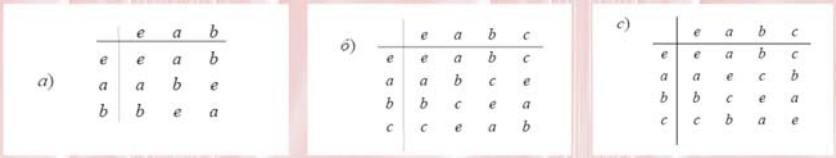
Министерство образования и науки Российской Федерации
Дальневосточный федеральный университет
Школа естественных наук
Кафедра информационной безопасности



Е.В. Закасовская

ОСНОВНЫЕ ПОНЯТИЯ ТЕОРИИ ГРУПП В ПРИМЕРАХ И ЗАДАЧАХ

Учебное электронное издание
Учебное пособие

Владивосток
Дальневосточный федеральный университет
2013

Министерство образования и науки Российской Федерации
Дальневосточный федеральный университет
Школа естественных наук
Кафедра информационной безопасности

Е.В. Закасовская

ОСНОВНЫЕ ПОНЯТИЯ ТЕОРИИ ГРУПП В ПРИМЕРАХ И ЗАДАЧАХ

Учебное электронное издание

Учебное пособие

Рекомендовано
Дальневосточным региональным учебно-методическим центром
(ДВ РУМЦ) в качестве учебного пособия для студентов
направления подготовки бакалавров 090900.62
«Информационная безопасность» вузов региона

Владивосток
Дальневосточный федеральный университет
2013

УДК 512.54
ББК 22.144
З-18

Рецензенты:
Ромашко Р.В., д-р физ.-мат. н.,
ведущий научный сотрудник ИАПУ ДВО РАН;
Гончаров С.М., канд. физ.-мат. н., заведующий кафедрой
информационной безопасности МГУ им. Г.И. Невельского

Закасовская, Е.В.

З-18 Основные понятия теории групп в примерах и задачах [Электронный ресурс] : учебное пособие / Е.В. Закасовская ; Дальневосточный федеральный университет, Школа естественных наук. – Электрон. дан. – Владивосток : Дальневост. федерал. ун-т, 2013. – 1 CD ROM. – Систем требов.: процессор с частотой 1,3 ГГц (Intel, AMD) ; оперативная память 256 МБ, свободное место на винчестере 335 МБ ; Windows (XP; Vista; 7 и т.п.); Acrobat Reader, Foxit Reader либо любой другой их аналог. – Загл. с экрана.

ISBN 978-5-7444-3220-1

Пособие включает раздел теории групп курса «Алгебра и теория чисел», который изучается в третьем семестре студентами ШЕН ДВФУ. По каждой теме кратко изложен теоретический материал, приведены образцы решения задач, предложены упражнения и задачи для самостоятельного решения. Пособие адресовано студентам математических специальностей университетов.

Может быть использовано студентами других специальностей, изучающих теорию групп.

УДК 512.54
ББК 22.144

В авторской редакции
Дизайн, верстка *Е.П. Давыгора*

Дальневосточный федеральный университет
690091, г. Владивосток, ул. Суханова, 8
. Тел./факс: (423) 226-54-43, 265-22-35 (∗2379)
E-mail: dvfutip@yandex.ru, editor_dvfu@mail.ru

Изготовитель CD-ROM: Дирекция публикационной деятельности,
690990, Владивосток, ул. Пушкинская, 10
Объем 0,6 МБ
Тираж 50 экз.
Регистрационное свидетельство №

ISBN 978-5-7444-3220-1

ОГЛАВЛЕНИЕ

РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА

1. Кострикин А.И. Введение в алгебру. В 3 тт. М.:Физматлит, 2001
2. Винберг Э. Б. Курс алгебры.-М.:Факториал 2001, 544с.
3. Фаддеев Д. К. Лекции по алгебре.-М.:Наука 1984, 416с.
4. Ленг С. Алгебра. М.: Мир, 1968
5. Курош А. Г. Теория групп. — 3-е изд. — М., Физматлит, 1967
6. Каргаполов М.И., Мерзляков Ю.И. Основы теории групп. М.:Н., 1977.

Задачники

7. Ляпин Е.С., Айзенштат А.Я., Лесохин М.М. Упражнения по теории групп. М.: Наука, 1967.
8. Проскуряков И.В. Сборник задач по линейной алгебре. М.: Наука, 1984.
9. Сборник задач по алгебре: Учебное пособие /Под ред. А.И. Кострикина. – М: Факториал, 1995.

ВВЕДЕНИЕ

К середине 20 столетия прочно установилась мода на алгебраические методы, которые стали весьма полезными как при исследовании математических объектов, так и в других фундаментальных областях, например, при исследовании элементарных частиц, свойств твердого тела, кристаллов. В алгебре весьма явно проступает сложное взаимодействие теоретических и практических аспектов, присущее всей математике. Это делает оправданным концентрический стиль изложения на первом уровне которого естественным образом возникают основные алгебраические структуры.

В данной работе предложено изучение первой из фундаментальных классических структур алгебры – групп. Важность понятия группы для математики в целом сопоставима только с важностью таких понятий как множество, отображение, кольцо, поле, топологическое пространство.

Учебно-методическое пособие автора “Основные понятия теории групп в примерах и задачах” написано на основе спецкурса “Теория групп” для студентов 4 курса отделения теоретическая математического факультета ДВГУ (1994 – 2002 гг.), а также общего курса алгебры для студентов 2 курса (3-й семестр), обучающихся по специальности 090301 «Компьютерная безопасность», прочитанного автором (2002 - 2013).

Фундаментальные понятия группы, кольца, поля становятся более привычными после самостоятельной работы над задачами и упражнениями, содержащимися в методическом пособии.

Для удобства выделяются несколько наиболее употребительных алгебраических систем:

– группы $(\mathbb{Z}, +)$, S_n, A_n, $GL(n, \mathbb{K})$, $SL(n, \mathbb{K})$, группа кватернионов $\mathbb{Q}_8$;

– кольца $\mathbb{Z}$, классов вычетов $\mathbb{Z}_m$, кольцо многочленов $\mathbb{K}[x]$;

– поля $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_p$,

на фоне которых демонстрируется язык алгебры.

Первоначально понятие группы возникло в форме группы преобразований (группы движений или, как частный случай, группы ортогональных преобразований). Конечные группы, которым мы отдаем предпочтение, связаны с преобразованиями конечного множества и преобразования в этом случае называются подстановками.

При первом знакомстве с группами важно иметь в виду следующие основные понятия.

1. Бинарная алгебраическая операция. Это понятие является фундаментом всего дальнейшего. Мы должны иметь возможность оперировать с этими объектами. Обычно на первом этапе изучения предмета операции сохраняют сходство с действиями над числами (например, сопоставление паре чисел a, b их суммы $a+b$ или произведения $a \cdot b$).

2. Понятие группы. Мы начали с изучения множества с операцией и обсуждения обычного набора аксиом группы и сопутствующих понятий, например, порядка элемента группы или порядка всей группы. Для более полного понимания аксиоматики групп особенно полезно самостоятельно изучить строение групп малых порядков (3, 4, 6).

3. Понятие подгруппы. Изучение внутренней структуры конкретной группы позволяет установить многие ее свойства. Внутреннюю структуру некоторых групп можно описать с помощью их подгрупп, т.е. групп внутри группы. Особенно интересно знать строение подгрупп некоммутативных групп, например групп подстановок S_n, A_n или

матричных групп $GL(n, \mathbb{K})$, $SL(n, \mathbb{K})$, где $\mathbb{K}$ – поле и представить их в наглядной форме в виде графов.

4. Изоморфизм. Понятие группы тесно связано с понятием отображения. Нас, в частности, интересуют гомоморфизмы. Алгебру интересует только вопрос, как действует та или иная алгебраическая операция, и вовсе не интересует, на чем она действует. Отвлечься от второго вопроса позволяет понятие изоморфизма, изоморфные объекты устроены одинаково с точки зрения алгебры.

Одна из целей курса “Теория групп”– это интенсивная подготовка студентов, изучающих фундаментальные дисциплины, к свободному владению языком современной науки, т.к. трудно недооценить ту роль, которую играют группы в теоретических исследованиях.

Важное свойство группы заключается в том, что для любых ее элементов уравнение имеет решение являющее элементом этой же группы. Т.е. операция обращения в группе является замкнутой. В группах ощущается некая завершенность. В них нет лишнего, и они могут существовать самостоятельно.

Природе характерна экономичность, которая может быть выражена в различных формах симметрии. А смысл той или иной формы может быть отображен структурными свойствами групп. Ярким примером сказанного могут служить систематизация элементарных частиц с помощью групп симметрии, в результате которого были предсказаны новые частицы.

Научный анализ с помощью теории групп - это некий тест на полноту и завершенность математических представлений реального мира. Все законы сохранения имеют смысл постольку, поскольку они опираются на групповые представления. Если мы говорим, что нечто не изменяется при свершении каких-то действий, то это просто констатация набора фактов. Научной гипотезой это становится, когда под набором действий

мы понимаем определенную группу преобразований (действий), которые оставляют неизменным это нечто. Здесь важна не формальная сторона дела, а то, что проверка гипотезы становится на рациональный путь: структурные свойства группы могут упростить доказательство гипотезы. Например, если группа циклическая, то достаточно рассмотреть один элемент. В то же время следует отметить, что все результаты, полученные с помощью теории групп, можно было бы получить другим путем (правда путь этот был бы более извилистым и долгим). В содержании теории групп нет ничего, чего не было бы в остальных разделах математики. Просто в ней в рамках единой концепции собраны наиболее общие свойства известных объектов и операций. Это позволяет находить те или иные характеристики решений многих математических задач, не прибегая к детальному анализу данной математической модели. К тому же такого рода результаты могут автоматически следовать для целого класса моделей, объединенных по некоторому групповому признаку. Когда мы в своих исследованиях прибегаем к аналогиям и параллелям или пытаемся упростить задачу, мы, часто не подозревая об этом, пользуемся элементами групповых представлений. Рационализм, свойственный математике, в теории групп, значительно усиливается. По своей четкости и простоте исходных положений теория групп не уступает ни одному разделу математики. В то же время теория групп изобилует чрезвычайным структурным разнообразием. Сочетание такой внутренней глубины с четкостью и простотой делают этот раздел одним из красивейших.

1. ПЕРВЫЕ ОПРЕДЕЛЕНИЯ И ПРИМЕРЫ

Определение 1. Множество $\mathbb{G}$ с бинарной алгебраической операцией $(\cdot)$ называется группой, если выполнены следующие аксиомы:

1) операция $(\cdot)$ ассоциативна, т.е. выполнено следующее равенство $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, для любых a, b, c из группы $\mathbb{G}$;

2) существует такой элемент e из группы $\mathbb{G}$, что для любого элемента $a \in \mathbb{G}$ выполняется $a \cdot e = e \cdot a = a$;

3) для любого $a \in \mathbb{G}$ существует такой элемент $a^{-1} \in \mathbb{G}$, что

$$a \cdot a^{-1} = a^{-1} \cdot a = e.$$

В дальнейшем, если это не приводит к недоразумениям, знак операции $(\cdot)$ будем опускать.

Задача № 1. Доказать, что введенное выше определение группы равносильно следующему определению:

Определение 1'. Множество $\mathbb{G}$ с введенной на нем бинарной алгебраической операцией называется группой, если

1) эта операция ассоциативна;

2) для любых двух элементов $a, b \in \mathbb{G}$ в группе $\mathbb{G}$ существуют такие элементы x и y, что $ax = b$, $ya = b$.

В этом случае элементы x и y называются, соответственно, левым и правым частными от деления b на a.

Решение. Из первого определения сразу следует существование левого и правого частных: в качестве таковых нужно взять

$$x = a^{-1}b\ ,\ y = ba^{-1}.$$

Если выполнены условия второго определения, то существует x из группы $\mathbb{G}$, что $ax = a$ для любого a из $\mathbb{G}$. Тогда для любого b из $\mathbb{G}$ существует y из $\mathbb{G}$: $ya = b$, $bx = yax = ya = b$, и т.е. x - правая единица группы $\mathbb{G}$. Аналогично доказывается существование левой единицы x'. Из того, что $x = x'x = x'$ следует существование единицы, ее удобно обозначить через e.

