p, yp$
10.	$1, (xy)^3$	$1, x$	$1, y, xyx, xyxy, yxyx, yxyxy$	$1, y, xyxyx, xyxyxy$
11.	$1, p$	$1, xy, yx$	$1, x, y, xy, yx, xyx$	$1, x, p, xp$
12.	$1, p$	$1, xy, yx$	$1, x, y, xy, yx, xyx$	$1, y, p, yp$

Блок самоконтроля

Контрольные вопросы для самопроверки

9. Привести пример подмножества группы, которое замкнуто относительно групповой операции и не является подгруппой.
10. Известно, что некоторое подмножество аддитивной группы замкнуто относительно сложения. Следует ли отсюда, что оно замкнуто и относительно вычитания?
11. Известно, что некоторое подмножество аддитивной группы замкнуто относительно вычитания. Следует ли отсюда, что оно замкнуто и относительно сложения?
12. Будет ли подгруппой объединение подгрупп некоторой группы?
13. Верно ли, что бесконечная группа содержит бесконечное количество подгрупп?
14. Может ли бесконечная числовая мультипликативная группа содержать бесконечное количество конечных подгрупп ?
15. Верно ли, что конечная циклическая группа – абелева ?
16. Какой наибольший порядок элементов симметрической группы S_7?
17. Элементы x и y абелевой группы имеют порядки 6 и 8. Какой порядок имеет элемент xy?
18. Пусть H – бесконечная подгруппа группы G. Можно ли утверждать, что: а) $|G:H|$ – конечен; б) $|G:H|$ – бесконечен?
19. Верно ли, что пересечение двух нормальных подгрупп группы G также является нормальной подгруппой?

Дополнительные задачи и упражнения

17. Для данных подстановок проверить указанные соотношения и, пользуясь ими, выписать в каноническом виде все элементы группы, порождённые этими подстановками:

a) $x=(1234)(5678),\quad y=(1836)(2547);\quad x^4=1,\quad y^2=x^2,\quad yx=xy;$

b) $x=(1234)(5678),\quad y=(1638)(2547);\quad x^4=1,\quad y^2=x^2,\quad yx=x^{-1}y;$

c) $x=(1234)(5678),\quad y=(15)(28)(37)(46);\quad x^4=y^2=1,\quad yx=x^{-1}y;$

d) $x=(12345),\quad y=(25)(34);\quad x^5=y^2=1,\quad yx=x^{-1}y;$

e) $x=(12345)(67);\quad x^{10}=1;$

f) $x=(123)(456)(789),\quad y=(147)(258)(369);\quad x^3=y^3=1,\quad yx=xy;$

g) $x=(1234),\quad y=(567);\quad x^4=y^3=1,\quad yx=xy;$

18. Установить изоморфизм группы (x,y) из задачи 17(c) с группой (A,B) из задачи 6(a).

19. Проверить, что множество A всех функций $x\to ax+b\quad (a,b\in R, a\neq 0)$ определённых на R, является группой относительно композиции функций. Проверить также, что подмножество H всех функций $x\to x+b$ и подмножество K всех функций $x\to ax$ является подгруппами группы A. Выяснить геометрический смысл этих функций как преобразований на числовой прямой.

20. Проверить, что множество A всех функций $z\to e^{i\varphi}z+u\quad (\varphi\in R,\quad u,z\in C)$ является группой относительно композиции функций. Проверить также, что подмножество H всех функций $z\to z+u$ и подмножество K всех функций $z\to e^{i\varphi}z$ являются подгруппами группы A. Выяснить геометрический смысл этих функций как преобразований на комплексной плоскости.

21. В задачах 19 и 20 найти левые и правые смежные классы группы A по подгруппе H и по подгруппе K. Выяснить, нормальны ли эти подгруппы.

22. Построить левые и правые смежные классы группы (x,y) из задачи 17(c):

а) по подгруппе (x), порождённой подстановкой x;

б) по подгруппе (y), порождённой подстановкой y;

в) по подгруппе (x^2,y), порождённой подстановками x^2 и y.

Выяснить, какие из подгрупп (x), (y), (x^2,y) нормальны в группе (x,y).

23. Многочлен $f(x)$ называется чётным, если $f(-x)=f(x)$, и нечётным, если $f(-x)=-f(x)$. Образует ли группу по сложению:

а) все чётные многочлены от x над R;

б) все нечётные многочлены от x над R;

Указание: достаточно выяснить, является ли каждое из этих множеств подгруппой аддитивной группы всех многочленов от x над R.

24. Многочлен $f(x,y)$ называется симметрическим, если $f(x,y)=f(y,x)$ и антисимметрическим, если $f(x,y)=-f(y,x)$. Образуют ли группу по сложению:

a) все симметрические многочлены от x и y над R?

b) все антисимметрические многочлены от x и y над R?

25. Матрица A называется симметрической, если $A^t=A$ и анти симметрической, если $A^t=-A$. Образуют ли группу по сложению:

а) все симметрические (2×2)-матрицы над R?

б) все антисимметрические (2×2)-матрицы над R?

26. Найти все подгруппы;

a) аддитивной группы Z всех целых чисел;

b) циклической группы 6-го порядка;

c) циклической группы 8-го порядка.

27. В аддитивной группе Z всех целых чисел найти наименьшую подгруппу, содержащую числа 4 и 6. Найти также пересечение подгрупп (4) и (6).

28. Каков порядок группы, порождённой подстановками 5-й степени (123) и (45)?

29. Найти все элементы конечного порядка в мультипликативных группах $C^*=C\setminus\{0\}$ и $R^*=R\setminus\{0\}$.

Задачи повышенной сложности

30. Доказать, что если данное подмножество группы вместе с любыми двумя элементами x и y содержит и $x\cdot y^{-1}$, то это подмножество является подгруппой.

31. Доказать, что если конечное подмножество данной группы замкнуто относительно групповой операции, то оно является подгруппой.

32. Доказать, что множество всех элементов, обратных к элементам правого (левого) смежного класса группы A по подгруппе H, является левым (правым) смежным классом группы A по подгруппе H.

33. Доказать, что если H - подгруппа группы A и p - произвольный фиксированный элемент из A, то $p^{-1}Hp$ - тоже подгруппа, изоморфная H.

34. Доказать, что если элемент y принадлежит левому смежному классу xH группы A по подгруппе H, то $xH = yH$.

35. Доказать, что два левых смежных класса группы по подгруппе либо не пересекаются, либо совпадают.

36. Доказать, что любые два левых (правых) смежных класса группы A по конечной подгруппе H содержат одинаковое число элементов.

37. Пусть H - подгруппа группы A и отношение $x\rho y$ $(x, y \in A)$ имеет место тогда и только тогда, когда $yx^{-1} \in H$. Доказать, что ρ есть отношение эквивалентности и что ρ-классы являются правыми смежными классами группы A по подгруппе H. *Указание:* проверить, что множество всех элементов y, удовлетворяющих условию $yx^{-1} \in H$, совпадает с Hx.

38. Центром группы называется множество всех ее элементов, каждый из которых коммутирует со всеми элементами группы. Доказать, что центр группы является ее нормальной подгруппой.

39. Доказать, что пересечение двух подгрупп данной группы также является подгруппой этой группы.

40. Пусть A – нормальная подгруппа группы B, B – нормальная подгруппа группы C. Обязательно ли при этом A – нормальная подгруппа группы C?

41. Доказать, что каждая подгруппа циклической группы также циклическая.

42. Доказать, что каждая группа простого порядка – циклическая.

43. Доказать, что всякая подгруппа индекса 2 – нормальна.

44. Доказать, что если m – порядок элемента x и $x^n = 1$, то n делится на число m.

45. Докажите, что в группе элементы a и a^{-1} имеют одинаковые порядки.

46. Доказать, что элементы xy и yx данной группы всегда сопряжены и потому имеют одинаковый порядок.

47. Доказать, что в каждой бесконечной группе имеется

бесконечно много подгрупп.

48. Доказать, что всякая группа четного порядка содержит элемент 2-го порядка.

Указание: рассмотреть пары элементов x и x^{-1}.

49. Доказать, что в любой группе нечетного порядка каждый элемент является квадратом некоторого элемента.

Указание: для каждого элемента x рассмотреть циклическую подгруппу (x).

ТЕМА 3.
ГОМОМОРФИЗМЫ ГРУПП, ФАКТОРГРУППЫ

Методический блок

В результате изучения темы студент должен знать определения и уметь приводить примеры следующих понятий: факторгруппа, гомоморфизм, канонический гомоморфизм, ядро гомоморфизма.

В результате изучения темы студент должен знать формулировки и уметь доказывать следующие факты: критерий принадлежности элементов группы одному смежному классу; свойства факторгрупп; свойства гомоморфизмов; свойства ядра гомоморфизма; критерий изоморфизма; теорема о гомоморфизмах групп.

В результате изучения темы студент должен уметь: распознавать гомоморфизмы, находить ядро гомоморфизма, строить факторгруппы.

Информационный блок

Определение 8. *Факторгруппой A* по нормальной подгруппе *H* называется множество *A/H* всех смежных классов *A* по *H*

(левых или правых, все равно), где операция умножения классов определяется операцией в группе A по формуле:$(Hx)\cdot(Hy) = H(xy)$.

Если определить произведение подмножеств K и P группы A как подмножество $KP = \{kp \mid k \in K,\ p \in P\}$, то операция в факторгруппе – это не что иное, как умножение подмножеств (смежных классов) данной группы:

$Hx \cdot Hy = H \cdot H \cdot x \cdot y = Hxy$ (здесь мы воспользовались ассоциативностью умножения подмножеств, нормальностью подгруппы H и тем, что $H^2 = H$).

Смежный класс Hx иногда обозначается $[x]$. Для описания смежных классов (элементов факторгрупп) достаточно найти систему представителей – по одному из каждого класса. В связи с этим важно знать, принадлежат или нет элементы группы одному смежному классу.

Критерий принадлежности одному смежному классу. Элементы x, y данной группы принадлежат одному смежному классу по подгруппе H тогда и только тогда, когда $xy^{-1} \in H$ (или $x-y \in H$, в аддитивной записи).

Пример 8. Построить факторгруппу S_3 / A_3.

Группа S_3 имеет порядок 6, а знакопеременная группа $A_3 = \{1, (123), (132)\}$ – порядок 3, следовательно, число смежных классов равно 2. Поэтому факторгруппа $S_3 / A_3 = \{A_3, K\}$, где $K = S_3 \setminus A_3$. Любая группа порядка 2 является циклической, но $A_3 \cdot A_3 = A_3$ (проверьте!). Значит, K – порождающий элемент циклической факторгруппы S_3 / A_3.

Определение 9. Отображение φ: $(A, *) \to (B, \circ)$ называется *гомоморфизмом* группы $(A, *)$ в группу $(B, \circ)$, если $\varphi(x*y)=\varphi(x)\circ\varphi(y)$ для всех $x, y \in A$.

