Федеральное агентство по образованию
ГОУ ВПО «Горно-Алтайский государственный университет»
Кафедра алгебры, геометрии
и методики преподавания математики

АЛГЕБРА
(общая алгебра)

Учебно-методический комплекс

Для студентов-бакалавров, обучающихся по направлению
010100 Математика

Горно-Алтайск
РИО Горно-Алтайского госуниверситета
2009

Печатается по решению редакционно-издательского совета
Горно-Алтайского государственного университета

УДК 512.57
ББК 22.14
П88

Алгебра (общая алгебра): учебно-методический комплекс (для студентов-бакалавров, обучающихся по направлению 010100 Математика) / Горно-Алтайск: РИО ГАГУ, 2009. – 100 с.

Составители:
Пуркина В.Ф., кандидат педагогических наук,
доцент кафедры алгебры, геометрии и МПМ
Горно-Алтайского государственного университета
Кайгородов Е. В., ст. лаборант
кафедры алгебры, геометрии и МПМ
Горно-Алтайского государственного университета
Рецензенты:
Кириченко Т. Ф., кандидат педагогических наук, доцент
кафедры алгебры и МПМ Санкт-Петербургского
государственного педагогического университета
им. А. И. Герцена
Деев М. Е., кандидат физико-математических наук, доцент
кафедры алгебры, геометрии и МПМ
Горно-Алтайского государственного университета

Пособие содержит учебно-методические материалы по дисциплине «Алгебра» для студентов дневного отделения физико-математического факультета I курса по направлению «010100 Математика» и рассчитано на 1 семестр. Дисциплина «Алгебра» является общепрофессиональной дисциплиной федерального компонента ОПД Ф.02 для данного контингента студентов.

ОГЛАВЛЕНИЕ

1. КВАЛИФИКАЦИОННАЯ ХАРАКТЕРИСТИКА БАКАЛАВРА

Бакалавр математики подготовлен к выполнению деятельности в областях, использующих математические методы и компьютерные технологии; созданию и использованию математических моделей процессов и объектов; разработке эффективных математических методов решения задач естествознания, техники, экономики и управления; программно-управленческому обеспечению научно-исследовательской, проектно-конструкторской и эксплуатациионно-управленческой деятельности.

Объектами профессиональной деятельности бакалавра математики являются научно-исследовательские центры, органы

управления, образовательные учреждения, промышленное производство. Исходя из своих квалификационных возможностей, выпускник по направлению 010100 Математика может занимать должности: математик, инженер-программист (программист) и др. в соответствии с требованиями Квалификационного справочника должностей руководителей, бакалавров и других служащих, утвержденного постановлением Минтруда России от 21.08.98 № 37.

2. НАБОР КОМПЕТЕНЦИЙ БАКАЛАВРА

После изучения курса «Алгебра» студенты должны:

- овладеть основными методами современной алгебры;
- приобрести опыт использования алгебраических методов в процессе решения задач смежных математических дисциплин (геометрии, мат. анализа и т. д.)
- получить представление о роли алгебры в системе математического знания и перспективах ее применения в естественных и гуманитарных науках.

3. РАБОЧАЯ ПРОГРАММА

Дисциплина «Алгебра» является общепрофессиональной дисциплиной федерального компонента. Данное учебно-методическое пособие предназначено для студентов первого курса дневных отделений физико-математических факультетов по направлению «010100 Математика» и рассчитано на один семестр.

3.1. Цели и задачи дисциплины

1) Познакомить студентов 1 курса с основными понятиями и методами современной алгебры;
2) Научить применять их в процессе решения различных задач;
3) Раскрыть роль современной алгебры в системе математического знания;

4) Сформировать у студентов алгебраическую составляющую математической культуры.

3.2. Обязательные требования к минимуму содержания дисциплины

Циклические группы. Разложение группы G по подгруппе H. Нормальные подгруппы. Фактор-группа. Морфизмы групп. Действие группы на множествах, представления групп. Теоретико-групповые конструкции. Внешнее и внутреннее прямое произведение групп. Коммутант, центр группы.

Кольца, области целостности, идеалы. Кольца главных идеалов. Отношение делимости в кольцах главных идеалов. Гомоморфизмы и идеалы колец, поля частных.

3.3. Распределение часов

Семестр	Учебные занятия						Контроль
	Общий объем	В том числе				Самост. работа	
		аудиторные					
		всего	из них				
			лекции	практич.	лабор.		
3	102	72	36	36	-	30	зач экз

3.4. Технологическая карта учебного курса «Алгебра»

№ п/п	Темы	Всего часов	Аудиторные занятия		Самост. занятия
			лекции	практ.	
Модуль 1					
1	Введение в теорию групп	42	16	16	10

Модуль 2					
2	Введение в теорию колец	30	10	10	10
Модуль 3					
3	Введение в теорию полей	30	10	10	10

3.5.Содержание дисциплины

Введение в теорию групп

Группа, подгруппа, примеры. Циклические группы. Разложение группы G по подгруппе H. Нормальные подгруппы. Фактор-группа. Морфизмы групп. Действие группы на множествах, представления групп. Теоретико-групповые конструкции. Прямое произведение групп. Коммутант, центр группы.

Введение в теорию колец

Типы колец. Евклидовы кольца, факториальные кольца. Области целостности, кольца главных идеалов. Отношение делимости в кольцах главных идеалов, его свойства. Гомоморфизмы и изоморфизмы колец, поля частных.

3.5.1. Лекционный курс — 36 часов

Лекция №1

Группы, подгруппы, примеры.

Лекция №2

Группа подстановок и ее подгруппы.

Лекция №3

Циклические группы. Теоремы о циклических группах.

Лекция №4

Разложение группы по подгруппе. Теорема Лагранжа и следствия из нее.

Лекция №5

Нормальные делители и их свойства.

Лекция №6

Фактор-группа и ее свойства.

Лекция №7

Морфизмы групп. Примеры.

Лекция №8

Теоретико-групповые конструкции.

Лекция №9

Групповое замыкание.

Лекция №10

Коммутант. Центр группы.

Лекция №11

Прямое произведение групп (внутреннее и внешнее).

Лекция №12

Действие группы на множестве. Примеры.

Лекция №13

Определение кольца и примеры колец.

Лекция №14

Евклидовы кольца. Примеры.

Лекция №15

Отношение делимости в областях целостности. Идеалы колец. Кольца главных идеалов.

Лекция №16

Отношение делимости в кольцах главных идеалов.

Лекция №17

Определение и примеры полей.

Лекция №18

Гомоморфизмы колец и полей. Поля частных.

3.5.2. Практические занятия — 36 часов

Практические занятия №1

Операции на множествах, их свойства.

Практические занятия №2

Группа, подгруппа, примеры.

Практические занятия №3

Вычисление порядка элемента в различных группах.

Практические занятия №4

Циклические группы.

Практические занятия №5

Разложение группы по подгруппе. Смежные классы.

Практические занятия №6

Факторгруппа и ее свойства. Нормальные делители.

Практическое занятие №7

Изоморфизмы групп.

Практическое занятие №8

Морфизмы групп.

Практическое занятие №9

Коммутатор и коммутант группы.

Практические занятия №10

Центр группы.

Практическое занятие №11.

Кольцо. Примеры колец.

Практическое занятие №12

Подкольца, поля, примеры.

Практическое занятие №13

Области целостности и их свойства.

Практические занятия №14

Кольца главных идеалов.

Практические занятия №15

Гомоморфизмы колец и полей.

Практическое занятие №16

Факторкольца и их свойства.

Практические занятия №17

Идеалы колец. Поля частных.

Практическое занятие №18

Контрольная работа.

3.5.3. Самостоятельная работа студентов — 30 часов

Самостоятельная работа студентов рассматривается как вид учебного труда, позволяющий целенаправленно формировать и развивать самостоятельность студента как личностное качество при выполнении различных видов заданий и проработке дополнительного учебного материала.

Для успешного выполнения расчетных заданий, написания рефератов и подготовки к коллоквиуму, помимо материалов лекционных и практических занятий, необходимо использовать основную и дополнительную литературу, указанную на стр. 95 настоящего пособия.

№	Темы	Кол-во часов	Формы отчетности	Сроки
1	Свойства и строение абелевых групп	10	Коллоквиум	март
2	Гиперкомплексные числа.	10	Реферат	апрель
3	Классификация линейных операторов.	10	Реферат	май

3.5.4. Темы курсовых работ

1. Функции от матриц.
2. Нормы векторов и матриц.
3. Абелевы группы.
4. Конечные группы.
5. Свободные группы и многообразия.
6. Нильпотентные группы.
7. Классификация линейных операторов.
8. Кватернионы.
9. Измерения в линейном пространстве.
10. Метрические свойства линейного оператора.

4. ВОПРОСЫ К ЭКЗАМЕНУ

1. Различные определения понятия «группа», их эквивалентность. Примеры групп.
2. Подгруппа, достаточные условия подгруппы. Примеры подгрупп.
3. Группа подстановок на множестве M = {1, 2, …, n}, ее подгруппы. Разложение подстановок в независимые циклы и транспозиции.

4. Циклические группы. Примеры.
5. Теорема о циклических группах.
6. Порядок элемента, его связь с порядком циклической группы G_a.
7. Разложение группы G по подгруппе H.
8. Теорема Лагранжа и ее следствие.
9. Нормальные подгруппы группы G, их свойства, примеры.
10. Фактор-группа, ее свойства, примеры фактор-групп.
11. Морфизмы групп, свойства, примеры.
12. Ядро и образ гомоморфизма, их связь с нормальными подгруппами.
13. Теорема о гомоморфизмах.
14. Теорема Кэли.
15. Действие группы G на множестве. Представление (реализация) группы G в группе S (M). Примеры.
16. Минимальная подгруппа, групповое замыкание.
17. G-орбиты элементов, стационарные подгруппы, примеры.
18. Коммутатор, коммутант группы G, его свойства.
19. Центр группы, его свойства.
20. Прямое произведение групп.
21. Необходимые и достаточные условия изоморфизма группы G и прямого произведения двух групп ($A \times B$).
22. Определение кольца и поля. Примеры.
23. Кольца главных идеалов. Примеры.
24. Отношение делимости в кольцах главных идеалов.
25. Гомоморфизмы и идеалы колец, поля частных.

5. ЛЕКЦИИ ПО АЛГЕБРЕ

ГЛАВА 1. Введение в теорию групп.

Основные знания, умения и навыки, которыми должны овладеть студенты в процессе изучения данной темы:

- знать различные определения понятия «группа» и уметь доказывать их эквивалентность;
- уметь доказывать, что заданное множество является группой (подгруппой), относительно указанной бинарной операции; знать определение порядка элемента в группе и уметь его находить;
- уметь строить подгруппы в заданной группе;
- понимать структуру циклических групп;
- уметь раскладывать группу по ее подгруппе, строить фактор-группы;
- знать различные типы гомоморфизмов групп, уметь доказывать, что заданные группы изоморфны (неизоморфны);
- знать определения ядра и образа заданного гомоморфизма и уметь их находить;
- знать основные теоремы о гомоморфизмах групп;
- уметь строить теоретико–групповые конструкции (коммутант, центр группы, прямое произведение групп).

§ 1. Группа, подгруппа. Примеры.

Понятие «группа» является частным случаем понятия «универсальная алгебра». Напомним основные понятия, которые с ней связаны.

Определение 1: *Пусть A - непустое множество, и $\{ f_i \ i \in I\}$ - множество n - арных операций f_i, заданных на A. Упорядоченную пару $< A,\{f_i / i \in I \}>$ называют универсальной алгеброй с множеством операций $\{f_i / i \in I \}$, а множество A - основным множеством или носителем алгебры. Пишут, $<A,\{ f_i \}>$.*

Замечание 1. Хотя понятия алгебра $<A,\{ f_i \}>$ и множество A различны, в том случае, когда ясно, какие операции заданы на A, говорят просто - алгебра A, то есть алгебру отождествляют с ее носителем.

Замечание 2: В том случае, когда множество операций $\{f_i / i \in I \}$ в универсальной алгебре A - конечно, его задают перечислением элементов $\{ f_1 f_2,...,f_k \}$ и в записи алгебры опускают фигурные скобки, то есть пишут, $<A,f_1 f_2,...,f_k>$.

Определение 2: *Алгебры* $<A, \{ f_i \}>$ *и* $<B, \{g_i\}>$ *называются однотипными, если существует биективное отображение множества* $\{ f_i \}$ *на множество* $\{ g_i \}$, *при котором соответственные операции* f_i *и* g_i *имеют один и тот же ранг.*

В случае, если множества операций, заданных на A и B - конечны, определение однотипных алгебр можно сформулировать так.

Определение 2': *Алгебры* $<A, f_1 f_2,...,f_k>$ *и* $<B, g_1, g_2.....g_m>$ *называются однотипными, если число их операций одинаково* $(k=m)$ *и эти операции можно упорядочить так, что* f_i *и* g_i $(i=1, 2,..., к)$ *будут иметь одинаковые ранги.*

Пример 1: Алгебры $<Q, +, \cdot >$ и $<C, \cdot , ->$ являются однотипными, а алгебры $<Z,+, \cdot >$ и $<R , + , \cdot ,1>$ однотипными не являются, так как число операций, заданных на Z и R различно.

Пример 2: Алгебры $<N, + , \cdot >$ и $<Z, - ,1 >$ разнотипны, так как на N обе операции бинарные, а на Z операция вычитания - бинарная, а операция фиксации единицы - нуль-арная.

Определение *3 Гомоморфизмом алгебры* $<A, \{ f_i \}>$ *в однотипную ей алгебру* $<B, \{g_i\}>$ *называется отображение* $\varphi: A \rightarrow B$ *такое, что при каждом* $i \in I$ *выполняется условие гомоморфности:*

$\forall\, i \in I, \forall a_1, ..., a_n \in A, \varphi(f_i(a_1, ..., a_n)) = g_i(\varphi(a_1),..., \varphi(a_n))$

Говорят также, что отображение φ сохраняет все операции, заданные на множестве A.

Определение 4 *Алгебры A и B называются гомоморфными алгебрами, если существует гомоморфизм* φ *алгебры A в алгебру B. Пишут* $\varphi: A \rightarrow B$ *- гомоморфизм.*

Пример 3: Отображение $lg: R^+ \rightarrow R$ является гомоморфизмом алгебры $< R^+, \cdot ,:>$ в алгебру <R,+,->, так как $\forall\, a,b \in R^+$,

lg $(ab)=lg$ a+lg b, то есть образ произведения двух элементов равен сумме образов;

lg (a:b)=lg a - lg b - образ частного двух элементов равен разности образов.

В зависимости от свойств отображений определяются различные виды гомоморфизмов.

Определение *5: Гомоморфизм φ: A—>B алгебры A алгебру B называется:*

а) *мономорфизмом* (или вложением *A* в *B),* если отображение φ - инъективно;

б) *эпиморфизмом* (наложением *A* на *B),* если отображение φ – сюръективно;

в) *изоморфизмом,* если отображение φ - биективно.

Если алгебра *A* изморфна алгебре *B,* то **пишут** $A \cong B$.

Определение 6: *Гомоморфизм* φ: *A —>A на себя называется:*

а) *эндоморфизмом, если* отображение φ - инъективно;

б) *автоморфизмом,* если отображение φ - биективно.

Все алгебры можно классифицировать с точки зрения свойств операций, заданных на множествах - носителях. Эта классификация позволяет выделить из множества алгебр алгебры определенного рода - **группоиды, полугруппы, моноиды, группы, кольца, поля** и т.д. Понятие изоморфизма алгебр дает возможность собрать в один класс алгебры определенного рода, которые будут одинаковы, с точностью до изоморфизма.

Определение *7: Алгебра <A, *>* с *одной бинарной операцией называется группоидом*

Например, <N, •>, <Z,+>, <*Q\{0},:*> - группоиды, а <*N,+,* •>, <*N,-*>, <*Z,:*>, <*Q,* √> - не являются группоидами.

Определение 8: *Полугруппой называется алгебра <A,*> с бинарной ассоциативной операцией:*

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

Можно сказать, что полугруппа - это ассоциативный группоид.

Например, <*N,* •>, <*Z,+*>, <*Q,* +> - полугруппы, так как это алгебры и операции сложения и умножения на множества *N, Z, Q* - ассоциативны. Алгебры <Z,->, <*Q\{0},:*> не являются полугруппами.

Определение 9: *Моноидом называется алгебра <A,*>, бинарная операция которой удовлетворяет условиям:*

1) $\forall a,b,c \in A, (a*b)*c = a*(b*c)$ - операция ассоциативна,

2) $\exists\ e \in A \mid \forall\ a \in A,\ e*a=a*e=a$ - существует нейтральный элемент, можно сказать, что моноид - это полугруппа с нейтральным элементом.

Например, <Z, •> является моноидом, так как e = 1, 1 ∈ Z, а <*N*,+> не является моноидом, так как e = 0, 0 ∉ N.

Определение 10: Группой <G,*> *называется алгебра, бинарная операция которой удовлетворяет условиям, называемым также аксиомами группы:*

A_1: $\forall\ a, b, c \in G,\ (a*b)*c = a*(b*c)$ (ассоциативность);

A_2: $\exists\ e \in G \mid \forall\ a \in G,\ e*a=a*e=a$ (существование нейтрального элемента);

A_3: $\forall\ a \in G,\ \exists\ a' \in G \mid a*a'=a'*a=e$ (симметризуемость каждого элемента).

Из определения видно, что любая группа является полугруппой и моноидом. Можно сказать, что группа это моноид, каждый элемент которого имеет симметричный элемент.

Определение 11: *Группа <G,*> называется коммутативной (или абелевой), если операция * коммутативна, то есть выполняется аксиома:*

A_4: $\forall\ a, b \in G,\ a*b=b*a$ (коммутативность).

(Абель Нильс Хенрик < 1802-1829 > - норвежский математик).

В некоторых случаях удобно использовать другое определение группы.

Определение 12: Алгебра <G, *> *с бинарной операцией * называется группой, если выполняются следующие условия:*

а) $\forall\ a, b, c \in G,\ (a*b)*c = a*(b*c)$

б) $\forall\ a, b \in G$ каждое из уравнений $a*x=b$ *и* $y*a=b$ имеет хотя бы одно решение.

Первое определение группы более удобно для проверки следующего факта - будет ли данная алгебра группой. Второе определение характеризует группу как алгебру, в которой разрешимы уравнения первой степени. Докажите, что *определения 11* и *12* равносильны.

Существование нескольких подходов к определению понятия «группа» связано с тем, что это понятие формировалось

в различных разделах математики на протяжении ста лет. От Лагранжа, стихийно применявшего группы подстановок для решения алгебраических уравнений в радикалах (1771г.), через работы Руффини (1799г.) и Абеля (1824г.) к Эвариcту Галуа (1830г.), в исследованиях которого впервые введен термин «группа» - вот путь развития этого понятия в алгебре. Совершенно независимо от алгебры, понятие «группа» формировалось в геометрии и теории чисел. Когда в XIX веке встал вопрос о классификации различных геометрий, то в ее основу было положено понятие группы преобразований. Теория групп как самостоятельная область математики окончательно сформировалась с выходом книги О.Ю. Шмидта «Абстрактная теория групп» (1916 г.)

В настоящее время теория групп является одной из самых развитых областей алгебры, которая имеет многочисленные применения как в самой математике, так и в других науках (топологии, теории функций, квантовой механике, кристаллографии и т.д.).

Основная задача теории групп - изучение всевозможных групп с точностью до изоморфизма.

В определении 10 заложен алгоритм решения всех задач, связанных с выяснением вопроса - будет ли данная алгебра группой?

Для доказательства того, что множество A с операцией * является группой, нужно:

Во-первых, показать, что операция * является бинарной операцией на множестве A, то есть выполнимой и однозначной операцией ранга 2 на A.

Во-вторых, проверить выполнимость аксиом A_1, A_2, A_3 группы для алгебры $<A,*>$, Если первое из этих условий не выполнятся, то нет смысла в проверке аксиом. Рассмотрим примеры групп, которые представляют различные разделы математики.

Пример 1. Мы уже отмечали, что исторически теория групп возникла из теории групп подстановок. Рассмотрим этот класс групп. Пусть дано конечное множество элементов $M = \{1,2,3,\ldots,n\}$.

Определение: *Биекция* $\varphi: M \to M$ *называется подстановкой.*

Обозначается: $\varphi = \begin{pmatrix} 1 & 2 & \dots & n \\ \varphi(1) & \varphi(2) & \dots & \varphi(n) \end{pmatrix}$

Самостоятельно докажите, что на конечном множестве из n-элементов можно задать n! различных подстановок {биекций}.

Пусть множество $S_n \overset{df}{=} \left\{ \varphi \mid \varphi = \begin{pmatrix} 1 & \dots & n \\ \varphi(1) & \dots & \varphi(n) \end{pmatrix} \right\}$

Зададим на множестве S_n операцию композиции подстановок - $\varphi^\circ\psi$. $\forall\, x \in M\ \ x(\varphi^\circ\psi) \overset{df}{=} (x\varphi)\psi$

***Теорема** 1:* $< S_n, ^\circ >$ *- группа*

Доказательство:

1. Множество S_n замкнуто относительно операции композиции, так как $\forall\ \varphi, \psi \in S_n$, $\varphi^\circ\psi \in S_n$ (по теореме о композиции биекций (подстановок)).

2. $\forall\ \varphi, \psi, \delta \in S_n$, $(\varphi^\circ\psi)^\circ\delta = \varphi^\circ(\psi^\circ\delta)$ (проверьте самостоятельно).

3. $\exists\, \varepsilon \in S : \forall\, \varphi \in S_n$, $\varepsilon^\circ\varphi = \varphi^\circ\varepsilon = \varphi$

Действительно, роль нейтрального элемента играет тождественная подстановка $\varepsilon = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}$

4. $\forall\, \varphi \in S_n\ \ \exists\, \varphi^{-1} \in S_n : \varphi^\circ\varphi^{-1} = \varphi^{-1\circ}\varphi = \varepsilon$

Действительно, так как φ - биекция, то будет существовать обратное соответствие, которое тоже будет биекцией и иметь вид:

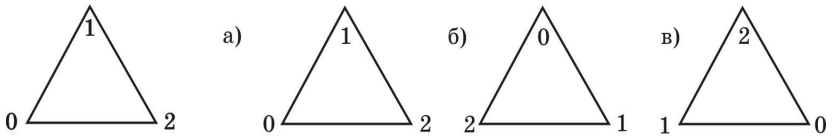
$$\varphi^{-1} = \begin{pmatrix} \varphi(1) & \dots & \varphi(n) \\ 1 & \dots & n \end{pmatrix}$$

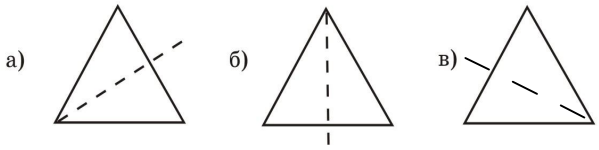
Итак, $< S_n, ^\circ >$ - группа. Порядок этой группы $| S_n | = n!$

Самостоятельно докажите, что эта группа некоммутативная. Построенная группа обозначается символом $\sigma(M) = < S_n , ^\circ >$ и называется симметрической группой подстановок множества *M*.

Пример 2: Интересный класс групп подстановок возникает как обобщение групп вращений правильных многоугольников.

Пусть дан правильный треугольник. Обозначим его вершины 0, 1, 2 и рассмотрим совокупность всех вращений и всех осевых симметрий, переводящих треугольник в себя. Мы будем иметь три вращения на углы 0, 2π/3, 4π/3 и три





осевые симметрии:

Вращение на $\angle\varphi=0$ определяет тождественную подстановку вершин $\varphi_0=\begin{pmatrix}0&1&2\\0&1&2\end{pmatrix}$

вращения на $\angle\varphi_1=2\pi/3$ и $\angle\varphi_2=4\pi/3$ определяют подстановки $\varphi_1=\begin{pmatrix}0&1&2\\1&2&0\end{pmatrix}$ и $\varphi_2=\begin{pmatrix}0&1&2\\2&0&1\end{pmatrix}$

Запишем подстановки множества вершин, соответствующие осевым симметриям треугольника:

$$\varphi_3=\begin{pmatrix}0&1&2\\1&0&2\end{pmatrix} \qquad \varphi_4=\begin{pmatrix}0&1&2\\2&1&0\end{pmatrix} \qquad \varphi_5=\begin{pmatrix}0&1&2\\0&2&1\end{pmatrix}$$

Указанными шестью подстановками исчерпываются всевозможные подстановки множества вершин треугольника. Как видим, это множество является симметрической группой подстановок множества *M={1,* 2, 3}, σ(M). Самостоятельно постройте группу самосовмещений квадрата.

Пример 3: Пусть дано множество $Z_m=\{\bar{1},\bar{2},...,\overline{m-1}\}$ - множество классов вычетов.

Зададим на этом множестве бинарные операции: сложение классов и умножение классов вычетов:

$\forall\ \bar{k}, \bar{s} \in Z_m$, $\qquad \bar{k} \oplus \bar{s} \overset{df}{=} \overline{k+s}$

$\forall\ \bar{k}, \bar{s} \in Z_m$, $\qquad \bar{k} \circ \bar{s} \overset{df}{=} \overline{k \circ s}$

Самостоятельно проверьте, будут ли $<Z_m,+>$ и $<Z_m, \circ>$ - коммутативными группами.

Пример 4. Рассмотрим множество M_{nn} квадратных матриц *n-го* порядка, на котором задана бинарная операция матричного сложения. Алгебра $<M_{nn},+>$ является аддитивной группой.

Действительно, как известно из теории матриц:

1 .$\forall\ A, B, C \in M_{nn}$, $(A+B)+C=A+(B+C)$,

2. $\exists\ O \in M_{nn} \mid \forall\ A \in M_{nn}$, $O+A=A+O=A$,

3.$\forall\ A \in M_{nn}\ \exists$ (-A) $\in M_{nn} \mid A+(-A)=(-A)+A=O$

4.$\forall\ A, B \in M_{nn}$,$A+B=B+A$.

Итак, $<M_{nn}, +>$ - аддитивная абелева группа.