Из второго определения, очевидно, что для любого a из $\mathbb{G}$ существует x: $ax = e$, откуда $axa = a$. Т.к. существует x': $x'a = e$, умножив $axa = a$ на x' слева, получим $x'axa = x'a$ или $xa = e$.

Тем самым равносильность определений доказана.

Заметим также, что

1) если e и e' - две единицы, то $e = ee' = e'$.

2) если x и x' - два обратных элемента к a, то

$$ax = e \Rightarrow x'ax = x' \Rightarrow ex = x' \Rightarrow x = x';$$

3) т.к. из $ax = b \Rightarrow x = a^{-1}b$, а из $ya = b \Rightarrow y = ba^{-1}$ и доказана единственность обратного элемента, то очевидна и единственность частных.

Определение 2. Наименьшее $n > 0$, для которого выполнено $a^n = e$ называется порядком элемента a и обозначается $|a|$. Если $a^n \neq e$ для любого

$n > 0$, то говорят, что элемент a имеет бесконечный порядок и пишут, $|a| = \infty$.

Задача № 2. Доказать, что для любого a из $\mathbb{G}$ выполнены равенства

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

Задача № 3. Если $a^n = e$, то n делится на $|a|$.

Решение. Обозначим $|a| = m$.

Представим n в виде (разделим n на m с остатком):

$$n = km + r,\ 0 \le r \le n,$$

тогда

$$a^n = a^{km+r} = (a^m)^k a^r = ea^r = a^r.$$

Из $a^r = e$ и $0 \le r < n$ следует, что $r = 0$.

Задача № 4. Доказать, что если элемент a группы имеет порядок n, то элемент a^k имеет порядок n/d, где $d = (n, k)$ - НОД чисел n и k.

Решение.

Нужно показать, что $(a^k)^{n/d} = e$, и что $(a^n)^m = e$ при m: $0 < m < n/d$.

Прежде всего, $(a^k)^{n/d} = a^{kn/d} = (a^n)^{k/d} = e$. Пусть теперь $m > 0$ таково, что $(a^k)^m = a^{km} = e$. Из предыдущего упражнения следует, что km делится на n. Значит, $m \cdot к/d$ делится на n/d. Но $(к/d, n/d)=1$ (взаимно просты), поэтому m делится на n/d откуда следует, что $m > n/d$.

Задача № 5. Найти все группы порядков 3, 4, 6 и написать для них таблицы умножения.

Решение.

Прежде всего, заметим, что если в группе квадрат любого элемента равен единичному элементу, то эта группа абелева. Действительно, если

любые a и b из группы $\mathbb{G}$, то $a^2 = e$, $b^2 = e$ и т.к. $ab \in \mathbb{G}$, то $(ab)^2 = e$. Далее, умножив $ab \cdot ab = e$ справа на b получим $aba = b$ и, умножив последнее равенство на a получим, $ab = ba$ т.е. коммутативность любых двух элементов группы $\mathbb{G}$.

1. Группа третьего порядка.

Рассмотрим группу, порожденную одним единственным элементом a, имеющим порядок 3, т.е. $a^3 = e$. Очевидно, что эта группа состоит из элементов a, $a^2 \neq e$, $a^3 = e$.

Обозначим a^2 через b: $b = a^2$. Тогда $ab = aa^2 = e$, $ba = e$, $b^2 = a^3\, a = a$,
а таблица Кели (таблица умножения) (рис. 1*а*) имеет вид, симметричный относительно «диагонали», т.е. эта группа коммутативна (абелева). Очевидно, что других групп третьего порядка не существует.

2. *а*) Группа 4-го порядка, порожденная одним элементом a: $a^4 = e$ состоит из элементов a, a^2, a^3, $a^4 = e$, причем a, a^2, $a^3 \neq e$. Обозначим a^2 через b, а a^3 через c: $b = a^2$, $cb = a^3$.

Таблица Кели имеет вид, представленный на рис.1*б*, т.к.
$ab = a\, a^2 = a^3 = c$, $ac = a\, a^3 = e$ и т. д.

а)

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

б)

	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

с)

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Рис. 1. Таблицы Кели
а) $n = 3$,
б) $n = 4$, циклическая,
в) $n = 4$, нециклическая.

б) Рассмотрим еще один возможный случай для группы четвертого порядка.

Пусть a, b два различных неединичных элемента этой группы.

Заметим, что если в группе квадрат любого элемента единичен, то эта группа абелева (упр.)

Таким образом, группа порожденная элементами a, b, для которых верно $a^2 = e$, $b^2 = e$, $ав = ва \neq e$ будет иметь следующий вид:

$$\mathbb{G} = \left\{ e, a, b, c \middle| a^2 = b^2 = e, c = ab = ba \right\}.$$

Очевидно, что эта группа абелева и, в отличие от предыдущих, порождена уже двумя элементами a и b, т. е. состоит из их степеней и произведений (рис.1c).

3. а) Группа, состоящая из различных степеней элемента a: $|a|=6$, т.е.

$$\mathbb{G} = \left\{ a, a^2, a^3, \ldots, a^5 \middle| a^6 = e \right\}.$$

Таблица умножения для этой группы составляется аналогичным образом, как и в случае $|\mathbb{G}|= 3, 4$.

б) Найдем теперь группу порядка 6, порожденную уже не одним, а несколькими элементами. Пусть эта группа содержит элементы a и b. Значит, $\mathbb{G}$ содержит и их всевозможные степени и произведения, т.е. элементы вида e, a, b, ab, ba, a^2, b^2 и прочие.

Если рассмотреть группу $\mathbb{H}$ с соотношениями между элементами a и b как в 2 б), т.е. $\mathbb{H} = \left\{ e, a, b, ab \middle| a^2 = b^2 = e, ab = ba \right\}$, то введение нового элемента $c \notin \mathbb{H}$ даст еще 4 элемента. Поэтому рассмотрим группу,

содержащую элементы e , a и b связанные соотношениями: $a^2 = b$, $a^3 = e$. Очевидно, что эти элементы сами образуют группу.

Введем в рассмотрение новый элемент группы c: $c \neq e, a, b$. Обозначим $ac = d$, $bc = f$. В результате получаем 6 элементов группы:

$$e, a, b, c, d, f.$$

Заметим, что $ec = ce = e$, т.к. e - единица в группе. Для новых элементов группы c, d и f обязательно выполнение равенств:

$$c^2 = e,\ d^2 = e,\quad f^2 = e,$$

т.к. в противном случае будем иметь группу $\mathbb{G}$ порядка больше, чем 6.

Далее, имеют место следующие равенства, необходимые для заполнения таблицы Кели:

$$af = abc = a\,a^2c = c,\ ad = a^2c = bc = f,$$
$$bf = bbc = b^2c = ac = d,\ bd = a^2ac = c.$$

А вот ca найти так же просто уже не удается. Очевидно, ca должен совпадать с одним из элементов группы, т.е. e, a, b, c, d, f.

Первые четыре возможности отпадают сразу, остаются две, менее очевидные: 1) $ca = d$ и 2) $ca = f$.

Рассмотрим первую из них, т.е. $ca = d = ac$. Умножим равенство $ca = ac$ слева на a^2 , а справа на c: $a^2cac = a^2cca = a^2ea = a^3 = e$.

Отсюда $fd = e$, а это значит, $fdd = d$ и получается, что $f = d$, т.е. противоречие.

Значит, остается единственная возможность: $ca = f$.

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

*Рис.*2. Таблица Кели для нециклической группы порядка 6.

Далее, легко видеть, что $cd = c^2b$ и, таким образом, $bc = d$.

Теперь легко получаем оставшиеся соотношения, необходимые для составления таблицы Кэли (рис.2):

$$da = aca = af = c,\ ca = a^2c,$$
$$db = aca^2 = acaa = a\,a^2ca = f,$$
$$dc = ac^2 = a,\ \ df = acca = a^2 = b,$$
$$fa = caa = cb = d,\ \ fb = caa^2 = c,$$
$$fc = a^2cc = a^2 = b,\ \ fd = caac = cbc = dc = a.$$

Задача № 6. Ассоциативна ли операция $*$ на множестве M, если

1) $M = \mathbb{N}$, $x*y = x^y$;

2) $M = \mathbb{N}$, $x*y = $ НОД(x, y);

3) $M = \mathbb{N}$, $x*y = 2xy$;

4) $M = \mathbb{Z}$, $x*y = x-y$;

5) $M = \mathbb{Z}$, $x*y = x^2-y^2$;

6) $M = \mathbb{R}$, $x*y = \sin x \sin y$;

7) $M = \mathbb{R}$, $x*y = xy^{x/|x|}$;

Задача № 7. Какие из указанных числовых множеств с указанными операциями являются группами:

1) $(A, +)$, где A - одно из множеств $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$;

2) $(A, \cdot)$, где A - одно из множеств $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$;

3) $(A_0, \cdot)$, где A - одно из множеств $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, а $A_0 = A - \{0\}$;

4) $(n\mathbb{Z}, +)$, где n - натуральное число;

5) $(\{-1, 1\}, \cdot)$;
6) множество степеней данного вещественного числа с целыми показателями относительно умножения;
7) множество всех комплексных корней степени n из единицы относительно умножения.

Задача № 8. Какие из указанных совокупностей отображений множества $M = \{1, 2, ..., n\}$ в себя образуют группу относительно умножения:

1) множество всех отображений;
2) множество всех инъективных отображений;
3) множество всех сюръективных отображений;
4) множество всех биективных отображений;
5) множество всех четных перестановок;
6) множество всех нечетных перестановок;
7) множество транспозиций;
8) множество всех перестановок, оставляющих неподвижными элементы некоторого подмножества $S \subseteq M$;
9) множество {E, (12)(34), (13)(24), (14)(23)};
10) множество {E, (13), (24), (12)(34), (13)(24), (14)(23), (1234), (1432)};

Задача № 9. Какие из указанных множеств квадратных вещественных матриц фиксированного порядка образуют группу:

1) множество симметрических матриц относительно сложения;

2) множество симметрических матриц относительно умножения;
3) множество невырожденных матриц относительно сложения;
4) множество невырожденных матриц относительно умножения;
5) множество матриц с фиксированным определителем d относительно умножения;
6) множество диагональных матриц относительно сложения;
7) множество диагональных матриц относительно умножения;
8) множество диагональных матриц, все элементы диагонали которых отличны от нуля, относительно умножения;
9) множество верхних треугольных матриц относительно умножения;
10) множество верхних нильтреугольных матриц относительно умножения;
11) множество верхних нильтреугольных матриц относительно сложения;
12) множество верхних унитреугольных матриц относительно умножения;
13) множество всех ортогональных матриц;
14) множество верхних нильтреугольных матриц относительно операции $x*y = x+y - xy$.
15) множество ненулевых матриц вида

$$\begin{pmatrix} x & y \\ -y & x \end{pmatrix}, x, y \in \mathbb{R}$$

относительно умножения;

16) множество ненулевых матриц вида

$$\begin{pmatrix} x & y \\ \lambda y & x \end{pmatrix}, x, y \in \mathbb{R},$$

где λ – фиксированное вещественное число, относительно умножения;

17) множество матриц вида

$$\left\{\pm\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix},\pm\begin{pmatrix}i & 0\\ 0 & -i\end{pmatrix},\pm\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix},\pm\begin{pmatrix}0 & i\\ i & 0\end{pmatrix}\right\}$$

относительно умножения.