При гомоморфизме φ нейтральный элемент e группы A отображается в нейтральный элемент e' группы B. Кроме того, $\varphi(x^{-1}) = (\varphi(x))^{-1}$ для каждого элемента $x \in A$. Наконец, множество $Ker\varphi = \{x \mid x \in A,\ \varphi(x) = e'\}$ является нормальной подгруппой группы A. Ее называют *ядром* гомоморфизма φ.

Важным примером гомоморфизма является отображение $\varphi : A \to A/H$, которое переводит каждый элемент $x \in A$ в смежный класс $[x] = Hx$. Его называют *каноническим (естественным)*

гомоморфизмом. Ядром этого гомоморфизма группы A на факторгруппу A/H является нормальная подгруппа H.

Теорема о гомоморфизмах групп. *Всякий гомоморфный образ группы A является группой, изоморфной факторгруппе A/H по некоторой нормальной подгруппе H.*

Пример 9. Проверить, что отображение $\varphi(z) = |z|$ является гомоморфизмом мультипликативной группы C^* в себя. Найти его ядро $Ker\varphi$, построить факторгруппу $C^*/Ker\varphi$ и установить ее изоморфизм с мультипликативной группой R^+ всех действительных положительных чисел.

Поскольку $\varphi(z_1 \cdot z_2) = |z_1 \cdot z_2| = |z_1| \cdot |z_2| = \varphi(z_1) \cdot \varphi(z_2)$, то φ – гомоморфизм группы C^* на группу R^+ . Далее, $Ker\varphi$ состоит из всех чисел z, для которых $\varphi(z)=|z|=1$, то есть из всех чисел вида $(cos\alpha + i \cdot sin\alpha)$. Воспользовавшись тригонометрической формой записи комплексных чисел, запишем смежный класс $z \cdot Ker\varphi$ в виде: $z \cdot Ker\varphi = r(cos\alpha + i \cdot sin\alpha)Ker\varphi = r \cdot Ker\varphi$, $r>0$. Причем, если $r_1 \neq r_2$, то $r_1 Ker\varphi \neq r_2 Ker\varphi$, поскольку $r_1 r_2^{-1} \neq 1$. Таким образом, систему представителей факторгруппы $C^*/Ker\varphi$ составляют все положительные действительные числа, поэтому отображение $\omega(x) = xKer\varphi$ группы R^+ на $C^*/Ker\varphi$ взаимно однозначно. Наконец,
$\omega(x \cdot y)=x \cdot yKer\varphi=xy(Ker\varphi)^2=xKer\varphi \; yKer\varphi = \omega(x) \cdot \omega(y)$, поэтому ω – изоморфизм.

Пример 10. Доказать, что факторгруппа аддитивной группы всех комплексных чисел по подгруппе всех мнимых чисел iR изоморфна аддитивной группе всех действительных чисел.

В силу теоремы о гомоморфизмах достаточно найти такой гомоморфизм φ группы $(C,+)$ на группу $(R,+)$, что $Ker\varphi = iR$. Рассмотрим отображение $\varphi(z) = Re\, z$, где $Re\ z$ – действительная часть числа z. Покажем, что φ является гомоморфизмом. Действительно, пусть $z = a + bi$, $t = u + iv$, тогда $\varphi(z + t) = a + u = \varphi(z) + \varphi(t)$. Далее, $z \in Ker\varphi$, если $\varphi(a + bi) = a = 0$, поэтому $Ker\varphi = iR$. Условия теоремы о гомоморфизмах выполнены, следовательно, по теореме о гомоморфизмах, $(C,+)/(iR,+) \cong (R,+)$.

Пример 11. Пусть A – аддитивная группа с образующими $\frac{1}{2}x$ и $\frac{1}{3}$. Построить факторгруппу группы A по подгруппе всех многочленов из A с целыми коэффициентами.

Все элементы группы A имеют вид $\frac{1}{2}mx+\frac{1}{3}n$, где $m, n\in Z$. Подгруппу H составляют все многочлены $ax + b$, где $a, b\in Z$. Смежные классы группы A по подгруппе H имеют вид $f(x) + H$, где $f(x)\in A$. Причем $f(x)+H = g(x)+H$ тогда и только тогда, когда $f(x)-g(x)\in H$, т.е. когда $f(x)-g(x)$ имеет целые коэффициенты. Отсюда следует, что существует 6 разных смежных классов:

$H, \frac{1}{3}+H, \frac{2}{3}+H, \frac{1}{2}x+H, \frac{1}{2}x+\frac{1}{3}+H, \frac{1}{2}x+\frac{2}{3}+H.$

Сумма смежных классов определяется как $f(x)+H+g(x)+H=f(x)+g(x)+H$, причем в $f(x)+g(x)$ надо «оставлять» только дробные части коэффициентов, т. к. целые части – «поглощаются» подгруппой H. Отметим также, что факторгруппа A/H является циклической и ее образующими являются, например, класс $\frac{1}{2}x+\frac{1}{3}+H$.

Как следует из теоремы о гомоморфизмах, все группы, на которые группа G может быть гомоморфно отображена, исчерпываются её факторгруппами, а все гомоморфизмы группы G – её естественными гомоморфизмами на свои факторгруппы.

Пример 12. Доказать, что множество G всех (2×2)-матриц A над R, удовлетворяющих условию $PA = – AP$, где $P=\begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix}$, является аддитивной группой. Показать, что отображение φ, при котором $\varphi(A)=P^tAP^t$, является гомоморфизмом. Найти его ядро $Ker\varphi$ и построить факторгруппу $G/Ker\varphi$.

Для того чтобы рассматриваемое множество G было группой, достаточно доказать, что G является подгруппой аддитивной группы всех (2×2)-матриц над R. Для этого достаточно проверить, что множество G замкнуто относительно сложения и вместе с каждым элементом содержит противоположный ему элемент. Пусть $A,B\in G$, тогда $PA = – AP$ и $PB = – BP$. Отсюда

$PA+PB = -AP - BP$ или $P(A+B) = -(A+B)P$ и $A+B \in G$. Равенство $PA= -AP$ эквивалентно $-PA = -(-AP)$, или $P(-A) = -(-A)P$, и $-A \in G$. Значит, G – группа.

Отображение φ является гомоморфизмом: $\varphi(a+b) = P'(A+B)P' = P'AP' + P'BP' = \varphi(A) + \varphi(B)$ для любых $A, B \in G$.

Чтобы найти ядро φ, прежде всего, выясним вид произвольной матрицы $A \in G$. Обозначим $A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$.

Условие $PA = -AP$ даёт $\begin{pmatrix} 0 & \alpha \\ 0 & \gamma \end{pmatrix} = -\begin{pmatrix} \gamma & \delta \\ 0 & 0 \end{pmatrix}$, откуда $\gamma = 0$ и $\alpha = -\delta$.

Итак, $A = \left\{ \begin{pmatrix} \alpha & \beta \\ 0 & -\alpha \end{pmatrix} | \, \alpha, \beta \in R \right\}$. Поэтому

$$\varphi(A) = P^t A P^t = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ 0 & -\alpha \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ \beta & 0 \end{pmatrix}.$$

Отсюда $\varphi(A) = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ тогда и только тогда, когда $\beta = 0$. Таким образом, $Ker\varphi = \left\{ \begin{pmatrix} \lambda & 0 \\ 0 & -\lambda \end{pmatrix} | \, \lambda \in \mathrm{R} \right\}$. Построим смежные классы по $Ker\varphi$: $A + Ker\varphi = \begin{pmatrix} \alpha & \beta \\ 0 & -\alpha \end{pmatrix} + \left\{ \begin{pmatrix} \lambda & 0 \\ 0 & -\lambda \end{pmatrix} | \, \lambda \in R \right\} = \left\{ \begin{pmatrix} \eta & \beta \\ 0 & \eta \end{pmatrix} | \eta \in R \right\}$,

так как α – фиксированное число, а λ пробегает R, то $\alpha + \lambda$ пробегает все R. Обозначим $\left\{ \begin{pmatrix} \eta & \beta \\ 0 & \eta \end{pmatrix} | \, \eta \in R \right\} = K_\beta$, тогда $\begin{pmatrix} 0 & \beta \\ 0 & 0 \end{pmatrix} + Ker\varphi = K_\beta$ и смежные классы K_β однозначно определяются заданием числа β.

Факторгруппа $G / Ker\varphi$ является бесконечной и состоит из всех классов K_β, $\beta \in R$, причём $K_\alpha + K_\beta = K_{\alpha+\beta}$, и $G / Ker\varphi \cong (R,+)$

Пример 13. Доказать, что факторгруппа мультипликативной группы ненулевых действительных чисел $(R^*,\cdot)$, где $R^* = R \setminus \{0\}$, по её подгруппе положительных действительных чисел R^+ является циклической группой второго порядка.

Рассмотрим отображение $\varphi : R^* \to C_2$,

где $\varphi(x) = signx = \begin{cases} -1, \text{если } x < 0; \\ 1, \text{если } x > 0. \end{cases}$

Покажем, что гомоморфным образом группы R^* является мультипликативная группа $(C_2,\cdot)$, где $C_2 = \{-1,1\}$, – циклическая группа порядка 2 с порождающим элементом –1.

Действительно, пусть x и y – действительные числа, имеющие один и тот же знак, тогда $xy > 0$ и $\varphi(xy) = 1 = \varphi(x)\varphi(y)$, ибо в этом случае значения $\varphi(x)$ и $\varphi(y)$ одновременно равны либо +1, либо –1. Если же x и y имеют различные знаки, то $xy < 0$ и $\varphi(xy) = -1$, но в этом случае значения $\varphi(x)$ и $\varphi(y)$ также различаются знаком и $\varphi(x)\varphi(y) = -1$. Итак, $\varphi(xy) = \varphi(x)\varphi(y)$ всегда. Ядром гомоморфизма φ является R^+ ибо $\varphi(x) = 1$ тогда и только тогда, когда $x > 0$. По теореме о гомоморфизмах получаем $(R^*,\cdot)/(R^+,\cdot) \cong C_2$.

Практический блок

Индивидуальные задания для домашней работы

Задача 11. Построить факторгруппу A/H_1 группы A из задачи 7 по подгруппе H_1 из задачи 8. Почему нельзя построить факторгруппу группы A по подгруппе H_4?

Задача 12. Построить факторгруппу K/M группы K из задачи 10 по её подгруппе M и установить изоморфизм $K/M \approx R^*$.

Задача 13. Проверить, что отображения $\alpha(x)=x^2$, $\beta(x)=x^3$, $\gamma(x)=x^5$ являются гомоморфизмами группы Z_n^* из задачи 6 в себя. Найти ядро каждого из этих гомоморфизмов. Какие из них являются изоморфизмами? Построить факторгруппу $Z_n^*/Ker\alpha$ и составить её таблицу Кэли.