Определение 13: *Группу $<G, *>$ называют бесконечной, если G - бесконечное множество:*

Пример 5: Пусть $\{a^к\}$ - множество целочисленных степеней некоторого целого числа a. Тогда $<\{a^к\},\circ\ >$ - бесконечная мультипликативная группа. Проверьте самостоятельно.

Определение 14: *Группу $<G,*>$ называют конечной, если G - конечное множество. Число элементов множества G называют порядком группы и обозначают* $|G|$ *(или Or G, или (G:1)).*

Пример 6: Пусть $\{\sqrt[n]{1}\}=\{\xi_0,\xi_1,...,\xi_{n-1}\}$ - множество комплексных корней n-ой степени из единицы. Тогда $<\{\sqrt[n]{1}\},\circ >$ - конечная группа.

Пример 7: Множество подстановок S_n на конечном множестве *A,* $|A| = n$, то есть множество преобразований этого множества на себя относительно операции композиции преобразований образует конечную группу $< S_n, \circ> = \sigma_n$

Пример 8: Множество классов вычетов по модулю *m,* то есть множество $Z_m=\{\bar{1}, \bar{2},..., \overline{m-1}\}$ относительно операции $\oplus$ сложения классов образует конечную аддитивную группу $<Z_m, \oplus>$, а множество $Z_p^{\,0} = Z_p \backslash \{0\}$ классов вычетов по простому модулю *p* образует относительно операции умножения классов конечную мультипликативную группу $<Z_p^{\,0}, >$.

Определение 15: *Пусть <G,*> - группа и H⊂G. Подалгебра* <H,*> *группы* <G,*> *называется подгруппой группы G, если алгебра* <H,*> *сама является группой относительно операции *.*

Если *H* - подгруппа *G,* то пишут *H<G.*

Замечание: Для того, чтобы выяснить является ли некоторое подмножество *H⊂G* подгруппой группы *G* относительно операции *, заданной на *G,* достаточно проверить следующие условия:

а) ∀ a ∈ H, ∀ b ∈ H, a*b∈H - условие замкнутости,

б) ∀ a ∈ H, a'∈ H - условие симметризуемости, называемые в дальнейшем достаточными условиями подгруппы.

Действительно, если ∀ a ∈ H, a'∈ H, то *a*a'∈H.* Так как *a*a'=e,* то нейтральный элемент *e* группы *G* также принадлежит и множеству *H.* операция * на множестве *H* является ассоциативной, так как она ассоциативна на множестве *G,* включающем *H.* Итак, *<H,*>* -группа.

Пусть дана аддитивная группа целых чисел <Z, +>. Попытаемся описать все подгруппы этой группы.

Теорема 2: *Все ненулевые подгруппы группы <Z,+ > исчерпываются совокупностями целых чисел кратных некоторому натуральному числу.*

Доказательство:

1. Пусть m∈N, рассмотрим множество *mZ* - множество целых чисел кратных натуральному числу *m.* Докажем, что <m*Z,+> < <Z,+>. Действительно:

а) ∀ ma, mb ∈ mZ , ma + mb = m(a + b) = mq ∈ mZ

б) ∀ ma ∈ mZ , -ma ∈ mZ

Итак, *mZ<Z.*

2. Теперь покажем, что других подгрупп в Z нет. Пусть *A<Z, n* - наименьшее натуральной число, принадлежащее подгруппе *A.* Тогда выберем ∀ a ∈ *A* и разделим его с остатком на *(n).* Получим: *a=nq+r,* где 0≤r<n, то есть мы получим противоречие с условием, что n-наименьшее натуральное число, принадлежащее *A.*

Следовательно, элемент (a) может быть только кратным числу (n), то есть $a=nq$. Таким образом, все подгруппы группы $<Z,+>$ исчерпываются подгруппами вида: $<mZ,+>$.

Пример 9. Рассмотрим аддитивные группы чисел $<Z,+>$, $<mZ,+>$, $<Q,+>$, $<R,+>$, $<C.+>$. Имеет место следующая цепочка: $mZ<Z<Q<R<C$. Проверьте это самостоятельно.

Пример 10: Подгруппами абстрактной группы G будут так называемые тривиальные подгруппы - сама группа G, то есть $G<G$ и группа $E=\{e \mid e \in G\}$, то есть $E<G$.

Пример 11: Показать, что алгебра $<R^+,+>$ не является подгруппой аддитивной группы $<R,+>$.

Действительно, $R^+ \subset R$. Кроме того,

а) $\forall\ a, b \in R^+$, $(a+b) \in R^+$ - условие замкнутости выполнено.

б) $\forall\ a \in R^+$, $-a \notin R^+$ - условие симметризуемости не выполняется на R^+.

Следовательно, алгебра $< R^+,+>$ не является подгруппой группы $<R,+>$.

Пример 12: Доказать, что множество четных подстановок группы $\sigma_n(M)$ образует подгруппу относительно операции композиции подстановок.

Доказательство:

Пусть $A_n=\{\varphi \mid \varphi \in \sigma(M)$ и φ - четная$\}$. Проверим достаточные условия подгруппы:

а) $\forall\ \varphi, \psi \in A$, $\varphi^{\circ}\psi \in A$ (так как композиция двух четных подстановок является четной подстановкой, см. гл. 2);

б) $\forall\ \varphi \in A$, $\varphi^{-1} \in A$, так как известно, что если φ - четная, то φ^{-1} - тоже четная.

Итак, $A_n<\sigma(M)$. Ее называют знакопеременной подгруппой симметрической группы подстановок.

Для описания всех других подгрупп группы $\sigma(M)$ используют представление подстановки циклами.

Пусть, например $M=\{0, 1, 2, 3, 4, 5, 6, 7 , 8, 9\}$ и $\varphi \in \sigma_{10}(M)$.

$$\varphi = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 5 & 8 & 7 & 2 & 0 & 9 & 1 & 4 & 6 \end{pmatrix}$$

Если все замены элементов осуществляемые этой подстановкой записать в указанной последовательности, то подстановку φ можно записать в виде:

$$\varphi=\begin{pmatrix}0 & 3 & 7 & 1 & 5 & 2 & 8 & 4 & 6 & 9\\ 3 & 7 & 1 & 5 & 0 & 8 & 4 & 2 & 9 & 6\end{pmatrix}$$

Нетрудно заметить, что подстановка φ оказалась разложенной на три независимые друг от друга части (подстановки), каждая из которых перемещает элементы, принадлежащие ее области определения:

$M_1=\{0,l,2,3,5,7,\};M_2=\{2,4,8\};M_3=\{6,9\}$.

То есть, $\varphi=\left[\begin{pmatrix}0 & 3 & 7 & 1 & 5\\ 3 & 7 & 1 & 5 & 0\end{pmatrix}\bullet\begin{pmatrix}2 & 8 & 4\\ 8 & 4 & 2\end{pmatrix}\bullet\begin{pmatrix}6 & 9\\ 9 & 6\end{pmatrix}\right]$

Замечание 1.Так как области определения M_1, M_2,M_3 этих подстановок разные, то чтобы определение операции композиции подстановок можно было здесь использовать, условимся, что все недостающие элементы эти подстановки переводят сами в себя (оставляют неподвижными).

Итак, с учетом этого замечания, подстановка

$$\varphi=\begin{pmatrix}0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9\\ 3 & 5 & 8 & 7 & 2 & 0 & 9 & 1 & 4 & 6\end{pmatrix}=\begin{pmatrix}0 & 3 & 7 & 1 & 5\\ 3 & 7 & 1 & 5 & 0\end{pmatrix}\circ\begin{pmatrix}2 & 8 & 4\\ 8 & 4 & 2\end{pmatrix}\circ\begin{pmatrix}6 & 9\\ 9 & 6\end{pmatrix}$$

(причем, порядок выполнения операций не играет роли).

Теперь отметим, что в правой части этого равенства нижние строчки всех подстановок можно не писать, так как верхние строчки состоят из тех же элементов, что и нижние, причем, каждый элемент под действием подстановки переходит в следующий. Поэтому, кратко можно записать, что

$$\begin{pmatrix}0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9\\ 3 & 5 & 8 & 7 & 2 & 0 & 9 & 1 & 4 & 6\end{pmatrix}=(0\ 3\ 7\ 1\ 5)\ (2\ 8\ 4)\ (6\ 9)$$

Подстановки, стоящие в правой части этого равенства, называют циклами или циклическими подстановками. Например, символ (р, *q, r, s)* обозначает циклическую подстановку, которая переводит элемент *p* в *q, q* в r, r в *s,* а s в *p* и оставляет все остальные элементы произвольного множества М неподвижными.

Замечание 3: Так как любая подстановка это биекция, то каждый элемент $a \in M$, в общем случае будет входить лишь в один какой-то цикл.

Определение 16: *Циклы, не имеющие общих элементов, называются независимыми.*

С учетом этого определения, можно сказать, что мы разложили подстановку

$\varphi = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 5 & 8 & 7 & 2 & 0 & 9 & 1 & 4 & 6 \end{pmatrix}$ в произведение трех независимых циклов (0 3 7 1 5), (2 8 4), (6 9).

Теорема 3: *Любая подстановка допускает единственное (с точностью до порядка следования сомножителей) разложение в произведение независимых циклов. (Докажите самостоятельно)*

Задача: Разложить подстановку в произведение независимых циклов

$\varphi = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 4 & 0 & 5 & 9 & 1 & 8 & 7 & 6 & 3 \end{pmatrix}$

Решение:

$$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 4 & 0 & 5 & 9 & 1 & 8 & 7 & 6 & 3 \end{pmatrix} = (0\ 2) \bullet (1\ 4\ 9\ 3\ 5) \bullet (6\ 8) \bullet (7)$$

Цикл (7) можно опустить в этой записи, так как мы условились считать, что неподвижные элементы не записываются.

Определение 17: *Длиной цикла называется число входящих в него элементов.* Например, циклы (0 2), (1 4 9 3 5) имеют длину, равную 2 и 5 .

Замечание*:* Цикл длины 1 представляет тождественную подстановку $\varepsilon = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}$

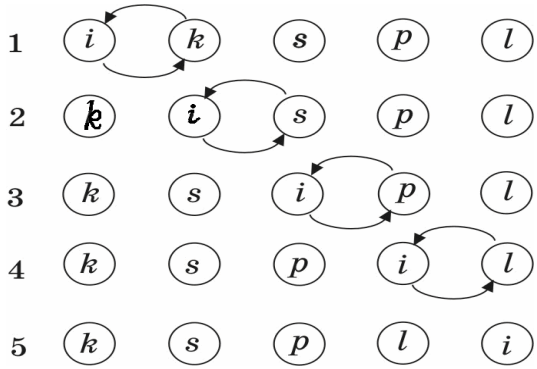
Определение 18: *Циклы длины 2 называются транспозициями* $\tau = \begin{pmatrix} 1 & 2 & \dots & k & \dots & i & \dots & n \\ 1 & 2 & \dots & i & \dots & k & \dots & n \end{pmatrix}$

Теорема: *Любая транспозиция является нечетной подстановкой* (см. доказательство Алгебра).

Теорема 4: *Любую подстановку можно разложить в произведение транспозиций.*

Доказательство:

Поскольку, любую подстановку $\varphi \in \sigma_n(M)$ можно представить в виде произведения независимых циклов, то достаточно доказать, что циклы допускают разложение в произведение транспозиций. Пусть подстановка φ имеет цикл *(i k s p l)*. Покажем разложение этого цикла в произведение транспозиций.



В результате (i к s p l)=(i k) (i s) (i p) (i l), то есть на месте каждого элемента оказался последующий за ним, а первый элемент перешел на последнее место.

На основе этой теоремы можно дать такие определения четной и нечетной подстановки.

Определение 17: *Подстановка $\varphi \in \sigma(M)$ называется четной (нечетной), ест число транспозиций в ее разложении четно (нечетно).* (Сравните это определение с определением четности (нечетности) через число инверсий. См. Алгебра)

Покажем теперь на конкретном примере, как использовать полученные результаты для нахождения всех подгрупп конкретной группы подстановок.

Пусть M={1, 2, 3} и дана симметричная группа подстановок этого множества $\sigma_3(M)$, которая в этом случае имеет шесть элементов:

$\varepsilon=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$ $\varphi_1=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$ $\varphi_2=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$ $\varphi_3=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$

$\varphi_4=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$ $\varphi_5=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$

Первая подгруппа - это $A_3=\{\varepsilon,\varphi_3,\varphi_4\}$ - знакопеременная подгруппа четных подстановок. Теперь представим каждую подстановку в виде произведения независимых циклов, а затем транспозиций $\varepsilon=(1)$, $\varphi_1=(1\ 3)\ (2)=(1\ 3)$, $\varphi_2=(1)\ (2\ 3)=(2\ 3)$, $\varphi_3=(1\ 2\ 3)=(1\ 2)\ (1\ 3)$, $\varphi_4=(1\ 3\ 2)=(1\ 3)(1\ 2)$, $\varphi_5=(1\ 2)\ (3)=(1\ 2)$.
$H_0=(1)$, $H_1=\{(1)\ (2\ 3)\}$, $H_2=\{(1)\ (1\ 3)\}$, $H_3=\{(1)\ (1\ 2)\}$, $H_4=\{(1)\ (1\ 2\ 3)\ (1\ 3\ 2)\}$ - искомые подгруппы группы $\sigma_3(M)$.

Вопрос о том, как построить некоторую подгруппу в заданной группе рассмотрим в следующем параграфе.

§ 2. Циклические группы.

Пусть <G,*> - произвольная группа. Ассоциативность операции * и замкнутость множества *G* относительно операции - позволяют определить степени произвольного элемента *a* из *G,* если группа *G* - мультипликативная и - кратные элемента *a,* если группа G -аддитивная.

Рассмотрим сначала мультипликативную группу $<G, \bullet>$. Тогда, $\forall\ a\in G$, $a\neq e$, $a\bullet a=a^2\in G$, $a^2\bullet a=a^3\in G$ и т.д., $a^{n-1}\bullet a=a^n\in G$. По определению $a^0=e$. Так как $\forall\ a\in G$, $\exists\ a^{-1}\in G$, то можно определить a^{-n} так, что $a^{-n}=(a^{-1})^n$. Таким образом, для мультипликативной группы <G, •> можно записать двухстороннюю последовательность, образованную любым элементом $a\neq e$:

$$..., a^{-(n+1)},a^{-n},...,a^{-2},a^{-1},a^0,a^1,a^2,...,a^n,a^{n+1},... \qquad (1)$$

Для аддитивной группы $<G, +>$, соответственно, получим последовательность:

..., -na,..., -3a, -2a, -a, 0a, a, 2a, 3a,..., na,... (2)

Определение 1: Если в последовательности (1) для элемента $a \in G$ мультипликативной группы $<G, \bullet>$ все степени элемента a - различны, то говорят, что a элемент бесконечного порядка. Аналогично, *если в последовательности (2) для элемента a аддитивной группы $<G,+>$ все кратные элемента a - различны, то говорят, что a - элемент бесконечного порядка. Если же в последовательности (I) или (2) имеются совпавшие элементы, то элемент $a \in G$ называют элементом конечного порядка.*

Пример 1. Дана группа $<Z,+>$, выберем $2 \in Z$, Для этого элемента можно записать двухстороннюю последовательность вида (2):

..., -6, -4, -2, 0, 2, 4, 6, ...

Ясно, что в ней нет одинаковых целых чисел. Следовательно, элемент 2 является элементом бесконечного порядка.

Пример 2: Рассмотрим мультипликативную группу $<Q^0, \bullet>$. Элемент $-1 \in Q$ является элементом конечного порядка, так как записанная для него последовательность вида: (1) ..., 1, -1, 1, -1,... имеет совпадающие элементы.

Пример 3: Рассмотрим аддитивную группу $<Z^{10}, \oplus>$ классов вычетов по модулю *10,* где $Z_{10}=\{\bar{0},\bar{1},\bar{2},\bar{3},\bar{4},\bar{5},\bar{6},\bar{7},\bar{8},\bar{9}\}$. Выясним, элементом какого порядка является класс $\bar{3}$. В последовательности (2), записанной для элемента $a=\bar{3}$,

$$..., \bar{2},\bar{5},\bar{8},\bar{1},\bar{4},\bar{7},\bar{0},\bar{3},\bar{6},\bar{9},\bar{2},\bar{5},\bar{8},\bar{1},\bar{4},\bar{7},\bar{0},\bar{3},\bar{6},...$$

имеются совпавшие элементы. Следовательно, класс $\bar{3}$ - элемент конечного порядка. Уточним понятие порядка элемента.

Определение 2: *Пусть G группа. Наименьшее натуральное число, $n \neq 0$ ($n \in N^0$), называется порядком элемента $a \in G$, если $a^n = e$ в случае, когда G - мультипликативная группа, и $na=0$ в случае, когда G - аддитивная группа.*

Говорят, что *a* - элемент порядка n и пишут $p(a)=n$.

Если же такого $n\neq 0$ не существует, то есть $\forall\, n\in N^0$, $a^n\neq e$, $(na\neq 0)$, то элемент a называется элементом бесконечного порядка.

***Пример 4**:* Рассмотрим мультипликативную группу $<\{\sqrt[4]{1}\},\bullet>$, где $\{\sqrt[4]{1}\}=\{1, -1, i, -i\}$ -множество комплексных корней 4-ой степени из единицы.

Так как, $1^1=1$, $(-1)^1=1$, $(-i)^4=1$, $(i)^4=1$, то $p(1)=1$, $p(-1)=2$, $p(i)=4$, $p(-i)=4$. Следовательно, в группе $<\{\sqrt[4]{1}\},\bullet>$ каждый элемент имеет конечный порядок.

***Пример* 5:** Рассмотрим аддитивную группу $<Z_6,\oplus>$ классов вычетов по модулю 6, где $Z_6=\{\bar{0},\bar{1},\bar{2},\bar{3},\bar{4},\bar{5}\}$. Найдем порядок каждого элемента. Так как, $e=\bar{0}$ и $6\cdot\bar{1}=\bar{0}$, $3\cdot\bar{2}=\bar{0}$, $6\cdot\bar{5}=\bar{0}$, $3\cdot\bar{4}=\bar{0}$, то $p(1)=6$, $p(2)=3$, $p(3)=2$, $p(4)=3$. Таким образом, в групne $< Z_6,,\oplus>$ классов вычетов по модулю 6 каждый элемент является элементом конечного порядка.

***Определение 3** Группа G, все элементы которой имеют конечный порядок, называется периодической группой.*

***Определение 4** Группа G называется группой без кручения, если все ее элементы, кроме нейтрального, являются элементами бесконечного порядка.*

***Определение 5:** Группа G называется смешанной, если в ней имеются элементы как конечного, так и бесконечного порядка.*

Пример 6: Группы $<\{\sqrt[4]{1}\},\bullet>$, $<Z_m,\oplus>$, $<Z_p^0,\bullet>$ являются периодическими. Группы $<Z, +>$, $<Q, +>$, $<R, +>$, $<C, +>$ являются группами без кручения, так как все их элементы, кроме $e=0$, являются элементами бесконечного порядка. Группа $<Q^\circ,\bullet>$ - смешанная, так как, например, элемент $2\leq Q$ - элемент бесконечного порядка, а элемент $-1\in Q$, ввиду того, что $(-1)^2=1$, имеет порядок 2.

***Теорема 1:** Пусть $<G,\bullet>$ - мультипликативная группа. Последовательность G_a всех степеней произвольного элемента $a\in G$ образует подгруппу $<G_a,\bullet>$ группы $<G,\bullet>$.*

Доказательство:

Очевидно, что $G_a\subset G$. Проверим выполнение достаточных условий подгруппы. Возьмем произвольный элемент $a\in G$. Тогда:

1) $\forall$ k,l$\in$Z (a^k, $a^l \in G_a \Rightarrow a^k \bullet a^l = a^{k+l} \in G_a$,), то есть G_a замкнуто относительно данной операции.

2) $\forall$ m$\in$Z ($a^m \in G_a \Rightarrow (a^m)^{-l} = a^{-m} \in G_a$),то есть G_a симметризуемо относительно данной операции.

Таким образом, $<G_a, \bullet>$ является группой, и $G_a < G$.

Теорема 2: *Пусть $<G, +>$ аддитивная группа. Последовательность G_a всех кратных произвольного элемента $a \in G$ образует подгруппу $<G_a, +>$ группы $<G, +>$.*

Доказать самостоятельно.

Определение 6: *Подгруппа G_a называется циклической подгруппой группы G, порожденной элементом $a \in G$.*

Поскольку в группе G_a, $a^k a^l = a^l \bullet a^k$, если G_a – мультипликативна, и $ka+la=la+ka$,если G_a -аддитивна, то подгруппы $<G_a, \bullet>$ и $<G_a, +>$ являются коммутативными группами.

Выясним, как связан порядок элемента $a \in G$ с порядком подгруппы G_a. Пусть $<G_a, \bullet>$ мультипликативная группа. Если элемент $a \in G$ бесконечного порядка, то в последовательности (1) все элементы ..., a^{-2}, a^{-1}, e, a, a^2,... различны, и тогда подгруппа G_a содержит бесконечное множество элементов, то есть порядок G_a бесконечен.

Если $a \in G$ - элемент конечного порядка, то имеет место следующая теорема.

Теорема 3: *Если порядок элемента a мультипликативной группы G равен n, то ее циклическая подгруппа G_a имеет порядок n, т.е.*

$\forall a \in G$, $p(a)=|G_a|$ *и* $G_a=\{e, a, a^2, a^3, \dots, a^{n-1}\}$

Доказательство:

Пусть элемент a группы G имеет порядок n, то есть $\exists$ n$\in N^0$ такое, что $a^n=e$. Значит элементы

$$e, a^1, a^2, a^3, \dots, a^{n-1} \qquad (3)$$

последовательности (1) различны. Покажем, что элементы подгруппы G_a совпадают с элементами последовательности (3). Возьмем $a^t \in G_a$, $t>n$. Поделим t на n с остатком, получим $t=nq+r$, $0 \le r < n$. Тогда, $a^t = a^{nq+r} = a^{nq} a^r = (a^n)^q a^r = e^q a^r = a^r$, то есть $a^t = a^r$, где a^r принадлежит последовательности (3). Таким образом, множество элементов подгруппы G_a исчерпывается множеством

элементов последовательности (3). Следовательно, $G_a=\{e, a^1, a^2, a^3,..., a^{n-1}\}$. Поэтому, если p(a)=n, то $|G_a|=n$.

Для аддитивной подгруппы $<G_a, +>$имеет место аналогичная теорема. Сформулируйте и докажите ее самостоятельно.

Пример 7: В группе $<\{\sqrt[4]{1}\},\bullet>$ элемент (-1) имеет порядок 2. Множество его степеней $(-1)^0=1$, $(-1)^1=-1$ образует подгруппу $<\{-1,1\},\bullet>$, состоящую их двух элементов 1 и -1. Элемент *i* имеет порядок 4. Множество его степеней $i^0=1$, $i^1=i$, $i^2=-1$, $i^3=-i$ образует мультипликативную подгруппу порядка 4, совпадающую с самой группой.

Пример 8*:* Рассмотрим аддитивную группу $<Z_6, \oplus>$, где $Z_6=\{\bar{0},\bar{1},\bar{2},\bar{3},\bar{4},\bar{5}\}$. Элемент $\bar{4}$ имеет порядок 3, так как $3\cdot\bar{4}=\bar{0}$. Его кратные: $0\cdot\bar{4}=\bar{0}$, $1\cdot\bar{4}=\bar{4}$, $2\cdot\bar{4}=\bar{2}$, $3\cdot\bar{4}=\bar{0}$ образуют циклическую подгруппу $<G_4, \oplus>$ порядка 3 с основным множеством $G_4=\{\bar{0},\bar{2},\bar{4}\}$.

Пример 9: Рассмотрим мультипликативную группу $<Z_7^0, \cdot>$, где $Z_7=\{\bar{0},\bar{1},\bar{2},\bar{3},\bar{4},\bar{5},\bar{6}\}$. Найдем порядок элемента $\bar{3}$. Так как $\overline{3^1}=\bar{3}$, $\overline{3^2}=\bar{2}$, $\overline{3^3}=\bar{6}$, $\overline{3^4}=\bar{4}$, $\overline{3^5}=\bar{5}$, $\overline{3^6}=\bar{1}$, то $p(\bar{3})=\bar{6}$. Тогда, $G_3=\{\bar{0},\bar{1},\bar{2},\bar{3},\bar{4},\bar{5},\bar{6}\}$, то есть $G_3=Z_7^0$.

Мы определили и рассмотрели примеры циклической подгруппы G_a, порожденной некоторым элементом *a* данной группы *G*. Встанем теперь на более общую точку зрения и рассмотрим любую группу G такую, что каждый ее элемент порожден некоторым фиксированным элементом *a* из группы *G*. А именно, имеют место следующие определения.

Определение 7: *Группа G называется циклической группой, порожденной элементом* ***a*** *из G, если она состоит из степеней элемента a, когда G - мультипликативна, и из элементов, кратных элементу a, когда G - аддитивна. Элемент* ***a*** *называется образующим или первообразным элементом группы G.*

Пример 10: $<\sqrt[n]{1},\cdot>$, где $\{\sqrt[n]{1}\}=\{\varepsilon_0,\varepsilon_1,...,\varepsilon_{n-1}\}$, конечная мультипликативная циклическая группа.

Здесь $\varepsilon_k=\sqrt[n]{1}=cos(2\pi k/n)+i\,sin(2\pi k/n)$, $k=0, 1, ..., n-1$.

Элемент $\varepsilon_1=cos(2\pi/n)+i\ sin(2\pi/n)$ можно взять в качестве образующего элемента, поскольку $(\varepsilon_1)^k=\varepsilon_k$.

Пример 11: $<Z, +>$ - бесконечная аддитивная циклическая группа целых чисел. Образующие элементы 1 и -1.

Пример 12: $<Z_P^0, \cdot >$, где $Z_P^0=\{1, 2, ...,p-1\}$ - конечная мультипликативная циклическая группа классов вычетов по простому модулю *p.* Найдите ее образующие элементы.

Пример 13*:* $<Z_m, \oplus>$ - конечная аддитивная циклическая группа классов вычетов по модулю *m,* образующий элемент $\bar{1}$.

Пример 14: $<\{a^\kappa\}, \cdot >$ - бесконечная циклическая группа целочисленных степеней некоторого целого числа a, являющегося образующим элементом этой группы.