Задача № 10. Какие из указанных множеств образуют группу при указанной операции над элементами:

1) корни n - й степени из единицы (как действительные, так и комплексные) относительно операции умножения;
2) корни всех целых положительных степеней из единицы относительно умножения;
3) матрицы порядка n с целыми элементами относительно умножения;
4) матрицы порядка n с целыми элементами и определителем, равным единице, относительно умножения;
5) матрицы порядка n с целыми элементами и определителем, равным ± 1, относительно умножения;
6) подстановки чисел 1, 2, ..., n относительно умножения;
7) нечетные подстановки чисел 1, 2, ..., n относительно умножения;
8) четные подстановки чисел 1, 2, ..., n относительно умножения;
9) векторы n - мерного линейного пространства $\mathbb{R}_n$ относительно сложения;

10) параллельные переносы трехмерного пространства $\mathbb{R}$, если за произведение переносов принято их последовательное выполнение;
11) повороты трехмерного пространства $\mathbb{R}$ вокруг данной точки O, если за произведение поворотов принято их последовательное выполнение;
12) все движения трехмерного пространства $\mathbb{R}$ вокруг данной точки O, если за произведение двух движений принято движение, получающееся при их последовательном выполнении;
13) положительные действительные числа относительно операции $a * b = a^b$;
14) положительные действительные числа относительно операции $a * b = a^2 b^2$;
15) действительные многочлены степени $\leqslant n$ (включая ноль) от переменной x относительно сложения;
16) действительные многочлены степени n от переменной x относительно сложения;
17) действительные многочлены любых степеней (включая ноль) от переменной x относительно сложения.

2. СИСТЕМЫ ОБРАЗУЮЩИХ

Определение. Пусть M не пустое подмножество группы $\mathbb{G}$. Совокупность всех элементов группы $\mathbb{G}$ равных конечным произведениям положительных и отрицательных степеней элементов из M, является подгруппой группы $\mathbb{G}$, называемой подгруппой, порожденной множеством M , и обозначаемой $\langle M \rangle$:

$$\langle M \rangle = \left\{ a_{\alpha_1}^{k_1} \cdot a_{\alpha_2}^{k_2} \cdot \ldots \cdot a_{\alpha_n}^{k_n}, k_i \in \mathbb{Z},\ a_i \in M \right\},$$

M называется *системой образующих* множества $\langle M \rangle$.

Если $\langle M \rangle = \mathbb{G}$, то M называется системой образующих группы $\mathbb{G}$.

Примеры систем образующих для групп малых порядков

1. Пусть $\mathbb{G}$ - группа 3-го порядка: $\mathbb{G} = \left\{ e, a, a^2 = b \right\} = \langle a \rangle$.

2. Пусть $\mathbb{G}$ - группа 4-го порядка. Из предыдущего упражнения следует, что возможно 2 случая:

а) $\mathbb{G} = \left\{ a, a^2, a^3,\ a^4 = e \right\} = \langle a \rangle$;

б) $\mathbb{G} = \left\{ a,\ b,\ c = ab = ba, a^2 = b^2 = e \right\} = \langle a \rangle$.

3. Пусть $\mathbb{G}$ - группа 6 - го порядка.

а) $\mathbb{G}=\left\{a,a^2,a^3,a^4,a^5,a^6=e\right\}=\langle a\rangle$;

б) $\mathbb{G}=\left\{e,\ a,\ b,\ c,\ d,\ f:\ a^2=b,a^3=c^2=d^2=f^2=ab=ba=e,ac=d,bc=f\right\}=$

$$=\langle a,c\rangle=\langle b,c\rangle=\langle a,f\rangle=\langle b,f\rangle=\langle a,d\rangle=\langle b,d\rangle=\langle c,d\rangle=\langle d,f\rangle=\langle c,f\rangle.$$

Задача № 11. Пусть K - поле,

$$GL(n,\mathbb{K})=\left\{A=\left(a_{ij}\right):a_{ij}\in K,\det A\neq 0\right\}.$$

Рассмотрим в $GL(n,\mathbb{K})$ матрицы вида:

$$t_{ij}(\alpha)=e+\alpha e_{ij}=i\begin{pmatrix} 1 & & \vdots & & \overset{j}{} \\ & 1 & \vdots & & \\ \cdots & \cdots & 1 & \alpha & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix},$$

называемые трансвекциями, и матрицы

$$d(\beta)=e+(\beta-1)e_{nn}=\begin{pmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & \\ & & & \beta \end{pmatrix},$$

где $\alpha,\beta\in K$, $\beta\neq 0$, $i\neq j$, e – единичная матрица, e_{ij} – матрица, содержащая на (i,j)-м месте единицу, а в остальных местах - нули.

Доказать, что

$$GL(n,\mathbb{K})\ =\left\langle t_{ij}(\alpha),d(\beta)/\alpha,\beta\in K,i\neq j\right\rangle.$$

Доказательство.

Для доказательства нужно проверить, что каждая матрица из $GL(n, \mathbb{K})$ представима в виде

$$t_1 \dots t_r \, d(\beta) \, t_{r+1} \dots t_s ,$$

где t_i – трансвекции.

Умножим матрицу $A = \left(a_{ij}\right)_{i,j}$ на трансвекцию $t_{ij}(\alpha)$ справа, считая для определенности $i > j$:

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1i} & \dots & a_{1j} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2i} & \dots & a_{2j} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{ni} & \dots & a_{nj} & \dots & a_{nn} \end{pmatrix} \cdot \begin{matrix} \\ \\ i \\ \\ j \\ \\ \\ \end{matrix} \begin{pmatrix} 1 & \vdots & & \vdots & & \\ \dots & 1 & & \alpha & & \\ & & \ddots & \vdots & & \\ \dots & \dots & \dots & 1 & & \\ & & & & 1 & \end{pmatrix} =$$

$$= \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1i} & \dots & \alpha\, a_{1i} + a_{1j} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2i} & \dots & \alpha\, a_{2i} + a_{2j} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{ni} & \dots & \alpha\, a_{ni} + a_{nj} & \dots & a_{nn} \end{pmatrix}.$$

Т. е. умножение матрицы A на трансвекцию $t_{ij}(\alpha)$ справа соответствует добавлению к j - му столбцу i - го столбца, умноженного на скаляр $\alpha \in \mathbb{K}$.

Пусть $A = GL(n, \mathbb{K})$. Умножая матрицу A слева или справа на соответствующие трансвекции, добиваемся, чтобы $a_{12} \neq 0$.

Далее последовательно применяя элементарные преобразования со столбцами матрицы, т.е. умножая справа на трансвекции, получаем матрицу, у которой на (1, 1) - м месте 1, а в остальных местах нули:

$$\begin{pmatrix} 1 & 0 & \dots & 0 \\ * & * & \dots & * \\ \dots & \dots & \dots & \dots \\ * & * & \dots & * \end{pmatrix}.$$

Умножая эту матрицу на соответствующие трансвекции, получаем матрицу, у которой 1-й столбец и 1-я строка состоят из нулей, за исключением места (1, 1), где стоит 1:

$$\begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & * & \dots & * \\ \dots & \dots & \dots & \dots \\ 0 & * & \dots & * \end{pmatrix}.$$

Применяя этот процесс к правой нижней клетке порядка n-1, получим матрицу вида:

$$\begin{pmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & \\ & & & \beta \end{pmatrix}.$$

Таким образом, $A = t_1 \dots t_r d(\beta) t_{r+1} \dots t_s$.

Задача *№* 12. Доказать, что

1. $SL(n, \mathbb{K}) = \langle t_{ij}(\alpha), \quad \alpha \in K, \quad i \neq j \rangle$.

2. $T(n, \mathbb{K}) = \{ A \in GL(n, \mathbb{K}) : a_{ij} = 0, \quad i > j \} =$

$= \langle t_{ij}(\alpha), diag(\beta_1, ..., \beta_n), \alpha, \beta_i \in \mathbb{K}, \ i > j \rangle$.

3. $SL(n, \mathbb{Z}) = \langle e + e_{ij} : \ 1 \leq i, j \leq n, \quad i \neq j \rangle =$

$= \langle e + e_{12}, \ e_{12} + e_{23} + \dots + e_{n-1,n} + (-1)^{n-1} e_{n1} \rangle$.

3. ГРУППЫ ДВИЖЕНИЙ

Определение. Преобразованием множества X называется взаимно однозначное отображение $f: X \to X$ этого множества на себя.

Для такого отображения, очевидно, существует обратное отображение $f^{-1}: X \to X$, $f^{-1} f = f f^{-1} = e$.

Здесь произведение отображений fg означает, последовательное их выполнение $(fg)(x) = f(g(x)), x \in X$, а e - тождественное преобразование: $e(x) = x$, для любого $x \in X$.

Совокупность $\mathbb{G}$ преобразований множества X называется группой преобразований, или $\mathbb{G}$ содержит тождественное преобразование e, вместе с любым $g \in \mathbb{G}$ существует $g^{-1} \in \mathbb{G}$ и вместе с любыми $g_1, g_2 \in \mathbb{G}$ их произведение $g_1 \cdot g_2 \in \mathbb{G}$.

Обычно эти условия выполняются, т.к. $\mathbb{G}$ определяется как группа преобразований, сохраняющая некоторое свойство.

Преобразования, сохраняющие расстояния $\rho(x, y)$ между точками евклидова пространства, т.е. для которых выполняется соотношение

$$\rho(g(x), g(y)) = \rho(x, y),$$

образуют группу, называемую группой движений.

Если все они сохраняют одну точку, то мы имеем дело с группой ортогональных преобразований (или группу поворотов).

Ортогональные преобразования, сохраняющие ориентацию пространства, называются вращениями. Группа тех или иных

преобразований, сохраняющих некоторый объект, может интерпретироваться как совокупность его симметрий.

Понятие группы позволяет в точных терминах охарактеризовать симметричность данной фигуры. Именно, каждой фигуре можно сопоставить совокупность всех преобразований пространства, совмещающих данную фигуру с нею самой. Эта совокупность будет группой, характеризующей симметричность фигуры.

Преобразования симметрии могут состоять только из поворотов вокруг некоторых осей, проходящих через точку O (рассматриваются повороты вокруг точки O), отражения в некоторых плоскостях, проходящих через точку O, зеркальных поворотов, для которых эта точка есть пересечение зеркальной плоскости с поворотной осью к инверсии, т. е. отражения в этой точке.

Задача № 13. Описать группу движений правильного n - угольника.

Решение. Рассмотрим в плоскости правильный n - угольник $A_1 \ldots A_n$, например, правильный шестиугольник $A_1\ A_2\ A_3\ A_4\ A_5\ A_6$ (рис. 3).

Опишем, во - первых, те преобразования плоскости, которые совмещают n-угольник с самим собой. Очевидно, что таких преобразований равно n и каждое из них есть поворот многоугольника вокруг центра на угол $k2\pi / n$, где $k \in \mathbb{Z}$.

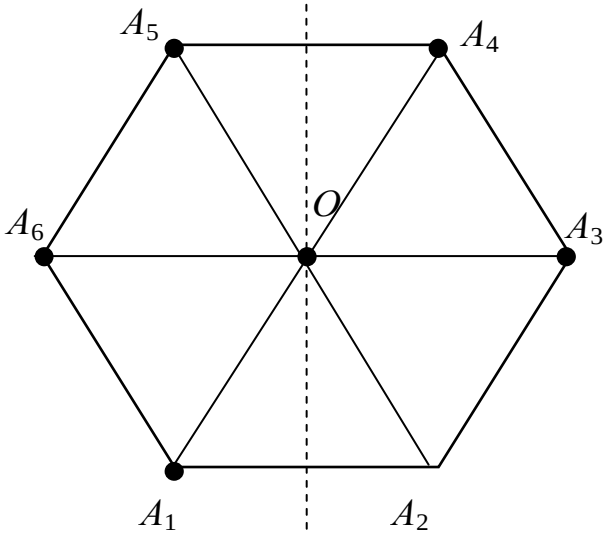


Рис. 3. Симметрии правильного 6-угольника

Эти перемещения образуют группу (за произведение берется последовательное выполнение перемещений). Очевидно, что эта группа циклическая.

Далее, если рассматривать перемещения не в плоскости, а в пространстве, то к перечисленным перемещениям прибавятся еще и “опрокидывания”, т. е. повороты на угол π вокруг осей симметрии. Правильный многоугольник имеет n осей симметрии:

1. если n четное, то осями симметрии являются $n/2$ прямых, соединяющих середины противоположных граней (рис. 3) и $n/2$ прямых, соединяющих противоположные вершины;

2. если n нечетное, то оси симметрии суть прямые, соединяющие вершину с серединой противоположной стороны.

Таким образом, группа движений правильного n-угольника имеет порядок $2n$ и содержит подгруппу вращений порядка n .