Задача 14. Выяснить, какое из следующих отображений $\alpha(A) = T + A - TA$, $\beta(A) = A^2$, $\gamma(A) = A^t$ является: а) гомоморфизмом группы H из задачи 10; б) гомоморфизмом группы K из того же задания в некоторую другую группу. Найти ядро каждого из гомоморфизмов и выяснить, какие из них являются изоморфизмами.

Задача 15. Доказать, что каждое из отображений α *и* β является гомоморфизмом аддитивной группы G из задания 9(а) на некоторую другую группу (определить, на какую именно): $\alpha(A)=AT, \beta(A)=trA$, где trA - след матрицы A (т.е. сумма всех её элементов на главной диагонали). Найти $Ker\beta$, построить факторгруппу $G/Ker\beta$ и установить её изоморфизм с аддитивной группой R всех действительных чисел.

Задача 16. Построить факторгруппу (и составить её таблицу Кэли):

1. аддитивной группы A всех многочленов вида $ax+b$ над Z по подгруппе H всех многочленов из A с чётными коэффициентами;
2. мультипликативной группы A с образующими $\begin{pmatrix}\sqrt{2} & 0\\ 0 & \sqrt{2}\end{pmatrix}$ по подгруппе H всех рациональных матриц из A;
3. аддитивной группы A с образующими $\sqrt{2}$ и $\sqrt{3}$ по подгруппе H всех рациональных чисел из A;
4. аддитивной группы A всех многочленов вида $ax+b$ над Z по подгруппе H с образующими $2x$ и 3;
5. мультипликативной группы A с образующим $P=\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$ по подгруппе H всех матриц с чётным следом;
6. аддитивной группы A с образующими $\frac{1}{2}x$ и $\frac{1}{2}$ по подгруппе всех многочленов из A с целыми коэффициентами;
7. мультипликативной группы A с образующим $\sqrt{2}$ по подгруппе всех рациональных чисел из A;
8. мультипликативной группы A с образующим $P=\begin{pmatrix}1 & 1\\ -1 & 1\end{pmatrix}$ по подгруппе H всех скалярных матриц из A;
9. аддитивной группы A с образующими $\frac{1}{2}$ и $\frac{1}{3}$ по подгруппе H всех целых чисел из A;
10. аддитивной группы A с образующим $\frac{1}{2}x+\frac{1}{4}$ по подгруппе всех многочленов из A с целыми коэффициентами;
11. мультипликативной группы A с образующим $P=\begin{pmatrix}0 & 1\\ \sqrt{2} & 0\end{pmatrix}$ по подгруппе H всех рациональных матриц из A;

12. мультипликативной группы A с образующим $1+i$ по подгруппе всех действительных чисел из A.

Блок самоконтроля

Контрольные вопросы для самопроверки

20. Верно ли, что композиция двух гомоморфизмов групп также является гомоморфизмом групп?
21. Почему нельзя определить факторгруппу по любой подгруппе (не обязательно по нормальной).
22. Пусть G – группа, а E – её единичная подгруппа. Что представляют собой факторгруппы G/G и G/E?
23. Изоморфны ли факторгруппы $Z/2Z$ и $2Z/4Z$?
24. Какой смежный класс является нейтральным элементом факторгруппы G/H группы G?
25. Какой смежный класс является обратным для класса gH в факторгруппе G/H группы G?
26. Может ли факторгруппа быть изоморфной данной группе?
27. Может ли факторгруппа быть изоморфной единичной группе?
28. Всегда ли гомоморфный образ группы является группой?
29. Может ли пятиэлементная группа быть гомоморфным образом бесконечной группы?

Дополнительные задачи и упражнения

50. Построить факторгруппу группы (x, y) из задачи 17(с) по подгруппе (x^2). Составить таблицу Кэли для факторгруппы.

51. В задачах 17 и 18 построить факторгруппу A/H и установить ее изоморфизм с подгруппой K.

52. Выясните, какие из следующих отображений являются гомоморфизмами. Найдите ядро каждого из гомоморфизмов:

а) $\varphi: R^* \to R^*$, где $\varphi(a) = a^{-1}$; б) $\varphi: C^* \to C^*$, где $\varphi(z) = z^2$;

в) $\varphi: C^* \to R_+$, где $\varphi(z) = |z|$; г) $\varphi: GL(2,R) \to GL(2,R)$, где $\varphi(A) = A^{-1}$;

д) $\varphi: GL(2,R) \to R^*$, где $\varphi(A) = |A|$.

53. Построить факторгруппу:

a) мультипликативной группы A с образующим $2i$ по подгруппе всех положительных действительных чисел из A;

b) мультипликативной группы A о образующими $\sqrt{2}$ и $\sqrt[3]{2}$ по подгруппе всех рациональных чисел из A;

c) мультипликативной группы A с образующими -1 и 2 по подгруппе, составленной из квадратов всех элементов из A;

d) аддитивной группы A всех многочленов вида $ax^2 + bx + c$ над по подгруппе всех многочленов из A с чётными коэффициентами;

e) аддитивной группы A всех многочленов вида $ax + b$ над Z по подгруппе с образующими $2x+1$ и $x-2$;

f) аддитивной группы A всех многочленов вида $ax + b$ над Z по подгруппе с образующими $x-3$ и $3x-1$;

g) аддитивной группы A с образующими $\frac{1}{2}x$ и $\frac{1}{4}$ по подгруппе всех многочленов из A с целыми коэффициентами;

h) мультипликативной группы A с образующим $\begin{pmatrix} 0 & 1 \\ \sqrt[3]{2} & 0 \end{pmatrix}$ по подгруппе всех рациональных матриц из A;

i) мультипликативной группы A с образующими $\begin{pmatrix} 1 & 0 \\ 0 & \sqrt{2} \end{pmatrix}$ и $\begin{pmatrix} \sqrt{3} & 0 \\ 0 & 1 \end{pmatrix}$ по подгруппе всех рациональных матриц из A;

j) мультипликативной группы A всех матриц вида $\begin{pmatrix} 1 & p \\ 0 & 1 \end{pmatrix}$ над Z по подгруппе, составленной из кубов всех элементов из A;

54. Построить факторгруппу $(R,+)/(Z,+)$ и показать на числовой оси расположение её элементов.

55. Построить факторгруппу аддитивной группы C всех комплексных чисел по подгруппе $Z[i]$ всех целых гауссовых чисел (то есть чисел вида $a+bi$, где $a,b \in Z$). Показать на комплексной плоскости расположение элементов факторгруппы.

56. Проверить, что отображение $\varphi(x) = e^{2\pi i x}$ является гомоморфизмом аддитивной группы R всех действительных чисел на мультипликативную группу и всех комплексных чисел с

модулем 1. Найти $Ker\varphi$ и построить факторгруппу $R/Ker\varphi$.

57. Доказать, что отображение $\varphi: f(x) \to f(x) + f(-x)$ является эндоморфизмом (гомоморфизмом в себя) аддитивной группы $R[x]$ всех многочленов от x над R. Найти $Ker\varphi$, построить факторгруппу $R[x]/Ker\varphi$ и установить её изоморфизм с подгруппой всех чётных многочленов из $R[x]$.

58. Доказать, что отображение $\varphi: f(x,y) \to f(x,y) + f(y,x)$ является эндоморфизмом (гомоморфизмом в себя) аддитивной группы $R[x,y]$ всех многочленов от x и y над R. Найти $Ker\varphi$, построить факторгруппу $R[x,y]/Ker\varphi$ и установить её изоморфизм с подгруппой всех симметрических многочленов из $R[x,y]$.

59. Доказать, что отображение $\varphi: A \to A + A^{'}$ является эндоморфизмом (гомоморфизмом в себя) аддитивной группы $M_2(R)$ всех $(2,2)$ матриц над R. Найти $Ker\varphi$, построить факторгруппу $M_2(R)/Ker\varphi$ и установить её изоморфизм с подгруппой всех симметрических матриц из $M_2(R)$.

Задачи повышенной сложности

60. Найдите все гомоморфизмы аддитивной группы Z_{12} в аддитивные группы Z_8 и Z_{24}. Указание: сначала выясните, какими могут быть ядра гомоморфизмов и образы единицы.

61. Найдите все автоморфизмы аддитивной группы Z целых чисел. Указание: выясните, какие элементы могут являться гомоморфными образами единицы.

62. Доказать, что гомоморфизм групп переводит нейтральный элемент в нейтральный и обратные элементы - в обратные.

63. Пусть φ – гомоморфизм группы G на группу G'. Докажите, что: а) если G' – не коммутативна, то и G – не коммутативна; б) если G' – бесконечна, то и G – бесконечна.

64. Пусть $\varphi: G \to G$ и $\psi: G \to G$, где φ и ψ – гомоморфизмы группы G такие, что $\varphi\psi$ и $\psi\varphi$ – тождественные отображения. Докажите, что φ является изоморфизмом.

65. Доказать, что ядро гомоморфизма $\varphi: A \to B$ группы A в группу B является нормальной подгруппой группы A.

66. Доказать, что гомоморфизм одной группы на другую тогда и только тогда является изоморфизмом, когда его ядро состоит из единственного элемента (определить также, что служит этим единственным элементом)

67. Проверить, что отображение $\varphi(x) = x^2$ является гомоморфизмом абелевой группы в себя. Верно ли аналогичное утверждение для произвольных групп?

68. Пусть A - циклическая группа. Проверить, что $\varphi(x) = x^2$ является эндоморфизмом (гомоморфизмом в себя) группы A. В каких случаях это отображение является изоморфизмом?

69. Доказать, что H - нормальная подгруппа группы A, если произведение любых двух левых смежных классов снова является левым смежным классом группы A по подгруппе H. *Указание:* рассмотреть отображение $x \to xH$ $(x \in A)$ и доказать, что оно является гомоморфизмом с ядром H.

ТЕМА 4.
ПРЯМЫЕ ПРОИЗВЕДЕНИЯ И ПРЯМЫЕ СУММЫ ГРУПП

Методический блок

В результате изучения темы студент должен знать определения и уметь приводить примеры следующих понятий: прямое произведение (прямая сумма) групп; внешняя и внутренняя прямые суммы (произведения) групп; примарные циклические группы; p-группы.

В результате изучения темы студент должен знать формулировки и уметь доказывать следующие факты: критерии разложимости группы в прямое произведение (сумму) своих подгрупп; теоремы о разложении циклических (конечных и бесконечных) групп в прямую сумму подгрупп; теорема о

примарных циклических группах; основная теорема теории конечных абелевых групп.

В результате изучения темы студент должен уметь: раскладывать группы в прямое произведение (сумму) подгрупп; описывать с точностью до изоморфизма конечные абелевы группы.