Итак, рассмотренные выше определения, теоремы и примеры, позволяют описать общий метод построения в заданной группе (конечной или бесконечной) циклической подгруппы. Для этого нужно брать любой элемент группы и находить его двухстороннюю последовательность G_a. Если группа $<G, \cdot >$ - бесконечна, то и подгрупп такого вида (в общем случае) можно построить сколь угодно много. Причем, здесь важно отметить, что если исходная группа $<G, \cdot>$ сама является циклической, то все ее подгруппы будут циклическими.

Теорема 4: *Любая подгруппа циклической группы - циклическая.*

Доказательство:

Пусть дана мультипликативная циклическая группа $<G, \cdot>$, то есть $\forall\ b\in G$ представляет собой степень образующего элемента (a): $b=a^n$, где $n\in N^0$. Пусть $H<G$ и a^m - элемент в H с наименьшим натуральным показателем. Докажем, что все остальные элементы из подгруппы H будут степенями этого элемента. Действительно, если a^s - произвольный элемент из H, то разделив s на *m* с остатком, получим, что $s=mq+r$, где $0\le r<m$, так как *m* - наименьшее число, то r=0 и $a^s=a^{mq}=(a^m)^q$, то есть H - циклическая.

Следствие: *если образующий элемент (a) имеет конечный порядок (n), то n/m.*

Доказательство:

Действительно, если $p(a) = n \Rightarrow a^n = e \Rightarrow a^n \in H$, тогда $n = mq \Rightarrow n/m$. Итак, любая подгруппа H циклической группы G будет состоять либо из e, либо из степеней элемента a с наименьшим положительным показателем (m) При этом для бесконечной циклической группы число (m) произвольно, *если* же $|G|=n$, то n/m и $|H|=k$, где $k=n/m$.

Теперь докажем, что с точностью до изоморфизма существует лишь одна бесконечная циклическая группа и одна конечная циклическая группа.

Теорема 5 (о циклических группах): Все бесконечные циклические группы изоморфны аддитивной группе целых чисел. Все конечные циклические группы порядка n изоморфны аддитивной группе классов вычетов по модулю n.

Доказательство:

Пусть $<G, \cdot>$ мультипликативная циклическая группа с образующим элементом a, то есть $G=\{a^n \mid n \in N\}$. Пусть $<Z, +>$ - аддитивная группа целых чисел, и $<Z_n, \oplus>$ - аддитивная группа классов вычетов по модулю n.

Рассмотрим первый случай: G - бесконечная группа, элемент a имеет бесконечный порядок, то есть $p(a)=\infty$. В этом случае все целочисленные степени образующего элемента a различны. Поэтому отображение $\varphi : G \to Z$ такое, что $\forall\ a_n \in G$, $\varphi(a^n)=n$ является инъективным. Очевидно, что φ сюръективно. Кроме того, отображение φ удовлетворяет условию гомоморфности, так как $\forall\ a^k, a^l \in G$, $\varphi(a^k \cdot a^l)=\varphi(a^k)+\varphi(a^l)$.

Действительно, $\varphi(a^k \cdot a^l)=\varphi(a^{k+l})=k+l$ и $\varphi(a^k)+\varphi(a^l)=k+l$. Следовательно, $<G, \cdot> \cong <Z, +>$. Рассмотрим второй случай: группа G - конечна, то есть $p(a)=n$. Покажем, что в этом случае группа G изоморфна группе $<Z_n, \oplus>$. Имеем $G=\{e, a, a^2, ..., a^{n-1}\}$. Рассмотрим отображение ψ: $G \to Z_n$, где $Z_n = \{\overline{0}, \overline{1}, ..., \overline{n-1}\}$, такое, что $\psi(a^r)=r$, где r=0, 1, ..., n-1. Покажем, что ψ инъективно, то есть

$\forall\ r, s \in \{0, 1, ..., n-1\}$, $(\psi(a^r)= \psi(a^s) \Rightarrow (a^r=a^s)$.

Действительно, так как $\psi(a^r) = r$ и $\psi(a^s) = s$, где $r, s = \{0, 1, ..., n-1\}$, то из равенства $r = s$ следует, что $a^r = a^s$. Итак,

ψ - инъективно. Очевидно, что ψ -сюръективно. Кроме того, ψ - удовлетворяет условию гомоморфности, так как $\forall$ k,l $\in$ {0,1,..., n-1}, $\psi(a^k a^l) = \psi(a^{k+l}) = k + l = k \oplus l = \psi(a^k) + \psi(a^l)$. Следовательно, и в этом случае группа G изоморфна группе $<Z_n, \oplus>$. Теорема доказана.

Пример 15: Мультипликативная группа $<\sqrt[n]{1}, \bullet>$ корней n-ой степени из единицы является конечной циклической группой порядка n, следовательно, по теореме 5 она изоморфна группе $<Z_n, \oplus>$.

Пример 16: Мультипликативная группа $<\{2^n\}, \bullet>$ целочисленных степеней двойки является бесконечной циклической группой, следовательно, по теореме 5 она изоморфна группе <Z, +>.

Итак, с точностью до изоморфизма, существуют одна бесконечная циклическая группа и одна конечная циклическая группа. Поэтому, например, чтобы описать все подгруппы бесконечной циклической группы можно описать все подгруппы аддитивной группы целых чисел, которые имеют вид: <mZ, +> и мы получаем еще одно доказательство того, что любая подгруппа бесконечной циклической группы тоже будет циклической.

§ 3. Разложение группы по подгруппе. Нормальные делители. Фактор-группа.

Пусть дана мультипликативная группа <G, •> и $H<G$. Возьмем произвольный элемент $x \in G$.

Определение 1: *Множество* $xH=\{x \cdot h_i \mid h_i \in H, x \in G\}$ *называется левым смежным классом мультипликативной группы G по подгруппе H, определяемым элементом x.*

Множество $Hx=\{h_i \cdot x \mid h_i \in H, x \in G\}$ называется правым смежным классом мультипликативной группы G по подгруппе H, определяемым элементом *x.*

Теперь рассмотрим аддитивную группу $<G,+>$, и пусть $H<G$. Возьмем произвольный элемент $x \in G$.

Определение 2: *Левым смежным классом аддитивной группы G по подгруппе H, определяемым элементом x, называется множество* $x + H = \{x + h_i \mid x \in G,\ h_i \in H\}$. *Правым смежным классом аддитивной группы G по подгруппе H, определяемым элементом x, называется* $H+x=\{h_i+x \mid h_i \in H, x \in G\}$.

Замечание 1*:* Элемент x всегда принадлежит смежному классу, который он определяет. Например, если <G, ·>, то $x \cdot e = x \in xH$.

Замечание 2: Подгруппа *H* сама является одним из левых (правых) смежных классов. Покажем (в мультипликативной терминологии), что если $x \in H$, то $xH=H$. Действительно, если x∈H, то $\forall\ h_i \in H\ x \cdot h_i \in H \Rightarrow xH \subset H$, а ∀ y∈H можно представить так: $y=x \cdot x^{-1} \Rightarrow y \in xH \Rightarrow H \subset xH$, следовательно, $xH=H$.

Пример 1: Найти все левые и правые смежные классы аддитивной группы <Z, +> целых чисел по подгруппе <3Z, +> целых чисел, кратных 3.

Решение:

Множества Z и 3Z можно записать в виде

Z={..., -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6,...},

3Z={...,-9, -6,-3, 0, 3, 6, 9, 12, ...}.

Найдем левые смежные классы для элементов x=0, 1, 2. Получим

0+3Z={..., -9, -6, -3, 0, 3, 6, 9, 12, ...}=3Z,

1+3Z={..., -8, -5,-2, 1, 4, 7, 10, 13, ...},

2+3Z={...,-7, -4, -1, 2, 5, 8, 11,...}.

Для элемента x=3 получим 3+3Z=3Z, для x=4 получим 4+3Z=1+3Z и т.д Следовательно, различных левых смежных классов будет всего три: 3Z, 1+3Z, 2+3Z. Все остальные левые смежные классы будут совпадать с одним из этих трех классов. Так как <Z, +> -коммутативная группа, то все левые смежные классы будут совпадать с соответствующими правыми смежными классами. Но всегда ли это будет так?

Выясним, существуют ли группы и их подгруппы такие, что

$\forall x \in G,\ xH \neq Hx$. Например, найдем левостороннее и правостороннее разложение группы $\sigma_3(M)$ по подгруппе $H = \langle (1\ 2),(1) \rangle$ и сравним их:

$\{(1), (1\ 2)\} \cup \{(1\ 3),(1\ 2\ 3)\} \cup \{(2\ 3),(1\ 3\ 2)\}$
$\{(1), (1\ 2)\} \cup \{(1\ 3),\{1\ 3\ 2)\} \cup \{(2\ 3),(12\ 3)\}$.

Видим, что множество левых смежных классов не совпадает с множеством правых смежных классов.

Задача 1: Выяснить, будет ли подгруппой группы G любой смежный класс *xH,* полученный при разложении G по H.

***Задача** 2:* Доказать, что отображение φ: $H \to xH$ является биекцией для любого элемента x. Это равносильно тому, что |xH|=|H|.

***Задача** 3:* Доказать, что $\forall\ x \in G$, $\forall\ y \in G$, ($xH=yH$) или ($xH \cap yH=\varnothing$). Из доказательства этого утверждения следует, что группа *G* распадается на непересекающиеся левые смежные классы.

Определение 3: *Представление группы G в виде объединения непересекающихся левых (правых) смежных классов называют левосторонним (правосторонним) разложением группы G по подгруппе* ***H.***

Например, аддитивную группу Z можно разложить по подгруппе 3Z в виде: $Z=3Z \cup (1+3Z) \cup (2+3Z)=3Z \cup (3Z+1) \cup (3Z+2)$.

***Задача** 5:* Доказать, что отображение φ: $xH \to Hx$ является биекцией для любого элемента *x.*

Из справедливости этого утверждения следует, что левостороннее и правостороннее разложения равномощны.

Определение 4: *Число смежных классов в любом из двух разложений группы G по подгруппе H, если оно конечно, называется индексом подгруппы H в группе G. Обозначается: ind H.*

Пример 2: В группе <Z,+>, *ind* 3Z=3. В общем случае, *ind mZ=m.*

Теорема 1 (Лагранжа): *Порядок и индекс любой подгруппы H конечной группы G является делителем порядка самой группы.*

Доказательство:

Пусть порядок группы *G* равен *n,* то есть |G|=n, $H<G$, |H|=*k, ind H=s.* Так как |*H*|=*k,* то |*xH*|=*k,* учитывая, что левые смежные

классы общих элементов не имеют, будем иметь, что то $n=k\cdot s \Rightarrow (n/k)\&(n/s)$.

Следствие 1: *Порядок любого элемента в конечной группе является делителем порядка самой группы.*

Доказательство:

Известно, что порядок элемента $a\neq e$, $a\in G$, совпадает с порядком порожденной им циклической группы G_a, которая является подгруппой группы G. Тогда по теореме Лагранжа, если $(p(a)=k$, то $|G_a|=k) \Rightarrow |G|:k$.

Следствие 2*. G не будет иметь, нетривиальных подгрупп, если $|G|=p$, где p - простое число.*

Доказательство:

Пусть $H<G$, тогда по теореме Лагранжа она может иметь порядок 1 или p. Если $|H|=1$, то она будет единичной подгруппой, если $|H|=p$, то она будет совпадать с группой G.

Следствие 3*: Любая группа простого порядка будет циклической и любой ее элемент ($a\neq e$) будет образующим.*

Доказательство:

Пусть $a\neq e$, $a\in G$. С помощью этого элемента построим подгруппу G_a: ..., a^{-s}, ..., a^{-1}, a^0, a^1, a^2, ..., a^s, ... Порядок этой подгруппы по теореме Лагранжа может быть равен только p, так как $a\neq e$. Тогда $|G_a|=|G|=p$ и, следовательно, $G_a=G$, а так как C_a - циклическая, то и G - будет циклической группой.

Задача *6:* Проверить, что $<Z_5, +>$ - циклическая группа, в которой каждый элемент ($a\neq o$) является образующим.

Доказательство:

$Z_5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$

$G_1 = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{0}\} = Z_5 \quad p(\bar{1}) = 5$

$G_2 = \{\bar{2}, \bar{4}, \bar{1}, \bar{3}, \bar{0}\} = Z_5 \quad p(\bar{2}) = 5$

$G_3 = \{\bar{3}, \bar{1}, \bar{4}, \bar{2}, \bar{0}\} = Z_5 \quad p(\bar{3}) = 5$

$G_4 = \{\bar{4}, \bar{3}, \bar{2}, \bar{1}, \bar{0}\} = Z_5 \quad p(\bar{4}) = 5$

Нормальные делители. Фактор-группа.

Пусть дана группа G и $H<G$.

Определение 1: *Подгруппа H называется нормальной в группе G, если $\forall\ x \in G$ выполняется условие: $xH=Hx$. Обозначается: $H \lhd G$.*

Равенство $xH=Hx$ означает совпадение левого и правого смежных классов для каждого элемента $x \in G$. Равенство $xH=Hx$ можно записать в виде: $H=xHx^{-1}$ Элементы h и xhx^{-1} называются сопряженными. Тогда определение 1 можно дать в терминах сопряженных элементов.

Определение 2: *Подгруппа H называется нормальной (нормальным делителем группы G), если $\forall\, x \in G,\ \forall\, h \in H\ (h \in H \Rightarrow xhx^{-1} \in H)$.*

Если дана группа $<G, *>$, $H \subset G$, и нужно доказать, что $H \lhd G$, то для этого необходимо проверить два условия:

а) проверить, что $H<G$ (достаточные условия подгруппы);

б) проверить, что $H \lhd G$ (по определению 1 или 2).

Лемма*: Любая нормальная подгруппа $H \lhd G$ является объединением некоторого множества сопряженных классов группы G.*

Действительно, если $x \in H$, где $H \lhd G$, то $\forall\ g \in G$, $gxg^{-1} \in H$. Следовательно, вместе с каждым элементом x в H содержится целиком класс сопряженных элементов.

Пример 1: Всякая подгруппа H абелевой группы G будет нормальным делителем, так как в силу коммутативности операции, $\forall\, x \in G,\ xH=Hx$.

Пример 2: Для всякой группы G ее нормальными делителями будут тривиальные подгруппы E и G. Разложение группы G по E совпадает с разложением группы G на отдельные элементы, а разложение G по G состоит из одного смежного класса, равного G.

Пример 3: Пусть $G=<M_{nn}(R), \cdot>$ - мультипликативная группа обратимых квадратных матриц n-порядка с действительными элементами. Множество $H=\{B \in M_{nn}(R) \mid |B|=1\}$ обратимых матриц, принадлежащих $M_{nn}(R)$, определитель

которых равен 1, будет мультипликативной подгруппой данной группы G (Проверьте!).

Найдем левосторонне разложение группы G по H. Пусть $A \in M_{nn}(R)$, тогда $AH=\{A \cdot B_i \mid A \in M_{nn}(R),\ B_i \in H\}$. Так как $B_i \in H$, то $|B_i|=1$ и тогда $|A \cdot B_i|=|A| \cdot |B_i|=|A| \cdot 1=|A|$, то есть левый смежный класс, порожденный матрицей A, будет состоять из таких матриц, определители которых равны определителю матрицы A.

Найдем правый смежный класс, порожденный матрицей A:

$HA=\{B_i \cdot A \mid B_i \in H,\ A \in M_{nn}(R)\}$, $|B_i \cdot A|=|B_i| \cdot |A|=1 \cdot |A|=|A|$

Таким образом, $\forall\ A \in M_{nn}(R),\ AH=HA$, следовательно, $H \nabla G$.

Пример 4. Докажем, что если $H_1 \lhd G$ & $H_2 \lhd G$, то $H_1 \cap H_2 \lhd G$. Нужно доказать, что 1) $H_1 \cap H_2 < G$ и *2)* $H_1 \cap H_2 \lhd G$.

Проверяем достаточные условия подгруппы (в мультипликативной терминологии):

а) замкнутость: $\forall\ a,\ b \in H_1 \cap H_2 \Rightarrow a,\ b \in H_1$ & $a,\ b \in H_2 \Rightarrow ab \in H_1$ & $ab \in H_2 \Rightarrow ab \in H_1 \cap H_2$,

б) симметризуемость: $\forall\ a \in H_1 \cap H_2 \Rightarrow a \in H_1$ & $a \in H_2$; $\Rightarrow a' \in H_1$ & $a' \in H_2 \Rightarrow a' \in H_1 \cap H_2$. Доказано, что $H_1 \cap H_2 < G$.

Покажем, что $H_1 \cap H_2 \lhd G$. Воспользуемся определением 2: $\forall\ h \in H_1 \cap H_2 \Rightarrow xhx^{-1} \in H_1 \cap H_2$. Действительно, пусть $h \in H_1 \cap H_2 \Rightarrow h \in H_1$ & $h \in H_2 \Rightarrow \forall\ x \in G\ (xhx^{-1} \in H_1$ & $xhx^{-1} \in H_2) \Rightarrow xhx^{-1} \in H_1 \cap H_2$. Значит, $H_1 \cap H_2 \lhd G$.

Определение 3*: Группа G, не имеющая нормальных делителей, отличных от E и G, называется простой группой.*

В теории групп до сих пор нет полного описания всех конечных простых групп. Важную роль играет теорема.

Теорема 2*: Знакопеременная группа A_5 является простой.*

Доказательство:

В группе A_5, помимо единичной подстановки e, имеется 15 элементов $(ij)(ke)$ порядка 2 (по три элемента этого вида в стационарной подгруппе каждой из точек 1, 2, 3, 4, 5), 20 элементов (ijk) порядка 3 и 24=4! элемента $(1, i_1, i_2, i_3, i_4)$ порядка 5.

Элементы порядка 2 все сопряжены, а так как стационарная подгруппа (относительно действия сопряжением) элемента (12)(34) содержит нечетную перестановку (12), то сопряжение может быть осуществлено четными перестановками.

То же самое относится и к элементам порядка 3. Однако, элементы порядка 5, сопряженные в группе σ_5, в группе A_5 распадаются на два класса с представителями (1 2 3 4 5) и (1 2 3 5 4). В самом деле, (4 5)(1 2 3 4 5)(4 5)$^{-1}$=(1 2 3 5 4), а стационарной подгруппой элемента (12345) в группе A_5 служит циклическая группа порядка 5, порожденная этим элементом.

Составим таблицу:

1	15	20	12	12
e	(1 2)(3 4)	(1 2 3)	(1 2 3 4 5)	(1 2 3 5 4)

В нижней строке указаны представители сопряженных классов, а в верхней - их мощности.

Пусть теперь $H \lhd A_5$, тогда согласно лемме и теореме Лагранжа $|H|=\lambda_1\cdot 1+\lambda_2\cdot 15+\lambda_3\cdot 20+\lambda_4\cdot 12+\lambda_5\cdot 12$, где $\lambda_1=1$ (так как $e\in H$), а ($\lambda_i=0$) V ($\lambda_i=1$) при i=2, 3, 4, 5.

Если а) $\lambda_2=\lambda_3=\lambda_4=\lambda_5=0$, то H=E

б) $\lambda_2=\lambda_3=\lambda_4=\lambda_5=1$, то $H=A_5$.

Следовательно, A_5 - простая группа.

Пусть дана мультипликативная группа G, $H<G$ & $H \lhd G$. Рассмотрим множество $M=\{xH \mid x\in G,\ H \lhd G\}$. Определим на этом множестве M операцию умножения классов: $\forall$ $xH\in M$, $\forall$ $yH\in M$, $xH\cdot yH \overset{df}{=} xyH$. Проверим, что результат операции не зависит от выбора x и y, то есть $\forall$ $a\in xH$ и $\forall$ $b\in xH$, $abH=xyH$. Так как $a\in xH$ & $b\in yH$ $\Rightarrow$ $(a=xh_1)$ & $(b=yh_2)$ $\Rightarrow$ $aH\cdot bH=xh_1H\cdot yh_2H=xH\cdot yH=xyH$. Итак, операция умножения смежных классов определена корректно.

Замечание 3: Аналогично для аддитивной группы можно определить операцию сложения смежных классов:

$\forall$ $(x+H)$, $\forall$ $(y+H)$, $(x+H)+(y+H) \overset{df}{=} (x+y)+H$.

Теорема 3. *Множество смежных классов группы G по нормальному делителю H образует группу.*

Доказательство: Пусть $M=\{xH \mid x\in G,\ H \lhd G\}$. Докажем, что $<M, \cdot>$ - группа.

1. $\forall$ $xH, yH \in M$, $xH\cdot yH=xyH=zH\in M$. Итак, M- замкнуто.
2. $\forall$ $xH, yH, zH\in M$, $(xH\cdot yH)zH=xH(yH\cdot zH)$, $xyzH=xyzH$.

3. $\exists\, eH\ \forall\, xH \in M, \quad eH \cdot xH = xH \cdot eH = xH.$

4. $\forall\, xH \in M\ \exists\, x^{-1}H \in M: \quad xH \cdot x^{-1}H = x^{-1}H \cdot xH = H.$

Итак, <M, •> - группа.

Построенная группа называется фактор-группой труппы *G* и обозначается *G/H* (читается:*G* по *H).*

Ее свойства зависят от свойств исходной группы *G.*

Теорема 4: *Если G циклическая группа, то и G/H - циклическая.*

Доказательство:

Пусть *G* - мультипликативная циклическая группа с образующим элементом *(a),* то есть $\forall\ x \in G\ x = a^k$, где $k \in N$. Пусть $H \lhd G$, тогда, $G/H = \{xH \mid x \in G,\ H \lhd G\}$ и $\forall\ xH \in G/H$ можно будет представить в виде $xH = a^k \cdot H = a^k \cdot H^k = (aH)^k$, то есть G/H – циклическая группа.

Теорема 5: *Если G - абелева, то G/H - абелева.*

Доказательство:

Действительно, $\forall\ xH,\ yH \in G/H,\ xH \cdot yH = yH \cdot xH,$ так как $xH \cdot yH = xyH,\ yH \cdot xH = yxH = xyH$ ($x, y \in G,$ и G - абелева).

Теорема 6 *Порядок любой фактор-группы конечной группы G является делителем порядка группы G.*

Доказательство очевидно, так как $|G/H| = ind\ H$ в группе *G* и по теореме Лагранжа он является делителем порядка группы *G.*

§ 4. Морфизмы групп.

Пусть даны две группы <A, *> и <*B*, ·>. Если они изоморфны, то мы уже знаем, что в этом случае будет существовать хотя бы одно отображение $\varphi: A \to B$, для которого будут выполнены условия:

1. $\varphi: A \to B$ - биекция $\Rightarrow$ а) φ - инъективно, то есть $\forall\ x, y \in A$ из того, что $(\varphi(x) = \varphi(y)) \Rightarrow (x = y);$ б) φ - сюрьективно, то есть $\forall\ x' \in B\ \exists\ x \in A: \varphi\{x) = x'.$

2. $\forall\ x, y \in A, \quad \varphi(x*y) = \varphi(x) \bullet \varphi(y)$

Пример 1*:* Даны две группы $<R^+, \cdot>$ и <*R*, +>, тогда отображение $\varphi: R^+ \to R$, определяемое формулой $\varphi(x) = lg(x),$ и

отображение ψ: $R \to R^+$, определяемое формулой $\psi(x)=2^x$, будут изоморфизмами.

Действительно: φ и ψ- биекции и $\forall$ $x,y \in R^+$, $lg(a \cdot b)=lga+lgb$; $\forall$ $x,y \in R$, $2^{x+y}=2^x \cdot 2^y$. Если даны две группы: $G=<A, *>$ и $<B, \bullet>=G'$, и отображение φ: $A \to B$ не является биекцией, но выполняется условие 2, то φ - называют гомоморфизмом группы G в группу G'.

Замечание 1: Если при этом, φ: $A \to B$ будет инъективно или сюръективно, то гомоморфизм называют соответственно мономорфизмом или эпиморфизмом.

Рассмотрим некоторые свойства и примеры гомоморфизмов групп.

Пусть φ -гомоморфизм группы G в группу G'.

Свойство 1: *Если e - нейтральный элемент группы G, то $\varphi(e)$ будет нейтральным элементом группы G'.*

Доказательство:

Так как φ - гомоморфизм, то $\forall$ *(a, e)* $\in G$, $\varphi(a) = \varphi(a \cdot e) = \varphi(a) \cdot \varphi(e)$ и $\varphi(a) = \varphi(e \cdot a) = \varphi(e) \cdot \varphi(a) \Rightarrow \varphi(e)$ - нейтральный элемент в группе G'.

***Свойство** 2: Если в группе G элемент a является симметричным к элементу a, то $\varphi(a')$ будет симметричным к элементу $\varphi(a)$ в группе G'.*

Доказательство:

Пусть a' симметричен (a) в группе G, так как φ-гомоморфизм, то $\varphi(e)=\varphi(a \cdot a')=\varphi(a) \cdot \varphi(a')$ и $\varphi(e)=\varphi(a' \cdot a)=\varphi(a') \cdot \varphi(a) \Rightarrow \varphi(a')$ - симметричен $\varphi(a)$ в группе G'.

Пример 2: Пусть даны две группы $\sigma_n(M)$ и $G=<\{-1, 1\}, \bullet>$. Отображение f: $\sigma_n(M) \to \{-1,1\}$, которое для $\forall$ $\varphi \in \sigma_n$:

$$f(\varphi) = \begin{cases} 1, & если \quad \varphi - четная \quad подстановка \\ -1, & если \quad \varphi - нечетная \quad подстановка \end{cases}$$

будет гомоморфизмом. Действительно, если φ и ψ- четные подстановки, то $\forall$ $\varphi, \psi \in \sigma_n$, $f(\varphi^\circ\psi)=f(\varphi) \cdot f(\psi)$, так как $f(\varphi^\circ\psi)=1$, $f(\varphi)=1$, $f(\psi)=1$.

Равенство будет выполняться и в том случае, когда φ и ψ - нечетные подстановки, а также когда одна из них четная, а другая - нечетная. Проверьте!

Очевидно, что отображение f сюръективно, но неинъективно, т.к. все четные подстановки отображаются в один элемент (1), а все нечетные в (-1). Следовательно f-эпиморфизм.