Задача № 14. Описать группу движений правильного тетраэдра. Доказать, что все вращения (повороты) правильного тетраэдра образуют подгруппу группы движений.

Решение. 1) Для каждой вершины рассмотрим вращения вокруг прямой, соединяющей эту вершину и центр противоположной грани. Эту прямую называют граневой медианой.

Такой осью вращения является, например, прямая AM (рис. 4).

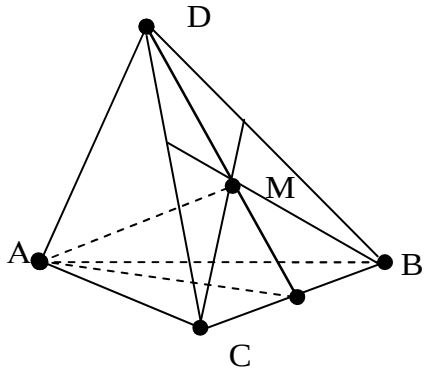


Рис. 4. Граневая медиана AM

Очевидно, что тетраэдр переходит в себя при повороте вокруг оси AM на углы: $2\pi/3, 4\pi/3, 2\pi$.

Поворот на угол 2π соответствует тождественному преобразованию.

Т.к. тетраэдр имеет 4 граневые медианы, то вокруг них существует 8 нетождественных поворотов. Каждому повороту соответствует подстановка, описывающая перестановку вершин. Так повороту вокруг прямой AM на угол $\varphi = 2\pi / 3$ соответствует подстановка

$$\begin{pmatrix} A & D & B & C \\ A & B & C & D \end{pmatrix} = (A)\cdot(DBC) = (DBC),$$

представляющая собой “тройной цикл”. Очевидно, что и остальные повороты вокруг граневых медиан описываются тройными циклами.

2) Далее существуют еще 3 поворота (нетождественных). Это повороты на угол π вокруг каждой из трех прямых, соединяющих середины противоположных ребер тетраэдра и называемых реберными медианами (рис. 5). Повороту вокруг прямой MN соответствует подстановка

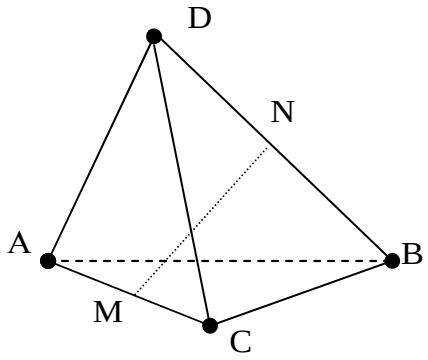


Рис. 5. Реберная медиана

$$\begin{pmatrix} A & B & C & D \\ C & D & A & B \end{pmatrix} = (AC)\cdot(BD).$$

Очевидно, что всем трем таким вращениям соответствуют подстановки, являющиеся произведениями двух “двойных циклов”.

Всего в 1) и 2) перечислены 12 различных поворотов (вращений). Подстановки, соответствующие этим вращениям, образуют знакопеременную группу A_4.

3) Очевидно, что еще не перечислены все движения, т.к. не учтены симметрии, такие как, например, симметрия относительно плоскости ADM, где M - середина стороны CB (рис. 6).

Очевидно, такой симметрии соответствует транспозиция

$$\begin{pmatrix} A & B & C & D \\ A & C & B & D \end{pmatrix} = (BC).$$

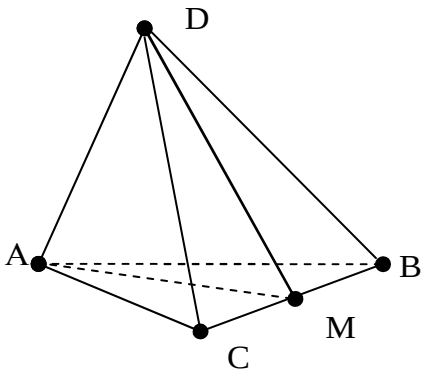


Рис. 6. Симметрия относительно плоскости

Теперь понятно, что все движения тетраэдра описываются всеми подстановками из группы S_4.

4. ГРУППЫ ПОДСТАНОВОК

Определение. Подстановкой на множестве $\Omega = \{1, 2, \ldots, n\}$ называется взаимно однозначное отображение этого множества на себя.

Удобно задавать подстановку прямым указанием образа каждого элемента:

$$\pi = \begin{pmatrix} 1 & 2 & \ldots & n \\ i(1) & i(2) & \ldots & i(n) \end{pmatrix}, \quad \pi: \begin{matrix} 1 & 2 & \ldots & n \\ \downarrow & \downarrow & & \downarrow \\ i(1) & i(2) & \ldots & i(n) \end{matrix}, \quad i(k) = \pi(k), \quad k \in \Omega.$$

Последовательное применение двух подстановок приводит к подстановке, называемой их произведением.

Например, если $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$, $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}$, то

$$\alpha\beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix} = \begin{matrix} 1 & 2 & 3 & 4 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 2 & 3 & 4 & 1 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 2 & 4 & 3 & 1 \end{matrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}.$$

Заметим сразу, что произведение подстановок (при $n \geq 3$) не коммутативно, т.к. $\alpha\beta \neq \beta\alpha$.

Число всех подстановок из *n* чисел равно *n!*. Подстановка называется четной, если четности верхней и нижней строк совпадают, и нечетной в противном случае.

Определение. Подстановка, получающаяся из тождественной при помощи одной замены любых 2-х элементов i и j называется транспозицией:

$$\begin{pmatrix} 1 & 2 & \dots & i & \dots & j & \dots & n \\ 1 & 2 & \dots & j & \dots & i & \dots & n \end{pmatrix}.$$

Обозначается символами (ij).

Удобно записывать подстановку в виде “циклов”.

Определение. Циклом называется последовательность нескольких чисел, в которой первое число переходит во второе, второе в третье и т. д., а последнее в первое. Цикл обозначается заключением его чисел в общие скобки.

Если число переходит в само себя, то оно одно образует цикл. Циклы, не имеющие общих чисел, называются независимыми. Любую подстановку можно разложить на независимые циклы. Например, $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 5 & 1 & 4 & 2 & 3 & 8 & 7 \end{pmatrix} = (1 \quad 6 \quad 3)(2 \quad 5)(1)(7 \quad 8).$

Задача № 15. Доказать, что любая транспозиция меняет четность перестановки на противоположную.

Задача № 16. Доказать, что число четных подстановок равно числу нечетных и равно $n!/2$.

Задача № 17. Доказать, что любая подстановка представима в виде произведения транспозиций.

Задача № 18. Доказать, что любая подстановка может быть получена из любой другой посредством нескольких транспозиций.

Задача № 19. Доказать, что каждая подстановка может быть представлена как произведение транспозиций вида:

а) $(1\quad 2),\ (1\quad 3),\ldots,(1\quad n)$; б) $(1\quad 2),\ (2\quad 3),\ldots,(n-1\quad n)$.

Задача № 20. Доказать, что любая подстановка может быть представлена как произведение нескольких сомножителей, равных $(1\quad 2)$ и $(1\quad 2\quad 3\quad \ldots\quad n)$.

Задача № 21. Доказать, что любая четная подстановка может быть представлена как

а) произведение тройных циклов $(i\quad j\quad k)$;

б) произведение циклов вида $(1\quad 2\quad 3),\ (1\quad 2\quad 4),\ldots,(1\quad 2\quad n)$.

Пусть Ω - произвольное множество, а $S(\Omega)$ - множество всех биективных (взаимно однозначных) преобразований f: $\Omega \to \Omega$.

Множество $S(\Omega)$ является группой относительно естественной бинарной операции, являющейся композицией преобразований.

Если $\Omega = \{1, 2, \ldots, n\}$ то мы приходим к группе S_n всех подстановок n-й степени, группе по умножению порядка $n!$ называемой симметрической группой n - й степени.

Все четные подстановки степени n образуют группу $A_n \subset S_n$ порядка $n!/2$, которая называется знакопеременной группой. Заметим сразу же, что нечетные подстановки группы не образуют, т.к. произведение двух нечетных подстановок является подстановкой четной.

5. ГРУППЫ И ИХ ПОДГРУППЫ

Напомним, что подгруппа $\mathbb{H}$ группы $\mathbb{G}$ есть часть группы $\mathbb{G}$, которая сама является группой относительно индуцированной операции из $\mathbb{G}$ и пишут $\mathbb{H} \leq \mathbb{G}$.

Подгруппа $\mathbb{H}$ в $\mathbb{G}$ называется собственной, если $\mathbb{H} \neq 1$ и $\mathbb{H} \neq \mathbb{G}$ и обозначается $\mathbb{H} < \mathbb{G}$.

Задача № 22. 1) Доказать, что $\mathbb{H}$ является подгруппой группы $\mathbb{G}$ тогда и только тогда, когда для любых двух элементов a, b из $\mathbb{H}$ выполняется условие $ab^{-1} \in \mathbb{H}$;

2) $\mathbb{H} \leq \mathbb{G} \Leftrightarrow ab \in \mathbb{H}$ и $b^{-1} \in \mathbb{H}$.

Приведем несколько примеров групп и их подгрупп.

1) Рассмотрим в полной линейной группе $GL(n, \mathbb{R})$ подмножество $SL(n, \mathbb{R})$ всех матриц с определителем, равным единице:

$$SL(n, \mathbb{R}) = \{ A \in GL(n, \mathbb{R}) : \det A = 1 \}.$$

Это подмножество является подгруппой в $GL(n, \mathbb{R})$, так как

а) $E = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix} \in SL(n, \mathbb{R})$;

б) Для любых $A, B \in SL(n, \mathbb{R})$, очевидно, что $AB \in SL(n, \mathbb{R})$, т.к. из $\det A = \det B = 1$ следует, что $\det A \cdot B = \det A \cdot \det B = 1$.

в) Для $A \in SL(n, \mathbb{R})$, $A^{-1} \in SL(n, \mathbb{R})$, так как $\det A = \det A^{-1} = 1$.

Эта подгруппа носит название специальной линейной группы.

2) $\mathbb{Z} < \mathbb{Q} < \mathbb{R} \leq \mathbb{C}$.

3) Очевидно, что рассматривая поле $\mathbb{Q}$ вместо $\mathbb{R}$, получим включение $GL(n, \mathbb{Q}) \geq SL(n, \mathbb{Q})$. Далее, $SL(n, \mathbb{Q}) \supseteq SL(n, \mathbb{Z})$ и $SL(n, \mathbb{R})$ является подгруппой в $SL(n, \mathbb{Q})$. Подгрупповые включения между группами $GL(n, \mathbb{K})$ и $SL(n, \mathbb{K})$ при $\mathbb{K} = \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ можно изобразить диаграммой, представленной на рис. 7.

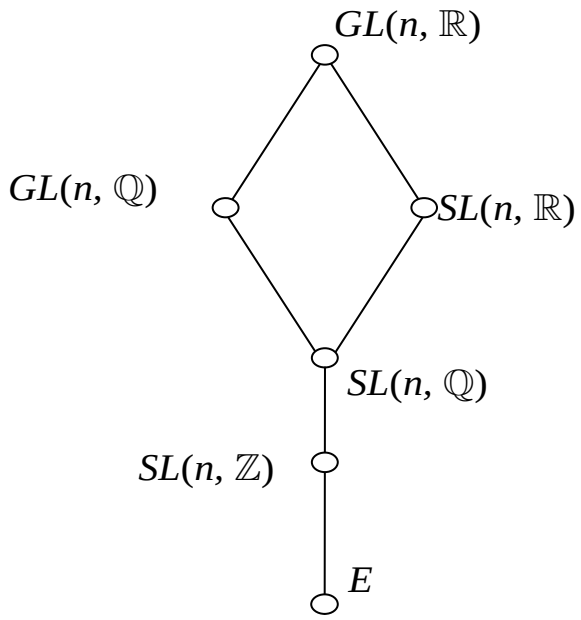


*Рис.*7. Подгруппы полной линейной группы

4) В симметрической группе S_n множество A_n всех четных подстановок образуют подгруппу, т.к. произведение двух четных подстановок является подстановкой четной. Эта группа называется знакопеременной группой n - й степени.