Информационный блок

Определение 10. Группа A называется *прямым произведением своих подгрупп* B и C (обозначается $A=B\times C$), если выполняются все следующие условия:

1. $A=B\cdot C$, то есть каждый элемент $z\in A$ можно представить в виде произведения $z=xy$, где $x\in B$, $y\in C$;
2. множители x и y из условия 1 однозначно определяются каждым элементом $z\in A$;
3. $xy=yx$ для всех $x\in B$, $y\in C$.

При разложении группы в прямое произведение подгрупп можно пользоваться ***критерием.*** Группа A тогда и только тогда является прямым произведением своих подгрупп B и C, когда выполняются все следующие условия:

1) данные подгруппы нормальны в A;
2) $B\bigcap C=\{e\}$;
3) $BC=A$.

Для групповой операции в абелевых группах обычно используют аддитивную запись. В этом случае вместо прямых произведений говорят о *прямых суммах* и обозначают $A=B\oplus C$. Понятно, что в абелевой группе любая подгруппа будет нормальной, а критерий прямой суммы будет содержать только два последних условия.

Для любого конечного числа слагаемых ***критерий прямой суммы*** формулируется так: группа G является прямым произведением своих подгрупп A_i $(i=\overline{1,k})$ тогда и только тогда, когда $G=A_1+A_2+\cdots+A_k$ и $(A_1+A_2+\cdots A_{i-1})\bigcap A_i=0$.

Определение 11. Пусть даны две группы *(B, $*$)* и *(C, $\circ$)*. *Внешним прямым произведением* этих групп называется

множество $B\times C$ всех упорядоченных пар вида (x, y), где $x\in B$, $y\in C$ относительно операции

$(x_1, y_1)(x_2, y_2)=(x_1*x_2, y_1 \circ y_2)$.

Внешнее прямое произведение $B\times C$ совпадает с обычным прямым произведением (в смысле определения 1) подгрупп $B\times\{f\}$ и $\{e\}\times C$, где e и f –нейтральные элементы групп B и C соответственно.

Пример 14. Мультипликативная группа C^* всех отличных от 0 комплексных чисел является прямым произведением подгруппы R^+ всех положительных действительных чисел и подгруппы U всех комплексных чисел с модулем 1.

Действительно, обе эти подгруппы нормальны в C^+, поскольку речь идёт о коммутативной группе. Кроме того, $U\bigcap R^+=\{1\}$ и $(R^+)\cdot U=C^*$ (вспомним тригонометрическую форму комплексных чисел). Мы воспользовались критерием прямого произведения, но можно было бы исходить из определения 10.

Пример 15. Доказать, что аддитивная группа $G=\left\{\begin{pmatrix}\alpha & \beta\\ 0 & -\alpha\end{pmatrix}\mid \alpha,\beta\in R\right\}$ является прямой суммой подгрупп, порожденных матрицами вида $\begin{pmatrix}\alpha & 0\\ 0 & -\alpha\end{pmatrix}$ и $\begin{pmatrix}0 & \beta\\ 0 & 0\end{pmatrix}$ соответственно.

Пусть $H=\left\{\begin{pmatrix}\alpha & 0\\ 0 & -\alpha\end{pmatrix}\mid \alpha\in R\right\}$, $K=\left\{\begin{pmatrix}0 & \beta\\ 0 & 0\end{pmatrix}\mid \beta\in R\right\}$.

Для доказательства достаточно показать, что выполнены условия:
а) каждая матрица из группы G представима в виде суммы матриц из подгрупп H и K; б) $H\bigcap K=\left\{\begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix}\right\}$.

а) Пусть $A\in G$, тогда $A=\begin{pmatrix}\alpha & \beta\\ 0 & -\alpha\end{pmatrix}=\begin{pmatrix}\alpha & 0\\ 0 & -\alpha\end{pmatrix}+\begin{pmatrix}0 & \beta\\ 0 & 0\end{pmatrix}$, где $\begin{pmatrix}\alpha & 0\\ 0 & -\alpha\end{pmatrix}\in H$, и $\begin{pmatrix}0 & \beta\\ 0 & 0\end{pmatrix}\in K$.

б) матрица $\begin{pmatrix} \alpha & \beta \\ 0 & -\alpha \end{pmatrix} \in H \bigcap K$ тогда и только тогда, когда $\begin{pmatrix} \alpha & \beta \\ 0 & -\alpha \end{pmatrix} \in H$ и $\begin{pmatrix} \alpha & \beta \\ 0 & -\alpha \end{pmatrix} \in K$, откуда имеем β=0 и α=0. Таким образом, $H \bigcap K$ содержит только нулевую матрицу.

Циклическая группа называется *примарной*, если её порядок является степенью простого числа. Примарную циклическую группу нельзя разложить в прямую сумму подгрупп, отличных от нулевой и самой группы. Если p – простое число, то p-группой называется группа, порядки всех элементов которой – степени числа p.

Пример 16. Найти все разложения мультипликативной группы Z_{36}^* в прямое произведение неразложимых циклических подгрупп.

Элементами группы Z_{36}^* являются все классы чисел по модулю 36, взаимно простых с числом 36.

Поэтому Z_{36}^*= $\left\{\overline{1},\overline{5},\overline{7},\overline{11},\overline{13},\overline{17},\overline{19},\overline{23},\overline{25},\overline{29},\overline{31},\overline{35}\right\}$. Порядок этой группы равен $\varphi(36)$=12. Найдем порядок каждого элемента группы Z_{36}^*. Для этого будем возводить элементы в целые положительные степени до получения элемента $\overline{1}$. Элементы $\overline{5},\overline{7},\overline{11},\overline{23},\overline{29},\overline{31}$ имеют порядок 6, элементы $\overline{13}$ и $\overline{25}$ – порядок 3, элементы $\overline{17},\overline{19},\overline{25}$ – порядок 2. Построим все примарные циклические подгруппы: $\langle\overline{13}\rangle = \left\{\overline{13},\overline{13}^2=\overline{25},\overline{13}^3=\overline{1}\right\} = \langle\overline{25}\rangle$ (порядка 3), $\langle\overline{17}\rangle = \left\{\overline{17},\overline{17}^2=\overline{1}\right\}$ (порядка 2), $\langle\overline{19}\rangle = \left\{\overline{19},\overline{19}^2=\overline{1}\right\}$ (порядка 2) и $\langle\overline{35}\rangle = \left\{\overline{35},\overline{35}^2=\overline{1}\right\}$ (порядка 2). Как видно, пересечением любых двух из них является единичная подгруппа $\left\{\overline{1}\right\}$. Окончательно с точностью до порядка сомножителей получаем:

$$Z_{36}^* = \langle\overline{17}\rangle \times \langle\overline{35}\rangle \times \langle\overline{13}\rangle = \langle\overline{19}\rangle \times \langle\overline{35}\rangle \times \langle\overline{13}\rangle = \langle\overline{17}\rangle \times \langle\overline{19}\rangle \times \langle\overline{13}\rangle .$$

Учитывая порядки этих циклических подгрупп, можно записать $Z_{36}^* \cong C_2 \times C_2 \times C_3$ (или $Z_{36}^* \cong Z_2 \oplus Z_2 \oplus Z_3$).

Теорема (основная для конечных абелевых групп). Любая конечная абелева группа является прямой суммой примарных циклических подгрупп.

Следует также знать, что *примарные циклические группы нельзя разложить в прямую сумму (нетривиально)*, а основная теорема усиливается теоремой об однозначности (с точностью до изоморфизма) разложения.

Основная теорема исчерпывает вопрос *о полном описании конечных абелевых групп порядка n:* берем всевозможные разложения числа $n=n_1 \cdot n_2 \cdot \ldots \cdot n_s$, где числа n_i, $i=1,\ldots,s$, обязательно отличны от единицы, но не обязательно различны, причем каждое из них должно быть степенью некоторого простого числа. Каждому набору чисел (n_1, n_2, ..., n_s) ставим в соответствие прямое произведение (прямую сумму) циклических групп, порядками которых служат числа из этого набора. Все полученные таким образом конечные абелевы группы, соответствующие разным наборам, будут попарно неизоморфными, а любая другая конечная абелева группа данного порядка n – изоморфна одной из этих групп.

Пример 17. Перечислить все неизоморфные абелевы группы от 10-го до 20-го порядков включительно.

Поскольку числа 11, 13, 17, 19 - простые, то существуют только неразложимые циклические группы таких порядков. Обозначим их C_{11}, C_{13}, C_{17}, и C_{19}. Числа 10, 14 и 15 разлагаются в произведение двух различных простых чисел. Из $10=2\cdot5$ следует, что группа порядка 10 имеет разложение $C_2 \times C_5$. Но если элемент a является образующим подгруппы C_2, а b – образующим подгруппы C_5, то элемент ab порождает циклическую группу порядка $2\cdot5=10$, т.е. абелева группа порядка 10 является разложимой и циклической $C_{10} \cong C_2 \times C_5$. Аналогично доказывается, что абелевы группы порядка 14 и 15 являются разложимыми и циклическими
$C_{14} \cong C_2 \times C_7$ и $C_{15} \cong C_3 \times C_5$. Двум представлениям числа 12: $12=3\cdot4$ и $12=2\cdot2\cdot3$ соответствуют две неизоморфные абелевы группы типов (4, 3) и (2, 3, 3) т.е., имеющие разложения $C_4 \times C_5$ и $C_2 \times C_3 \times C_3 \cong C_6 \times C_3$ соответственно, из которых группа $C_{12} \cong C_4 \times C_3$ является циклической (в силу взаимной простоты порядков). Для порядка 16 есть неразложимая циклическая группа 16-го порядка C_{16} и четыре неизоморфных абелевых группы, имеющих разложения $C_2 \times C_8$, $C_4 \times C_4$, $C_2 \times C_2 \times C_4$ и $C_2 \times C_2 \times C_2 \times C_2$. Существуют две

неизоморфные абелевы группы порядка 18, имеющие разложения $C_2 \times C_9$ и $C_2 \times C_3 \times C_3 \cong C_6 \times C_3$, из которых разложимая группа $C_{18} \cong C_2 \times C_9$ является циклической. Если порядок группы равен 20, то имеем две неизоморфные разложимые абелевы группы: $C_{20} \cong C_4 \times C_5$ (циклическая) и $C_2 \times C_2 \times C_5$.

Практический блок

Индивидуальные задания для домашней работы

Задача 17. Выяснить, является ли группа A из задач 7 и 8 прямым произведением подгрупп:

а) H_1 и H_3; б) H_2 и H_3; в) H_2 и H_4; г) H_3 и H_4.

Задача 18. Мультипликативную группу K из задачи 10 разложить в прямое произведение двух ее подгрупп.

Указание: одним из прямых множителей можно взять множество невырожденных скалярных матриц, то есть матриц вида xE, но можно взять и другую подгруппу, например подгруппу M.