Пример 3: пример 2 можно видоизменить. Так как G=<{1,-1}, • > является подгруппой группы <Q^0, •>, то отображение f: $\sigma_n(M) \to Q^0$,

$$f(\varphi) = \begin{cases} 1, & \textit{если} \quad \varphi - \textit{четная} \quad \textit{подстановка} \\ -1, & \textit{если} \quad \varphi - \textit{нечетная} \quad \textit{подстановка} \end{cases},$$

будет просто гомоморфизмом. Проверьте!

Пример 4: Дана группа <G, *> и ее фактор-группа <*G/H*, *>. Тогда отображение φ: $G \to G/H$ такое, что $\forall$ x∈G, φ(x)=xH, будет эпиморфизмом. Действительно:

а) отображение φ - сюръективно, так как $\forall$ $xH \in G/H$ $\exists x \in G$ | φ(x)=xH;

б) отображение φ удовлетворяет условию гомоморфности, т.е. $\forall$ $x_1, x_2 \in G$, $\varphi(x_1 * x_2) = \varphi(x_1) * \varphi(x_2)$, так как $(x_1 * x_2 H) = x_1 H * x_2 H$.

Этот эпиморфизм называют каноническим эпиморфизмом группы G в свою собственную фактор-группу. Определим новое понятие, которое позволит нам связать понятия «нормальная подгруппа» и «канонический эпиморфизм».

Пусть даны две произвольные группы G и G' и φ - любой гомоморфизм группы G в G'.

Определение 1: *Множество Ker* φ = *{x∈G | φ(x)=e'} называется ядром гомоморфизма* φ *группы G в группу G' (kernel – ядро).*

Из определения ядра следует, что *Ker* φ⊂*G* и представляет собой множество элементов группы *G,* которые под действием гомоморфизма φ отображаются в нейтральный элемент группы *G'*. Или, можно сказать, что ядро - это множество прообразов нейтрального элемента *e'∈C*.

Замечание 2: Ядро является мерой неинъективности отображения φ, если *Ker* φ={e}, то *f:G→G* будет изоморфизмом.

Найдем ядро гомоморфизмов в рассмотренных выше примерах 2,3,4.

В примерах 2 и 3 *Ker* φ={φ | φ - четная подстановка}. В примере 4 *Ker* φ={*x∈G* | φ (x)=H}, так как *H* играет роль

нейтрального элемента в фактор-группе *G/H*. Однако, все элементы, которые отображаются в H содержатся в подгруппе H, то есть *Ker* φ=H. Как известно, подгруппа H в группе *G* - нормальная, так как *G* разложена в фактор-группу. Поэтому мы получили доказательство следующей теоремы.

Теорема 1: *Любая нормальная подгруппа H группы G является ядром канонического эпиморфизма* $\sigma : G \to G/H$.

Справедливо и обратное утверждение.

Теорема 2: *Если* $\varphi: G \to G'$ *- гомоморфизм, то Ker* $\varphi \lhd G$.

Доказательство: Для доказательства теоремы нужно показать:

а) *Ker* $\varphi < G$.

б) *Ker* $\varphi \lhd G$.

Пусть $\varphi: G \to G'$ - гомоморфизм. Тогда $\forall\ x, y \in Ker\ \varphi \Rightarrow$

$\varphi(x)=e' \ \&\ \varphi(y)=e'$, $\varphi(x \cdot y)=\varphi(x)\cdot\varphi(y)=e'\cdot e'=e' \Rightarrow (x \cdot y) \in Ker\ \varphi$.

$\varphi(x^{-1})=(\varphi(x))^{-1}=(e')^{-1}=e' \Rightarrow x^{-1} \in Ker\ \varphi$.

Итак, $Ker\ \varphi < G$.

Докажем, что $Ker\varphi \lhd G$. Пусть $h \in Ker\varphi$, тогда $\forall\ z \in G$, $\varphi(zhz^{-1})=\varphi(z)\cdot\varphi(h)\cdot\varphi(z^{-1})=\varphi(z)\cdot e'\cdot(\varphi(z))^{-1}=e'$.

Итак, $Ker\ \varphi \lhd G$.

Замечание 3: Из теоремы 1 и 2 можно сделать вывод, что нормальные подгруппы любой группы G, и только они, служат ядрами гомоморфизмов этой группы.

Пусть даны две группы *G* и *G′,* и φ: $G \to G'$ - гомоморфизм.

Определение 2: *Множество Im* $\varphi=\{x' \in G' \mid \exists\ x \in G: \varphi(x)=x'\}$ *называют образом группы G при гомоморфизме* φ *(image - образ).* Из определения следует, что *Im* $\varphi \subset G'$.

Например, в примере 2, *Im* $\varphi=\{1, -1\}$, в примере 4, *Im* $\varphi=G/H$.

Задача: Доказать, что *Im* $\varphi < G'$

Теорема (о гомоморфизмах): *Пусть f: G→G'- произвольный эпиморфизм,* φ: *G→ G/H – канонический эпиморфизим, тогда существует изоморфизм* ψ: *G/H→ G', такой, что* $\varphi \cdot \psi = f$.

Доказательство:

По условию теоремы *f*,φ - эпиморфизмы. Это значит, что $\forall\ x' \in G'\ \exists\ x \in G \mid f(x)=x'$ и $\forall\ xH \in G/H\ \exists\ x \in G \mid \varphi(x)=xH$.

Известно, что $H \lhd G$ и $H=Ker\ \varphi$. Найдем полный прообраз элемента $x' \in G'$ для эпиморфизма f. Так как f - эпиморфизм, то существует $x \in G \mid f(x)=x'$, найдем все остальные элементы группы G, которые отображаются в x'. Элемент $x \in G$, но он одновременно принадлежит и смежному классу $xH \in G/H$. Посмотрим, куда будут отображаться все элементы этого класса. Пусть $xh \in xH$. Тогда, $f(xh)= f(x)\cdot f(h)=x'\cdot e'=x'$, так как f - гомоморфизм, и $H=Ker\ f$, то есть все элементы подгруппы H отображаются в e'. Мы получили, что все элементы смежного класса xH отображаются в x', то есть $f(xH)=x'$.

Покажем, что все другие элементы группы G, порождающие смежные классы $yH, zH,...$, не будут отображаться в x'. Действительно, путь $y \in G$, тогда, $y \in yH$ и $f(yh)=f(y)\,f(h)=y'\cdot e'=y'$. Если теперь задать отображение $\psi: G/H \to G'$, $\psi: xH \mapsto x'$, то ψ - будет биекцией.

Выше мы показали, что отображение ψ - инъективно и сюръективно. Действительно, а) сюръективность: $\forall\ x' \in G'\ \exists\ x \in G$, а значит $\exists\ xH \in G/H \mid \psi(xH) = x'$; *б)* инъективность: мы уже показали, что $\exists\ !\ xH \in G/H \mid \psi(xH) = x'$. Отображение ψ удовлетворяет условию гомоморфности, так как

$\forall\ xH, yH \in G/H,\ \psi(xH\cdot yH)= \psi(xH)\cdot\psi(yH)$.

$$\| \qquad \| \qquad \|$$

$\psi(xyH)=(xy)' = x'\cdot y'=(xy)'$. Итак, $G/H \cong G'$.

Осталось доказать равенство $\varphi\circ\psi=f$ Возьмем произвольный элемент $x \in G$. Тогда $(x)(\varphi\circ\psi)=((x)\varphi)\psi=(xH)\psi=x'$ и $(x)f=x'$. Значит, $\psi\circ\varphi=f$. Теорема доказана.

На основе этой теоремы можно сделать следующие выводы:

- группы, на которые группа G отображается эпиморфно, исчерпываются ее собственными фактор-группами:
- группа $G' \cong G/Ker\ \varphi$;
- если φ будет гомоморфизмом группы G в группу G', то $G/Ker\varphi \cong Im\varphi$;
- если φ будет инъективным гомоморфизмом (мономорфизмом), то $Ker\ \varphi=\{e\}$ и $G \cong G/e$.

Теорема Кели: *Всякая конечная группа изоморфна некоторой группе подстановок.*

Доказательство: Пусть дана конечная группа $<G, \cdot>$.

1. Зададим отображение t_g: $G \to G$, так, что $\forall x \in G$, $\forall g \in G$, t_g: $x \mapsto xg$ (правая трансляция, сдвиг). Докажем, что t_g - подстановка, то есть

$$t_g = \begin{pmatrix} x_1 & x_2 & \dots & x_k \\ x_1 g & x_2 g & \dots & x_k g \end{pmatrix} \quad - \textit{биекция } G \textit{ на } G$$

а) Проверим инъективность:

Пусть $(x_1)t_g=(x_2)t_g$, для $\forall$ $x_1, x_2 \in G$. Тогда из того, что $(x_1 g = x_2 g) \Rightarrow (x_1 = x_2)$, так как $\forall g \in G \; \exists \, g^{-1} \in G \mid g \cdot g^{-1} = e$;

б) сюръективность: $\forall x_s g \;\; \exists x_s \mid (x_s)t_g = x_s g$.

Из условий а) и б) следует, что отображение t_g биекция.

2. Образуем множество $G' = \{t_g \mid g \in G\}$ правых трансляций. Докажем, что $<G', \circ>$ - группа относительно операции композиции подстановок.

а) Проверяем условие замкнутости:

$\forall x \in G$, $\forall t_g, t_k \in G'$, $(x)(t_g \circ t_k) = (xt_g)t_k = (xg)t_k = xgk \Rightarrow t_g \circ t_k \in G'$;

б) $\exists t_e \in G'$: $t_e \circ t_g = t_g \circ t_e = t_g$. Действительно, $\forall x \in G$

$x(t_e \circ t_g) = (xt_e)t_g = (xe)g = xeg = xg$

$x(t_g \circ t_e) = (xt_g)t_e = (xg)e = xg$

в) условие симметризуемости:

$$\forall \; t_g \in G' \; \exists \quad t_g^{-1} = \begin{pmatrix} x_1 g & x_2 g & \dots & x_k g \\ x_1 & x_2 & \dots & x_k \end{pmatrix} : t_g \cdot t_g^{-1} = t_g^{-1} \cdot t_g = t_1,$$

где t_e – тождественная подстановка.

г) ассоциативность:

$\forall \; t_g, t_k, t_s \in G'$ $\quad (t_g \circ t_k) \circ t_s = t_g \circ (t_k \circ t_s)$. Действительно, $\forall x \in G$, $(x)[(t_g \circ t_k) \circ t_s] = xgks$, $(x)[t_g \circ (t_k \circ t_s)] = xgks$, то есть операция композиции ассоциативна.

Таким образом $<G, \circ>$ - группа.

3. Докажем, что $<G, \cdot> \cong < G', \circ>$.

а) зададим отображение $\psi: G \to G'$ такое, что $\forall g \in G$, $\psi: g \mapsto f_g$:

б) докажем, что ψ - биекция.

Инъективность:

Пусть $\forall \; g_1, g_2 \in G$, $\psi(g_1) = \psi(g_2)$. Тогда $t_{g1} = t_{g2} \Rightarrow \forall x \in G$, $(x)\,t_{g_1} = (x)\,t_{g_2} \Rightarrow (xg_1 = xg_2) \Rightarrow (x^{-1}xg_1 = x^{-1}xg_2) \Rightarrow (eg_1 = eg_2) \Rightarrow (g_1 = g_2)$.

Сюръективность очевидна, так как $\forall\ t_g\ \exists\ g \mid \psi(g)=t_g$.

в) проверим условие гомоморфности: $\forall\ g_1,\ g_2 \in G$, $(g_1 \cdot g_2)\psi=(g_1)\psi^{\circ}(g_2)\psi$. Действительно, $(g_1 \cdot g_2)\psi=f_{g_1 g_2}$ $(g_1)\psi^{\circ}(g_2)\psi=f_{g_1}{}^{\circ} f_{g_2}=f_{g_1 g_2}$. Итак, $G \cong G'$.

Рассмотрим частные случаи теоремы Кели.

Пример 5: Пусть $<G,*>$ конечная мультипликативная группа третьего порядка, где $G=\{a, b, c\}$ и операция * задана таблицей Кели:

*	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

Каждому элементу $a \in G$ поставим в соответствие преобразование t_a: $G \to G$, определяемое формулой $\forall\ x \in G$, $t_a(x)=ax$. Так как

$$t_a: \begin{cases} a \mapsto a \\ b \mapsto b, \\ c \mapsto c \end{cases} \quad t_b: \begin{cases} a \mapsto b \\ b \mapsto c, \\ c \mapsto a \end{cases} \quad t_c: \begin{cases} a \mapsto c \\ b \mapsto a \\ c \mapsto b \end{cases},$$

то преобразования t_a, t_b, t_c является подстановками множества G и называются левыми трансляциями G. Множество $T(G) = \{t_a, t_b, t_c\}$ называется множеством левых трансляций. Оно является группой подстановок $<T(G), \circ>$ относительно операции композиции. (Проверьте!)

Покажем, что группы $<G,*>$ и $<T(G),\circ>$ изоморфны. Зададим отображение φ: $G \to T(G)$ формулой: $\forall\ a \in G$, $\varphi(a)=t_a$. Отображение φ - биективно. Кроме того, φ удовлетворяет условию гомоморфности, так как $\forall\ x, y \in \{a, b, c\}$, $\varphi(x*y)=t_{xy}=t_x \circ t_y=\varphi(x)\circ\varphi(y)$. Таким образом, $<G,*> \cong <T(G),\circ>$. Мы указали еще один конструктивный способ построения для произвольной конечной группы G изоморфной ей группы подстановок T(G) - группы левых трансляций. Очевидно, что если G — коммутативна, то множества ее левых и правых трансляций совпадают.

***Пример 6**:* Рассмотрим аддитивную группу $<Z_3, \oplus>$ классов вычетов по модулю 3. Покажем, что она изоморфна некоторой группе подстановок. Составим таблицу Кэли для группы Z_3:

$\oplus$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Учитывая первую, вторую и третью строку таблицы, образуем подстановки:

$\varphi_0 = \begin{pmatrix} 0 & 1 & 2 \\ 0 & 1 & 2 \end{pmatrix}$ $\varphi_1 = \begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \end{pmatrix}$ $\varphi_2 = \begin{pmatrix} 0 & 1 & 2 \\ 2 & 0 & 1 \end{pmatrix}$. Легко показать, что множество $\{\varphi_0, \varphi_1, \varphi_2\}$ относительно операции $\circ$ композиции преобразований является группой. Составим таблицу Кэли для этой группы подстановок:

$\circ$	φ_0	φ_1	φ_2
φ_0	φ_0	φ_1	φ_2
φ_1	φ_1	φ_2	φ_0
φ_2	φ_2	φ_0	φ_1

Покажем, что группы $<Z_3,+>$ и $<\{\varphi_0, \varphi_1, \varphi_2\},\circ>$ изоморфны.

1) Зададим отображение $f: Z_3 \to \{\varphi_0, \varphi_1, \varphi_2)$ так, что $f(s)=\varphi_s$, где s=0, 1, 2.

2) Отображение f удовлетворяет условию гомоморфности, то есть $\forall\ r, s \in \{0, 1, 2\}$, $f(r \oplus s)=\varphi_r \circ \varphi_s$.

Действительно, если сравнить обе таблицы, то видно, что они устроены одинаково, то есть поэлементно совпадают с точностью до обозначений, при этом $r \oplus s \mapsto \varphi_r \circ \varphi_s$. Значит, f— гомоморфизм.

3) Очевидно, что f - биекция.

Таким образом, рассматриваемые группы изоморфны. Так как $<Z_3,+>$ - циклическая группа, то и группа $<\{\varphi_0, \varphi_1, \varphi_2\},\circ>$

является конечной циклической группой с образующим элементом φ_2, соответствующим образующему элементу 2 группы $<Z_3,\oplus>$.

Пусть дано произвольное множество *M.* Обозначим через *S(M)* - множество всех биекций (преобразований) множества *M,* то есть $S(M)=\{\varphi \mid \varphi: M\to M\}$. Как известно, множество *S(M)* относительно операции композиции биекций будет группой. Рассмотрим гомоморфизмы произвольной группы G в группу $<S(M), \circ>$.

Определение 1: *Представлением (реализацией) группы G в группе S(M) называют любой гомоморфизм f: G→S(M).*

Выясним, каким образом можно задать этот гомоморфизм?

$\forall$ $g\in G$, обозначим через φ, - биекцию из группы *S(M),* которая соответствует элементу (g) в том смысле, что $\varphi_g(x)=gx$, где $x\in M$. Тогда, $\varphi_e(x)=ex=x$, а $\varphi_g\circ\varphi_h=\varphi_{gh}$, где $g, h\in G$, $\varphi_g,\varphi_h\in S(M)$. Действительно, $(\varphi_g\circ\varphi_h)(x)= \varphi_g(\varphi_h(x))= \varphi_g(hx)=ghx$. Образ элемента $(x)\in M$ относительно биекций φ_g часто обозначают просто символом $g\cdot x$, что дает право говорить об отображении φ_g: $(g,x) \mapsto g\cdot x$ декартова произведения $G\times M\to M$.

Определение 2: *Говорят, что группа G действует (слева) на множестве M, M - является G — множеством, если задано отображение из* $G\times M\to M$, $(g,x) \mapsto g\cdot x$, *удовлетворяющее условиям:*

1. $ex=x, x\in M$.
2. $gh(x)=g(hx), g, h\in G, x\in M$.

Имея теперь *G* - множество множества *M,* которое получено с помощью отображения $\varphi_g(x)=gx$, можно определить отображение *f* - группы *G* в группу S(M) так: $\forall$ $g\in G$ $f(g)=\varphi_g$. Это отображение будет гомоморфизмом. Действительно, $\forall$ $g, h\in G$, $f(g\cdot h)=f(g)\circ f(h)$ так как $f(g\cdot h)=\varphi_{gh}$, $f(g)\circ f(h)=\varphi_g\circ\varphi_h=\varphi_{gh}$

Рассмотрим теперь на конкретном примере действие группы *G* на множестве *M.* Выберем в качестве множества *M* - множество точек плоскости $(M=R^2)$. Тогда группа *S(M)* будет представлять собой группу биекций φ: $R^2\to R^2$.

В качестве группы *G* рассмотрим группу вращений точек плоскости вокруг центра *O,* то есть $G=<\{\varphi_k\},\circ>$. Отображение

$\Phi_{\varphi k}$: $G x R^2 \to R^2$ можно задать так: $\Phi_{\varphi k}$: $<\varphi_k, A> \mapsto (\varphi_k(A)=B)$, оно и будет определять действие группы G на множестве $(R^2=M)$, так как выполняются условия:

1. $\Phi_{\varphi 0}(\varphi_0, A)=\varphi_0(A)=A$.

2. $\Phi_{\varphi k \varphi s}(A)=(\varphi_k \circ \varphi_s)A=\varphi_k(\varphi_s(A))$.

Если теперь задать отображение f: $G \to S(R^2)$, f: $\varphi_k \mapsto \Phi_{\varphi k}$, то оно будет гомоморфизмом. Действительно, $\forall$ φ_k, $\varphi_s \in G$, $f(\varphi_k \circ \varphi_s)=f(\varphi_k) \circ f(\varphi_s)$, так так $f(\varphi_k \circ \varphi_s)=f(\varphi_{ks})=\Phi_{\varphi ks}$, $f(\varphi_k) \circ f(\varphi_s)=\Phi_{\varphi k} \circ \Phi_{\varphi s}=\Phi_{\varphi ks}$

Таким образом, мы представили (реализовали) группу вращений плоскости G в группе биекций точек плоскости.

Замечание 1: Ядро $Ker f=\{g \in G \mid f(g)=e \in (S(M))\}$ гомоморфизма f: $G \to S(M)$ называют ядром действия группы G. Если f - мономорфизм, то говорят, что группа G действует на множестве M эффективно.

Определение 3: *Два элемента $x, y \in M$ называются эквивалентными относительно группы G, действующей на M, если $x=gy$ для некоторого элемента $g \in G$.*

Замечание 2: Если задать отношение ρ на множестве M,

$\forall$ $x, y \in M$, $x \rho y \overset{df}{\Leftrightarrow}$ $(x=gy)$, то это отношение будет отношением эквивалентности на M (проверьте самостоятельно).

Определение 4: *Классы эквивалентности по отношению ρ называют G - орбитами множества M. Орбиту, содержащую элемент $x_0 \in M$, обозначают символом $G(x_0)$, то есть $G(x_0) = \{gx_0 \mid g \in G\}$.*

Замечание 3: Понятие орбиты пришло в алгебру из геометрии. Если рассматривать группу вращений точек плоскости вокруг начальной точки O, то орбитой точки A будет служить окружность с центром в O, проходящая через точку A, $A \rho B \Leftrightarrow A=\varphi_k(B)$, а множество $M=R x R=R^2$ будет объединением концентрических окружностей (классов эквивалентности), включая окружность нулевого радиуса (точка O).

Для нас понятие орбиты также не является новым. Мы им пользовались, когда раскладывали перестановки $\varphi \in \sigma(M)$ в произведение независимых циклов.

Пусть теперь x_0 - фиксированный элемент множества M. Рассмотрим множество $S_t(x_0) \overset{df}{\Leftrightarrow} \{g \in G \mid gx_0=x_0\}$. Из этого определения следует, что $S_t(x_0) \subset G$. Покажем, что $S_t(x_0)<G$. Действительно, так как $ex_0=x_0$ и $\forall$ g, $h \in S_t(x_0)$ будем иметь: $(hx_0=x_0)$ & $(gx_0=x_0)$, тогда, $(gx_0=hx_0) \Rightarrow (x_0=g^{-1} \cdot hx_0) \Rightarrow g^{-1} \cdot h \in S_t(x_0) \Rightarrow S_t(x_0)$ будет подгруппой группы *G*.

***Определение* 5:** *Подгруппа* $S_t(x_0)<G$ *называется стационарной подгруппой (стабилизатором) элемента* $x_0 \in M$ *в группе G.*

Для рассмотренного выше действия группы *G* на R^2 будем иметь, что $S_t(A)=\{\varphi_k \in G \mid \varphi_k(A)=A\}$, тогда $S_t(0)=G$, так как $\forall$ $\varphi_k \in G$, $\varphi_k(0)=0$. Если $A \neq 0$, то $S_t(A)=\varphi_0$, где φ_0 - поворот на нулевой угол, так как $\varphi_0(A)=A$.

Определение 6*: Порядок группы* $|S_t(x_0)|$ *- называется длиной G - орбиты точки* x_0.

Для конечной группы *G,* длина любой *G* - орбиты элемента x_0 является делителем порядка группы *G* (это следует из теоремы Лагранжа).

Рассмотрим еще несколько примеров действия группы на множествах.

Пример 2: При доказательстве теоремы Кели мы рассматривали действие группы *G* на себе. Действительно, была дана произвольная конечная группа *G.* В качестве множества M мы брали носитель группы *G,* то есть *M=G.* Затем, на *G* задали биекции:

$$\varphi_g = \begin{pmatrix} x_1 & x_2 & \dots & x_n \\ x_1 g & x_2 g & \dots & x_n g \end{pmatrix},$$

т. е. $\varphi_g(x_i)=x_i \cdot g$, которые назвали правым сдвигом на элемент *g*.

Доказали, что множество $S(G)=\{\varphi_g \mid g \in G\}$ является группой. Затем задали отображение f: $G \to S(G)$, f: $g \mapsto \varphi_g$ и доказали, что оно является изоморфизмом. Таким образом, конечная группа *G* была эффективно реализована (представлена) группой подстановок элементов этой же группы. Следует отметить, что правые (левые) сдвиги задают действие группы *G* не только на себе, но и на ее фактор-множествах. Если, например, $H \lhd G$ и

G/H — множество левых смежных классов, то есть $G/H = \{gH \mid g \in G, H<G\}$, то отображение $\varphi_x(x, gH) \mapsto x(gH)=xgH$ определяет действие группы G на G/H, а отображение f: $G \to S(G/H)$, $f: x \mapsto \varphi_x$ будет гомоморфизмом. Ядром этого действия (гомоморфизма f) будет множество $Ker\ f=\{x \in G \mid f(x)=\varphi_e\}$.

Пусть дана произвольная группа $<G, \cdot>$.

Пример 3*:* Если множество M=G, то действие группы на себе можно определить действием любого элемента $g \in G$ посредством автоморфизма: φ_g: Gx$G \to$G, $\varphi_g(g,x) \to gxg^{-1}$, то есть $\varphi_g(x)=g \cdot x \cdot g^{-1}$, где $g \in G$, $x \in G$.

Действительно, $\varphi_e(e,x)=e \cdot x \cdot e^{-1}=x$ и $(h \cdot g)(x)=h(g(x))$, так как $(hg)x(hg)^{-1}=h(gxg^{-1})h^{-1}$. Это действие называется сопряжением. Тогда отображение $f: G \to S(G)$, $f: g \mapsto \varphi_g$ будет гомоморфизмом, представляющим группу G в группе ее внутренних автоморфизмов. Ядром этого гомоморфизма будет множество:

$Ker\ f=\{g \in G \mid f(g)=\varphi_e\}=\{g \in G \mid x=gxg^{-1}\}= =\{g \in G \mid xg=gx\}$.

Если в группе G задать отношение: $\forall\ x,g \in G$, $x \rho g \overset{df}{\Leftrightarrow} x=gxg^{-1}$, то оно будет отношением эквивалентности, задающим разбиение G на классы сопряженных элементов - (G - орбиты).

Действие сопряжением группы G на себе можно перенести на подмножества и подгруппы группы G, определив для этого понятия сопряженных множеств.

Определение 7*: Два подмножества $A, B \in G$ называют сопряженными, если $A=gBg^{-1}$, при некотором $g \in G$.*

В этом случае, отображение φ_g: GxБ$(G) \to Б(G)$ на элементах будет задано так: φ_g: $<g, H> \mapsto gHg^{-1}$, где $H<G$. Тогда $S_t(H)=\{g \in G \mid gHg^{-1}=H\}$, ясно, что, если $S_t(H)=G$, то $H \lhd G$.

Пример 4*:* Пусть дана группа σ_3(M). Зададим отображение $\varphi \mapsto f \circ \varphi \circ f^{-1}$, $\forall\ \varphi \in \sigma_3$(M). Это действие сопряжением задает разбиение σ_3(M) на сопряженные классы (орбиты).