Задача № 23. Описать все подгруппы симметрической группы S_3.

Решение. Из общего курса алгебры известно, что элементы группы S_3 исчерпываются шестью подстановками:

$$e=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix},\alpha_1=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix},\alpha_2=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix},\alpha_3=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix},$$

$$\alpha_4=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix},\alpha_5=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$$

Таблица Кэли представлена на рис. 8.

Из этой таблицы видно, что S_3 является на самом деле группой, причем некоммутативной, т.к. таблица не симметрична относительно диагонали.

	e	α_1	α_2	α_3	α_4	α_5
e	e	α_1	α_2	α_3	α_4	α_5
α_1	α_1	e	α_3	α_2	α_5	α_4
α_2	α_2	α_4	e	α_5	α_1	α_3
α_3	α_3	α_5	α_1	α_4	e	α_2
α_4	α_4	α_2	α_5	e	α_3	α_1
α_5	α_5	α_3	α_4	α_1	α_2	e

*Рис.*8. Таблица Кели для группы S_3

Обратим внимание на то, что $\alpha_1\alpha_1 = \alpha_1^2 = e$ и, следовательно, α_1 порождает циклическую группу второго порядка: $\langle\alpha_1\rangle = \{e, \alpha_1\}$.

Аналогично, подгруппы $\langle\alpha_4\rangle = \{e, \alpha_4\}$, $\langle\alpha_5\rangle = \{e, \alpha_5\}$ являются циклическими группами 2-го порядка.

Найдем теперь другие множества, замкнутые относительные операции умножения.

Рассмотрим подстановку $\alpha_3=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}=(1\ 2\ 3)$ и все ее различные степени:

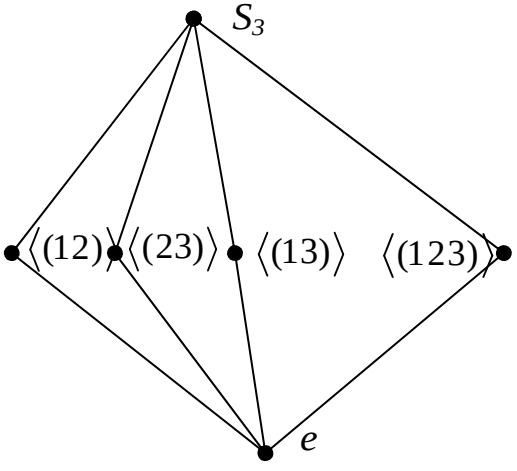


Рис. 9. Подгрупповая структура группы S_3

$$\alpha_3^2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 3 & 2 \end{pmatrix} = \alpha_4,$$

$$\alpha_3^3 = \alpha_4\alpha_3 = e.$$

Таким образом, мы получили циклическую подгруппу 3-го порядка, состоящую из всех степеней α_3: $<\alpha_3> = \{e, \alpha_3, \alpha_4\}$.

Нетрудно понять, что циклическими подгруппами 2-го и 3-го порядка исчерпываются все собственные подгруппы симметрической группы S_3, включения между которыми изображено на рис. 9.

Задача № 24. Найти все подгруппы в группах:

1) D_4 (группа движений квадрата);

2) A_4 (знакопеременная группа 4-го порядка).

Задача № 25. В множестве $\mathbb{Q}_8$, состоящем из восьми элементов:

$$\pm 1, \pm i, \pm j, \pm k,$$

задано действие при помощи таблицы умножения, представленной на рис. 10.

	1	-1	$-i$	i	$-j$	j	$-k$	k
1	1	-1	$-i$	i	$-j$	j	$-k$	k
-1	-1	1	i	$-i$	j	$-j$	k	$-k$
i	i	$-i$	1	-1	$-k$	k	j	$-j$
$-i$	$-i$	i	-1	1	k	$-k$	$-j$	j
j	j	$-j$	k	$-k$	1	-1	$-i$	i
$-j$	$-j$	j	$-k$	k	-1	1	i	$-i$
k	k	$-k$	$-j$	j	i	$-i$	1	-1
$-k$	$-k$	k	j	$-j$	$-i$	i	-1	1

Рис. 10. Таблица Кели для группы кватернионов

Доказать, что $\mathbb{Q}_8$ является группой, найти все ее подгруппы.

Указанная группа называется группой кватернионов.

Задача № 26. Пусть $\mathbb{G}$ конечная циклическая группа порядка n, порожденная элементом x. Для натурального числа d, являющегося делителем n, обозначим через $\mathbb{H}_d$ совокупность элементов вида

$$x^{d}, x^{2d}, x^{3d},..., x^{(n/d)d} = x^{n}.$$

Доказать, что

1. $\mathbb{H}_d$ является подгруппой группы $\mathbb{G}$;
2. если $d_1 \neq d_2$, то $\mathbb{H}_{d1} \neq \mathbb{H}_{d2}$;
3. $\mathbb{G}$ не имеет других подгрупп, кроме подгрупп $\mathbb{H}_d$ при всевозможных делителях d числа n.

Задача № 27. Пусть $\mathbb{G}$ бесконечная циклическая группа, порожденная элементом x. Для целого неотрицательного числа d обозначим через $\mathbb{H}_d$ совокупность элементов вида x^{kd} ($k = 0, \pm 1, \pm 2, ...$).

Доказать, что

1. $\mathbb{H}_d$ является подгруппой группы $\mathbb{G}$;
2. если $d_1 \neq d_2$, то $\mathbb{H}_{d1} \neq \mathbb{H}_{d2}$;
3. $\mathbb{G}$ не имеет других подгрупп, кроме подгрупп $\mathbb{H}_d$.

Задача № 28. Доказать, что всякая бесконечная группа имеет бесконечное множество подгрупп.

Задача № 29. Выяснить, каковы группы, у которых множество всех подгрупп:

1. состоит из одной подгруппы;
2. состоит из двух подгрупп;
3. состоит из трех подгрупп.

Задача № 30. Доказать, что пересечение любого множества подгрупп само является подгруппой.

Задача № 31. Пусть все неединичные элементы группы имеют порядки, равные 2. Доказать, что группа абелева.

Задача № 32. Доказать, что подмножество

$\mathbb{H} = \{e,\ (12)(34),\ (13)(24),\ (14)(23)\}$ группы S_4 является коммутативной группой. Составить таблицу умножения группы $\mathbb{H}$.

Группу $\mathbb{H}$ называют *четверной группой Клейна*.

Задача № 33. Доказать, что следующие множества матриц образуют подгруппы в $GL(n, \mathbb{R})$:

1. стохастические матрицы

$$St\,(n, \mathbb{R}) = \{\ a \in GL(n, \mathbb{R}) : \sum_j a_{ij} = 1,\ j = 1, \ldots, n\};$$

2. дважды стохастические матрицы

$$St(n, \mathbb{R})^* = \{a \in GL(n, \mathbb{R}) : \sum_j a_{ij} = \sum_i a_{ij} = 1,\ i, j = 1,\ldots,n\};$$

Задача № 34. Доказать, что множество теплицевых матриц

$$Tep(n,\mathbb{R}) = \left\{ \begin{pmatrix} a_1 & a_2 & a_3 & \cdots & a_n \\ 0 & a_1 & a_2 & \cdots & a_{n-1} \\ 0 & 0 & a_1 & \cdots & a_{n-2} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & a_1 \end{pmatrix} \in GL\left(n,\mathbb{R}\right) \right\}$$

образует абелеву подгруппу в $GL(n, \mathbb{R})$.

Задача № 35. Доказать, что множество циркулянтов

$$Cir(n,\mathbb{R}) = \left\{ \begin{pmatrix} a_0 & a_1 & a_2 & \cdots & a_{n-1} \\ a_{n-1} & a_0 & a_1 & \cdots & a_{n-2} \\ a_{n-2} & a_{n-1} & a_0 & \cdots & a_{n-3} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ a_1 & a_2 & a_3 & \cdots & a_0 \end{pmatrix} \in GL\left(n,\mathbb{R}\right) \right\}$$

образует абелеву подгруппу в $GL(n, \mathbb{R})$.

6. РАЗЛОЖЕНИЕ ГРУППЫ ПО ПОДГРУППЕ

Пусть $\mathbb{H}$ – подгруппа группы $\mathbb{G}$ и $a \in \mathbb{G}$. Множество вида

$$\mathbb{H}a = \{ha, h \in \mathbb{H}\}$$

называется левым классом смежности группы $\mathbb{G}$ по подгруппе $\mathbb{H}$, а

$$a\mathbb{H} = \{ah, h \in \mathbb{H}\}$$

называется правым классом смежности группы $\mathbb{G}$ по подгруппе $\mathbb{H}$.

Задача № 36. Если элемент b содержится в некотором правом классе смежности $a\mathbb{H}$ группы $\mathbb{G}$ по подгруппе $\mathbb{H}$, то $a\mathbb{H} = b\mathbb{H}$. Аналогично и для левых классов смежности. Доказать.

Задача № 37. Пусть $\mathbb{H}$ – подгруппа группы $\mathbb{G}$ и $a, b \in \mathbb{G}$. Доказать, что правые классы смежности $a\mathbb{H}$ и $b\mathbb{H}$ либо совпадают, либо не пересекаются. Аналогично и для левых классов смежности. Доказать.

Если группа $\mathbb{G}$ представлена в виде попарно непересекающегося объединения своих правых классов смежности по $\mathbb{H}$:

$$\mathbb{G} = a\mathbb{H} \cup b\mathbb{H} \cup \ldots \cup c\mathbb{H} \cup \ldots,$$

то такое разбиение называется правым разложением группы $\mathbb{G}$ по подгруппе $\mathbb{H}$. Множество элементов $\{a, b, \ldots, c, \ldots\}$ называется множеством представителей этого правого разложения $\mathbb{G}$ по $\mathbb{H}$. Аналогично определяется левое разложение

$$\mathbb{G} = \mathbb{H}a \cup \mathbb{H}b \cup \ldots \cup \mathbb{H}c \cup \ldots \quad .$$

Следует иметь в виду, что понятия левого и правого разложения условны и иногда их меняют местами.

Если число левых классов смежности конечно, то оно называется индексом подгруппы $\mathbb{H}$ в группе $\mathbb{G}$ и обозначается $|\mathbb{G} : \mathbb{H}|$.

Пусть $\mathbb{F}$, $\mathbb{H}$ являются подгруппами группы $\mathbb{G}$ и $a \in \mathbb{G}$. Множество $\mathbb{F}a\mathbb{H}$ называется двойным классом смежности группы $\mathbb{G}$ по паре подгрупп $(\mathbb{F}, \mathbb{H})$.

Задача № 38. Доказать, что для любой подгруппы $\mathbb{H}$ группы G всегда существует левое и правое разложение $\mathbb{G}$ по $\mathbb{H}$. (Указание. Объединение всевозможных правых классов смежности равно $\mathbb{G}$. Исключить из этого объединения повторяющиеся классы, а далее воспользоваться результатом предыдущего упражнения.)

Задача № 39. Пусть x - некоторый элемент и $\mathbb{H}$ - некоторая подгруппа группы $\mathbb{G}$, то x содержится в правом смежном классе $x\mathbb{H}$ и в левом смежном классе $\mathbb{H}x$. Доказать.

Задача № 40. Пусть даны два правых разложения группы $\mathbb{G}$ по подгруппе $\mathbb{H}$. Доказать, что они представляют собой одно и то же разбиение множества всех элементов группы $\mathbb{G}$. Доказать то же для левых разложений.

Задача № 41. Найти правое разложение симметрической группы S_3 по подгруппе, состоящей из двух элементов e и (12).

Задача № 42. Найти левое разложение знакопеременной группы A_4 по подгруппе, состоящей из трех элементов e и (123), (132).

Задача № 43. Найти правое и левое разложения группы кватернионов $\mathbb{Q}_8$ по подгруппе, состоящей из двух элементов: ± 1. Сравнить их и объяснить результат сравнения.

Задача № 44. Найти разложения циклической группы десятого порядка по всем ее подгруппам.

Задача № 45. Найти разложение бесконечной циклической группы, порожденной элементом x, по подгруппе, порожденной элементом x^3.