Задача 19. Мультипликативную группу Z^*_n разложить в прямое произведение неразложимых циклических подгрупп.

Вариант	1	2	3	4	5	6	7	8	9	10	11	12
n	40	45	48	70	56	36	42	39	72	60	35	63

Задача 20. Описать, с точностью до изоморфизма, все абелевы группы таких порядков:

1) 8, 432;	2) 343, 330;	3) 27, 85;	4) 64, 70;
5) 32, 77;	6) 243, 95;	7) 625, 42;	8) 16, 65;
9) 128, 105;	10) 1000, 55;	11) 288, 210;	12) 400, 35.

Блок самоконтроля

Контрольные вопросы для самопроверки

30. Справедливо ли утверждение, что если A и B – конечные подгруппы G и $G=A\times B$, то $|G|=|A|\cdot|B|$?
31. Является ли абелевой группой прямая сумма абелевых групп?
32. Может ли прямое произведение неабелевых групп быть абелевой группой?
33. Верно ли, что $Z_2+Z_2\cong Z_2\oplus Z_2$?
34. Обязательно ли абелева группа порядка 15 имеет элемент порядка 3?
35. Верно ли, что циклическая группа четвертого порядка не раскладывается в прямую сумму собственных подгрупп?
36. Верно ли, что все абелевы группы пятнадцатого порядка изоморфны между собой?
37. Сколько различных подгрупп порядка p имеется в абелевой группе (p,p)?
38. Можно ли разложить в прямую сумму собственных подгрупп;
    a) циклическую группу порядка 16?
    b) циклическую группу порядка 12?
    c) аддитивную группу всех целых чисел?
    d) аддитивную группу всех рациональных чисел?
    e) аддитивную группу всех комплексных чисел?
39. Изоморфны ли группы:
    a) $C_6\times C_{36}$ *и* $C_9\times C_{24}$;
    b) $C_6\times C_{36}$ *и* $C_{12}\times C_{18}$;
    c) $Z_{12}\oplus Z_{22}$ и $Z_{18}\oplus Z_{48}$;
    d) $Z_{42}\oplus Z_{18}$ и $Z_6\oplus Z_{36}$;
    e) $Z/2Z\oplus Z/2Z$ и $Z/4Z$?

Дополнительные задачи и упражнения

70. Доказать следующие утверждения:

a) аддитивная группа $R[x]$ всех многочленов от x над R является прямой суммой подгруппы всех чётных и подгруппы всех нечётных многочленов;

b) аддитивная группа $R[x,y]$ всех многочленов от x и y над R является прямой суммой подгруппы всех симметрических и подгруппы всех антисимметрических многочленов;

c) аддитивная группа $M_2(R)$ всех (2×2)-матриц над R является прямой суммой подгруппы всех симметрических и подгруппы всех антисимметрических матриц;

d) мультипликативная группа R^* всех отличных от нуля действительных чисел является прямым произведением подгруппы $\{1,-1\}$ и подгруппы всех положительных действительных чисел;

e) мультипликативная группа C^* всех отличных от нуля комплексных чисел является прямым произведением подгруппы R всех действительных чисел и подгруппы U всех комплексных чисел с модулем 1.

71. Проверить, является ли прямым произведением подгрупп H и K группа A из задачи 19; группа A из задачи 20?

72. Разложить:

a) аддитивную группу Z_{12} в прямую сумму неразложимых подгрупп;

b) мультипликативную группу Z_{12}^* в прямое произведение неразложимых подгрупп.

Однозначны ли эти разложения?

Задачи повышенной сложности

73. Докажите, что аддитивная группа всех рациональных чисел не разложима в прямую сумму своих собственных подгрупп.

74. Доказать, что если $H=A\times B$, то A и B – нормальные подгруппы группы H.

75. Доказать, что если A и B – две нормальные подгруппы группы H, причём $A\cap B=\{e\}$, то каждый элемент из A коммутирует с каждым элементом из B.

76. Доказать, что если A и B – нормальные подгруппы

группы H, такие, что $AB = H,\ A \cap B = \{e\},\ то\ H = A \times B$.

77. Доказать, что если $H = A \times B,\ то\ H / A \cong B$.

78. Доказать, что центр прямого произведения двух подгрупп данной группы равен прямому произведению их центров.

79. Доказать, что если p и q – различные простые числа, то абелева группа порядка pq – циклическая.

80. Найти все подгруппы абелевой группы типа $(3,3)$.

ТЕМА 5. КОЛЬЦА И ПОЛЯ

Методический блок

В результате изучения темы студент должен знать определения и уметь приводить примеры следующих понятий: кольцо, подкольцо, поле, подполе; единица (односторонняя, двусторонняя), идемпотенты; коммутативное кольцо, кольцо с единицей, кольцо целостности; делители нуля; изоморфизм и гомоморфизм колец.

В результате изучения темы студент должен знать формулировки и уметь доказывать следующие факты: простейшие свойства колец; критерий подкольца; простейшие свойства изоморфизмов колец.

В результате изучения темы студент должен уметь: распознавать кольцо, находить в нем (при наличии) единицу, делители нуля, обратимые элементы; распознавать поле; устанавливать изоморфизм колец.

Информационный блок

***Определение* 12.** Множество K называется *кольцом*, если на нем определены две бинарные операции $"+"$ (сложения) и $"\cdot"$ (умножения), которые удовлетворяют условиям:

1) $(K,+)$ – абелева группа (*аддитивная группа кольца*);

2) $(K, \cdot)$ – полугруппа (*мультипликативная полугруппа кольца*);

3) обе операции связаны дистрибутивными законами:

$(x+y)\cdot z=(x\cdot z)+(y\cdot z)$, $z\cdot(x+y)=(z\cdot x)+(z\cdot y)$ для всех $x,y,z \in K$.

Мультипликативная полугруппа кольца не обязательно коммутативна. Если же $x\cdot y=y\cdot x$ для всех $x, y \in K$, то *кольцо K называется коммутативным*.

Произведение двух ненулевых элементов кольца может равняться нулю: $x\cdot y=0$, $x\neq 0$, $y\neq 0$, при этом x и y называются, соответственно, левым и правым *делителями нуля*.

Если кольцо K содержит нейтральный элемент по умножению, то оно называется кольцом с единицей.

Коммутативное кольцо с единицей без делителей нуля называется *целостным кольцом или областью целостности*. Если кольцо содержит единицу и $xy=1$, или $zx=1$, то элементы y и z называются, соответственно, правым и левым обратным для x. Если элемент x обладает правым y и левым z обратными элементами, то $y=z$. В этом случае элемент x называется обратимым, и обратный к нему обозначается x^{-1}: $xx^{-1}=x^{-1}x=1$.

Все обратимые элементы кольца с единицей образуют группу относительно умножения. Её называют *мультипликативной группой кольца K* и обозначают K^*.

Определение 13. Ненулевое коммутативное кольцо P с единицей называется *полем*, если все его ненулевые элементы обратимы. В этом случае $P^*=P\backslash\{0\}$.

Определение 14. Отображение $\varphi: K\to K'$ кольца K на кольцо K' называется изоморфизмом, если отображение взаимно однозначно и сохраняет операции, то есть $\varphi(x+y)=\varphi(x)+\varphi(y)$ и $\varphi(xy)=\varphi(x)\varphi(y)$.

Два кольца называются *изоморфными*, если существует изоморфизм одного из них на другое.

Чтобы установить изоморфизм двух колец, достаточно найти какое-нибудь взаимно однозначное отображение одного из них на другое с сохранением операций.

Для доказательства того, что два кольца не изоморфны, следует указать какое-нибудь абстрактное свойство (то есть свойство, сохраняющееся при изоморфизмах), которым одно кольцо обладает, а другое нет. К числу таких абстрактных свойств относятся коммутативность, существование единицы, существование делителей нуля и т. д.

Определение 15. *Подкольцом* называется непустое подмножество A кольца K, которое само является кольцом относительно операций, определённых в K. Подкольцо, являющееся к тому же полем, называется *подполем*.

Для выяснения того, является ли данное подмножество подкольцом, можно пользоваться ***критерием подкольца***: непустое подмножество кольца тогда и только тогда является его подкольцом, когда оно замкнуто относительно вычитания и замкнуто относительно умножения.

Чтобы построить подкольцо, порождённое данными элементами, нужно составить всевозможные конечные произведения этих элементов и образовать множество всех их конечных сумм и разностей.

Пример 18. Пусть дана матрица $T=\begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}$. Выяснить, является ли кольцом относительно операций $A \oplus B = A+B-T$ и $A \circ B = AB$ множество всех (2×2)-матриц над R следующего вида:

а) $\begin{pmatrix} x & x \\ 1-x & 1-x \end{pmatrix}$; б) $\begin{pmatrix} 1-x & 0 \\ x & 1 \end{pmatrix}$; в) $\begin{pmatrix} 0 & 0 \\ x & x \end{pmatrix}$.

Обе операции определены на каждом из трёх данных множеств (проверить самостоятельно). Операция $\oplus$ ассоциативна:

$(A \oplus B) \oplus C = (A+B-T) \oplus C = A+B+C-2T;$

$(A \oplus (B \oplus C) = A \oplus (B+C-T) = A+B+C-2T.$

Очевидно, относительно операции $\oplus$ матрица T является нейтральным элементом, а матрица $2T-A$ - "противоположным"

элементом для A (так как $A\oplus(2T-A)=T$). Кроме того, операция $\oplus$ коммутативна, и каждое из трёх приведенных множеств содержит вместе с любым элементом A и его "противоположный" $2T-A$. Таким образом, доказано, что каждое из трёх множеств является абелевой группой относительно первой операции и полугруппой – относительно второй. Остаётся проверить дистрибутивность.

В случае (а) получаем, что $A\circ B=A$ для любых A и B .Отсюда и из того, что $A\oplus B=A+B-T,$ имеем:

$(A\oplus B)\circ C=A\oplus B=A+B-T,\quad (A\circ C)\oplus(B\circ C)=A\oplus B=A+B-T;$

$C\circ (A\oplus B)= C,\quad (C\circ A)\oplus(C\circ B)=C\oplus C=C+C-T=2C-T.$

Следовательно, правая дистрибутивность выполняется, а левая - нет.