σ_3(M)=$\{e\} \cup \{(1\ 2), (1\ 3), (2\ 3)\} \cup \{(1\ 2\ 3), (1\ 3\ 2)\}$. Длины орбит: 1, 2, 3 являются делителями порядка самой группы ($|\sigma_3(M)|=6$).

§ 5. Теоретико-групповые конструкции.

П. 1. Групповое замыкание.

Пусть дана абстрактная группа *G*. Мы уже знаем, что, выбрав любой элемент $a \in G$, мы можем построить циклическую подгруппу этой группы - G_a, причем, $|G_a| = p(a)$. Кроме того, пересечение любого числа таких подгрупп снова будет подгруппой данной группы ($\bigcap_{a \in G} G_a < G$).

Как показывают простейшие примеры, объединение подгрупп, в общем случае, подгруппой не будет.

Пример 1: Объединение подгрупп $<R^2, +>$ и $<R, +>$ группы $<R^3, +>$ будет подгруппой $<R^2, +>$.

Пример 2: Пусть даны две группы $G_1 = <R^+, \cdot>$ и $G_2 = <\{1,-1\}, \cdot>$. Их объединение $G_1 \cup G_2$ уже не является группой, так как множество $R^+ \cup \{1,-1\}$ не будет замкнуто относительно операции умножения.

***Пример 3*:** Пусть даны две подгруппы $H_1 = \{(1), (1\ 2)\}$ и $H_2 = \{(1), (1\ 3)\}$ симметрической группы подстановок $\sigma_3(M)$.

Их объединение $\{(1), (1\ 2), (1\ 3)\}$ подгруппой не будет, так как оно не содержит элемента $(1\ 2)(1\ 3) = (1\ 2\ 3)$.

Поэтому, для всех подгрупп $H_i < G$ операцию их теоретико-множественного объединения заменяют операцией сопоставления заданным подгруппам наименьшей подгруппы, содержащейся в них.

Рассмотрим эту операцию более подробно. Найдем сначала наименьшую подгруппу H, содержащую заранее выбранные элементы группы G.

Пусть, например, $a, b, c \in G$ (дальнейшие рассуждения не зависят от количества выбранных элементов). Итак, три элемента искомой группы уже известны. Так как мы строим подгруппу, то нейтральный элемент *(e)* должен принадлежать H. Кроме этого, множество H должно быть замкнуто относительно групповой операции ($\forall\ a, b \in H,\ a \cdot b \in H$) и симметризуемо ($\forall\ a \in H,\ a^{-1} \in H$), поэтому *H* будут принадлежать все целые степени элементов *a, b, c,* а также их произведения.

Следовательно, подгруппа H будет состоять из элементов вида: $a^m \cdot b^n \cdot c^k$,где *m, n, k*$\in Z$. Тогда $\forall$ *x, y*$\in H$, если $x=a^s \cdot b^p \cdot c^q$, $y=a^m \cdot b^n \cdot c^k$, то $x \cdot y = a^{s+m} \cdot b^{p+n} \cdot c^{q+k}$, то есть любые произведения степеней образующих элементов *a, b, c* также представимы в виде произведения степеней этих элементов. Причем, $e=a^0 \cdot b^0 \cdot c^0$, а если $x=a^m \cdot b^n \cdot c^\kappa$, то $x^{-1}=c^{-k} \cdot b^{-n} \cdot a^{-m}$.

Построенная подгруппа H будет содержаться в любых других подгруппах $H_i<G$ которые содержат элементы *a, b, c* и еще какие-то другие элементы. Подгруппу H обозначают так: *H={a, b, c}*. Элементы *a, b, c* называют образующими элементами подгруппы H в группе *G* (для циклических подгрупп, как мы знаем, система образующих состоит из одного элемента).

Замечание 1: Для построения подгруппы *H,* в общем случае, мы могли взять не три элемента a, b, *c,* а любое подмножество *M*$\subset G$. В этом случае множество *M* будет системой образующих элементов для минимальной подгруппы H, то есть *H={M}*.

Пример 4*:* Найти подгруппу *H*={*4,* 6} в группе <*Z,+*>.

Решение:

Так как подгруппа аддитивная, то элементы искомой подгруппы H будут иметь вид: *4k+6n,* где k, *n*$\in Z$. Ясно, что все эти целые числа четные, поскольку их можно представить в виде: *2(2k+3n)*. Но все ли четные числа принадлежат интересующей нас подгруппе?

Да, все, так как при *k=-1, n=1, 4k+6n=2,* а двойка порождает подгруппу <2Z,+>. Следовательно, H={4, 6}=<2Z,+>.

Если теперь рассмотреть пересечение всех подгрупп H_i группы G, которое содержит подмножество *M,* то это пересечение (как мы уже доказали раньше) будет подгруппой группы *G*. Обозначим эту подгруппу через $\overline{M}$. Она и будет минимальной подгруппой группы G с системой образующих *M.*

Определение 1*:Подгруппа* $\overline{M} \overset{df}{=} \bigcap_{M \subset H_i} H_i$ *называется групповым замыканием подмножества M или группой, порожденной множеством M, и обозначается:* $\overline{M}$ *={M}.*

***Замечание 2**:* Подгруппа *M* будет состоять из нейтрального элемента *(e)* и всевозможных произведений элементов $a^1, a^2, ..., a^k, k=1, 2, .., n,...,$ если $a_i \in M,$ или $a_i^{-1} \in M.$

***Замечание 3**:* Если H подгруппа группы G, M⊂H и $\overline{M} = H,$ то говорят, что *M* является системой образующих для подгруппы *H*.

П.2. Коммутант. Центр группы.

Пусть дана произвольная группа $<G, \cdot>$. Известно, что не для любых x, $y \in G, x \cdot y = y \cdot x.$

***Определение 2**: Выражение $[x, y] = x \cdot y \cdot x^{-1} \cdot y^{-1}$ называется коммутатором элементов x, y группы G.*

Коммутатор служит корректирующим членом, необходимым для того, чтобы поменять местами *x* и y в группе G, $x \cdot y = [x,y] \cdot yx$.

Замечание 4: Если $x \cdot y = y \cdot x$ для ∀x, y∈G, то $[x,y]=e.$

Если $[x_1, y_1]$ и $[x_2, y_2]$ - коммутаторы, то $[x_1,y_1] \cdot [x_2,y_2]$ в общем случае не будет коммутатором.

Чем больше будет в группе *G* коммутаторов, отличных от (*e*), тем значительнее отклонение закона умножения в *G* от коммутативного.

Обозначим через S - множество всех коммутаторов в группе G, то есть S={[x, y], *x, y*∈G}.

***Определение 3:** Подгруппа G′, порожденная множеством S, называется коммутантом группы G (производной подгруппой), G′={S}.*

***Замечание5**:* Подгруппа G состоит из всевозможных произведений вида: $[x_1,y_1] \cdot [x_2,y_2] \cdot ... \cdot [x_k,y_k]$, где $x_i, y_i \in G$

***Пример* 5**: Пусть дана группа $\sigma_3(M)$. Выберем в ней две подстановки, например, $\varphi_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ и $\varphi_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$. Найдем их коммутатор.

$$[\varphi_1,\varphi_2]=\varphi_1\circ\varphi_2\circ\varphi_1^{-1}\circ\varphi_2^{-1}=\left(\left(\left(\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\circ\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\right)\circ\begin{pmatrix}2&3&1\\1&2&3\end{pmatrix}\right)\circ\begin{pmatrix}1&3&2\\1&2&3\end{pmatrix}\right)=$$

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

Подстановка $\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$ - четная. Проверьте, что коммутатор любых двух подстановок из группы $\sigma_3(M)$ будет четной подстановкой, то есть $S=A_3$ и коммутант $G'=A_3$, а так как $A_3 \lhd \sigma_3(M)$, то и $G' \lhd \sigma_3(M)$.

Докажите, что если дана группа $\sigma_n(M)$, то $G'=A_n$, то есть $(A_n=G') \lhd G_n(M)$.

Теорема 1: *Любая подгруппа $H<G$, содержащая коммутант G' группы G, нормальна в G.*

Доказательство:

Пусть $H<G$ и $G'\subset H$. Докажем, что $H \lhd G$. Для этого возьмем любой элемент $x\in H$ и покажем, что сопряженный к нему элемент $g\cdot x\cdot g^{-1}= =(g\cdot x\cdot g^{-1}) \cdot (x^{-1}\cdot x)=(g\cdot x\cdot g^{-1}\cdot x^{-1})\cdot x=[g, x]\cdot x \in(G'\cdot H=H) \Rightarrow H \lhd G$, что и требовалось доказать.

Пусть G' коммутант группы G. В подгруппе $G'<G$ также можно построить подгруппу $(G')'=G''$, которую называют второй производной подгруппой (вторым коммутантом) группы G. Продолжая этот процесс, можно определить k-ую производную группу $G^k=(G^{k-1})'$.

Согласно выше доказанной теореме (1), можно записать ряд нормальных подгрупп $\dots G^k \lhd G^{k-1} \lhd G^{k-2} \lhd \dots \lhd G^2 \lhd G^1 \lhd G(*)$

Определение 4: *Группа G называется разрешимой, если ряд (*) обрывается на единичной подгруппе, то есть $G^m=e$, m - называют ступенью разрешимости.*

Пример 6*:* Любая абелева группа является разрешимой ступени 1, так как $G'=\{e\}=E$.

Пример 7*:* Знакопеременная группа A_4 - разрешимая ступени 2, а симметрическая группа $\sigma_4(M)$ - разрешимая ступени 3, так как $\sigma_4'=A_4$, $A_4'=V_4$, $V_4'=E$.

Своему названию разрешимые группы обязаны теории Галуа. Знаменитый математик Эварист Галуа показал, что разрешимость алгебраических уравнений:
$a_n x^n+a_{n-1}x^{n-1}+\ldots+a_1x+a_0=0$, степени n=4, в радикалах связана с разрешимостью группы подстановок σ_4(M) и всех ее подгрупп.

В § 3 мы доказали, что подгруппа A_5 - простая, то есть она не содержит нетривиальных нормальных подгрупп и, следовательно, не является разрешимой. Поэтому и алгебраические уравнения степени n>4 неразрешимы в радикалах.

Степень отклонения от коммутативного закона в группе *G* можно характеризовать не только с помощью коммутанта, но и с помощью понятий «централизатор», «центр группы».

Пусть дана произвольная группа G. Определим в ней отношение сопряженности: $\forall\ a,\ x\in G\ afx \Leftrightarrow a=x\cdot a\cdot x^{-1}$ (часто используются степенные обозначения: $x\cdot a\cdot x^{-1}=a^x$). Мы уже знаем, что это отношение является отношением эквивалентности. Следовательно, группа *G* разбивается на непересекающиеся классы сопряженных элементов.

Пример 8: Пусть дано произвольное поле <P,+,·>, так как его аддитивная и мультипликативная группы- <P,+> и $<P^0,\cdot>$ абелевы, то любой их класс сопряженных элементов будет состоять из одного элемента.

Действительно, $afx \Leftrightarrow a=x\cdot a\cdot x^{-1}=x\cdot x^{-1}\cdot a=a$.

Пример 9: В симметрической группе подстановок $\sigma_n(M)$ две подстановки φ_i и φ_k будут относиться к одному классу сопряженных элементов, если они имеют одинаковое циклическое строение. Например, подстановки φ_1=(1 5)(2 4 3 6) и φ_2=(1 2)(3 4 5 6) сопряжены в группе $\sigma_6(M)$ (проверьте!)

Пример 10: **В** мультипликативной группе матриц $M_{nn}(F)$ над алгебраически замкнутым полем *F,* две матрицы *A* и *B* будут сопряжены, если существует $T\in M_{nn}(F) : A=T\cdot B\cdot T^{-1}$.

Замечание 6: В отличие от смежных классов *xH,* полученных при разложении группы *G* по подгруппе H, классы сопряженных элементов не всегда равномощны.

Пример 11: Непосредственным подсчетом можно убедиться, что группа σ_3(M) распадается на следующие три класса

сопряженных элементов, имеющих разное количество подстановок:

$$\left\{\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}\right\};\left\{\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix},\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix},\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}\right\};u\left\{\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix},\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\right\}.$$

При вычислении мощности сопряженных классов важную роль играет понятие нормализатора.

Пусть H подгруппа группы *G* и подмножество *M* содержится в *H*.

Определение 5: *Нормализатором множества M в подгруппе H группы G называется множество элементов из H, которые перестановочны с множеством M, то есть*

$N_H(M) \stackrel{df}{=} \{h \mid h \in H,\ hM=Mh\}$ *или* $N_H(M) \stackrel{df}{=} \{h \mid h \in H,\ h \cdot M \cdot h^{-1}=M\}$.

Замечание 7: Если не указано, в какой подгруппе *H* группы *G* берется нормализатор, то это означает, что он берется во всей группе G, то есть $N_G(M) \stackrel{df}{=} \{g \mid g \in G,\ gM=Mg\}$.

Замечание 8: Если подгруппа H является нормальной в группе *G,* то ее нормализатор будет совпадать со всей группой, так как $N_G(H)=\{x \mid x \in G,\ xH=Hx\}=\{G\}$.

Теорема 2: *$N_G(H)<G$ (нормализатор любой подгруппы H в группе G является ее подгруппой).*

Доказательство:

Действительно, для $\forall\ a,\ b \in N_G(H)$ по определению будет следовать, что $H^a = H$ и $H^b = H$, тогда $H^{ab} = (H^a)^b = H^b = H \Rightarrow (a \cdot b) \in N_G(H)$.

$\forall\ a \in N_G(H) \Rightarrow H^a=H,$ тогда $H^{a^{-1}}=(H^a)^{-1}=H \Rightarrow a^{-1} \in N_G(H)$. Итак, $N_G(H)<G$.

Из определения нормализатора множества $M \subset H$, где $H<G$ следует, что его элементы перестановочны с множеством M в целом *(hM=Mh* или $M^h=M$).

Однако, можно определить также множество тех элементов из H, которые перестановочны с *M* поэлементно, то есть $\{x \mid x \in H,\ mx=xm,\ \forall\ m \in M\}$.

Это множество называется централизатором множества *M* в подгруппе H группы *G* и обозначается символом $Z_H(M)$.

Замечание 9: Если множество M состоит из одного элемента, то есть $M=\{a\}$, то его нормализатор и централизатор совпадают.

Замечание 10: Если не указано, в какой подгруппе H группы G берется централизатор, то это означает, что он берется во всей группе G.

Определение 6: Централизатор всей группы G называется ее центром и обозначается символом $Z(G)$.

Из определения следует, что центр группы G - это множество ее элементов, которые перестановочны с каждым элементом этой группы.

Пример 12*:* Если группа G - абелева, то ее центр совпадает с самой группой, то есть $Z(G)=G$, так как $\forall\ x, y\in G\ x\cdot y=y\cdot x$.

Теорема 3: *Центр группы является ее нормальной подгруппой* $(Z(G)\lhd G)$.

Доказательство:

а) Докажем сначала, что $Z(G)<G$. Из определения центра, ясно, что нейтральный элемент $e\in Z(G)$. Если $x,y\in Z(G)$, то $\forall g\in G$ будем иметь: $(x\cdot y)\cdot g=x\cdot(y\cdot g)=x\cdot(g\cdot y)=(x\cdot g)\cdot y=(g\cdot x)\cdot y=g\cdot(x\cdot y)$, то есть $x\cdot y\in Z(G)$.

Если $x\in Z(G)$, то $\forall\ g\in G\ g\cdot x=x\cdot g$. Отсюда

$x^{-1}\cdot g=x^{-1}\cdot(g\cdot x)\cdot x^{-1}=(x^{-1}\cdot x)\cdot g\cdot x^{-1}=g\cdot x^{-1}$, то есть $x^{-1}\in Z(G)$. Итак, $Z(G)<G$.

б) Докажем, что $Z(G)\lhd G$. Пусть $h\in Z(G)$, $g\in G$, тогда $ghg^{-1}=g\cdot g^{-1}\cdot h=h\Rightarrow g\cdot h\cdot g^{-1}\in H$. Итак, $Z(G)\lhd G$.

Рассмотренные выше понятия коммутанта и центра группы позволяют судить о степени некоммутативности группы G. Чем меньше коммутант и больше центр, тем группа G ближе к абелевой.

п.3 Прямое произведение групп.

Пусть даны две абстрактные группы $<A, \cdot>$ и $<B,*>$. Построим с помощью этих групп новую группу. Для этого нам нужно указать элементы новой группы и групповую операцию. Пусть элементами новой группы будут пары элементов $<a, b>$, где $a\in A$, $b\in B$, то есть множеством - носителем новой группы

будет декартово произведение AxB=$\{<a, b> \mid a \in A, b \in B\}$. Операцию на множестве AxB определим так: $\forall$ $<a, b>$, $<c, d> \in (A$x$B)$, $<a, b> \otimes <c, d> \Leftrightarrow <a \cdot c, b*d>$, то есть над первыми компонентами пары производится операция, заданная в группе $<A, \cdot>$, а над вторыми - операция, заданная в группе <B, *>. Докажите самостоятельно, что $<(A$x$B), \otimes>$ будет группой.

Полученная группа $G=<A$x$B, \otimes >$ называется внешним прямым произведением групп $<A, \cdot>$ и $<B, *>$ и обозначается $G=A$xB.

Если группы $<A, \cdot>$ и <B, *> - аддитивные, то говорят о прямой сумме, то есть $G= A$x$B = A \oplus B$.

Пример 13*:* Найти прямую сумму двух групп $<R^1, +>$ и $<R^1, +>$.

Решение:

$G=R^1$x$R^1=\{<a, b> \mid a \in R, b \in R\}=R^1 \oplus R^1$

$<a, b> + <c, d>=<a+c, b+d>$, то есть G - аддитивная группа векторов плоскости.

Пример 14*:* Поле комплексных чисел является прямой суммой двух абелевых групп $A=<R, +>$ и $B=<Ri, +>$. Действительно, $G=R \oplus Ri$ $<a,bi>+<c, di>=<(a+c), (b+d)i>$.

Пример 15*:* Найти прямое произведение групп: $<R^+, \cdot>$ и $<\{1, -1\}, \cdot>$.

Решение:

$$G=R^+ \text{x} \{1,-1\}=\{<a,1>,<b,-1> \mid a,b \in R^+\},$$

$<a,1> \bullet <b,1>=\{<a \bullet b,1>\}$ *или* $<a,1> \bullet <b,-1>=<\{<ab,-1>\}$.

Проверьте самостоятельно, что в группе $G = A$xB $(G = A \oplus B)$ можно выделить две подгруппы $G_1 = <\{A$x$e'\}, \cdot>$, где Ax$e' = \{<a, e'> \mid a \in A, e' \in B\}$ и $G_2 = <\{e$xB$\}, \cdot>$, где ex$B = \{<e, b> \mid e \in A, b \in B\}$.

Зададим отображения:

$\varphi: A \to G_1$, $\varphi: a \mapsto (a, e')$ и $\psi: B \to G_2$, $\psi: b \mapsto$ (e, b).

Проверьте, что отображение φ будет изоморфизмом группы A на G_1,а отображение ψ будет изоморфизмом группы B на G_2.

Следовательно, группа $G=A\text{x}B$ будет содержать подгруппы, изоморфные A и B, $(A\cong G_1)$, $(B\cong G_2)$.

Теорема 4*: В группе $G=A\text{x}B$ подгруппы G_1 и G_2 являются нормальными делителями, причем $G_1\cap G_2=e(G)$.*

Доказательство:

Покажем, что подгруппы G_1 и G_2 замкнуты относительно сопряженных элементов.

$\forall(a,e')\in G_1\ \forall(c,d)\in G$ будем иметь

$(c,d)(a,e')(c,d)^{-1}=(ca,d)(c^{-1},d^{-1})=(cac^{-1},e')\in G_1 \Rightarrow G_1 \lhd G.$

Аналогично, $\forall(e,b)\in \text{G}_2\ \forall(c,d)\in G$

$(c,d)(e,b)(c,d)^{-1}=(\text{c, db})(\text{c}^{-1}, \text{d}^{-1})=(e,dbd^{-1})\in G_2 \Rightarrow \text{G}_2 \lhd \text{G}.$

Очевидно, что $\text{G}_1\cap\text{G}_2=(e,e')\in\text{G}$, действительно, если $\text{c}\in \text{G}_1\cap\text{G}_2 \Rightarrow \text{c}\in\text{G}_1$ & $\text{c}\in\text{G}_2 \Rightarrow [\text{c}=(a,e')]\&[\text{c}=(e,b)] \Rightarrow (a,e')=(e,b) \Rightarrow (a=e)\&(b=e') \Rightarrow \text{c}=(e,e')\in\text{G}$.

Теорема 5: *Любой элемент группы $G=A\text{x}B$ однозначно представим в виде произведения $g=g_1\cdot g_2$, где $g_1\in G_1$, $g_2\in G_2$,* $\text{g}\in\text{G}$.

Доказательство:

Действительно, $\forall\ g\in G$ будет парой, то есть $g=(a,b)=(a,e')\cdot(e,b)$, где $(a,e')\in\text{G}_1$, $(e,b)\in G_2$. Единственность, если $g=(a,b)=(a',e')\cdot(e,b')=(a',b')$, то $(a=a')\&(b=b')$. Итак, группа G порождается подгруппами G_1 и G_2, то есть $G=G_1\cdot G_2$.

Рассмотренная выше конструкция *($G=A\text{x}B$)* внешнего прямого произведения групп позволяет из двух заданных групп построить новую, более сложно устроенную группу, причем, если $|\text{A}|=n$, $|B|=k$, то $|\text{G}|=n\cdot k$. Понятно, что в общем случае можно рассматривать и группу $G=A_1\text{x}A_2\text{x}...\text{x}A_k$.

Теперь попытаемся ответить на следующий вопрос. Если дана сложно устроенная группа G, то нельзя ли ее разложить в прямое произведение двух других групп?

Ответ на этот вопрос дает следующая теорема.

Теорема 6: *Для того, чтобы группа G была изоморфна прямому произведению двух групп A и B, необходимо и достаточно, чтобы группа G содержала нормальные делители G_1 и G_2, изоморфные, соответственно группам A и B, чтобы пересечение $G_1\cap G_2=e(G)$ и чтобы группа G порождалась нормальными делителями G_1 и G_2.*

Доказательство:

Нужно доказать, что $G \cong A \times B \Leftrightarrow (G_1 \lhd G) \& (G_2 \lhd G) \& \& (G_1 \cap G_2 \in e(G)) \& (G_1 \cong A) \& (G_2 \cong B) \& (G = G_1 \cdot G_2)$.

Необходимость указанных условий следует из теорем 4 и 5, докажем достаточность, то есть дано, что $(G_1 \lhd G) \& (G_2 \lhd G) \& (G_1 \cap G_2 = e(G)) \& (G_1 \cong A) \& (G_2 \cong B) \& (G = G_1 \cdot G_2)$, тогда G будет изоморфна $A \times B$.

Сначала докажем, что если два нормальных делителя G_1 и G_2 группы G пересекаются по $e(G)$, то они поэлементно перестановочны, то есть $\forall \ (h_1 \in G_1) \ \forall \ (h_2 \in G_2) \ [h_1 \cdot h_2 = h_2 h_1]$. Действительно, рассмотрим элемент $c = h_1 \cdot h_2 \cdot h_1^{-1} \cdot h_2^{-1}$. Если в этой записи скобки расставить так: $c = (h_1 \cdot h_2 \cdot h_1^{-1}) \cdot h_2^{-1}$ то видно, что элемент c принадлежит группе G_2 ($G_2 \lhd G$).

Аналогично, записав элемент c в виде: $c = h_1 \cdot (h_2 \cdot h_1^{-1} \cdot h_2^{-1})$, видим, что $c \in G_1$ ($G_1 \lhd G$).

Таким образом, $c \in G_1 \cap G_2$, а так как $G_1 \cap G_2 = e(G)$, то $c = h_1 \cdot (h_2 \cdot h_1^{-1} \cdot h_2^{-1}) = e(G) \Rightarrow h_1 \cdot h_2 = h_2 \cdot h_1$. По условию теоремы дано, что группа G порождается своими нормальными делителями G_1 и G_2, это означает, с учетом доказанной перестановочности G_1 и G_2, что каждый $g \in G$ представим в виде произведения $g = g_1 \cdot g_2$, где $g_1 \in G_1$, $g_2 \in G_2$, то есть $G = G_1 \cdot G_2$.

Покажем, что это представление однозначно. Предположим противное.

Пусть

$$g = g_1 \cdot g_2 \text{ и } g = c_1 \cdot c_2, \text{ где } g_1, c_1 \in G_1, \ g_2, c_2 \in G_2,$$

тогда

$$g_1 \cdot g_2 = c_1 \cdot c_2 \Rightarrow c_1^{-1} \cdot g_1 = c_2 \cdot g_2^{-1} \in G_1 \cap G_2 \Rightarrow c_1^{-1} \cdot g_1 = c_2 \cdot g_2^{-1} = e(G) \Rightarrow$$

$$\begin{vmatrix} c_1 c_1^{-1} g_1 = c_1 e \\ c_2 g_2^{-1} g_2 = e g_2 \end{vmatrix} \Rightarrow \begin{vmatrix} g_1 = c_1 \\ c_2 = g_2 \end{vmatrix}.$$

Зададим теперь отображение φ: $G \to A \times B$, которое $\forall \ g \in G$ равному $g = g_1 \cdot g_2$, где $g_1 \in G_1$, $g_2 \in G_2$ ставит в соответствие пару $(g_1, g_2) \in A \times B$, то есть φ: $g \mapsto (g_1, g_2)$. Это отображение будет изоморфизмом.

Действительно,

а) сюръективность отображения φ очевидна, так как $\forall (g_1, g_2) \in A \times B \; \exists (g=g_1 \cdot g_2) \in G$: $\varphi(g)=(g_1;g_2)$

б) Докажем инъективность отображения φ: $\forall \; a,b \in G, \; (a=a_1 \cdot a_2) \& (b=b_1 \cdot b_2)$, если $\varphi(a)=\varphi(b)$, то $(a_1,a_2)=(b_1,b_2) \Rightarrow (a_1=b_1) \& (a_2=b_2) \Rightarrow (a=b)$.