Задача № 46. Пусть $\mathbb{G}$ - конечная группа порядка n, $\mathbb{H}$ - ее подгруппа порядка h и k - индекс $\mathbb{H}$ в $\mathbb{G}$. Доказать, что $n = hk$.

Замечание. Отсюда следует важный вывод: в конечной группе порядок всякой подгруппы, также как и индекс, является делителем порядка группы.

Задача № 47. Доказать, что в конечной группе порядок всякого ее элемента является делителем порядка группы.

Задача № 48. В симметрической группе S_5 выяснить, какие из нижеследующих множеств будут смежными по каким-либо подгруппам:

1. $K_1 = \{(234), (1234)\}$;
2. $K_2 = \{(12), (123), (1234)\}$;
3. $K_3 = \{e, (13)(24),(1234), (1432)\}$;
4. $K_4 = \{(12), (13),(14), (15)\}$;
5. $K_5 = \{(12), (152)(34)\}$.

Задача № 49. Пусть $\mathbb{F}$, $\mathbb{H}$ являются подгруппами группы $\mathbb{G}$. Доказать, что всегда существует разложение $\mathbb{G}$ по паре подгрупп $(\mathbb{F}, \mathbb{H})$.

Задача № 50. Найти разложение симметрической группы S_4 по паре подгрупп: $\mathbb{F} = \{e, (123), (132)\}$, $\mathbb{H} = \{e, (12)(34)\}$.

Задача № 51. Найти разложение симметрической группы S_3 по паре подгрупп $(\mathbb{F}, \mathbb{H})$, где $\mathbb{F} = \mathbb{H} = \{e, (12)\}$.

7. НОРМАЛЬНЫЕ ПОДГРУППЫ И ФАКТОРГРУППЫ

Определение. Если для элементов a и b группы $\mathbb{G}$ найдется элемент x из группы $\mathbb{G}$ такой, что $x^{-1} a x = b$, то говорят, что элемент b сопряжен с элементом a.

Часто используют обозначения $x^{-1} a x = a^{x}$. Легко проверить, что

$$(ab)^{x} = a^{x} b^{x}, (a)^{xy} = a^{xy}.$$

Определение. Пусть S – подмножество группы $\mathbb{G}$. Подмножество вида $S^{x} = \{x^{-1} s x, s \in S\}$ называется сопряженным с S в группе $\mathbb{G}$.

Очевидно, что любое подмножество, сопряженное с группой само является группой (проверить это).

Определение. Пусть S – подмножество группы $\mathbb{G}$, а $\mathbb{H}$ – подгруппа группы $\mathbb{G}$. Подмножество вида

$$\{ x \in \mathbb{H} : x^{-1} S x = S \} = N_{\mathbb{H}}(S)$$

называется нормализатором множества S в подгруппе $\mathbb{H}$.

Очевидно, что множество $N_{\mathbb{H}}(S)$ является подгруппой (проверить).

Аналогично определяется множество

$$\{x \in \mathbb{H} : x^{-1} s x = s, \forall x \in \mathbb{H}\} = Z_{\mathbb{H}}(S),$$

называемое централизатором множества S в подгруппе $\mathbb{H}$.

Заметим, что

1) если S одноэлементное множество, т.е. $S = \{s\}$, то нормализатор совпадает с централизатором;

2) $Z_H(S) \subseteq N_H(S)$;

3) если подгруппа совпадает со всей группой ($H = \mathbb{G}$), то говорят просто о *нормализаторе* и *централизаторе* множества *S*. Централизатор всей группы называется ее *центром*.

Предложение. Доказать, что число множеств, сопряженных с S в $\mathbb{H}$, равно индексу нормализатора множества S в $\mathbb{H}$, т.е. $|\mathbb{H}: N_{\mathbb{H}}(S)|$.

(Доказать самостоятельно.)

Задача № 52. Доказать, что отношение сопряженности элементов в группе является отношением сопряженности.

Задача № 53. Доказать, что если два элемента в группе сопряжены, то их порядки равны.

Задача № 54. Доказать, что если два подмножества группы сопряжены, то их порядки равны.

Задача № 55. Распределить по классам сопряженных элементов элементы следующих групп: *a*) S_3 , *b)* A_4 , *c)* S_4 , *d)* $\mathbb{Q}_8$.

Задача № 56. В группе $GL(2, \mathbb{R})$ найти нормализаторы элементов:

$$x=\begin{pmatrix}1 & 0\\ 0 & 2\end{pmatrix}, y=\begin{pmatrix}-1 & 0\\ -1 & 0\end{pmatrix}, z=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}.$$

Задача № 57. Доказать, что в симметрической группе S_n два элемента сопряжены тогда и только тогда, когда они имеют одинаковый цикленный тип, т.е. они имеют одинаковое строение при разложении на независимые циклы;

Задача № 58. Используя предыдущую задачу описать элементы классов сопряженности в группе S_5.

Особенно важную роль в группах играют те подгруппы, относительно которых левые и правые классы смежности совпадают.

Определение. Подгруппа $\mathbb{H}$ группы $\mathbb{G}$ называется нормальной, пишут $\mathbb{H} \trianglelefteq \mathbb{G}$, если $\mathbb{H}x = x\mathbb{H}$ для любого элемента $x \in \mathbb{G}$.

Ясно, что условие $\mathbb{H}x = x\mathbb{H}$ равносильно условию $x^{-1}\mathbb{H}\, x = \mathbb{H}$. Теперь можно сказать, что

1. подгруппа $\mathbb{H}$ группы $\mathbb{G}$ тогда и только тогда нормальна в группе $\mathbb{G}$, если вместе с каждым своим элементом она содержит и все элементы с ним сопряженные посредством элементов из $\mathbb{G}$, т.е. $\mathbb{H}^{\mathbb{G}} \subseteq \mathbb{H}$ или

2. подгруппа $\mathbb{H}$ группы $\mathbb{G}$ тогда и только тогда нормальна в группе $\mathbb{G}$, когда она совпадает со всеми своими сопряженными (по этой причине

нормальные подгруппы еще называют *самосопряженными*). Употребляют также названия *нормальный делитель* и *инвариантная* подгруппа.

Предложение. Классы смежности по нормальной подгруппе образуют группу относительно операции умножения подмножеств. Единицей этой группы является сама нормальная подгруппа.

(Доказать самостоятельно.)

Определение. Группа, образованная классами смежности группы $\mathbb{G}$ по нормальной подгруппе $\mathbb{H}$, называется *факторгруппой* $\mathbb{G}$ по $\mathbb{H}$ и обозначается $\mathbb{G}/\mathbb{H}$.

Задача № 59. Найти все нормальные подгруппы симметрической группы S_3;

Задача № 60. Выяснить, какие нормальные делители порождаются следующими подмножествами группы S_4:

$$M_1 = \langle (12), (1234) \rangle,\ M_2 = \langle (123), (132) \rangle,\ M_3 = \langle e \rangle.$$

Задача № 61. Доказать, что аддитивная и мультипликативная группы поля нормальны.

Задача № 62. Доказать, что четверная группа Клейна является нормальной подгруппой в группе S_4.

Задача № 63. Доказать, что

$$A_n \trianglelefteq S_n,$$

$$SL(n, \mathbb{K}) \trianglelefteq GL(n, \mathbb{K}),$$

$$UT(n, \mathbb{K}) \trianglelefteq T(n, \mathbb{K}).$$

Задача № 64. Доказать, что все подгруппы группы $\mathbb{Q}_8$ являются нормальными.

8. МОРФИЗМЫ ГРУПП

Напомним, что на множестве M задана бинарная алгебраическая операция, если задано отображение $M \times M \to M$ декартова квадрата $M \times M$ в множество M.

Пусть $(M_1, *)$ – множество M_1 с бинарной операцией $*$, а $(M_2, \bullet)$ – множество M_2 с бинарной алгебраической операцией $\bullet$.

Отображение $\varphi : M_1 \to M_2$ называется гомоморфизмом, если для любых $x, y \in M_1$ выполняется равенство $\varphi(x*y) = \varphi(x)\bullet\varphi(y)$.

Взаимно однозначное отображение, являющееся гомоморфизмом, называется изоморфизмом. Иногда полезно рассматривать мультипликативные множества, т.е. множества для любых двух элементов которого определена операция умножения.

Задача № 65. Пусть $(\mathbb{C}, \times)$ – мультипликативное множество всех комплексных чисел, а $(\mathbb{R}, \times)$ – мультипликативное множество вещественных чисел,

$\varphi_1: \mathbb{C} \to \mathbb{R}$, такое что для $\forall z \in \mathbb{C} \Rightarrow \varphi_1(z) = |z|$;

$\varphi_2: \mathbb{C} \to \mathbb{R}$, такое что для $\forall z \in \mathbb{C} \Rightarrow \varphi_2(z) = |z| + 1$;

$\varphi_3: \mathbb{C} \to \mathbb{R}$, такое что для $\forall\, z \in \mathbb{C} \Rightarrow \varphi_3(z) = 0$;

$\varphi_4: \mathbb{C} \to \mathbb{R}$, такое что для $\forall\, z \in \mathbb{C} \Rightarrow \varphi_4(z) = 2$;

$\varphi_5: \mathbb{C} \to \mathbb{R}$, такое что для $\forall\, z \in \mathbb{C} \Rightarrow \varphi_5(z) = |z|^2$;

φ_6: $\mathbb{C} \to \mathbb{R}$, такое что для $\forall z \in \mathbb{C} \Rightarrow \varphi_6(z) = 2|z|$;

φ_7: $\mathbb{C} \to \mathbb{R}$, такое что для $\forall z \in \mathbb{C} \Rightarrow \varphi_7(z) = 1/|z|$;

Выяснить, какие из отображений φ_i являются гомоморфизмами.

Задача № 66. Пусть M – мультипликативное множество всех комплексных матриц порядка $n > 1$, а $\mathbb{C}$ – мультипликативное множество всех комплексных чисел. Определим отображения φ_1, φ_2, φ_3: $M \to \mathbb{C}$, полагая

$$\varphi_1(a) = det\ a,\ \varphi_2(a) = a_{11},\ \varphi_3(z) = 1.$$

Выяснить, какие из отображений являются гомоморфизмами.

Задача № 67. Доказать, что φ: $(M_1, *) \to (M_2, \bullet)$ является изоморфизмом мультипликативных множеств тогда и только тогда, когда между всеми элементами M_1 и всеми элементами M_2 можно установить такое взаимно однозначное соответствие при котором

$$x_1 \leftrightarrow x_2,\ y_1 \leftrightarrow y_2\ \ (x_1, y_1 \in M_1,\ x_2, y_2 \in M_2) \Leftrightarrow x_1 * y_1 \leftrightarrow x_2 \bullet y_2.$$

Задача № 68. Пусть φ – изоморфизм M_1 на M_2 мультипликативных множеств. Доказать, что обратное отображение φ^{-1} является изоморфизмом M_2 на M_1.

Задача № 69. Для мультипликативного множества всех целых чисел вида 5^n (n = 1, 2, 3, ...) найти все гомоморфизмы его в себя. Выяснить, какие их них являются изоморфизмами.

Задача № 70. Пусть φ: $(M_1, *) \to (M_2, \bullet)$ является гомоморфизм мультипликативных множеств. Пусть M_1 обладает каким либо из основных свойств: ассоциативностью, коммутативностью, обратимостью справа, обратимостью слева, наличием левых единиц, наличием правых единиц. Доказать, что тогда и M_2 будет обладать соответствующим свойством.

Задача № 71. Пусть φ_i: $(\mathbb{C}[x], \times) \to (\mathbb{C}, \times)$ – отображение множества всех ненулевых комплексных полиномов в множество всех комплексных чисел,

$$F = a_0 x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n \ (a_0 \neq 0).$$

Выяснить, какие из отображений φ_i будут гомоморфизмами:

$$а)\ \varphi_1(F) = a_0;\ б)\ \varphi_2(F) = a_0 + a_1 + \ldots + a_{n-1} + a_n;$$
$$в)\ \varphi_3(F) = a_0 + a_n;\ г)\ \varphi_4(F) = |a_n|;$$

Отображение группы в группу называется изоморфизмом, если оно взаимно однозначно и сохраняет операцию, если отказаться от требования взаимной однозначности, то приходим к понятию гомоморфизма групп. Две группы называются изоморфными, если между ними можно установить изоморфизм. Изоморфные объекты устроены одинаково в смысле операций, поэтому их в алгебре не различают или рассматривают как точные копии друг друга и изучают группы с точностью до изоморфизма. При гомоморфизме некоторые свойства алгебраической операции могут потеряться, например, некоммутативность, хотя наиболее памятные (конечность, коммутативность) сохраняются.