В случае (б) вместо действий над матрицами

$$A\oplus B=\begin{pmatrix}1-x & 0\\ x & 1\end{pmatrix}+\begin{pmatrix}1-y & 0\\ y & 1\end{pmatrix}-\begin{pmatrix}0 & 0\\ 1 & 1\end{pmatrix}=\begin{pmatrix}2-x-y & 0\\ x+y-1 & 1\end{pmatrix};$$

$$A\circ B=\begin{pmatrix}1-x & 0\\ x & 1\end{pmatrix}\begin{pmatrix}1-y & 0\\ y & 1\end{pmatrix}=\begin{pmatrix}1-x-y+xy & 0\\ x+y-xy & 1\end{pmatrix}$$

удобнее рассматривать соответствующие операции над числами (элементами матриц):

$x\oplus y=x+y-1;\qquad x\circ y=x+y-xy.$

Обе операции коммутативны, поэтому достаточно проверить лишь одну дистрибутивность, например правую:

$(x\oplus y)\circ z=x+y+2z-xz-yz-1=(x\circ z)\oplus(y\circ z).$

В случае (в) также вместо операций над матрицами удобнее рассматривать соответствующие операции над числами (элементами матриц): $x\oplus y=x+y-1;\quad x\circ y=xy.$ Здесь также обе операции коммутативны, но дистрибутивность нарушается:

$(x\oplus y)\circ z=xz+yz-z;\quad (x\circ z)\oplus(y\circ z)=zx+yz-1.$

Таким образом, только в случае (б) имеем кольцо. Можно проверить, что это кольцо К изоморфно кольцу R всех действительных чисел. При этом опять удобнее иметь дело не с матрицами, а с числами и операциями $x\oplus y=x+y-1$, $x\circ y=x+y-xy$.

Изоморфизмом служит отображение $\varphi:(K,\oplus,\circ)\to(\mathrm{R},+,\circ)$, заданное формулой:

$\varphi(x)=1-x$. Действительно, это отображение - взаимно однозначно и сохраняет операции:

$\varphi(x \oplus y)=\varphi(x+y-1)=1-(x+y-1)=2-x-y=(1-x)+(1-y)=\varphi(x)+\varphi(y);$
$\varphi(x \circ y)=\varphi(x+y-xy)=1-(x+y-xy)=1-x-y-xy=(1-x)(1-y)=\varphi(x)\varphi(y).$

Пример 19. Существует ли поле, содержащее матрицу $A=\begin{pmatrix} 1 & -2 \\ -1 & 2 \end{pmatrix}$?

Поскольку $A^2=3A$ (проверьте!), матрица $P=\frac{1}{3}A$ – идемпотентна. Следовательно, множество всех матриц вида xA, где $x \in Q$, является полем, а P – его единицей.

Пример 20. Построить кольцо, порожденное матрицей $A=\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$.

Вместе с матрицей A искомому кольцу должны принадлежать матрицы $A^2=\begin{pmatrix} 2 & 2 \\ 2 & 2 \end{pmatrix}, A^3=\begin{pmatrix} 4 & 4 \\ 4 & 4 \end{pmatrix},\ldots, A^n=\begin{pmatrix} 2^{n-1} & 2^{n-1} \\ 2^{n-1} & 2^{n-1} \end{pmatrix}$, а также, их всевозможные суммы и разности, т.е. матрицы вида $\begin{pmatrix} a & a \\ a & a \end{pmatrix}$, где $a \in Z$. Множество $\left\{X : X=\begin{pmatrix} a & a \\ a & a \end{pmatrix}, a \in Z\right\}$ замкнуто относительно сложения, вычитания и умножения, и потому является подкольцом кольца $M_2(Z,+,\cdot)$.

Практический блок

Индивидуальные задания для домашней работы

Задача 21. Выяснить, является ли кольцом

а) данное числовое множество К относительно операций $\oplus$ и $*$ в случаях (1), (2), (3) (таблица 6)

б) каждое из множеств $К_1$, $К_2$ относительно операций $\oplus$ и $\circ$ (таблица 2).

Задача 22. Проверить, что следующее отображение φ (таблица 8) является изоморфизмом кольца $(K,+,*)$ из задачи 21(а) на некоторое известное числовое кольцо (определить, на какое именно). Выяснить смысл отображения φ как геометрического преобразования на числовой прямой или на комплексной плоскости.

Таблица 6

№	K	(1)		(2)		(3)	
		$x \oplus y$	$x * y$	$x \oplus y$	$x * y$	$x \oplus y$	$x * y$
1	R	$x+y$	$2xy$	$x+y+1$	$2xy$	$x+y+1$	$xy+x+y$
2	C	$x+y+i$	$x+y-ixy$	$x+y$	$x+y-ixy$	$x+y$	$x-ixy$
3	C	$x+y$	$-xy$	$x+y-1$	$-xy$	$x+y-1$	$xy-x-y-2$
4	Z	$x+y$	$-xy$	$x+y$	$-xy+x+y$	$x+y+1$	$xy+x+y$
5	C	$x+y$	$-ixy$	$x+y-i$	$-ixy$	$x+y$	$i+xy$
6	Q	$x+y+\frac{1}{2}$	$xy + x + y$	$x+y+\frac{1}{2}$	$2xy+x+y$	$x+y$	$2xy+x$
7	Z	$x+y-1$	$x+y-xy$	$x+y$	$x+y-xy$	$x+y$	$y+xy$
8	C	$x+y$	ixy	$x+y+i$	ixy	$x+y$	$ixy-x-y$
9	C	$x+y-i$	$x+y+ixy$	$x+y$	$x+y+ixy$	$x+y$	$x+ixy$
10	Z	$x+y+1$	$x+y+xy$	$x+y$	$x+xy$	$x+y$	$x+y+xy$
11	Q	$x+y$	$-2xy$	$x+y+1$	$-2xy$	$x+y+1$	$x+y+xy$
12	R	$x+y-\frac{1}{2}$	$x+y-2xy$	$x+y$	$y-2yx$	$x+y$	$x+y-2xy$

Задача 23. Пусть E – единичная (2×2)-матрица и P – одна из приведённых ниже матриц (таблица 7).

Таблица 7

1	2	3	4	5	6	7	8	9	10	11	12
$\begin{pmatrix} 0 & 1 \\ 3 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} -1 & 1 \\ 0 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & -1 \\ 2 & 0 \end{pmatrix}$	$\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & -2 \\ 2 & 0 \end{pmatrix}$	$\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 2 \\ 3 & 0 \end{pmatrix}$

Доказать, что множество всех матриц вида $xE+yP$ является кольцом относительно обычных операций в случаях:

а) $x, y \in Z$; б) $x, y \in Q$; в) $x, y \in R$; г) $x, y \in C$.

В каких случаях это кольцо является полем?

Таблица 8

	Отображение	Указание
1.	$\varphi(x)=2x$	гомотетия с центром в точке О
2.	$\varphi(x)=1-ix$	поворот с центром $\frac{1}{2}(1-i)$
3.	$\varphi(x)=-\bar{x}$	осевая симметрия с осью $ix\,(x\in R)$
4.	$\varphi(x)=-x$	центральная симметрия с центром в точке O
5.	$\varphi(x)=i\bar{x}$	осевая симметрия с осью $(1+i)x \quad (x\in R)$
6.	$\varphi(x)=2x+1$	гомотетия с центром в точке *-1*
7.	$\varphi(x)=1-x$	центральная симметрия с центром в точке $\frac{1}{2}$
8.	$\varphi(x)=ix$	поворот с центром в точке O
9.	$\varphi(x)=1+ix$	поворот с центром $\frac{1}{2}(1+i)$
10.	$\varphi(x)=x+1$	сдвиг
11.	$\varphi(x)=-2x$	гомотетия с центром в точке O
12.	$\varphi(x)=1-2x$	гомотетия с центром $\frac{1}{3}$

Таблица 9

1	2	3	4	5	6	7	8	9	10	11	12
0	0	0	0	0	0	0	0	0	0	0	0
$\begin{pmatrix}1&0\\0&1\end{pmatrix}$	$\begin{pmatrix}1&0\\0&1\end{pmatrix}$	$\begin{pmatrix}1&0\\0&0\end{pmatrix}$	$\begin{pmatrix}1&0\\0&0\end{pmatrix}$	$\begin{pmatrix}1&0\\0&1\end{pmatrix}$	$\begin{pmatrix}0&0\\0&1\end{pmatrix}$	$\begin{pmatrix}1&0\\0&1\end{pmatrix}$	$\begin{pmatrix}0&0\\0&1\end{pmatrix}$	$\begin{pmatrix}1&0\\0&1\end{pmatrix}$	$\begin{pmatrix}1&1\\0&0\end{pmatrix}$	$\begin{pmatrix}1&0\\1&0\end{pmatrix}$	$\begin{pmatrix}1&0\\0&1\end{pmatrix}$
$\begin{pmatrix}1&0\\0&0\end{pmatrix}$	$\begin{pmatrix}0&1\\1&0\end{pmatrix}$	$\begin{pmatrix}0&1\\0&0\end{pmatrix}$	$\begin{pmatrix}0&0\\1&0\end{pmatrix}$	$\begin{pmatrix}1&1\\1&0\end{pmatrix}$	$\begin{pmatrix}0&0\\1&0\end{pmatrix}$	$\begin{pmatrix}0&1\\0&0\end{pmatrix}$	$\begin{pmatrix}0&1\\0&0\end{pmatrix}$	$\begin{pmatrix}0&0\\1&1\end{pmatrix}$	$\begin{pmatrix}0&0\\1&1\end{pmatrix}$	$\begin{pmatrix}0&1\\0&1\end{pmatrix}$	$\begin{pmatrix}1&1\\0&0\end{pmatrix}$
$\begin{pmatrix}0&0\\0&1\end{pmatrix}$	$\begin{pmatrix}1&1\\1&1\end{pmatrix}$	$\begin{pmatrix}1&1\\0&0\end{pmatrix}$	$\begin{pmatrix}1&0\\1&0\end{pmatrix}$	$\begin{pmatrix}0&1\\1&1\end{pmatrix}$	$\begin{pmatrix}0&0\\1&1\end{pmatrix}$	$\begin{pmatrix}1&1\\0&1\end{pmatrix}$	$\begin{pmatrix}0&1\\0&1\end{pmatrix}$	$\begin{pmatrix}1&0\\1&0\end{pmatrix}$	$\begin{pmatrix}1&1\\1&1\end{pmatrix}$	$\begin{pmatrix}1&1\\1&1\end{pmatrix}$	$\begin{pmatrix}0&1\\0&1\end{pmatrix}$

Задача 24. Доказать, что следующие 4 матрицы (таблица 9) над Z_2 образуют кольцо относительно обычных операций

сложения и умножения матриц по модулю 2. Выяснить, есть ли в этом кольце делители нуля, коммутативно ли оно, образует ли оно поле.

