Учреждение образования
«Брестский государственный университет имени А.С. Пушкина»
Кафедра алгебры, геометрии и математического моделирования

Е.В. Зубей
А.А. Трофимук

Алгебра

Алгебраические структуры

Часть 2

Электронный учебно-методический комплекс в 3-х частях
для студентов дневной формы получения образования специальности
1-02 05 01 «Математика и информатика»
физико-математического факультета

Брест
БрГУ им. А.С.Пушкина
2021

Авторы-составители:

Зубей Екатерина Владимировна — доцент кафедры алгебры, геометрии и математического моделирования БрГУ имени А.С. Пушкина, кандидат физико-математических наук

Трофимук Александр Александрович — доцент кафедры алгебры, геометрии и математического моделирования БрГУ имени А.С. Пушкина, кандидат физико-математических наук, доцент

Редактор:

Ткач Светлана Николаевна — старший преподаватель кафедры прикладной математики и информатики БрГУ имени А.С. Пушкина

Технический редактор:

Яцук Татьяна — студентка IV-ого курса специальности «Прикладная математика» физико-математического факультета БрГУ им. А.С. Пушкина

Рецензенты:

Грицук Дмитрий Владимирович — заведующий кафедрой прикладной математики и информатики БрГУ имени А.С. Пушкина, кандидат физико-математических наук, доцент

Кафедра высшей математики Брестского государственного технического университета

ЭУМК написан в соответствии с действующей учебной программой по дисциплине «Алгебра» и состоит из трех частей: «Линейная алгебра», «Алгебраические структуры» и «Алгебра многочленов». Вторая часть «Алгебраические структуры» знакомит студентов с основами теории алгебраических структур (группы, кольца, поля, идеалы) в объеме, необходимом для понимания современного уровня работ по прикладной алгебре, призвана обучить студентов умению применять основные методы алгебраических структур в других разделах математики и ее приложениях.

СОДЕРЖАНИЕ

Кафедра АГ и ММ

Предисловие

Настоящий ЭУМК предназначен для студентов дневной формы получения образования специальности 1-02 05 01 «Математика и информатика» физико-математического факультета. ЭУМК разработан в соответствии с образовательным стандартом высшего образования ОСВО 1-02 05 01-2013; учебным планом учреждения высшего образования по специальности 1-02 05 01 «Математика и информатика», рег. №ФМ-24-19/уч., утвержденным 30.05.2019.

Комплекс содержит вспомогательный раздел, который включает в себя примерный тематический план и содержание учебного материала. В курсе лекций излагается теоретический материал, содержащий вопросы, связанные с понятием основных алгебр (группы, кольца, поля), с полем комплексных чисел, с теорией групп и теорией колец. Теоретический материал иллюстрируется многочисленными примерами решения задач. В практикуме студентам предложено большое количество индивидуальных задач с приведенными типовыми примерами их решения. Логическим завершением ЭУМК является раздел контроля знаний, состоящий из вопросов к экзамену и итогового теста.

ЭУМК ставит своей целью облегчить самостоятельную работу студентов с теоретическим материалом при подготовке к лекциям, практическим занятиям и экзамену.

Авторы-составители

ПРИМЕРНЫЙ ТЕМАТИЧЕСКИЙ ПЛАН

№	Название раздела, перечень изучаемых вопросов	УСР	ЛК	ПР
1	**Алгебры (24 ч.)**		**12**	**12**
1.1	Алгебраические операции. Алгебры. Виды бинарных операций. Нейтральный и симметричные элементы..		2	2
1.2	Группы, простейшие свойства группы, примеры.		2	2
1.3	Гомоморфизмы групп (определение, виды гомоморфизма, примеры).		2	2
1.4	Кольца, простейшие свойства кольца, примеры.		2	4
1.5	Гомоморфизмы колец (определение, виды гомоморфизма, примеры).		2	2
1.6	Поля, простейшие свойства поля, примеры.		2	4
2	**Поле C (28 ч.)**		**14**	**14**
2.1	Построение поля C. Числовые поля. Поле Q.		4	
2.2	Алгебраическая форма комплексного числа. Сопряжённые комплексные числа. Действия над комплексными числами в алгебраической форме.		2	4
2.3	Решение квадратных уравнений. Геометрическая интерпретация комплексных чисел. Тригонометрическая форма комплексного числа.		6	4
2.4	Действия над комплексными числами в тригонометрической форме. Двучленные уравнения.		2	2
	Контрольная работа (2 ч.)			2
3	**Теория групп (30 ч.)**		**16**	**14**

3.1	Группы. Порядок элемента группы. Циклические группы.		4	2
3.2	Теорема Кэли. Разложение группы по подгруппе. Смежные классы, индекс подгруппы.		4	4
3.3	Теорема Лагранжа. Следствия из неё.		2	4
3.4	Нормальная подгруппа. Факторгруппа. Критерий нормальной подгруппы.		4	2
3.5	Ядро гомоморфизма групп. Теорема о гомоморфизмах групп.		2	2
4	**Идеалы кольца (12 ч.)**		**6**	**6**
4.1	Идеалы кольца. Операции над идеалами.		2	2
4.2	Кольца главных идеалов. Фактор-кольца.		2	2
4.3	Гомоморфизмы и изоморфизмы колец.		2	2

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

РАЗДЕЛ 1
Алгебры

1.1. Алгебраическая операция

Пусть X – непустое множество. Произвольное отображение множества X^2 в X называется *(бинарной) алгебраической операцией*, заданной на множестве X.