Примеры гомоморфных отображений

1) $\mathbb{Z} \to \mathbb{Z}_n$, сопоставляющее целому числу его вычет по модулю n;

2) $\mathbb{R}^* \to \mathbb{Z}^*$, сопоставляющее каждому числу из $\mathbb{R}^*$ его знак;

3) $GL(n, \mathbb{K}) \to \mathbb{K}^*$, сопоставляющее матрице ее определитель.

Задача № 72. Найти все изоморфизмы между группами

$$(\mathbb{Z}_4, +) \text{ и } (\mathbb{Z}_5^*, \cdot).$$

Решение.

Во-первых, выясним строение этих групп. Множество $\mathbb{Z}_4$ состоит четырех классов вычетов по модулю 4:

$$\mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$$

и является группой относительно операции умножения классов вычетов, класс $\bar{0}$ играет роль нейтрального элемента, элементы $\bar{0}$ и $\bar{2}$ имеют порядок 2, а элементы $\bar{1}$ и $\bar{3}$ имеют порядок 4.

Множество $\mathbb{Z}_5$ состоит из классов вычетов по модулю 5:

$$\mathbb{Z}_5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$$

и является группой относительно операции умножения классов вычетов. Роль нейтрального элемента играет класс $\bar{1}$, элементы $\bar{1}$ и $\bar{4}$ имеют порядок 2, а элементы $\bar{2}$ и $\bar{3}$ имеют порядок 4. Во-вторых, воспользуемся следующими фактами: при любом гомоморфизме групп нейтральный элемент переходит в нейтральный элемент, а элемент

порядка n переходит в элемент порядка n. Следовательно, возможны только два варианта изоморфизма:

$$\varphi_1: \begin{matrix} \bar{0} & \to & \bar{1} \\ \bar{1} & \to & \bar{1} \\ \bar{2} & \to & \bar{4} \\ \bar{3} & \to & \bar{3} \end{matrix}, \quad \varphi_2: \begin{matrix} \bar{0} & \to & \bar{1} \\ \bar{1} & \to & \bar{3} \\ \bar{2} & \to & \bar{4} \\ \bar{3} & \to & \bar{2} \end{matrix}.$$

Предложение. Пусть φ: $\mathbb{G} \to \mathbb{G}'$ – гомоморфизм групп. Тогда

1) Ядро гомоморфизма $Ker\ \varphi = \{\varphi^{-1}(e')\}$ является нормальной подгруппой в группе $\mathbb{G}$.

2) В этом случае полные прообразы элементов $\mathbb{G}'$ являются классами смежности по ядру гомоморфизма $Ker\ \varphi$ (доказать самостоятельно).

Теоремы о гомоморфизмах

Теорема *(Первая теорема о гомоморфизме).* Гомоморфный образ группы изоморфен ее факторгруппе по ядру гомоморфизма.

Теорема (*Вторая теорема о гомоморфизме или о* ***изоморфизме***).

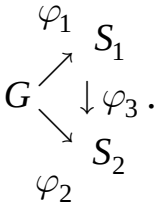
Пусть $\mathbb{H}, \mathbb{K} \leq \mathbb{G}$, $\mathbb{H} \trianglelefteq \mathbb{G}$. Тогда имеет место следующий изоморфизм

$$\mathbb{H} \cdot \mathbb{K} / \mathbb{H} \cong \mathbb{K} / \mathbb{K} \bigcap \mathbb{H}.$$

Теорема (*Третья теорема о гомоморфизме или* ***универсальность***).

Пусть φ_1: $\mathbb{G} \to S_1$ и φ_2: $\mathbb{G} \to S_2$ – эпиморфизмы групп, причем $Ker\ \varphi_2 \supseteq Ker\ \varphi_1$.

Тогда существует эпиморфизм φ_3: $S_1 \to S_2$: $\varphi_3\varphi_1 = \varphi_2$, т.е. коммутативна следующая диаграмма:



Задача № 73. Доказать существование следующих изоморфизмов:

1) $GL(n, \mathbb{K}) / SL(n, \mathbb{K}) \cong \mathbb{K}^*$;2) $S_n / A_n \cong \mathbb{Z}^* \cong \mathbb{Z}_2$;3) $\mathbb{Z} / (n) \cong \mathbb{Z}_n$.

Решение.

1) Рассмотрим отображение φ: $GL(n,\mathbb{K}) \to \mathbb{K}^*$, сопоставляющее матрице ее определитель. Это отображение является гомоморфизмом, так как $\varphi(AB) = det(AB) = det\,(A)\ det\,(B) = \varphi\,(A)\ \varphi(B)$.

Очевидно, что $Ker\ \varphi = SL(n, \mathbb{K})$, являющаяся нормальной подгруппой в $GL(n, \mathbb{K})$. Теперь осталось воспользоваться первой теоремой о гомоморфизме для получения требуемого изоморфизма.

Заметим, что классами смежности по ядру являются невырожденные матрицы, имеющие один и тот же определитель.

2) Рассмотрим отображение φ: $S_n \to \mathbb{Z}^* = \{\pm 1\}$, сопоставляющее подстановке ее знак в зависимости от четности. Так как четным подстановкам при этом гомоморфизме соответствует + 1, то $Ker\ \varphi = A_n$ и,

следовательно, по первой теореме о гомоморфизме имеет место требуемый гомоморфизм.

3) Для доказательства последнего изоморфизма нужно рассмотреть следующий гомоморфизм φ: $\mathbb{Z} \to \mathbb{Z}_n$, сопоставляющий целому числу его вычет по модулю n и вычислить ядро: $Ker\ \varphi = (n)$.

Задача № 74. Привести примеры плоских геометрических фигур, группы движения которых изоморфны: 1) $\mathbb{Z}_2$; 2) $\mathbb{Z}_3$; 3) S_3; 4) V_4.

Задача № 75. Какие из следующих групп изоморфны между собой:

1) группа движений квадрата D_4;

2) группа кватернионов $\mathbb{Q}_8$;

3) группа, состоящая из следующих элементов группы S_4:

$\{E,$ (13), (24), (12)(34), (13)(24), (14)(23), (1234), (1432)$\}$;

4) группа относительно умножения, состоящая из следующих матриц

$$\{\pm\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix},\pm\begin{pmatrix}i & 0\\ 0 & -i\end{pmatrix},\pm\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix},\pm\begin{pmatrix}0 & i\\ i & 0\end{pmatrix}\};$$

Задача № 76. Доказать, что группы собственных движений тетраэдра, куба и октаэдра изоморфны соответственно группам A_4, S_4, S_4.

Задача № 77. Найти в соответствующих группах S_n подгруппы, изоморфные группам: 1) $\mathbb{Z}_3$, 2) $\mathbb{Q}_8$, 3) D_4.

Задача № 78. Найти в соответствующих группах $GL(n, \mathbb{C})$ подгруппы, изоморфные группам: 1) $\mathbb{Z}_2$, 2) $\mathbb{Z}_3$, 3) S_3, 4) V_4.

Задача № 79. Найти в группе вещественных матриц порядка 4 подгруппу, изоморфную группе $\mathbb{Q}_8$.

Задача № 80. Разбить на классы попарно изоморфных друг другу групп следующий набор групп:

1) $SL(2, \mathbb{F}_2)$, 2) $SL(2, \mathbb{F}_3)$, 3) A_4, 4) A_5, 5) S_4, 6) S_5.

9. ДЕЙСТВИЕ ГРУПП НА МНОЖЕСТВАХ

Определение. Пусть Ω – некоторое множество, а $\mathbb{G}$ – группа и имеется отображение $\mathbb{G}\times\Omega \to \Omega$, удовлетворяющее свойствам:

1) $ex = x$, для любых $x \in \Omega$,
2) $(gh)\,x = g(h\,x)$, для любых $g, h \in \mathbb{G}$.

В этом случае говорят, что группа $\mathbb{G}$ действует на множестве Ω, а Ω является $\mathbb{G}$ – множеством.

Определение. Две точки x, $x' \in \Omega$ называются эквивалентными относительно группы $\mathbb{G}$, действующей на множестве Ω, если существует $g \in \mathbb{G}$ такой, что $x' = g\,x$.

Определение 2 задает «отношение эквивалентности», разбивающее множество Ω на классы. Эти классы называются $\mathbb{G}$–орбитами.

Орбиту, содержащую элемент $x_0 \in \Omega$ обозначают через $G(x_0)$ и $G(x_0) = \{g(x_0)$: для любых $g \in \mathbb{G}\} \subseteq \Omega$.

Задача № 81. Доказать, что орбиты любых двух точек либо совпадают, либо не пересекаются.

Определение. Зафиксируем любую точку $x_0 \in \Omega$. Подмножество вида

$$St(x_0)=\{g\in \mathbb{G}: g(x_0)=x_0\}$$

называется *стабилизатором*.

Задача № 82. Доказать, что стабилизатор элемента группы $St(x_0)$ является подгруппой в этой группе.

Эта подгруппа называется *стационарной*.

Теорема (*о длине орбиты*). Длина орбиты относительно конечной группы является делителем порядка этой группы.

Теорема (*о сопряженности стационарных подгрупп*). Пусть группа $\mathbb{G}$ действует на множестве. Если две точки x_0 и x_0' лежат на одной орбите, то их стационарные подгруппы сопряжены, т.е. если $x_0' = g\, x_0$ для некоторого $g \in \mathbb{G}$, то выполняется

$$St\,(x_0') = g\, St\,(x_0)\, g^{-1}.$$

Если $\mathbb{G}$ – конечная группа, и $\mathbf{\Omega} = \mathbf{\Omega}_1 \cup \mathbf{\Omega}_2 \cup \ldots \cup \mathbf{\Omega}_r$ конечное разбиение на орбиты с представителями $x_1, x_2, \ldots, x_r$, то

$$\left| \mathbf{\Omega} \right| = \sum_{i=1}^{r} \left| G : St(x_i) \right|.$$

Примеры действия групп на множествах

1. Пусть $\mathbf{\Omega} = \mathbb{G}$. Тогда для любого $x \in \mathbb{G}$ действие группы можно определить как $x \rightarrowtail g^{-1}\, x\, g$. Это действие называется сопряжением или трансформированием. Для него $G(x)$ – класс сопряженных элементов, а

$St(x)$ – централизатор элемента x. Действие сопряжением очевидным образом переносится на подгруппы.

Две подгруппы $\mathbb{H}_1$ и $\mathbb{H}_2$ сопряжены, если $\mathbb{H}_1 = g^{-1}\,\mathbb{H}_2\,g$, для некоторого $g \in \mathbb{G}$. Для подгруппы $\mathbb{H}$ в $\mathbb{G}$ очевидно, роль стабилизатора играет нормализатор и имеет вид

$$N(\mathbb{H}) = St(\mathbb{H}) = \{g \in \mathbb{G}: g\,\mathbb{H}\,g^{-1} = \mathbb{H}\}.$$

В частности, для нормальной подгруппы $\mathbb{H}$ группы $\mathbb{G}$, т.е. $\mathbb{H} \trianglelefteq \mathbb{G}$, верно $N(\mathbb{H}) = St(\mathbb{H}) = \mathbb{G}$. Длина орбиты $\mathbb{H}^{\mathbb{G}}$, т.е. число подгрупп, сопряженных с $\mathbb{H}$ в группе $\mathbb{G}$ равно индексу нормализатора $\mathbb{H}$ в группе $\mathbb{G}$, т.е. $(\mathbb{G}: N(\mathbb{H}))$ или кратко $\text{card}(\mathbb{H}^{\mathbb{G}}) = |\mathbb{G} : N(\mathbb{H})|$.