Задача 25. Пусть на множестве упорядоченных пар *(x, y)* действительных чисел заданы операции сложения $(x,y)+(z,t)=(x+z,y+t)$ и умножения следующим образом: $(x,y)\cdot(z,t)$ =

1) *(xz + 3yt, xt + yz);* 2) *(xz + yt, xt + yz);* 3) *(xz, xt + yz - yt);*
4) *(xz - 2yt, xt + yz);* 5) *(xz, xt + yt + yz);* 6) *(xz - 4yt, xt + yz);*
7) *(xz, xt + yz + 2yt);* 8) *(xz + 2yt, xt + yt);* 9) *(xz - yt, xt +yz);*
10) *(xz +2yt, xt + yz)* 11) *(xz,xt + yz);* 12) *(xz + 2yt, xt+yz).*

Доказать, что относительно указанных операций множество всех пар *(x, y)* является кольцом. Установить изоморфизм этого кольца с кольцом из задания 23 (в).

Блок самоконтроля

Контрольные вопросы для самопроверки

40. Можно ли на любой абелевой группе построить кольцо, доопределив определённым образом операцию умножения?
41. Можно ли утверждать, что любое непустое множество, замкнутое относительно сложения, вычитания и умножения является кольцом?
42. Имеет ли кольцо многочленов с комплексными коэффициентами делители нуля?
43. Может ли поле иметь подкольцо, не являющееся полем?
44. В поле *R* приведите примеры подколец, которые не являются полями.
45. Может ли в кольце, не являющимся полем, содержаться некоторое подполе?
46. Известно, что данное подмножество кольца замкнуто относительно сложения и умножения. Следует ли отсюда, что это подмножество является подкольцом?
47. Привести пример подмножества в кольце, замкнутого относительно деления и умножения и не являющегося подкольцом.

48. Изоморфны ли кольцо всех целых чисел и кольцо всех четных чисел?
49. Выполняется ли для колец аналог теоремы Лагранжа?
50. Может ли кольцо иметь такие элементы a, b, c, что $a \neq b$, но $ac = bc$?
51. Верно ли, что кольцо Z_m является подкольцом кольца Z?
52. Верно ли, что если $ab = 0$, то $ba = 0$ в произвольном кольце?
53. Верно ли, что конечное коммутативное кольцо без делителей нуля является полем?
54. Может ли бесконечное поле содержать конечное подполе?
55. Могут ли числовые поля быть конечными?

Дополнительные задачи и упражнения

81. Какие из следующих множеств являются кольцами (относительно обычных операций сложения и умножения чисел или функций):

а) множество нечетных чисел; множество чисел, кратных 5;

б) множество всех непрерывных функций на R;

в) множество всех четных (всех нечетных) функций, определенных на R?

82. Выяснить, является ли кольцом относительно обычных операций:

a) множество всех чётных многочленов от x над R;

b) множество всех нечётных многочленов от x над R;

c) множество всех симметрических многочленов от x и y над R;

d) множество всех антисимметрических многочленов от x и y над R;

e) множество всех симметрических $(2,2)$-матриц над R;

f) множество всех антисимметрических $(2,2)$-матриц над R;

g) множество всех дробей $\frac{m}{n}$ из Q, с нечётными знаменателями n;

h) множество всех чисел вида $m2^k, (m, k \in Z)$;

i) множество всех чисел вида $a + ai, \ (a \in Z)$;

j) множество всех многочленов $f(x)$ над R, удовлетворяющих

условию $f(0)=1$;

k) множество всех многочленов $f(x)$ над R, удовлетворяющих условию $f(1)=0$;

l) множество всех вырожденных $(2,2)$-матриц над R;

Указание: проверить, является ли каждое из перечисленных множеств подкольцом некоторого другого кольца.

83. Выяснить, является ли кольцом:

a) множество всех линейных функций, определённых на R, относительно обычного сложения и композиции функций;

b) семейство 2^A всех подмножеств множества A относительно операций $X \oplus Y = (X \cup Y) - (X \cap Y)$, $X \bullet Y = X \cap Y$.

c) множество R всех действительных положительных чисел относительно операций $x \oplus y = xy$, $x \bullet y = x^{\ln y}$;

d) множество Z всех целых чисел относительно операций $x \oplus y = \begin{cases} x+y, \text{ если } x \text{ чётно}, \\ x-y, \text{ если } x \text{ нечётно} \end{cases}$, $x \bullet y = xy$.

84. Изоморфны ли:

a) кольцо Z всех целых чисел и кольцо $2Z$ всех чётных чисел?

b) кольцо $2Z$ и кольцо $3Z$?

c) поле $Q(\sqrt{2})$ всех чисел вида $a+b\sqrt{2}$ и поле $Q(\sqrt{3})$ всех чисел вида $a+b\sqrt{3},\ (a,b \in Q)$?

d) кольцо всех верхнетреугольных $(2,2)$-матриц над Q и кольцо всех нижнетреугольных $(2,2)$-матриц над R?

85. Изоморфны ли:

a) мультипликативная группа, порожденная числом 2, и мультипликативная группа, порождённая числом $\frac{1}{2}$?

b) кольцо, порождённое числом 2, и кольцо, порождённое числом $\frac{1}{2}$?

86. Найти в кольце R всех действительных чисел:

a) наименьшее подполе, содержащее число $\sqrt{2}$; число $\sqrt{3}$; числа $\sqrt{2}$ и $\sqrt{3}$; число $\sqrt{2}+\sqrt{3}$;

b) наименьшее подкольцо, содержащее число $\sqrt{2}$;

87. В кольце $M_2(R)$ всех $(2,2)$-матриц над R найти

наименьшее поддкольцо, содержащее матрицу $A=\begin{pmatrix}0 & 1\\ 2 & 0\end{pmatrix}$ и установить его изоморфизм с подкольцом в R из задачи 87(6). Построить также наименьшее поле, содержащее матрицу A. Существует ли поле, содержащее матрицы $\begin{pmatrix}0 & 1\\ 2 & 0\end{pmatrix}$ и $\begin{pmatrix}0 & 1\\ 3 & 0\end{pmatrix}$?

Задачи повышенной сложности

88. Вывести из аксиом кольца: $x\cdot 0=0, -(-x)=x, (-x)\cdot(-y)=xy$ для всех элементов x и y данного кольца.

89. Доказать, что в кольце с единицей обратимый элемент не может быть делителем нуля.

90. Доказать, что в кольце с единицей коммутативность сложения следует из остальных аксиом.

91. Доказать, что кольцо Z_p тогда и только тогда является полем, когда p – простое число.

92. Доказать, что пересечение двух подколец данного кольца также является подкольцом этого кольца.

93. Доказать, что если H – подкольцо кольца K с единицей и p - произвольный обратимый элемент из K, то $p^{-1}Hp$ – также подкольцо, изоморфное H.

ТЕМА 6.
ИДЕАЛЫ КОЛЕЦ, ГОМОМОРФИЗМЫ, ФАКТОРКОЛЬЦА

Методический блок

В результате изучения темы студент должен знать определения и уметь приводить примеры следующих понятий: идеал (левый, правый, двусторонний), главный идеал; сравнимость по идеалу, классы вычетов по идеалу, факторкольцо; гомоморфизм колец, канонический гомоморфизм, ядро гомоморфизма.

В результате изучения темы студент должен знать формулировки и уметь доказывать следующие факты: критерий идеала кольца, теорема о гомоморфизмах колец.

В результате изучения темы студент должен уметь: распознавать идеалы кольца, гомоморфизм колец; строить идеал кольца, порожденный данными элементами; находить ядро гомоморфизма колец; строить факторкольца.

Информационный блок

Определение 16. Подкольцо A кольца K называется его *левым (правым) идеалом*, если $KA \subseteq A$ (соответственно $AK \subseteq A$). Если подкольцо является одновременно и левым и правым идеалом, то его называют *двусторонним идеалом (*или просто *идеалом).*

Для коммутативных колец понятие левого, правого и двустороннего идеалов совпадают.

Для проверки того, является ли подмножество A идеалом кольца K, можно воспользоваться следующим ***критерием.*** Подмножество A тогда и только тогда является идеалом кольца K, когда одновременно выполняются условия:

1) вместе с любыми элементами x и y оно содержит также их разность x-y (то есть A замкнуто относительно вычитания, а поэтому является подгруппой аддитивной группы K);

2) $KA \subseteq A$ и $AK \subseteq A$ (то есть A выдерживает умножение слева и справа на элементы кольца K).

Для того чтобы в коммутативном кольце с единицей построить *идеал* $(p_1,p_2,.....,p_n)$, *порождённый элементами* $p_1,p_2,.....,p_n$, необходимо составить множество всех сумм вида $p_1x_1+p_2x_2+ .....+p_nx_n$ $(x_i \in K)$. В частности, *главный идеал* (p), порождённый одним элементом p состоит из всех элементов вида px $(x \in K)$, то есть кратных элементу p.

Два элемента x и y кольца K называются *сравнимыми по идеалу* A, если x-$y \in A$ (обозначают $x \equiv y(A)$). Сравнимость идеалу является отношением эквивалентности, а поэтому разбивает кольцо K на *классы вычетов по идеалу* A (другое название -

смежные классы аддитивной группы K по подгруппе A). Класс, содержащий элемент x, обозначается $[x]$.

Полезно знать, что каждый элемент из класса вычетов может быть его представителем, и элементы x, y принадлежат одному и тому же классу по модулю A тогда и только тогда, когда $x\text{-}y \in A$.

В кольце Z всех целых чисел $x \equiv y (mod\ m)$ обозначает, что $x\text{-}y$ делится на m. На языке идеалов можно сказать, что $x \equiv y (mod\ m)$ тогда и только тогда, когда $x \equiv y (mZ)$.

Определение 17. Факторкольцом кольца K по идеалу A называется кольцо K/A всех классов вычетов по идеалу A относительно следующих операций сложения и умножения классов: $[x]+[y]=[x+y]$, $[x]\cdot[y]=[x\cdot y]$.

Классы $[xy]$ и $[x+y]$ в этом определении не зависят от выбора представителей x и y в классах $[x]$ и $[y]$. Это следует из согласованности отношения сравнимости с операциями в K: если $x \equiv z$, $y \equiv t$, то $x+y \equiv z+t$, $xy \equiv zt\ (A)$.

Определение 18. Отображение $\varphi : K \to K'$ называется *гомоморфизмом кольца* K в кольцо K', если оно сохраняет операции, то есть

$\varphi(x+y)=\varphi(x)+\varphi(y)$, $\varphi(xy)=\varphi(x)\varphi(y)$ для всех $x, y \in K$.

Определение 19. *Ядром гомоморфизма* φ называется множество $Ker\ \varphi$ всех прообразов нуля, то есть таких элементов a, для которых $\varphi(a)=0', 0' \in K'$.

Теорема. Ядро гомоморфизма $\varphi : K \to K'$ является идеалом кольца K.

Отображение $\varphi : K \to K/A$, которое переводит каждый элемент x из K в класс вычетов $[x]=x+A$ по идеалу A, является гомоморфизмом кольца K на факторкольцо K/A. Этот гомоморфизм называют *каноническим*. Его ядро совпадает с идеалом A.