Проверим условие гомоморфности: $\forall \; a, \; b \in G, \; a \cdot b = (a_1, a_2) \cdot (b_1,b_2) = (a_1 \cdot b_1) \cdot (a_2 \cdot b_2)$ в силу поэлементной перестановочности групп G_1 и G_2.

Итак, мы разложили группу G в прямое произведение своих нормальных делителей G_1 и G_2.

При этом каждый элемент группы G однозначно представим в виде произведения $g_1 \cdot g_2$, *где* $g_1 \in G_1, \; g_2 \in G_2$, а операция умножения определяется по правилу: $a \cdot b=(a_1 \cdot b_1) \cdot (a_2 \cdot b_2)$. В этом случае говорят о внутреннем прямом произведении нормальных делителей G_1 и G_2 группы G. Отличие внутреннего произведения от внешнего прямого произведения состоит в том, что G содержит в качестве прямых множителей сами группы, а не их изоморфные образы. Разумеется, внешнее прямое произведение $A=A \times B$ является также внутренним произведением подгрупп $A \times e(B)$, $e(A) \times B$, и при некотором навыке можно не делать различия между ними, употребляя сокращенное словосочетание «прямое произведение».

***Замечание 11**:* Для всякой группы G существует тривиальное разложение в прямое произведение нормальных делителей $e(G)$ и G.

***Замечание 12**:* Если дана аддитивная абелева группа G, то ее разложение называют прямой суммой и обозначают: $G=A \oplus B$, $G=\{<a,b> \mid a \in A, \; b \in B\}$.

Операция определяется так: $(a, b)+(c, d)=(a+c, b+d)$.

Пример 15: Группа $<R^2,+>=<R',+> \oplus <R,+>$.

Пример 16: Группа $C=<R,+> \oplus <R_i,+>$.

В теории абелевых групп понятие прямой суммы групп играет очень важную роль, так как позволяет доказать основную теорему о конечных абелевых группах.

***Теорема 7**: Всякая конечная абелева группа G является прямой суммой циклических групп.*

Для доказательства этой теоремы вводят понятие *p*-группы и доказывают ряд вспомогательных теорем.

Определение 7: *Конечная группа G, порядок которой является степенью простого числа (p) называется p-группой (примарной группой).*

Согласно теореме Лагранжа, порядки всех элементов *p*-группы являются степенями числа *p.*

Теорема 7'*: Всякая конечная абелева группа является внутренней прямой суммой своих максимальных абелевых p-групп, соответствующих различным простым числам p; прямые слагаемые при этом однозначно определены.*

Теорема 7"*: Всякая конечная абелева p-группа допускает однозначное (с точностью до изоморфизма) разложение в прямую сумму циклических групп порядков, равных степеням простого числа p.*

Эта теорема позволяет описать весь класс конечных абелевых групп.

ГЛАВА 2. Введение в теорию колец и полей.

§ 1. Определения кольца и поля. Примеры.

В этой главе мы рассмотрим основные свойства коммутативных колец, которые связаны с понятием «поле».

Определение 1. *Алгебра $<K, +, \circ>$ называется кольцом, если бинарные операции $+, \circ$ удовлетворяют условиям (аксиомам):*

1-4) $<K, +>$ - коммутативная группа;

5) $\forall\, a,b,c \in K \quad a\cdot(b+c)=ab+ac$

$(b+c)\cdot a=ba+ca.$

Из этого определения следует, что любое кольцо - это аддитивная абелева группа, в которой операция умножения связана с операцией сложения дистрибутивными законами. На операцию умножения, в общем случае, никаких ограничений не накладывается. Однако, если операция умножения обладает

свойствами коммутативности, ассоциативности и нейтральным элементом, то кольцо $<K, +, \circ>$ называют ассоциативно-коммутативным кольцом с единицей.

Определение 2: *Алгебра $<P, +, \circ>$ называется полем, если бинарные операции сложения и умножения удовлетворяют условиям:*

1-4) $<P, + >$ - абелева группа;

5-8) $<P\backslash\{0\}, \circ>$ - абелева группа,

9) $\forall\, a, b, c \in K \quad a\cdot(b+c)=ab+ac$

$(b+c)\cdot a=ba+ca.$

Из определения 2 следует, что любое поле - это аддитивная группа, без нулевого элемента - мультипликативная группа, а также коммутативно-ассоциотивное кольцо с единицей, в котором каждый ненулевой элемент обратим.

Определение 3: *Подмножество L кольца K называется подкольцом кольца K, если L является кольцом относительно операций сложения и умножения, заданных в K.*

Определение 4*: Подмножество A поля P называется подполем поля P, если A является полем относительно операций сложения и умножения. заданных в P.*

Замечание 1*:* Поле *P* называют расширением поля *A*.

Замечание 2*:* Из определения 3, 4 вытекают достаточные условия подкольца и подполя: замкнутость множества A относительно операций и их симметризуемость.

Для кольца:		Для поля:	
а) $\forall\, a, b \in K,$	$(a+b)\in K$	а) $\forall\ a, b \in P,$	$(a+b)\in$P
б) $\forall\, a, b \in K,$	$(a\circ b)\in K$	б) $\forall\, a, b \in P,$	$(a\circ b)\in$P
в) $\forall\, a \in K,$	$(-a)\in K$	в) $\forall\, a, b \in P,$	$(-a)\in$P
		г) $\forall\, a \neq 0,$	$(a^{-1})\in$P

Пример 1: $<2Z, +, \circ >$ является подкольцом кольца $<Z, +, \circ >$ (проверьте!).

Пример 2: $<Q, +, \circ >$ является подполем поля $<R, +, \circ >$ (проверьте!).

Определение *5: Поле, не имеющее собственных подполей, называется простым.*

Теорема 1*: В каждом поле $<P, +, \circ>$ содержится одно и только одно простое поле P_0.*

Доказательство:

Предположим противное, пусть P_0 и P_1 два простых подполя поля P, тогда их пересечение $P_0 \cap P_1$ будет непусто, поскольку 0 и 1 содержатся как в P_0, так и в P_1. Кроме этого, $P_0 \cap P_1$ будет подполем поля P (проверьте!). Мы получили противоречие с условием простоты полей P_0 и P_1. В §2 мы докажем, что простое подполе любого поля P будет изоморфно полю $<Q, +, \circ>$, либо $<Z_P, +, \circ>$.

Приведем примеры колец и полей, которые мы уже изучили в курсе «Алгебра».

Примеры колец и полей:

Пример 3: $<Z, +, \circ>$ - коммутативно-ассоциативное кольцо целых чисел с 1.

$<mZ, +, \circ>$, где mZ — множество целых чисел, делящихся на m, $m \in N$, будет подкольцом кольца Z.

Пример 4: $<$C, +, $\circ >$ - кольцо и поле комплексных чисел.
$<Z, +, \circ>$, $<Q, +, \circ>$, $<R, +, \circ>$ - его подкольца.
$<Q, +, \circ>$, $<R, +, \circ>$ - его подполя.

***Пример* 5**: $<M_{nn}(R), +, \circ>$ - некоммутативное, ассоциативное кольцо квадратных матриц над полем R.
$< M_{nn}(Q), +, \circ>$, $<M_{nn}(Z), +, \circ>$ - его подкольца.

Пример 6: $<P[x], +, \circ>$ - коммутативно-ассоциативное кольцо многочленов от одной переменной над полем P.
$<Q$[x], +, $\circ>>$ <R[x], +, $\circ>$, <C[x], +, $\circ>$ - его подкольца.

***Пример* 7**: $<Z_m, +, \circ>$ - конечное коммутативно-ассоциативное кольцо классов вычетов по модулю (m).

Пример 8: $<Z_p, +, \circ>$, где p - простое число, будет конечным полем.

Пример 9: Пусть X - произвольное множество, K - произвольное кольцо. Обозначим через K^X - множество функций $f: X \to K$ с операциями +, °, которые определим так:

а) $(f+g)(x)=f(x) \oplus g(x)$.

б) $(f \cdot g)(x)=f(x) \otimes g(x)$

Проверьте самостоятельно, что $<K^X, +, \circ>$ - кольцо. Как известно из курса математического анализа, это кольцо содержит разнообразные подкольца, определяемые

специальными свойствами функций (непрерывностью, дифференцируемостью, ограниченностью и т.д.).

***Пример 10**:* На любой аддитивной группе $<A, +>$, равенством $x \cdot y = 0$ для $\forall$ x, $y \in A$, можно задать структуру кольца с нулевым умножением.

Основные свойства коммутативных колец и полей вытекают из свойств аддитивных и мультипликативных абелевых групп.

***Теорема 2:** Если $<K, +, \circ>$ - произвольное кольцо, то*

а) $\forall\ a \in K, \quad -(-a)=a$

б) $\forall\ a, b \in K, \quad b-a=b+(-a)$

в) $\forall\ a, b \in K, \quad -(a+b)=(-a)+(-b)$

г) $\forall\ a \in K, \quad a-a=0$

д) $\forall\ a, b \in K, \quad a(b-c)=ab-ac$

е) $\forall\ a \in K, \quad 0 \cdot a=0$

ж) $\forall\ a, b \in K, \quad (-a) \cdot b=-ab.$

Докажем, например, последнее свойство. Так как $<K, +>$ - абелева группа, то $\forall\ a \in K\ \exists\ (-a)$: $(-a)+a=a+(-a)=0$. Тогда $[(-a)+a] \cdot b=[a+(-a)] \cdot b$. Пользуясь аксиомой дистрибутивности, получим $(-a) \cdot b+ab=ab+(-a) \cdot b$. Из последнего равенства видно, что элемент $(-a)b$ является противоположным элементом ab, то есть $(-a)b=-ab$. Остальные свойства докажите самостоятельно.

***Теорема 3**: Если $<P, +, \circ>$ поле, то*

а) $-a=(-1) \cdot a \quad , \quad \forall\ a \in P,$

б) $\dfrac{b}{a} = b \cdot a^{-1} \quad , \quad \forall\ a, b \in P,$

в) $\dfrac{1}{a \cdot b} = \dfrac{1}{a} \cdot \dfrac{1}{b} \quad , \quad \forall\ a,b.$

Докажем первое свойство. Используя последовательно свойство единицы в кольце, правую дистрибутивность и свойство (*е*) из теоремы 1, получим: $a+(-1) \cdot a = 1 \cdot a+(-1) \cdot a = (1+(-1)) \cdot a = 0 \cdot a = 0$. Итак, $(-1) \cdot a = -a$.

Остальные свойства докажите самостоятельно.

Из теорем 1 и 2 видно, что в произвольных кольцах и полях выполняются многие свойства арифметических операций, однако, существуют кольца и поля, в которых некоторые

свойства числовых операций не выполняются. Например, если в числовых кольцах $<Q,+,\circ>$, $<R,+,\circ>$:

1) $\forall\, a \in Q \;\forall\, a \in R$, $a+a+\ldots+a \neq 0$, если $a \neq 0$

2) $\forall\, a, b \in Q \;\forall\, a, b \in R$, $a \cdot b \neq 0$, если $(a \neq 0)\&(b \neq 0)$,

то в кольце $<Z_6, +, \circ>$ мы получим:

а) $\bar{1}+\bar{1}+\bar{1}+\bar{1}+\bar{1}+\bar{1}=\bar{0}$, $\bar{2}+\bar{2}+\bar{2}=\bar{0}$, $\bar{3}+\bar{3}=\bar{0}$

б) $2 \cdot \bar{3} = \bar{0}$.

Замечание 3: Отличные от нуля элементы кольца, произведение которых равно нулю, называют делителями нуля.

Теорема 4*: В поле делителей нуля не существует.*

Доказательство:

Пусть дано поле $<P, +, \circ>$. Предположим противное, пусть $a \neq 0$, $b \neq 0$, а $a \cdot b = 0$. Тогда уравнение $a \cdot x = 0$ будет иметь два различных решения: $x = b$ и $x = 0$, что противоречит тому, что $<P\backslash\{0\}, \cdot>$ - группа.

Существуют и кольца, в которых нет делителей нуля, такие кольца называют областями целостности.

Пример 11: Кольца $<Z, +, \circ>$, $<Q, +, \circ>$, $<R, +, \circ>$, $<C, +, \circ>$ - области целостности, так как $\forall\, (a, b \in Z \;\forall\, a, b \in Q \;\forall\, a, b \in R \;\forall\, a, b \in C)$, если $(a \cdot b = 0) \Rightarrow (a = 0) \vee (b = 0)$.

Пример 12: Пусть дано множество $R^2 = \{<a, b> \mid a, b \in R\}$. Зададим на этом множестве операции:

а) $\forall <a, b>, <c, d> \in R^2$, $<a, b>+<c, d>=<a+c, b+d>$

б) $\forall <a, b>, <c, d> \in R^2$, $<a, b> \cdot <c, d> = <ac, bd>$.

Докажем, что $<R^2, +, \cdot>$ - кольцо с делителями нуля.

1. Очевидно, что R^2 замкнуто относительно операций.

2. $<R^2, +>$ - будет аддитивной группой, так как

а) $\forall <a, b>, <c, d> \in R^2$, $<a, b>+<c, d>=<c, d>+<a, b>$

б) $\forall <a, b>, <c, d>, <m, n> \in R^2$,

$(<a, b>+<c, d>)+<m, n>=<a,b>+(<c, d>+<m, n>)$

в) $\exists <0, 0> \;\forall <a, b> \in R^2$, $<0, 0> + <a,b> = <a,b> + <0,0>=<a,b>$

г) $\forall <a, b> \in R^2 \;\exists <-a, -b> \in R^2$,

$<a,b>+<-a,-b>=<-a,-b>+<a, b>=<0,0>$.

3. Выполняется левый и правый дистрибутивный закон, то есть $\forall <a,b>, <c,d>, <m,n> \in R^2$

$<a,b>\cdot[<c,d>+<m,n>]=<a,b>\cdot<c,d>+<a,b>\cdot<m,n>$.

$[<c, d>+<m, n>]\cdot$ <a, $b>=<c, d>\cdot<a, b>+<m, n>\cdot<a, b>$ (проверьте самостоятельно).

Итак, $<R^2, +, \cdot>$ - кольцо, в котором существуют делители нуля, например, <0, 1> и <1, 0> такие, что <0, 1>·<1, 0>=<0, 0>. Причем, таких элементов можно указать множество. Следовательно, кольцо $<R^2, +, \cdot>$ не является областью целостности.

Пусть $<K, +, \circ>$ - кольцо с единицей *(e)*. Построим в кольце *K* наименьшее подкольцо L, содержащее *(e)*. По определению подкольца, из того, что $e \in L$ будет следовать, что $(-e) \in$ L. Далее $e+e+e+...+e=n\cdot e \in L$ и $(-e)+(-e)+(-e)+...+(-e)=-n\cdot e \in L$. Искомое подкольцо *L* должно содержать и элементы $n\cdot e+m\cdot e=(n+m)e \in L$, $ne\cdot me=n\cdot me \in L$.

Итак, наименьшее подкольцо $L=<\{ne\}, +, \circ>$. При этом возможны два случая:

а) $\forall\ n \neq 0, ne \neq 0;$

б) $\exists\ n \neq 0, ne=0$.

Так как, любое поле является кольцом, то можно дать такое определение.

Определение 6: *Поле $<P, +, \circ>$ называется полем положительной характеристики (n), если существует наименьшее натуральное число (n), при котором ne=0.*

Если $\forall\ n \neq 0, ne \neq 0$, то поле называют полем нулевой характеристики.

Теорема 5: *Если $<P, +, \circ>$ - поле характеристики (n), то $\forall\ a \in P,\ n\cdot a = 0$.*

Доказательство:

$n\cdot a = n(ea) = (n\cdot e)a = 0\cdot a = 0$.

Следствие: *Характеристика любого числового поля равна нулю.*

Действительно, так как $e=1$, то n·1=0 только при условии, что n=0.

Пример 13: Дано поле $<Z_5, +, \circ>$, так как $\bar{1}+\bar{1}+\bar{1}+\bar{1}+\bar{1}=5\cdot\bar{1}=\bar{0}$, то Z_5 поле характеристики 5.

Пример 14: $<Q, +, \circ>$, $<R, +, \circ>$, $<C, +, \circ>$ - поля нулевой характеристики, так как $1 + 1+1+...+1 = n\cdot 1 \neq 0, \forall\ n \neq 0$.

§ 2 Отношение делимости в кольцах главных идеалов.

Основные свойства отношения делимости в кольцах $<Z, +, \circ>$ и $<P[x], +, \circ>$мы уже изучили. Напомним основные определения и теоремы.

Определение 1: *Целое число (a) делится на целое число* $(b\neq 0)$, *если* $\exists\ q \in Z$ *такое, что* $a=bq$.

Это отношение рефлексивно, антисимметрично и транзитивно, то есть является отношением частичного порядка на множестве *Z*.

Определение 2: *Целое число (a) делится на* $(b \in Z\ \&\ b\neq 0)$ *с остатком, если* $\exists\ q, r \in Z : a=bq+r$, *где* $0 \leq r < |b|$.

Теорема 1: *В кольце* $<Z, +, \circ>$ *любое целое число (a) можно разделить на целое число* $b\neq 0$ *с остатком, причем, единственным образом.*

Теорема 2: *Любое натуральное число* $(n>1)$ *может быть представлено единственным образом и виде произведения простых чисел, с точностью до порядка следования сомножителей, то есть* $n=P_1^{\alpha 1}\cdot P_2^{\alpha 2}\cdot \ldots \cdot P_k^{\alpha k}$.

Определение 3: *Многочлен* $f(x)$ *из кольца* $P[x]$ *делится на многочлен* $g(x) \in P[x]$, $(g(x)\neq 0)$, *если* $\exists\ h(x) \in P[x] : f(x)=g(x)\cdot h(x)$.

Определение 4: *Многочлен* $f(x) \in P[x]$ *делится на многочлен* $g(x)\neq 0$ *из этого же кольца с остатком, если* $\exists\ h(x), r(x) \in P[x] : f(x)=g(x)\cdot h(x)+r(x)$, *где* $cm\ r(x) < cm\ g(x) \vee r(x)=0$.

Теорема 3: *Для* $\forall\ f(x), g(x) \in P[x]$, *где* $g(x)\neq 0$, *существует единственная пара многочленов* $h(x), r(x) \in P[x]$: $f(x)=g(x)\cdot h(x)+r(x)$, *причем* $cm\ r(x) < cm\ g(x) \vee r(x)=0$.

Теорема 4: $\forall\ f(x) \in P[x]$, $f(x)\neq 0$, $cm\ f(x)>0$ *разлагается в произведение неприводимых многочленов единственным способом, с точностью до порядка следования многочленов нулевой степени, то есть* $f(x) = P_1^{\alpha_1}(x)\cdot P_2^{\alpha_2}(x)\cdot \ldots \cdot P_k^{\alpha_k}(x)$.

Сравнивая свойства отношения делимости в *Z* и $P[x]$, мы видим, что отношение делимости в кольце $P[x]$ обладает почти

теми же свойствами, что и в кольце *Z,* однако есть и небольшие различия, например, кольцо *P*[*x*] более богато обратимыми элементами, чем кольцо *Z.* Так, относительно операции умножения в кольце *Z* всего два обратимых элемента 1, -1, а в кольце *P*[*x*] - это все многочлены нулевой степени, то есть элементы поля *P.* Далее, понятие НОД(*f*, g) и НОК(*f*, *g)* в кольце *P*[*x*] определяются с точностью до постоянного множителя *(c),* а в кольце Z с точностью до знака.

Пусть теперь дано произвольное кольцо <K, +, °>. Выясним, всегда ли можно в нем определить отношение делимости, и будет ли оно обладать свойствами, характерными для этого отношения в кольцах *Z и P[x]?*

Определение 5: *Если < K, +, °> произвольное кольцо и a,b∈K, то будем говорить, что (b) делится на (a) если уравнение ax=b имеет хотя бы одно решение.*

Если кольцо <*K,* +, °> является полем, то ∀ *a≠0* из *K* уравнение *ax=b* разрешимо для любого *(b)* (так как в поле всегда разрешимо уравнение a*x=1)*. Именно это свойство выделяет поля среди колец. Однако, и в кольцах, не являющихся полями, могут существовать элементы, делящие все элементы кольца. Например, в кольце <Z, +, °> - это обратимые элементы 1, -1 в кольце <*P[x],* +, °> - это многочлены нулевой степени (элементы поля *P),* которые тоже играют роль обратимых элементов. Поэтому, есть смысл дать общее определение обратимых элементов в любом кольце <*K,* +, °>.

Определение 6*: Элемент (a) кольца <K, +, °> называется обратимым, если он делит все элементы из K.*

Однако, в общем случае, в кольцах, которые не являются полями уравнение *ax=b* может вообще не иметь решений, или, напротив, таких решений может быть несколько. Например, рассмотрим кольцо классов вычетов $<Z_8, +, °>$. В этом кольце уравнение $\bar{2}\bar{x} = \bar{3}$ не имеет решения, а уравнение $\bar{2}\bar{x} = \bar{4}$ имеет два решения: $\bar{x} = \bar{2}$ *и* $\bar{x} = \bar{6}$ и мы получим, что $\bar{2}(\bar{6} - \bar{2}) = \bar{0}$, то есть $\bar{2} \cdot \bar{4} = \bar{0}$, следовательно, $\bar{2}$ и $\bar{4}$ делители нуля в этом кольце.

Таким образом, для задания отношения делимости в произвольных кольцах, приходится выделять класс колец, которые не имеют делителей нуля, то есть являются *областями целостности.* В них имеют место теоремы о делении с остатком и алгоритм Евклида.

***Определение** 7: Область целостности $<K, +, \circ>$ называется евклидовым кольцом, если существует отображение* φ: $K\backslash\{0\}\to N^0$ *такое, что* $\forall$ *a,* $(b\neq 0)\in K$ $\exists$ *q,* $r\in K$: $a=bq+r$; *причем,* $\varphi(r)<\varphi(b)$ *или* $(r=0)$.

***Замечание 1**:* Отображение φ называют евклидовой нормой.

***Пример 1**:* Кольцо $<Z, +, \circ>$ - евклидово кольцо. Евклидова норма в нем определяется равенством $\varphi(a)=|a|$, для $\forall$ $(a\neq 0)\in Z$ и тогда, $\forall$ *a,* $(b\neq 0)$ $\exists$ *q,* $r\in Z$: $a=bq+r$, где $0\leq r<|b|$.

***Пример 2**:* Кольцо $<P[x], +, \circ>$ - евклидово, отображение φ определяется равенством $\varphi(f(x))=cm(f(x))$ и тогда, для

$\forall$ $f(x)$, $(g(x)\neq 0)\in P[x]$ $\exists$! $h(x)$, $r(x)\in P[x]$: $f(x)=g(x)\cdot h(x)+r(x)$, где $cm\ r(x)<cm\ g(x) \vee r(x)=0$.

Если $<K, +, \circ>$ - произвольное евклидово кольцо, то в нем будут справедливы следующие утверждения:

***Теорема 3:** Всякое конечное множество элементов* $\{a_1, a_2, \ldots, a_k\}\in K$, $a_i\neq 0$, *обладает НОД*$(a_1, a_2, \ldots, a_k)$, *который определяется с точностью до обратимых элементов кольца К.*

Теорема 4: $\forall$ *НОД(a,b), где* $a,b\in K$ $(a,b\neq 0)$ $\exists$ $x, y\in K$: $ax+by=$*НОД(a b).*

Теорема 5: $\forall$ $(a\neq 0)\in K$ *будет однозначно разложим (с точностью до сомножителей из К) в произведение степеней простых элементов.*

Докажите самостоятельно эти утверждения, учитывая доказанные теоремы в кольце Z и $P[x]$. Заметим, что в определении евклидова кольца не дается никакого правила для нахождения отображения φ, поэтому, в общем случае, бывает довольно трудно определить, является ли область целостности евклидовым кольцом или нет.

Тем не менее, во многих случаях существование евклидовой нормы легко усматривается.

***Пример 3**:* Кольцо $<Z(i), +, \circ>$ является евклидовым.

Доказательство:

По условию $Z(i)=\{a+bi,\ a,\ b\in Z\}$, которое называется множеством гауссовых чисел. Легко проверить, что $Z(i)$ является кольцом и содержит в качестве своего подкольца кольцо <Z, +, °> (проверьте!).

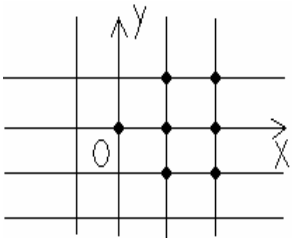
Кольцо $<Z(i),\ +,\ °>$ является областью целостности, так как $\forall\ (a+bi),\ (c+di)$ из того, что $[(a+bi)\cdot(c+di)=0] \Rightarrow [(a+bi)=0]\vee[(c+di)=0]$ (проверьте!).

Докажем, что <Z(i), +, °> - евклидово кольцо. В качестве евклидовой нормы возьмем норму комплексного числа, то есть $\forall\ (z\neq 0)\in Z(i)$, $\varphi(z)=|z|^2=a^2+b^2$. (норма комплексного числа равна квадрату модуля комплексного числа). Поэтому, $\varphi(z_1,\ z_2)=\varphi(z_1)\cdot\varphi(z_2)$.

Покажем, что $\forall\ z\in C\ \exists\ z_0\in Z(i)$ такое, что $\varphi(z_0-z)=|z_0-z|^2<1$.

Для этого рассмотрим расположение целых гауссовых чисел на комплексной плоскости. Это будут точки с целочисленными координатами, образующими узлы покрытия комплексной плоскости сеткой квадратов со стороной, равной 1.

Любое комплексное число z (точка плоскости) будет попадать хотя бы в один из квадратов сетки. Но произвольная точка квадрата отдалена от ближайшей вершины на расстояние меньшее, чем длина стороны квадрата.



Следовательно, для точки z найдется точка z_0 с целочисленными координатами такая, что $|z_0-z|<1$, а тогда и $\varphi(z_0-z)<1$.