Пусть теперь $\mathbb{G}$ - конечная группа и $x_1^G,...,x_q^G,...,x_r^G$ - ее классы сопряженных элементов, первые q которых одноэлементные, т.е.

$$x_1^G,...,x_q^G:\ x_i^G = \{x_i\}, i = 1,...,q, x_1 = e.$$

Т.к. центр группы по определению это множество всех перестановочных элементов, то $Z = Z(\mathbb{G}) = \{x_1,...,x_q\}$ и для длин орбит верно, что $\left|x_i^G\right| = (\mathbb{G}:C(x_i))$, где $C(x_i)$ – централизатор x_i в группе $\mathbb{G}$, то для порядка группы выполняется равенство

$$|\mathbb{G}| = |Z(\mathbb{G})| + \sum_{i=q+1}^{r} (\mathbb{G}:C(x_i)).$$

2. Пусть, как и раньше $\Omega = \mathbb{G}$. Тогда для любого $x \in \mathbb{G}$ действие группы можно определить как L_a: $x \longmapsto a\,g$. Это действие называется левым сдвигом. Аналогично определяется правый сдвиг как R_a: $x \longmapsto g\,a$.

Задача № 83. Опишите орбиты и стабилизаторы следующих действий:

1) действие G на себе левыми сдвигами: $(g, x) \to gx$;

2) действие G на себе правыми сдвигами$(g, x) \to xg^{-1}$;

3) действие подгруппы H группы G на группе G левыми (соответственно правыми) сдвигами.

Задача № 84. Доказать, что правило $g*x = gx$ задает действие группы $GL(\mathrm{R}, n)$ на множестве R^n, где gx означает обычное умножение матрицы $g \in GL(\mathrm{R}, n)$ на столбец $x \in R^n$. Описать орбиты всех элементов из R^n.

Задача № 85. *Лемма Бернсайда.* Множество

$$\mathrm{Fix}(g) = \{ x \in X : g * x = x\}$$

называется *множеством неподвижных точек* элемента g из группы G. Доказать, что число различных орбит, получающихся при действии конечной группы G на множестве X, равно

$$r_G(X) = \frac{1}{|G|}\sum_{g \in G} \left|Fix(g)\right|.$$

Применение действия групп на множествах к конечным p-группам

Определение. Конечная группа порядка $p^n > 1$, где p – простое число называется конечной p – группой.

Задача № 86. *Теорема* (*о центре конечной p-группы*). Доказать, что всякая конечная p – группа обладает нетривиальным центром.

Задача № 87. *Теорема Коши.* Доказать, что если порядок конечной группы G делится на простое число p, то G содержит элемент порядка p.

Задача № 88. Доказать, что группа порядка p^2, где p – простое число, абелева и изоморфна либо $\mathbb{Z}_{p^2}$, либо $\mathbb{Z}_p \times \mathbb{Z}_p$.

Задача № 89. Доказать, что если группа G неабелева и $|G| = p^3$, где p – простое число, то $|Z(G)| = p$.

Задача № 90. Доказать, что подгруппа, индекс которой есть наименьший простой делитель порядка группы, является нормальным делителем. Привести доказательство, использующее действие групп.

10. ТЕОРЕМЫ СИЛОВА

В теории групп теоремы Си́лова (1872 г.) представляют собой неполный вариант обратной теоремы к теореме Лагранжа и для некоторых делителей порядка группы $\mathbb{G}$ гарантируют существование подгрупп такого порядка. Среди многих теорем о конечных группах, выводящих глубокие свойства этих групп из арифметических свойств их порядков, одними из важнейших являются теоремы Силова.

Ложность обращения теоремы Лагранжа

Согласно теореме Лагранжа, порядок подгруппы конечной группы является делителем порядка группы. Обратное, вообще говоря, не верно, т.е если $|\mathbb{G}| = n$, n делится на m, то подгруппы порядка m может и не существовать. Например, знакопеременная группа A_4, имеющая порядок 12, не имеет подгруппы шестого порядка. Это «минимальный» пример.

Однако, если $m = p$ – простое число или его степень, то такая подгруппа точно существует.

Определение. Пусть $|\mathbb{G}| = p^n m$, где p – простое число, $m \in \mathbb{Z}$, $(p, m) = 1$. Подгруппа P порядка $p^n > 1$, т.е. $|P| = p^n$, если она существует, называется силовской p – подгруппой группы $\mathbb{G}$.

Теорема 1 (***существование***). Силовские p – подгруппы существуют.

Теорема 2 (***сопряженность***). Пусть P и P_1 две силовские p – подгруппы в группе $\mathbb{G}$. Тогда существует элемент $a \in \mathbb{G}$, что $P_1 = aPa^{-1}$.

Теорема 3 (***количество*** *силовских p-подгрупп*). Для числа N_p всех силовских p – подгрупп имеет место равенство $N_p = (\mathbb{G} : N(P))$ и сравнение $N_p \equiv 1(\mathrm{mod}\ p)$.

Следствие. Всякая p-подгруппа содержится в некоторой силовской p-подгруппе.

Задача № 91. Опишите силовские подгруппы в следующих группах:
1)в конечных абелевых группах, 2) S_3, 3) A_4, 4) S_4, 5) D_5, 6) D_6.

Решение.

1) Пусть $\mathbb{G}$ – конечная абелева группа. Для каждого простого делителя p числа $|\mathbb{G}|$ имеется ровно одна силовская p – подгруппа; она состоит в точности из всех p – элементов группы $\mathbb{G}$;

2) $|S_3| = 2 \cdot 3$; в S_3 три силовские 2-подгруппы (каждая порождена транспозицией) и одна силовская 3-подгруппа (именно, A_3);

3) $|A_4| = 2^2 \cdot 3$; в A_4 одна силовская 2-подгруппа

$$\{e, (12)(34), (13)(24), (14)(23)\} \cong \mathbb{Z}(2) \times \mathbb{Z}(2)$$

и четыре силовские 3-подгруппы (каждая порождена циклом длины 3);

4) $|S_4| = 2^3 \cdot 3$; в S_4 три силовские 2-подгруппы (каждая изоморфна D_4; при интерпретации S_4 как группы вращений куба каждая силовская 2-подгруппа состоит из вращений, оставляющих на месте пару

параллельных граней куба) и четыре силовские 3-подгруппы (каждая порождена циклом длины 3);

5) $|D_5| = 2 \cdot 5$; в D_5 пять силовских 2-подгрупп (каждая порождена отражением) и одна силовская 5-подгруппа (именно, подгруппа вращений);

6) $|D_6| = 2^2 \cdot 3$; в D_6 три силовские 2-подгруппы (каждая изоморфна $\mathbb{Z}(2)\times\mathbb{Z}(2)$ и является группой симметрий одного из трех описанных вокруг правильного шестиугольника ромбов) и одна силовская 3-подгруппа (именно, группа вращений любого из двух вписанных в правильный 6-угольник правильных треугольников).

Задача № 92.

1) Доказать, что группа порядка 196 содержит нормальную подгруппу;
2) Доказать, что существует только две неизоморфные группы из 6 элементов циклическая $\mathbb{Z}_6$ и симметрическая S_3;
3) Показать, что каждая группа порядка 15 циклическая;
4) Доказать, что среди простых групп нет групп порядка 12, 28, 56;
5) Доказать, что $UT_n(p)$ является силовской p-подгруппой группы $GL_n(p)$;
6) Доказать, что все силовские подгруппы группы порядка 100 коммутативны;
7) Доказать, что любая группа порядка 15 коммутативна;
8) Доказать, что любая группа порядка 35 коммутативна;
9) Доказать, что любая группа порядка 185 коммутативна;
10) Сколько различных силовских 2-подгрупп и силовских 5-подгрупп в некоммутативной группе порядка 20?

Задача № 93. Докажите, что силовские подгруппы в следующих группах в группе нормальны, то сама группа изоморфна их прямому произведению.

Задача № 94. Докажите, что если порядок группы равен 15, 35 или 1001, сама группа циклична.

Задача № 95. Докажите, что если порядок группы равен 56, 80, 196 или 200, то эта группа содержит силовскую подгруппу (в частности, не является простой).

Решение. Докажем это, если порядок группы равен $|\mathbb{G}| = 56 = 2^3 \cdot 7$.

Для этого достаточно доказать, что силовская 2 – подгруппа или силовская 7 – подгруппа единственна. По 3-й теореме Силова, число силовских 2 – подгрупп равно 1 или 7, число силовских 7 – подгрупп равно 1 или 8. Пусть группа содержит 8 силовских 7 – подгрупп. Поскольку все они - порядка 7 (7 – простое число), то их объединение содержит $1+6 \cdot 8 = 49$ элементов. Отсюда следует, что силовская 2 – подгруппа единственна.

Задача № 96. Докажите, что если порядок группы равен $|\mathbb{G}| = p^2 \cdot q$, где p и q различные простые числа, группа $\mathbb{G}$ содержит нормальную силовскую подгруппу (в частности, не является простой).

Решение. Достаточно доказать, что силовская p – подгруппа или силовская q – подгруппа единственна. Предположим, что силовская p – подгруппа неединственна. Тогда по 3-й теореме Силова, их число равно q,

причем $q \equiv 1(\mathrm{mod}\ p)$. В частности, $p > q$. Но тогда $q \not\equiv 1(\mathrm{mod}\ p)$, т.е. число всех силовских q – подгрупп не может равняться p. Если и силовская q – подгруппа неединственна, то число силовских q – подгрупп равно p^2. Это значит, что $p^2 \equiv 1(\mathrm{mod}\ q)$, откуда $p \equiv -1(\mathrm{mod}\ q)$, т.е. $p = q-1$. Итак, $p = 2$, $q = 3$. Далее можно рассуждать аналогично решению предыдущей задачи.

Задача № 97. Докажите что любая группа порядка 6 изоморфна группе $\mathbb{Z}_6$ или группе S_3.

Решение. Пусть $\mathbb{G}$ – группа порядка 6, H – ее силовская 2-подгруппа, F – ее силовская 3-подгруппа. Очевидно, что F – нормальная подгруппа группы $\mathbb{G}$: $F \trianglelefteq \mathbb{G}$.

Если $H \trianglelefteq \mathbb{G}$, то $\mathbb{G} \cong H \times F \cong \mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6$.

Если $H \not\trianglelefteq \mathbb{G}$, то $\bigcap_{x \in G} xHx^{-1} = \{1\}$ и по теореме Кэли $\mathbb{G} \cong S_3$.

ВОПРОСЫ К ЭКЗАМЕНУ

Элементы теории групп

1. Определение группы. Левые, правые единицы и обратные
2. Симметрическая и знакопеременная группы
3. Примеры групп.
4. Классические линейные группы
5. Циклические группы
6. Подгруппы. Необходимое и достаточное условие подгруппы
7. Циклические подгруппы. Примеры подгрупп
8. Классические группы малых размерностей
9. Группа корней из единицы, первообразные корни
10. Описание подгрупповой структуры групп S_3, S_4, A_3 , A_4 , V_4 , D_4
11. Классы сопряженных элементов в симметрических группах и их подгруппах
12. Теорема Кэли.
13. Порождающие множества $GL(\mathrm{n} , \mathbb{K})$, $SL(\mathrm{n} , \mathbb{K})$, S_n, A_n
14. Конечные и бесконечные циклические группы
15. Теоремы о классах смежности.
16. Теорема Лагранжа и ее следствия
17. Нормализатор и централизатор.
18. Теорема о числе множеств, сопряженных данному
19. Нормальные подгруппы.
20. Фактор-группа
21. Гомоморфизмы и изоморфизмы.
22. Предложение о ядре гомоморфизма и полных прообразах.
23. Теоремы о гомоморфизмах
24. Эндоморфизмы и автоморфизмы.
25. Внутренние автоморфизмы

26. Центр и коммутант.
27. Фактор-группа по коммутанту
28. Действие групп на множествах.
29. Отношение эквивалентности. Стационарные подгруппы.
30. Длина орбиты. Сопряженность стационарных подгрупп
31. Примеры действия групп
32. Центр конечной p-группы
33. Ложность обращения теоремы Лагранжа.
34. Теоремы Силова
35. Внешнее прямое произведение.
36. Разложение группы в прямое произведение подгрупп
37. Следствие теорем Силова для разложения в прямое произведение подгрупп