Теорема о гомоморфизмах колец. *Всякий гомоморфный образ кольца K изоморфен факторкольцу K/A кольца K по некоторому идеалу A.*

Пример 21. Отображение $\varphi : Z[x] \to Z$ кольца $Z[x]$ всех многочленов от x с целыми коэффициентами в кольцо Z всех

целых чисел, которые задаются формулою $\varphi(f(x))=f(1)$, является гомоморфизмом колец.

Действительно,
$\varphi(f(x)+g(x))=(f+g)(1)=f(1)+g(1)=\varphi(f(x))+\varphi(g(x))$ и $\varphi(f(x)g(x))=(fg)(1)=f(1)g(1)=\varphi(f(x))\varphi(g(x))$, то есть φ сохраняет операции. Ядром этого гомоморфизма является множество всех многочленов $f(x)$, для которых $\varphi(f(x))=0$, то есть $f(1)=0$. Это множество всех многочленов, которые имеют корень 1 (или многочленов, сумма всех коэффициентов которых равна 0). Это множество является идеалом кольца $Z[x]$. Обозначим его для удобства через A и построим фактор-кольцо $Z[x]/A$. Классами вычетов будут множества $f(x)+A$, причём $f(x)+A=g(x)+A$ тогда и только тогда, когда $f\ x-g\ x\in A$. Это означает, что $f(1)-g(1)=0$, то есть $f(x)-g(x)$ имеет корень 1, и поэтому делится на $x-1$ без остатка.

Теперь мы можем описать все классы вычетов без повторений в виде $r+A$, где r - всевозможные остатки от деления $f(x)$ на $x-1$. То есть все классы вычетов имеют вид $r+A$, где $r\in Z$. Иначе говоря, каждый класс вычетов, полученный с помощью числа r, состоит из всех многочленов $h(x)$, для которых $h(1)=r$, то есть сумма всех коэффициентов $h(x)$ равняется r. Действия над классами выполняются по формулам: $(a+A)+(b+A)=a+b+A$; $(a+A)(b+a)=ab+A$. Отсюда видно, что $Z[x]/A\cong Z$.

Практический блок

Индивидуальные задания для домашней работы

Задача 26. Пусть T - матрица из таблицы 2. Выяснить, является ли кольцом относительно обычных операций сложения и умножения множество всех (2×2)-матриц A над R, удовлетворяющих условию:

а) $TAT=0$; *б)* $TA=AT$; *в)* $TA=-AT$.

Имеют ли данные кольца делители нуля? *Указание*: достаточно проверить, является ли каждое из указанных множеств подкольцом кольца всех (2×2)-матриц над R.

Задача 27. Выяснить, является ли гомоморфизмом отображение кольца из задания 26(б) на некоторое другое кольцо (определить на какое) каждое из отображений:

а) $\varphi(A)=TA$; б) $\varphi(A)=\frac{1}{2}TA$; в) $\varphi(A)=trA$; г) $\varphi(A)=\frac{1}{2}trA$.

Найти ядро каждого гомоморфизма. Для каждого из найденных в задаче гомоморфизмов φ построить факторкольцо $K/Ker\varphi$ и установить его изоморфизм с кольцом действительных чисел.

Задача 28. Выяснить, является ли кольцевым гомоморфизмом отображение $\alpha: Z_p \to Z_p$ и отображение $\beta: Z_p \to Z_p$ где $\alpha(x)=ax$, $\beta(x)=bx$, в следующих случаях (таблица 10).

Задача 29. В кольце $Q[x]$ всех многочленов от x над Q построить главный идеал M, образующим которого является многочлен:

1) x^2-3; 2) x^2-1; 3) x^2+x; 4) x^2+2; 5) x^2-x; 6) x^2+4;
7) x^2-2x; 8) x^2-2; 9) x^2+1; 10) x^2-2; 11) x^2; 12) x^2-6.

Построить факторкольцо $Q[x]/M$ и установить его изоморфизм с кольцом из задачи 23(б).

Таблица 10

№ варианта	1	2	3	4	5	6	7	8	9	10	11	12
p	15	24	12	21	15	20	14	28	18	20	24	18
a	6	8	8	6	9	5	8	8	6	10	8	8
b	8	9	9	15	10	6.	9	10	10	16	16	9

Задача 30. **.** В кольце $Z[x]$ всех многочленов от x над Z построить главный идеал A, образующим которого является многочлены:

1) $2, x^2+x$; 2) $2, x^2-1$; 3) $2, x^2+x+2$; 4) $2, x^2+x+1$;
5) $2, x^2-x+1$; 6) x^3+1, x^2+x+1; 7) $2, x^2$; 8) $2, x^2+1$;
9) x^2-1, x^2+1; 10) x^2, x^2-2 11) $2, x^2-x$; 12) x^3-1, x^2-x+1.

Построить факторкольцо $Z[x]/A$ и выяснить, изоморфно ли оно кольцу из задачи 23.

Блок самоконтроля

Контрольные вопросы для самопроверки

56. Пусть подмножество коммутативного кольца с единицей замкнута относительно сложения и умножения на элементы кольца. Образует ли она идеал кольца?
57. Верно ли, что сумма идеалов кольца является идеалом?
58. Верно ли, что поле не содержит идеалов?
59. Пусть I_1, I_2 - идеалы кольца, $I_1 \subset I_2$ и $a \equiv b\ (I_2)$. Верно ли, что $a \equiv b\ (I_1)$?
60. Верно ли, что в коммутативном кольце K главный идеал (a) равен aK?
61. Верно ли, что в кольце главных идеалов $(x) + (y) = (x + y)$?
62. Является ли факторкольцо $Q[x]/(x^2 - 1)$ полем?
63. Может ли поле быть гомоморфным образом кольца?
64. Может ли кольцо, которое не является полем, быть гомоморфным образом поля?
65. Какую характеристику имеет восьмиэлементное поле?
66. Изоморфны ли поля $Q(\sqrt{2})$ и $Q(\sqrt{3})$?

Дополнительные задачи и упражнения

94. В кольце $Z[i]$ целых гауссовых чисел найти наименьший идеал, который содержит число $2i$, и построить факторкольцо $Z[i]/(2i)$.

95. Пусть $C=\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$, K - кольцо всех (2×2)-матриц над R, перестановочных с матрицей C. Доказать, что отображение $\varphi(A)=\frac{1}{2}CA$ является эндоморфизмом кольца K. Найти $Ker\,\varphi$ и установить изоморфизм $K/Ker\,\varphi \cong R$.

96. В кольце $Z[i]$ найти наименьший идеал, который содержит число 2. Равняется ли он идеалу $(2i)$? Построить факторкольцо $Z[i]/(2)$. Является ли оно полем?

97. В кольце *Z[i]* найти наименьший идеал, который содержит число 3. Является ли полем факторкольцо *Z[i]/(3)*?

98. В кольце *R[x]* построить идеалы $A=(x^2+x)$ и $B=(x^2-x)$. Найти $A\cdot B$, $A\cap B$, $A+B$.

Задачи повышенной сложности

99. Найти все идеалы в кольце Z_{12}.

100. Найти все гомоморфизмы кольца Z_{12} в кольца Z_{24} и Z_8.

101. Доказать, что $R[x, y]/(x-y)\cong R[x]$.

102. Кольцо всех (2×2)-матриц над *R*, перестановочных с матрицей $\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$, разложить в прямую сумму двух собственных идеалов.

103. Разложить кольцо Z_{36} в прямую сумму двух собственных идеалов.

104. При каких значениях *m* кольцо Z_m является прямой суммой идеалов, каждый из которых – поле?

105. Доказать, что все идемпотенты коммутативного кольца сами образуют кольцо относительно операций $e\oplus f = e + f-ef$ *и* ef.

106. Построить поле $Q(\sqrt{2})$ и доказать, что отображение $a+b\sqrt{2}\to a-b\sqrt{2}$ является его автоморфизмом. Существуют ли другие автоморфизмы этого поля?

107. Построить поле $Q(\sqrt{2}+\sqrt{3})$ и найти все его подполя.

108. Изоморфны ли между собой поля $Q(\sqrt{2})$ и $Q(\sqrt{3})$?

109. Доказать, что все элементы $(1+\sqrt{2})^n$ $(n\in Z)$ принадлежат мультипликативной группе кольца $Z(\sqrt{2})$. Пользуясь этим фактом, решить в целых числах уравнения $x^2-2b^2=1$ и $x^2-2b^2=-1$.

110. В поле $Q(\sqrt[3]{2})$ вычислить $(1-\sqrt[3]{2}+\sqrt[3]{4})^{-1}$ и $\frac{1+\sqrt[3]{2}}{1+\sqrt[3]{4}}$.

111. Доказать, что $Q(\sqrt{2}+\sqrt{3})=Q(\sqrt{2}-\sqrt{3})$.

112. Найти все неприводимые над Z_3 многочлены третьей степени.

113. Построить поле $Z_2(\alpha)$,где α - корень многочлена x^4+x+1.

ЛИТЕРАТУРА

1. Аржанцев И.В. Алгебра / И.В. Аржанцев. – Москва: Издательство Мехмат МГУ, 2013. – 52 с.

2. Бахтурин Ю.А. Основные структуры современной алгебры / Ю.А. Бахтурин. – М.: Наука. Гл. ред. физ.-мат. лит. 1990. – (Совр. алгебра). – 320 с.

3. Кострикин А.И. Введение в алгебру. Часть I. Основы алгебры Учебник для вузов. / А.И. Кострикин. – М.: Физико-математическая литература, 2000. – 272 с.

4. Кострикин А.И. Введение в алгебру. Часть III. Основные структуры. Учебник для вузов. – 3-е изд. / А.И. Кострикин. – М.: Физматлит, 2004. – 272 с.

5. Курош А. Г. Курс высшей алгебры / А. Г. Курош. – Москва: R & C dynamics; Ижевск: РХД, 2003. – 431 с.

УЧЕБНО-МЕТОДИЧЕСКОЕ ИЗДАНИЕ

Селякова Людмила Ивановна

АЛГЕБРАИЧЕСКИЕ СТРУКТУРЫ В СИСТЕМЕ ФУНДАМЕНТАЛЬНОЙ ПОДГОТОВКИ БУДУЩЕГО УЧИТЕЛЯ

учебно-методическое пособие

Подписано в печать 22.02.2016 г. Формат 60x84/16. Бумага типографская.
Печать офсетная. Усл. печ. л. 4,01. Тираж 100 экз. Заказ № 24/2

Издательство ГОУ ВПО «Донецкий национальный университет»
283001, г.Донецк, ул.Университетская, 24

Отпечатано в «Цифровой типографии» (ФЛП Артамонов Д.А.)
г. Донецк, ул. Челюскинцев, 291а, тел. (050) 886-53-63

Свидетельство о регистрации ДНР серия АА02 № 51150
от 9 февраля 2015 г.