Теперь покажем, что $\forall\ z_1\ z_2\in Z(i),\ z_2\neq 0\ \exists\ q_1,\ r_1\in Z(i)$ такие, что $z_1=z_2q_1+r_1$, причем $\varphi(r_1)<\varphi(z_2)$

Выберем для гауссова числа $\frac{z_1}{z_2}$ такое целое гауссово число z_0, что $\varphi\left(\frac{z_1}{z_2}-z_0\right)<1$, (выше мы показали, что оно всегда существует). Обозначим разность $z_1-z_2\cdot z_0=r_1$ (r_1 - будет тоже

гауссовым числом). Тогда, $\varphi(r_1) = \varphi(z_1 - z_2 \cdot z_0) = \varphi(z_2(\frac{z_1}{z_2} - z_0)) =$

$= \varphi(z_2) \cdot \varphi(\frac{z_1}{z_2} - z_0) < \varphi(z_2)$, то есть $\varphi(r_1) < \varphi(z_2)$.

Итак, *<Z(i), +, °>* является евклидовым кольцом, его называют кольцом целых гауссовых чисел.

В евклидовых кольцах выполняется основная теорема об однозначном (с точностью до обратимых множителей) разложении элементов в произведение степеней простых элементов.

Уточним понятия простого и составного элемента для любой области целостности с единицей.

Определение 8*: Необратимый элемент p из области целостности <K, +, °> называется простым, если его любой делитель d либо обратим в K, либо ассоциирован с p.*

Определение 9*: Элемент a из области целостности K называется составным, если a=b·c, где b,c - необратимые элементы в K.*

Таким образом, все элементы области целостности можно разбить на четыре класса:

1. нуль.
2. обратимые элементы (делители единицы кольца и всех остальных элементов).
3. простые элементы.
4. составные элементы.

Примеры: *в кольце <Z, +, °>*

1. нуль - 0;
2. обратимые элементы - 1,-1;
3. простые - 3,-3, 5,-5 и т.д.;
4. составные - 4, 8, -4, -10 и т.д.

в кольце <C, +, °>:

1. нуль - 0+0*i*;
2. так как <C\{0}, °> - группа, то все остальные элементы обратимы.

в кольце <P[x], +, °>:

1. нуль - $0x^n+0x^{n-1}+...+0x+0$ - нуль-многочлен

2. обратимые элементы - многочлены нулевой степени, то есть элементы поля *P,* отличные от нуля.

3. простые элементы - неприводимые многочлены над полем *P.*

4. составные элементы - приводимые многочлены над полем *P.*

Из приведенных примеров видно, что в каждом конкретном случае смысл понятий «простой» и «составной» элемент зависит от множества, на котором задана структура кольца, причем, если кольцо является полем, то необходимость введения этих понятий отпадает. Мы уже знаем, что в известных нам евклидовых кольцах *Z, P[x], Z(i)* каждый элемент может быть разложен в произволение степеней простых элементов (с точностью до обратимых элементов). Возникает вопрос, существуют ли области целостности с единицей, не являющихся евклидовыми кольцами, в которых разложение определяется также однозначно? Да, существуют. Например, кольцо р-целых рациональных чисел. Пусть р-простое рациональное число.

Определение 10*: $r \in Q$ называется р-целым, если оно равно пулю, либо в представлении его как частного двух взаимно-простых целых чисел: $r = \frac{s}{t}$, (s, t)=1, знаменатель t не делится на р.*

Обозначим множество всех р-целых чисел через *Z(p)*. Докажите самостоятельно следующие утверждения:

Теорема 4: *$<Z(p), +, \cdot>$ - является областью целостности.*

Теорема 5: *Каждое р-целое число $r \neq 0$ однозначным образом представило в виде: $r=up^m$, где (u) обратимый элемент, а $m \geq 0$.*

Теорема об однозначном разложении элементов в этом кольце выполняется тривиальным образом из-за того, что это кольцо содержит лишь один, с точностью до обратимого множителя простой элемент, а именно – число р.

Теперь выясним вопрос о том, существуют ли области целостности с единицей, в которых элементы допускают неоднозначное разложение на простые множители?

Прежде всего определим, какие два разложения элемента а из области целостности $<K,+,\circ>$ будем считать одинаковыми?

***Определение 11**: Два разложения элемента $a \in K$ на простые множители, $a=p_1 \cdot p_2 \cdot \ldots \cdot p_k$ и $a=s_1 \cdot s_2 \cdot \ldots \cdot s_p$ называют одинаковыми, если (k=p) и разложения могут быть переведены друг в друга перестановкой множителей и умножением их на обратимые элементы.*

Например, в кольце Z_4, $\overline{4} = \overline{2} \cdot \overline{2}$ и $\overline{4} = (\overline{-2}) \cdot (\overline{-2})$

В кольце $P[x]$, $(x^2-1)=(x-1)\cdot(x+1)$ и $(x^2-1)=(-x+1)\cdot(-x-1)$.

Пример 5: Рассмотрим множество $Z(\sqrt{-5}) \overset{df}{=} \{a+b\sqrt{-5} \mid a, b \in Z\}$. Проверьте самостоятельно, что $<Z(\sqrt{-5}), +, \circ>$ образует область целостности, которая содержит кольцо $<Z, +, \circ>$. В этом кольце числа 2, 3, $(1+\sqrt{-5})$,$(1-\sqrt{-5})$ будут простыми, так как уравнения: $x^2+5y^2=2$ и $x^2+5y^2=3$ в целых числах неразрешимы.

Тогда, элемент $6=6+0\sqrt{-5}$ будет иметь два различных разложения:

а) $6=2\cdot3$

б) $6=(1+i\sqrt{5})(1-i\sqrt{5})$.

Действительно, в кольце $Z(\sqrt{-5})$ два обратимых элемента: $1=1+0\sqrt{-5}$ и $-1=-1+0\sqrt{-5}$ и с помощью их нельзя перевести одно разложение в другое. Существование таких колец требует рассмотрения новых понятий для изучения свойств отношения делимости в областях целостности с единицей. К ним, прежде всего, относятся понятия идеала и главного идеала.

Пусть дано коммутативно-ассоциативное кольцо с единицей $<K, +, \circ>$.

***Определение 12:** Главным идеалом кольца $<K, +, \circ>$, порожденным элементом $a \in K$, называют множество элементов кольца К, кратных элементу (а), то есть $(a) = \{ra \mid a \in K, r \in Z\}$*

***Замечание 2**:* Из этого определения следует, что

$(\forall\ b \in (a) \Leftrightarrow (b:a))$ & $(a) \subset K$.

Примеры главных идеалов:

В кольце $<Z, +, °>$ элементы 3, 5 порождают главные идеалы (3)=3Z, (5)=5Z. В общем случае, $(m)=mZ$.

В кольце $<P[x], +, °>$ элемент x порождает главный идеал $(x)=\{f(x) \mid f(x)=a_n x^n+a_{n-1}x^{n-1}+a_1 x+0\}$

В кольце $<Z[x], +, °>$ элемент 2 порождает главный идеал $(2)=\{f(x) \mid f(x)= a_n x^n+a_{n-1}x^{n-1}+a_1 x+0$, *где все* a_i *– четные числа*$\}$

В любом кольце $<K, +, °>$ с единицей $(0)=\{0\}$, $(e)=K$.

Определение 13*: Область целостности* $<K, +, °>$*, все идеалы которой главные, называется кольцом главных идеалов.*

Теорема 6: *Любое евклидово кольцо является кольцом главных идеалов.*

Доказательство:

Пусть $<K, +, °>$ - евклидово кольцо, то есть в нем определено отображение $\varphi: K\backslash\{0\}\to N^0$ такое, что $\forall\ a, (b\neq 0)\in K$ $\exists\ q,r\in K : a=bq+r$, причем, $\varphi(r)<\varphi(b)$ или $(r=0)$.

Пусть (a) любой идеал кольца K отличный от (0). Возьмем элемент $d\in(a), (d\neq 0)$, для которого $\varphi(a)$ принимает наименьшее значение из N^0, то есть $\varphi(d)=min(\varphi(a))$. Покажем, что (a)=(d), ясно, что $(d)\subseteq(a)$. Для доказательства того, что $(a)\subseteq(d)$ достаточно показать, что каждый элемент $a\in(a)$ - кратен элементу d. Согласно свойству евклидовости, элемент a можно разделить на d с остатком: $a=dq+r$, где $\varphi(r)<\varphi(d)$ или (r=0). Но $(r=a-dq)\in(a)$, то есть $a=dq$ и $(a:d)$. Значит, $(a)\subseteq(d)$. Так как, мы показали, что $(d)\subseteq(a)\&(a)\subseteq(d)$, то $(a)=(d)$.

Из этой теоремы следует, что кольца $<Z, +, °>$, $<P[x], +, °>$, $<Z(i), +, °>$, которые являются евклидовыми, будут и кольцами главных идеалов. Однако, класс евклидовых колец также не исчерпывает весь класс колец главных идеалов, как он не исчерпывал класс колец, являющихся областями целостности, в которых разложение на простые множители определялось однозначно.

Пример 6: Кольцо $<Z_{(p)}, +, °>$ - p-целых чисел является неевклидовым кольцом главных идеалов.

Из теоремы 5 следует, что каждое p-целое число $(r\neq 0)$ однозначным образом представимо в виде $r=up^m$, где u

обратимый элемент, а m≥0, то есть *Z(p)* - кольцо главных идеалов, которое не является евклидовым.

Пусть теперь дано кольцо главных идеалов <*K*, +, °> определим отношение делимости в этом кольце.

Определение 14: *Идеал (a) кольца K делится на идеал (b) этого же кольца, если (a)⊂(b).*

Замечание 3:

а) (0) : (b), где *(b)* - любой идеал из *K,* так как (0) ⊂ (b).

б) ∀ *(a)* из кольца *K* делится на (*e*), так как *(e) = K* и *(a)* ⊆ K.

в) отношение делимости идеалов транзитивно, то есть, если [*(a):(b)*]&[*(b):(c)*] ⇒ [*(a):(c)*].

Действительно, из того, что (a)⊆(b)&(b)⊆(c) ⇒ (a)⇒(c), а это означает, что *(a):*(c).

***Пример* 7**: В кольце <*Z*, +, °> идеал 10Z делится на идеал 5Z, так как 10*Z*⊂*5Z,* а идеал 3Z не делится на идеал 2Z, так как 3Z⊄2Z.

Определение 15: *Идеал (d) кольца K называется НОД((a), (b)) идеалов (a) и (b) этого кольца, если:*

а) (a):(d)&(b) :(d);

б) (d) делится на ∀ (d_i) из кольца K.

Теорема 7*: Если (d)=НОД((a), (b)), то (d)={ra+sb | r, s∈K}.*

Доказательство:

Пусть (d)=НОД((*a*), (*b*)) ⇒ *(a):(d)&(b):(d)* ⇒ *(a)⊂(d)&(b)⊂(d)* ⇒ ((a)∪(b))⊂(d) ⇒ (*d*)={*ra+sb* | *s,b*∈*K*}.

Пример 8*:* В кольце <*Z*, +, °> НОД ((2), (3))={2x+3y | x,y∈Z}=(1). НОД((4), (8))={4x+8y}=(4).

Теорема 8*: Если <K, +, °> кольцо главных идеалов, то*

а) ∀ a, b∈K имеют НОД(a,b);

б) все НОД ассоциированы друг с другом;

в) если d=НОД(a,b), то в K ∃ r,s :d=ax+by, где x,y∈K.

Доказательство:

а) Пусть элементы *a* и *b* принадлежат K, а *(a)* и *(b)* - главные идеалы этого кольца. Обозначим через *(d)=НОД((a),* (b)), так как *(d)* тоже главный идеал, то в *K* будет существовать элемент *d,* который порождает идеал *(d).* Докажем, что *d=НОД(a, b).*

Действительно, так как $(a):(d) \Rightarrow (a) \subset (d)$, так как $a \in (a) \Rightarrow a \in (d) \Rightarrow (a:d)$.

Аналогично $(b):(d) \Rightarrow (b) \subset (d) \Rightarrow b \in (b) \& b \in (d) \Rightarrow (b:d)$. Следовательно, d общий делитель элементов a и b.

Покажем, что $d = НОД(a, b)$.

Пусть d_1 - общий делитель a и b, то есть $(a:d_1)\&(b:d_1) \Rightarrow (a) \subset (d_1)\&(b) \subset (d_1) \Rightarrow (d) \subset (d_1) \Rightarrow (d:d_1) \Rightarrow d = НОД(a, b)$.

б) докажите самостоятельно.

в) уже доказано в теореме 7.

Существование НОД(a, b) для любой пары элементов a и b из кольца главных идеалов позволяет строить теорию делимости и этих кольцах, точно также, как в кольце целых чисел Z и доказать основную теорему 9.

Теорема 9: *В кольце главных идеалов каждый элемент, отличный от нулевого, однозначно, с точностью до обратимых элементов, разложим в произведение степеней простых элементов.*

Следует отметить, что эта теорема может выполняться и в областях целостности, не являющихся кольцами главных идеалов, например, в кольце $<P[x_1,x_2, ...,x_n]>$ многочленов от нескольких переменных с коэффициентами из поля P, поэтому, изучение свойств отношения делимости в произвольных кольцах является центральной задачей теории колец.

§ 3. Гомоморфизмы и идеалы колец, поля частных.

Пусть даны два кольца $<K, +, \bullet>$ и $<A, \oplus, \circ>$.

Определение 1*: Отображение $f: K \to A$ называется гомоморфизмом, если*

а) $\forall\ a, b \in K,\ \varphi(a+b) = \varphi(a) \oplus \varphi(b)$;

б) $\forall\ a, b \in K,\ \varphi(a \cdot b) = \varphi(a) \circ \varphi(b)$.

Замечание 1*:* Из определения следует, что $\varphi(0) = 0'$ и $\varphi(na) = n\varphi(a)$, где $n \in Z$.

Определение 2: *Множество Кег* $\varphi \overset{df}{=} \{a \in K \mid \varphi(a)=0'\}$ *называется ядром гомоморфизма* φ.

Как и в случае групп, *Кег* φ будет подкольцом кольца $<K, +, \circ>$ (проверьте!).

Это подкольцо обладает такими свойствами: если $(L=Ker\ \varphi) \subset K$, то $L \cdot x \subseteq L$ и $x \cdot L \subseteq L$ для всех $x \in K$. Действительно, $\forall\ l \cdot x \in L \cdot x$ будем иметь: $\varphi(l \cdot x)=\varphi(l) o \varphi(x)=0' \cdot x'=0'$ для $\forall\ l \in L$, $\forall\ x \in K$ и $\varphi(xl)=\varphi(x) o \varphi(l)=x' \cdot 0'=0'$ для $\forall\ l \in L$, $\forall\ x \in K$.

Следовательно, $(KL \subset L) \& (LK \subset L)$, то есть подкольцо $L=Ker\ \varphi$ является двусторонним идеалом кольца К. Итак, ядра гомоморфизмов колец всегда являются идеалами.

Определение 3: *Множество Im* $\varphi \overset{df}{=} \{x' \in A \mid x'=\varphi(x)\}=\varphi(K)$ *называется образом гомоморфизма* φ.

Как и в случае групп, гомоморфизм $\varphi: K \to A$ называется мономорфизмом, если φ -инъективно *(Кег* φ= 0), эпиморфизмом, если φ - сюръективно, то есть *Im* $\varphi=\varphi(K)=A$ и изоморфизмом, если отображение φ - биективно $(K \cong A)$.

Пример 1: Рассмотрим отображение φ кольца $<Z,+,\circ>$ в кольцо $<Z_m,+,\circ>$: $\varphi(k)=\overline{k}$.

Это отображение является эпиморфизмом, так как

$\forall\ k, r \in K$, $\varphi(k+r)=\varphi(k) \oplus \varphi(r)$;

$$\begin{array}{ccc} \| & & \| \\ \overline{k+r} & = & \overline{k} \oplus \overline{r} \end{array}$$

$\forall\ k, r \in K$, $\varphi(k \cdot r)=\varphi(k) o \varphi(r)$;

$$\begin{array}{ccc} \| & & \| \\ \overline{k \cdot r} & = & \overline{k} \cdot \overline{r} \end{array}$$

$\forall\ \overline{k} \in Z_m\ \exists\ k \in Z : \varphi(k)=\overline{k}$.

Ядро этого гомоморфизма *Кег* $\varphi=mZ$, так как все целые числа кратные (m) будут отображаться в нулевой класс. Мы уже знаем, что *mZ* является главным идеалом кольца $<Z, +, \circ>$. Итак, нормальные подгруппы и идеалы колец имеют общее происхождение - они являются ядрами гомоморфизмов. Этот факт находит свое выражение и в общем подходе к построению

факторколец. Пусть дано кольцо $<K, +, \circ>$, L - его идеал. Построим факторкольцо K/L. Будем исходить из того, что любое кольцо это аддитивная абелева группа $<K, +>$. Поэтому за элементы множества K/L будем брать смежные классы $a+L$ (называемые классами вычетов по модулю идеала L), сложение и умножение которых осуществляется по правилам:

$$\forall\ a,b \in K,\ (a+L) \oplus (b+L) \overset{df}{=} (a+b)+L$$

$$-(a+L) = -a+L$$

$$\forall\ a,b \in K,\ (a+L) o (b+L) \overset{df}{=} a \cdot b + L.$$

Проверьте, что эти операции не зависят от выбора элементов a и b и докажите теорему 1.

Теорема 1: *Алгебра $<K/L, \oplus, o>$, где $K/L=\{a+L \mid a \in K, L$ - идеал$\}$, является кольцом.*

Нулем в кольце K/L является класс $0+L$, единицей - $e+L$ (если в K есть e). Кольцо K/L называют факторкольцом кольца K по идеалу L.

Отображение φ: $K \to K/L$, $\varphi(a)=a+L$, $\forall\ a \in K$, очевидно, будет эпиморфизмом, а $Ker\ \varphi=L$.

Таким образом, от частного примера факторкольца $Z_m=Z/mZ$ и эпиморфизма φ: $Z \to Z_m$ мы пришли к аналогичной ситуации в произвольных кольцах.

Также как и теории групп, в теории колец справедлива основная теорема 2 о гомоморфизмах колец.

Теорема 2: *Пусть φ- произвольный эпиморфизм кольца $<K, +, \circ>$ на кольцо $<K', +. \circ>$, σ: $K \to K/L$ — канонический эпиморфизм кольца K в свое факторкольцо по идеалу L, тогда $\exists$ изоморфизм ψ: $K/L \to K'$: $\sigma \cdot \psi = \varphi$.*

Доказательство этой теоремы и выводы из нее, с точностью до обозначений, повторяет доказательство и выводы для групп (проверьте самостоятельно).

В заключение рассмотрим конструкцию, которая позволяет для любого кольца, являющегося областью целостности, построить минимальное поле, содержащее это кольцо. Аналогично тому, как поле $<Q, +, \circ>$ является наименьшим полем, содержащим кольцо $<Z, +, \circ>$.

Пусть дана произвольная область целостности с *e*, <*K*, +, °>. Рассмотрим множество $M=\{(a,\ b) \mid a,\ b\in K,\ b\neq 0\}$, то есть $M=K\times(K\setminus\{0\})$. Зададим на множестве М бинарное отношение $(a,\ b)\varphi(a',\ b') \overset{df}{\Leftrightarrow} (ab'=a'b)$. Самостоятельно проверьте, что φ - отношение эквивалентности. Оно задает разбиение множества *M* на классы эквивалентности. Класс эквивалентности, представителем которого является пара *(a, b)* будем обозначать $\frac{a}{b}$; понятно, что пара (*ac, bc)* будет определять этот же класс (проверьте!).

Множество всех классов обозначим символом М/φ: $M/\varphi=\{\frac{a}{b} \mid a,b\in K,\ b\neq 0\}$.

Теперь на множестве *M/*φ зададим операции:

$$\frac{a}{b}\oplus\frac{c}{d}=\frac{ad+bc}{bd};$$

$$\frac{a}{b}o\frac{c}{d}=\frac{ac}{bd}.$$

Покажите самостоятельно, что эти операции не зависят от выбора представителей и, что $<M_\varphi, \oplus,$ o> является полем, то есть, что

а) $< M_\varphi, \oplus>$ - абелева группа,

б) $< M_\varphi\text{-}(\frac{0}{b}))$, °> - абелева группа,

в) операция ⊕ связана с операцией o левым и правым дистрибутивным законами.

В этом поле роль нуля играет класс $\frac{0}{b}$, где $b\neq 0$, роль единицы - $\frac{c}{c}$, $c\neq 0$, противоположным элементом к элементу $\frac{a}{b}$

будет элемент -$\frac{a}{b}$, так как $\frac{a}{b}+\left(-\frac{a}{b}\right)=\frac{0}{b}$; $\frac{b}{a}$ обратный к $\frac{a}{b}$, так как $\frac{a}{b}\cdot\frac{b}{a}=\frac{c}{c}$..

Теперь покажем, что построенное поле *M/φ* содержит мономорфный образ кольца <*K*,+,°>. Действительно, отображение φ: $K\to M/\varphi$, φ: $a\mapsto\frac{ab}{b}$ (b≠0) является инъективным так как, если φ(a)=φ(b), то *(a=b)*. Действительно, φ(a)=$\frac{ab}{b}$, φ*(b)*=$\frac{bc}{c}$, то из того, что $\frac{ab}{b}=\frac{bc}{c}\Rightarrow(a=b)$.

Кроме этого, отображение φ удовлетворяет условиям гомоморфности для колец:

а) ∀ a,b∈*K*, $\varphi(a+b)=\varphi(a)\oplus\varphi(b)$;

б) ∀ a,b∈*K*, $\varphi(a\cdot b)=\varphi(a)o\varphi(b)$. (проверьте!)

Таким образом, мы построили поле M_φ, которое содержит φ(K). Это поле называют полем частных кольца *K*.

Докажите самостоятельно, что это поле является наименьшим из всех полей, содержащих кольцо φ(K).

6. ПРАКТИКУМ ПО АЛГЕБРЕ

Практическое занятие №1
Операции на множествах, их свойства.

1**.** Являются ли операциями и какого ранга следующие действия:

а) вычисление десятичных логарифмов на множестве *R;*

б) вычисление среднего геометрического двух чисел на множестве R^+ - положительных действительных чисел;

в) вычисление среднего арифметического трех чисел на множестве *Q;*

г) вычисление наибольшего делителя *n* чисел на множестве *N;*

д) скалярное умножение на множестве векторов плоскости V_2,

е) векторное умножение на множестве векторов пространства V_3,

ж) преобразование параллельного переноса T_a на вектор $\vec{a}$ на множестве точек плоскости;

з) композиция $R_\alpha * R_\beta$ поворотов на угол α и на угол β вокруг фиксированной точки O на множестве всех поворотов плоскости с центром O;

и) нахождение обратной матрицы на множестве квадратных матриц;

к) вычисление определителя матрицы на множестве квадратных матриц;

л) вычисление площади треугольника на множестве треугольников.

2. Исследовать свойства операции *, заданной на множестве {a, b, c} элементов произвольной природы *таблицей Кэли:*

*	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

(**Артур Кэли** <1821-1895> английский математик)

3. Исследовать свойства операции *, заданной на множестве R формулой $a*b=(a+b)^2$.

4. Рассмотрим множество $Z_m=\{\bar{1}, \bar{2},..., \overline{m-1}\}$ - классов вычетов по модулю m, где класс $\bar{r}$ состоит из целых чисел, которые при делении на m дают в остатке r. Операции сложения $\oplus$ и умножения классов на множестве Z_m задаются так: $\bar{r} \oplus \bar{s} = \overline{r+s}$; $\bar{r} \circ \bar{s} = \overline{r \cdot s}$. Исследовать свойства этих операций на множестве Z_5.

Практическое занятие №2
Группа, подгруппа, примеры.

1. Доказать, что множество M_n невырожденных матриц n-порядка с действительными элементами образует относительно операции матричного умножения мультипликативную группу.

2. Проверить, что множество $\{\sqrt[3]{1}\}$ (корней третьей степени из единицы) образует относительно операции умножения комплексных чисел конечную мультипликативную группу. Составить таблицу Кэли.

3. Проверить, что множество подстановок четвертой степени S_4 относительно операции композиции преобразований образует группу. Будет ли она коммутативной?

4. Проверить, что следующие алгебры являются группами:

а)$<Z_3,+>$ б)$<Z_3^0, \cdot>$ в)$<Z_4,+>$ г)$<Z_5^0,\cdot>$

Для каждого случая составить таблицу Кэли.

5. Проверить, будут ли следующие множества группами относительно указанных операций:

а)$<\{\sqrt[4]{1}\}, \circ>$

б)$S_3 = < \left\{ \begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}, \begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}, \begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}, \begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix} \right\}, \circ >$

6. Показать, что множество всевозможных параллельных переносов $\{T_a\}$ точек плоскости образует группу относительно операции композиции преобразований $T_a \circ T_b = T_{a+b}$.

7. Показать, что множество $\{R\alpha\}$ всевозможных вращений точек плоскости вокруг центра O относительно операции композиции образует группу.

8. Проверить, является ли группой множество $\{S_d\}$ симметрией относительно прямой d, заданных на множестве точек плоскости, относительно операции композиции.

9. Показать, что алгебра $<R, T>$ является полугруппой и найти нейтральный элемент (когда он имеется), если операция T задана так:

а) $a\ T\ b = a\ (1-b)+b$; *в)* $a\ T\ b = 2ab-a-b+1$

б) $a\ T\ b = ab\ (a+1\ )+2a-1$; *г)* $a\ T\ b = -2a-2b+6+ab$

10.Будет ли $<A, \cdot>$ являться подгруппой группы $<M_3, \cdot>$ матриц третьего порядка относительно операции матричного умножения, где множество A составляют матрицы:

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

11. Пусть M_2^0 - множество невырожденных матриц второго порядка с действительными элементами. Выяснить, является ли подгруппой группы $<M_2^0, \cdot>$ множество H относительно матричного умножения, если:

а) $H = \left\{\begin{pmatrix}a&b\\-b&a\end{pmatrix} \mid a,b\in R\right\}$, в) $H = \left\{\begin{pmatrix}a&b\\b&b\end{pmatrix} \mid a,b\in R\right\}$,

б) $H = \left\{\begin{pmatrix}a&b\\0&c\end{pmatrix} \mid a,b,c\in R\right\}$, г) $H = \left\{\begin{pmatrix}1&0\\0&1\end{pmatrix}, \begin{pmatrix}-1&0\\0&-1\end{pmatrix}, \begin{pmatrix}0&-1\\1&0\end{pmatrix}, \begin{pmatrix}0&1\\-1&0\end{pmatrix}\right\}$.

12. Доказать, что множество параллельных переносов T_a точек плоскости является подгруппой группы движений <D,°> относительно операции композиции преобразований плоскости.

13.Пусть $<V_2, +>$ аддитивная группа векторов плоскости. Выяснить, в каком случае множество V_1 векторов произвольной прямой, лежащей на плоскости, относительно операции сложения векторов образует подгруппу группы $<V_2, +>$.

14. Разложить подстановки а) $\varphi=\begin{pmatrix}1&2&3&4&5&6&7&8\\3&2&4&1&7&6&8&5\end{pmatrix}$;

б) $\varphi=\begin{pmatrix}1&2&3&4&5&6&7&8\\4&5&7&2&1&6&8&3\end{pmatrix}$

в произведение независимых циклов, а затем транспозиций.

Практическое занятие №3
Вычисление порядка элемента в различных группах.

1. В следующих группах найти порядки их элементов, определить тип группы (периодическая, без кручения, смешанная). Для элемента а найти подгруппу G_a и составить для нее таблицу Кэли:

а)$<\{\sqrt[3]{1}\}, \bullet>$, $\{\sqrt[3]{1}\} = \{1,-1/2+i\sqrt{3}/2,-1/2-i\sqrt{3}/2\}$,a=-l/2+i√3/2.

б) $<Z_4, \oplus>$, $Z_4=\{\ \overline{0},\overline{1},\overline{2},\overline{3}\ \}$, $a=\overline{2}$.

в)$<Z_5^{\,0}, \bullet>$, $Z_5^{\,0}=\{\ \overline{0},\overline{1},\overline{2},\overline{3},\overline{4}\ \}$, $a=\overline{3}$.

г)$<S_3, \circ>$, $S_3=\left\{\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}, \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}, \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}, \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}, \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}, \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}\right\}$, $a=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$

д) $<Z_8, \oplus>$, $a=\overline{4}$.

е) $<2Z, +>$, $a=4$.

2. Докажите, что если порядок элемента a группы равен n и $a^m=e$, то m делится на n.

3. Докажите, что если порядок элемента a группы равен n, то $a^s=a^t$ в том и только в том случае, когда s-t делится на n.

4. Доказать, что $\forall\ a,b\in<G, \bullet>$ элементы $a\cdot b$ и $b\cdot a$ имеют одинаковый порядок.

Практическое занятие №4
Циклические группы.

1. Выяснить, являются ли группы циклическими. Найти все их образующие элементы:

а) $<Z_4, \oplus>$, б) $<Z_5, \oplus>$, в) $<2Z, +>$, г) $<Z_7^{\,0}, \cdot>$, д) $<\sqrt[3]{1}, \bullet>$, е)$<\sqrt[4]{1}, \bullet>$, ж)$<S_3, \circ>$, з)$<\{2^k\}, \cdot>$, и)$<\{(-3)^k\}, \cdot>$, к)$<Q, +>$, л)$<Q^0, \cdot>$.

2. Выяснить, являются ли циклическими группами, и найти все образующие элементы для группы поворотов правильного:

а) четырехугольника; б) шестиугольника;

в) двенадцатиугольника.

3. Пусть $<M_2, \cdot>$ — мультипликативная группа невырожденных матриц второго порядка над полем С. Найти порядок элемента a и подгруппу G_a, если:

а)$a=\begin{pmatrix}1&0\\0&-1\end{pmatrix}$; б)$a=\begin{pmatrix}1&1\\0&1\end{pmatrix}$; в)$a=\begin{pmatrix}1&0\\0&i\end{pmatrix}$; г)$a=\begin{pmatrix}i&0\\0&-i\end{pmatrix}$; д)$a=\begin{pmatrix}i&0\\0&-1\end{pmatrix}$

4. В следующих группах найдите циклические подгруппы:

а) $<S_4, \bullet>$ - группа подстановок 4-ой степени,

б) группа самосовмещений правильного ромба,

в) группа самосовмещений правильного треугольника.

5. Доказать, что все конечные циклические группы изоморфны мультипликативной группе корней n-ой степени из единицы.

6. Доказать, что группа простого порядка не содержит нетривиальных подгрупп.

7. Доказать, что всякая группа простого порядка будет циклической и любой элемент в ней, отличный от единичного, является образующим.

Практическое занятие №5
Разложения группы по подгруппе. Смежные классы.

1. Найти смежные классы и индекс подгруппы:

а) группы $<Z, +>$ по подгруппе $<mZ, +>$;

б) группы $<R, +>$ по подгруппе $<Z, +>$;

в) группы $<C, +>$ по подгруппе $<\{a+bi \mid a, b \in Z\}, +>$;

г) группы $<C\backslash\{0\}, \cdot>$ по подгруппе $<\{a+bi \mid |a+bi|=1, \cdot>$;

д) группы $<C\backslash\{0\}, \cdot>$ по подгруппе $<R\backslash\{0\}, \cdot>$;

е) аддитивной группы векторов плоскости, выходящих из начала координат, по подгруппе векторов, лежащих на оси *Ox;*

ж) доказать, что в циклической группе нет двух подгрупп с равными индексами.

2. Найти разложения циклической группы десятого порядка по всем ее подгруппам.

3. Найти разложение бесконечной циклической группы, порожденной элементом *(a)* по подгруппе, порождаемой элементом (a^3).

4. Доказать, что знакопеременная группа $A_4(M)$ не имеет подгрупп шестого порядка.

Практическое занятие №6
Фактор-группа и ее свойства. Нормальные делители.

1. Найти фактор-группы:

а) группы $<Z, +>$ по подгруппе $<7Z, +>$;

б) группы $<R\backslash\{0\}, \bullet>$ по подгруппе $<R^+, \bullet>$;

в) группы $<C, +>$ по подгруппе $<R, +>$.

2. Пусть G - группа всех движений трехмерного пространства, H-ее подгруппа параллельных переносов. Доказать, что $H \lhd G$.

3. Доказать, что множество M всех элементов группы G, каждый из которых перестановочен со всеми элементами группы, является нормальным делителем (называемым центром группы G).

4. Доказать, что любая подгруппа индекса два является нормальным делителем в группе.

5. Найти все нормальные делители симметрической группы $\sigma_3(M)$.

6. Доказать, что $A_n(M) \lhd \sigma_n(M)$.

7. Найти все нормальные делители абелевой группы пространства R^3.

8. Пусть $H_1 \lhd G$, $H_2 \lhd G$. Выяснить, будет ли в общем случае $H_1 \cup H_2 \lhd G$?

Практическое занятие №7
Изоморфизмы групп.

1. Доказать, что группа <R,+> изоморфна группе $<M_2+>$, где $M_2 = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}, \quad a \in R, a \neq 0 \right\}$.

2. Выяснить будут ли изоморфны группы $<A, \cdot>$ и <B, $\cdot>$, где $A = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} | \quad a,b \in R, a \neq 0 \right\}$,

$B=\{f(x)=ax+b \mid a,b \in R, a \neq 0\}$.

3. Доказать, что если каждому элементу (a) группы <A,$\cdot$> поставить в соответствие элемент $g^{-1}ag$, где g - фиксированный элемент из A, то получим изоморфное отображение группы $<A, \cdot>$ на себя.

4. Выяснить, изоморфна ли группа всех самосовмещений ромба группе всех самосовмещений прямоугольника.

5. Выяснить, гомоморфизмами какого вида являются следующие отображения групп:

а) $<\sqrt[2]{1}, \cdot>, <\sqrt[4]{1}, \cdot>, \varphi: \begin{cases} 1 \to i \\ -1 \to -i \end{cases}$;

б) $<\sqrt[2]{1}, \cdot>, <\sqrt[4]{1}, \cdot>, \varphi: \begin{cases} 1 \to 1 \\ -1 \to -1 \end{cases}$;

в) $<Z,+>, <Z,+>, \forall\ a \in Z, \varphi(a)=3a$;

г) $<Z,+>, <Z,+>, \forall\ x \in Z, \varphi(x)=x^2$;

д) $<\sqrt[3]{1}, \cdot>, <2S_3, \circ>, \varphi: \begin{cases} \varepsilon_0 \to a_0, \\ \varepsilon_1 \to a_1, \\ \varepsilon_2 \to a_2, \end{cases}$ где $2S_3$ - группа четных подстановок третьей степени ;

е) $<S_3, \circ>, <\{\sqrt[3]{1}\}, \cdot>, \varphi: \begin{cases} a_i \to 1 \\ a_{i+1} \to -1 \end{cases}$, i=0,2,4.

6. Доказать или опровергнуть, что следующие группы изоморфны:

а) $<M, \cdot>$ - группа поворотов правильного треугольника и группа $<2S_3, \circ>$ четных подстановок третьей степени;

б) $<2Z, +>$ и $<\{2^k\}, \cdot>$;

в) $<R,+>$ и $<M_2, \cdot>$, где $M_2 = \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}, \quad x \in R \right\}$;

г) $<C, +>$ и $<V_2,+>$, где $V_2=\{(x,y) \mid x,y \in R\}$;

д) $<C, \cdot>$ и $<M_2, \cdot>$, где $M_2 = \left\{ \begin{pmatrix} x & y \\ -y & x \end{pmatrix} \mid \quad x, y \in R \right\}$;

е) $<\{\sqrt[3]{1}\}, \cdot>$ и $<Z_3, \oplus>$;

ж) $<\{\sqrt[4]{1}\}, \cdot>$ и $<Z_4, \oplus>$.

Практическое занятие №8
Морфизмы групп.

1. Пусть даны мультипликативная группа невырожденных квадратных матриц над полем F - $<M_{nn}(F), \cdot>$ и мультипликативная группа этого поля $<F^0, \circ>$. Доказать, что отображение $f: A \to |A|$, сопоставляющее каждой матрице A ее определитель, будет гомоморфным. Определить тип и ядро этого гомоморфизма.

2. Доказать, что отображение $f: Z \to Z_m$, $f: a \mapsto \bar{a}$, сопоставляющее каждому целому числу его класс вычетов но модулю *(m),* будет эпиморфизмом. Найти его ядро.

3. Построить фактор-группу группы $G=<Q\backslash\{0\}, \cdot>$ по подгруппе $H=<\{1, -1\}, \cdot>$, указать гомоморфизм φ: $G \to G/H$ и найти ядро этого гомоморфизма.

4. Доказать, что отображение φ: $<R\backslash\{0\}, \cdot>$ в $<R^+, \cdot>$ такое, что $\varphi(x)=|x|$, является гомоморфизмом.

5. Задать гомоморфизм $<V^2, +>$ на группу $<R, +>$.

6. Доказать, что если φ_1: $G_1 \to G_2$ и φ_2: $G_2 \to G_3$ - гомоморфизмы, то и $\varphi_1 \circ \varphi_2$: $G_1 \to G_3$ – гомоморфизм.

7. Доказать, что аддитивную группу функций вида:

$\{y=ax+b \mid a,b \in R\}$ можно гомоморфно отобразить на аддитивную группу $<R,+>$. Указать ядро этого гомоморфизма.

8. Доказать, что фактор-группа симметрической группы σ_n по знакопеременной группе A_n изоморфна фактор-группе аддитивной группы целых чисел по подгруппе $2Z$.

9. Доказать, что если на плоскости дан правильный n-угольник с центром O и G -группа всех поворотов этой плоскости вокруг точки O, а A - подгруппа тех поворотов плоскости, которые переводят правильный n-угольник в себя, то A - нормальный делитель группы G и $G/A \cong G$.

10. Доказать, что группа $<\{\sqrt[3]{1}\}, \cdot>$ изоморфна некоторой группе подстановок, указать порядок этой группы, составить таблицу Кэли.

17. Доказать, что все группы четвертого порядка можно представить квадратными матрицами второго порядка.

11. Доказать, что если **а** образующий элемент произвольной группы третьего порядка, то эту группу можно представить комплексными числами. Указание: $a \mapsto z \in C \mid z^3=1$.

12. Доказать, что отображение f: $S_3 \to M_{3x3}(R)$ такое, что

$$f: \begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix} \to \begin{pmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix}, \quad f: \begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix} \to \begin{pmatrix}0 & 1 & 0\\ 0 & 0 & 1\\ 1 & 0 & 0\end{pmatrix},$$

(остальные образы построить самостоятельно) задает представление

группы $<S_3, \circ>$ матрицами третьего порядка.

13. Используя теорему Кэли для группы *G,* найдите изоморфную ей группу левых трансляций *T(G):*

а) $G=<\{\sqrt[4]{1}\}, \cdot>$; б) $G=<Z_4, \oplus>$;

в) G - группа поворотов правильного треугольника;

г) G - мультипликативная группа невырожденных матриц 2-го порядка с элементами из поля *R.*

Практическое занятие №9
Коммутатор и коммутант группы.

1. Пусть группа G действует на множестве *M,* доказать, что если две точки x_0, $x_1 \in M$ принадлежат одной орбите, то их стационарные подгруппы (стабилизаторы) сопряжены, то есть, если $x_0=gx_1 \Rightarrow St(x_1)=gSt(x_0)g^{-1}$.

2. Пусть дана G-орбита точки $x_0 \in G$, $G(x_0)=\{gx_0 \mid g \in G\}$. Доказать, что если $|G|=n$, $|G(x_0)|=k$, то n/k.

3. Пусть $[x, y]$ - коммутатор элементов x и y группы G. Доказать, что:

а) $[x,y]^{-1}=[y,x]$, $\forall\, x,y \in G$;

б) если $[x,y]$ - коммутатор, то $z^{-1}[x,y]\cdot z$ также будет коммутатором для $\forall\, z \in G$.

4. В группе целочисленных матриц второго порядка с определителем, равным ±1, для элементов

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

Найти коммутаторы $[x, y]$, $[y, z]$, $[z, x]$.

5. Доказать, что коммутант всегда является нормальным делителем группы.

6. Доказать, что фактор-группа группы G по ее коммутанту всегда абелева.

7. Пусть $H \lhd G$. Доказать, что фактор-группа G/H будет абелевой тогда и только тогда, когда H содержит коммутант группы.

8. Доказать, что отношение сопряженности элементов в группе G является отношением эквивалентности.

9. Доказать, что если $a=x\cdot b\cdot x^{-1}$, то $p(a)=p(b)$.

10. Элементы симметрической группы $\sigma_3(M)$ распределить по классам сопряженных элементов.

Практическое занятие №10
Центр группы.

1. В группе всех вещественных обратимых матриц второго порядка найти нормализаторы следующих элементов: $x=\begin{pmatrix}1 & 0\\ 0 & 2\end{pmatrix}, y=\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}, z=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$.

2. Выяснить, какие из следующих матриц сопряжены между собой в группе всех вещественных обратимых квадратных матриц второго порядка: $A=\begin{pmatrix}-1 & 1\\ -1 & 1\end{pmatrix}, B=\begin{pmatrix}3 & 1\\ 1 & 1\end{pmatrix}, C=\begin{pmatrix}2 & 1\\ -2 & 0\end{pmatrix}$.

3. Пусть H - подгруппа группы G и $x \in G$. Доказать, что $x^{-1}Hx$ также является подгруппой группы G.

4. Доказать, что центр группы Z(G) является ее нормальной подгруппой.

5. Доказать, что группа внутренних автоморфизмов группы G изоморфна фактор-группе группы G по ее центру.

Практическое занятие №11
Кольцо. Примеры колец.

1. Выяснить, будет ли <A,⊕, °>-кольцом, полем, если A={0,1}, $a \oplus b = \begin{cases} 0, \text{ если } a = b \\ 1, \text{ если } a \neq b \end{cases}$

$\forall\ a,b \in A,\ a \cdot b$ - обычное произведение.

2. Выяснить, будет ли <*R*, +, 0> кольцом, полем, если $a \cdot b = b$.

3. Выяснить, будет ли <*M*,+, °> - кольцом, полем, если $M=\{a+b\sqrt{3} \mid a,b \in Q\}$.

4. Какие из указанных множеств матриц образуют подкольцо кольца $<M_{nn}(P), +, °>$:

а) множество верхних треугольных матриц порядка $n \geq 2$;

б) множество матриц порядка $n \geq 2$, у которых две последние строки - нулевые;

в) множество матриц вида: $\begin{pmatrix} x & y \\ 2y & x \end{pmatrix}$, где $x,y \in Z$;

г) множество комплексных матриц вида: $\begin{pmatrix} z & u \\ -u & \bar{z} \end{pmatrix}$?

5. Какие из указанных множеств функций образуют кольцо относительно обычных операций сложения и умножения функций:

а) множество функций вещественного переменного, непрерывных на отрезке $[a,b]$;

б) множество целых рациональных функций вещественного переменного.

6. Является ли множество $\{f(x) \mid f(x)= a_n x^n+...+a_1 x+a_0,\ a_i \in R\}$ кольцом относительно операции сложения многочленов и умножения, заданного правилом $(f°g)(x)=f(g(x))$?

7. Образует ли кольцо множество всех подмножеств некоторого множества относительно операций пересечения и объединения множеств?

Практическое занятие №12
Подкольца, поля, примеры.

1. Для каких чисел n=2, 3, 4, 5, 6 существует поле из (n) элементов?

2. Доказать, что любое конечное поле имеет положительную характеристику.

3. Доказать, что в конечном кольце с единицей каждый ненулевой элемент либо обратим, либо является делителем нуля.

4. Доказать, что множество обратимых элементов кольца с единицей образуют мультипликативную группу.

5. Найти все делители нуля в кольцах $<Z_8, +, \circ>$, $<Z_{10}, +, \circ>$ и их мультипликативные группы обратимых элементов.

6. Дано кольцо $<K, +, \circ>$, U и L его подкольца. Выяснить, будет ли пересечение $U \cap L$ подкольцом кольца K?

7. Дано поле $<P, +, \circ>$, A и B его подполя. Выяснить, будет ли пересечение $A \cap B$ подполем поля P?

Практическое занятие №13
Области целостности и их свойства.

1. $<K, +, \circ>$ - область целостности. Доказать, что

а) если $a, b, c \in K$ и $(a \neq 0)$, то из равенства $(ab=ac) \Rightarrow (b=c)$.

б) если $a, b \in K (b \neq 0)$ и $(a:b)$, то $\exists\, !\, q \in K : a=bq$.

в) $\forall\ a, b \in K\ (a:b) \& (b:a) \Leftrightarrow (a=b\varepsilon)$, где ε - обратимый элемент.

2. Доказать, что $<Q(i), +, \circ>$ является полем, где $Q(i)=\{a+bi \mid a, b \in Q\}$.

3. Доказать, что если $z_1, z_2 \in Z(i)$ и $(z_1 : z_2)$, то $\varphi(z_1) / \varphi(z_2)$.

4. Доказать, что если z_0 - обратимый элемент кольца $Z(i)$, то $\varphi(z_0)=1$.

5. Доказать, что в кольце $<Z(i), +, \circ>$ обратимые элементы исчерпываются множеством $\{1, -1, i, -i\}$.

6. Найти обратимые, простые и составные элементы кольца $<Z_{10}, +, \circ>$.

7. Докажите теоремы 4 и 5 из §7.

8. Доказать, что в кольце $<Z(\sqrt{3}), ^{+}, \circ>$ число 4 разлагается на простые множители двумя различными способами.

Практическое занятие №14
Кольца главных идеалов.

1. Пусть $<K, +, \circ>$ - кольцо главных идеалов, (a)≠(0) его любой идеал.

Доказать следующие утверждения:

а) если *(a)* - идеал, то *(a)* является подкольцом кольца K.

б) если $b, c \in (a) \Rightarrow (b-c) \in (a)$

с) если $b \in (a) \Rightarrow rb \in (a)$, где $r \in K$

д) если обратимый элемент $\varepsilon \in (a)$, то $(\varepsilon)=K$.

е) если $(a)=(b)$, то $a=b\varepsilon$, где ε - обратимый элемент кольца *K,*

ж) $(a:b) \Leftrightarrow (a) \subset (b)$

з) если *(a)* и *(b)* идеалы, то $(a) \cap (b)$ - идеал.

2. Доказать, что кольца $Z(\sqrt{5})$ и $Z(\sqrt{3})$ не являются кольцами главных идеалов.

Практическое занятие №15
Гомоморфизмы колец и полей.

1. Доказать, что множество всех автоморфизмов кольца R образуют группу относительно операции композиции.

2. Доказать, что отображение $x \to a^{-1}xa \ \ (x, a \in R)$ в кольце R является автоморфизмом.

Изоморфны ли поля Q и R, R и C?

3. Пусть *f*- гомоморфизм кольца $<K, +, \circ>$ в кольцо $<A, \oplus, o>$. Доказать, что *Ker* φ является подкольцом кольца *K.*

4. Показать, что эпиморфный образ коммутативного кольца является коммутативным кольцом.

5. Найти все гомоморфизмы:

а) группы *Z* в группу *Q;*

б) кольца Z в кольцо *Q.*

Практическое занятие №16
Факторкольца и их свойства.

1. Доказать, что если <*K*, +, °> кольцо с единицей и *L* - идеал, то факторкольцо *K/L* тоже имеет единицу.

2. Построить факторкольцо кольца *Z* по идеалу 5*Z*.

3. Доказать, что факторкольца $R[x]/(x^2+1)$ и $R[x]/(x^2+x+1)$ изоморфны полю C.

4. Доказать, что

а) факторкольцо *Z(i)/(2)* не является полем;

б) факторкольцо *Z(i)/(3)* является полем из 9 элементов.

5. Изоморфны ли факторкольца $Z[x]/(x^2-2)$ и $Z[x]/(x^2-3)$?

Практическое занятие №17
Идеалы колец. Поля частных.

1. Найти все идеалы кольца многочленов *P[x],* где *P* - поле.

2. Доказать, что кольцо *Z[x]* не является кольцом главных идеалов.

3. Найти все идеалы кольца верхних треугольных матриц порядка 2 с целыми числами.

4. Доказать, что если идеал кольца содержит обратимые элементы, то этот идеал совпадает со всем кольцом.

5. Доказать, что $\forall a \in Z$ отображение $a \to \frac{a}{1}$ является вложением Z в Q.

Практическое занятие №18
Контрольная работа.

Задание I. Разложить подстановку в произведение независимых циклов, а затем — транспозиций:

а) $\varphi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 4 & 1 & 5 & 2 & 7 & 6 & 9 & 8 \end{pmatrix}$;

б) $\varphi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 2 & 1 & 3 & 9 & 6 & 5 & 7 & 8 \end{pmatrix}$.

Задание II. Найти все подгруппы группы:

а) $\langle Z_6, + \rangle$ б) $\langle Z_8, + \rangle$.

Задание III. Описать группы симметрий:

а) квадрата б) ромба.

Задание IV. Докажите, что:

а) группа $\langle R_+ \setminus \{0\}, \bullet \rangle$ изоморфна группе $\langle R, + \rangle$;

б) группа $\langle Q_+ \setminus \{0\}, \bullet \rangle$ не изоморфна группе $\langle Q, + \rangle$.

Задание V. Построить вложение кольца

а) $\langle R, +, \bullet \rangle$ в $\langle C, +, \bullet \rangle$.

б) $\langle R, +, \bullet \rangle$ в $\langle M_{nn}(R), +, \bullet \rangle$.

Задание VI. Построить факторкольцо кольца:

а) Z по идеалу 7Z;

б) R по идеалу (3).

7 . ГЛОССАРИЙ

Группа — моноид, в котором каждый элемент имеет симметричный.

Евклидово кольцо — кольцо, в котором можно задать евклидову норму.

Кольцо главных идеалов — область целостности, все идеалы которой главные.

Коммутант — подгруппа, порожденная коммутаторами.

Нормальный делитель — подгруппа, содержащая все свои сопряженные элементы.

Область целостности — кольцо без делителей нуля.

Подгруппа — подмножество группы, само являющееся группой.

Поле **—** коммутативно-ассоциативное кольцо с единицей, в котором каждый элемент, отличный от нуля, имеет симметричный элемент.

Фактор-группа **—** группа, элементами которой являются смежные классы по нормальному делителю.

Центр группы **—** подгруппа, все элементы которой перестановочны.

8. ОСНОВНАЯ И ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА

8.1. Основная литература

1. *Кострикин А. М.* Введение в алгебру. - М.: Наука, 2001.
2. *Кострикин А. М.* Основные структуры алгебры. - М.: 2001.
3. *Кострикин А. И.* Сборник задач по алгебре. - М.: 2005.
4. *Калужнин Л. А.* Введение в общую алгебру. - М.: Наука, 2001.
5. *Крылов П. А., Туганбаев А. А., Чехлов А. Р.* Упражнения по группам, кольцам и полям. – Томск, 2008.
6. *Курош А. Г.* Лекции по общей алгебре. - М.: Наука, 2006.

8.2. Дополнительная литература

1. В*ан-дер-Варден.* Алгебра.. – М.: Наука, 1979.
2. *Скорняков Л. А.* Элементы алгебры. - М.: Наука, 1980.
3. *Каргаполов М. И., Мерзляков Ю. И.* Основы теории групп. - М.: Наука, 1977.
4. *Мальцев А. И.* Алгебраические системы. - М.: Наука, 1970.
5. *Куликов Л. Я.* Алгебра и теория чисел. - М.: Высшая школа, 1979.
6. *Ленг .С.* Алгебра. - М.: Издательство Мир, 1968.
7. *Белоногов В. А.* Задачник по теории групп. - М.: Наука, 1977.
8. *Воеводин В. В.*, *Кузнецов Ю. А.* Матрицы и вычисления. – М.: Наука, 1984.

Для заметок

Для заметок

Для заметок

Учебное издание

Учебно-методический комплекс
«Алгебра (общая алгебра)»

Составители:
Пуркина Валентина Федоровна
Кайгородов Евгений Владимирович

Подписано в печать Формат 60*84/16
Бумага офсетная. Усл.печ.л.-
Заказ № . Тираж

РИО Горно-Алтайского госуниверситета,
649000, г. Горно-Алтайск, ул. Ленкина, д. 1

Отпечатано полиграфическим отделом
Горно-Алтайского госуниверситета,
649000, г. Горно-Алтайск, ул. Ленкина, д. 1