Иными словами, на множестве X задана алгебраическая операция, если каждой упорядоченной паре (x, y) элементов этого множества поставлен в соответствие определённый элемент z множества X. Этот элемент z называют *композицией элементов* x и y.

Сложение и умножение чисел – алгебраические операции, заданные на множестве всех комплексных чисел. Деление – алгебраическая операция на множестве всех отличных от нуля комплексных чисел. Умножение преобразований – алгебраическая операция на множестве всех преобразований произвольного непустого множества.

Обозначим символом $\circ$ алгебраическую операцию, заданную на множестве X, и символом $x \circ y$ – композицию элементов x и y. Пусть n – такой элемент множества X, что для любого x из X $n \circ x = x \circ n = x$. Тогда n называют *нейтральным относительно операции* $\circ$ *элементом.*

Теорема 1.1.1. Относительно любой алгебраической операции существует не более одного нейтрального элемента.

Доказательство. Пусть m и n – нейтральные относительно операции $\circ$ элементы. Тогда $m \circ n = n$, ибо m – нейтральный элемент, $m \circ n = m$, ибо n - нейтральный элемент. Поэтому $m = n$. □

Алгебраическую операцию $\circ$ называют *ассоциативной*, если для любых элементов x, y, z множества X $(x \circ y) \circ z = x \circ (y \circ z)$.

Сложение чисел, их умножение, умножение преобразований – ассоциативные алгебраические операции. Деление отличных от нуля чисел – неассоциативная алгебраическая операция.

Пусть $\circ$ – алгебраическая операция, заданная на множестве X; $x_1, x_2, \ldots, x_n$ – конечная последовательность элементов этого множества. Индуктивно определяется композиция $x_n \circ \cdots \circ x_2 \circ x_1$: $x_2 \circ x_1$ уже определена; если $i < n$ и композиция

$$x_i \circ \cdots \circ x_2 \circ x_1$$

уже определена, положим

$$x_{i+1} \circ x_i \circ \cdots \circ x_2 \circ x_1 = x_{i+1} \circ (x_i \circ \cdots \circ x_2 \circ x_1).$$

Если операция $\circ$ ассоциативна, то для любого натурального числа i, удовлетворяющего неравенствам $1 \leq i < n$,

$$(x_n \circ \cdots \circ x_{i+1}) \circ (x_i \circ \cdots \circ x_1) = x_n \circ \cdots \circ x_{i+1} \circ x_i \circ \cdots \circ x_1.$$

Пусть $\circ$ – алгебраическая операция, заданная на множестве X, n – нейтральный относительно этой операции элемент, $x \in X$. Если в множестве X есть такой элемент y, что $x \circ y = y \circ x = n$, то y называют *симметричным элементу x*.

Если элемент y симметричен элементу x, то, очевидно, и x симметричен y, т. е. x и y симметричны друг другу.

Теорема 1.1.2. Пусть на множестве X задана ассоциативная алгебраическая операция $\circ$ с нейтральным элементом n. Тогда для каждого элемента множества X в этом множестве существует не более одного симметричного.

Доказательство. Пусть x, y, z – элементы множества X, причём y и z симметричны x. Тогда $y \circ x \circ z = (y \circ x) \circ z = n \circ z = z$. С другой стороны, $y \circ x \circ z = y \circ (x \circ z) = y \circ n = y$. Следовательно, $z = y$. □

Операцию $\circ$ называют *коммутативной*, если для любых элементов x и y множества X $x \circ y = y \circ x$.

Если операция $\circ$ ассоциативна и коммутативна, то в композиции

$$x_1 \circ x_2 \circ \cdots \circ x_n$$

можно произвольным образом группировать элементы и менять их порядок.

Например,

$$x_1 \circ (x_2 \circ x_3) \circ x_4 = (x_1 \circ x_4) \circ (x_2 \circ x_3).$$

Часто бывает удобно и естественно называть алгебраическую операцию умножением или сложением (умножение и сложение чисел, умножение преобразований). Если операцию называют *умножением*, то композиция элементов (подмножеств) x и y называют *произведением* и записывают в виде xy. Нейтральный элемент при этом называют *единицей*, а симметричный – *обратным*. Если же алгебраическую операцию называют *сложением*, то композиция элементов x и y (подмножеств A и B) называют *суммой* и обозначают символом $x + y$ $(A + B)$. Нейтральный элемент при этом называют *нулём*, а симметричный – *противоположным*.

1.2. Группа

Определение 1.2.1. ***Полугруппой*** называется непустое множество $\mathbf{P}$ с бинарной алгебраической операцией $\circ$, удовлетворяющей следующим требованиям:

1) операция определена на $\mathbf{P}$, т.е. $a \circ b \in \mathbf{P}$ для всех $a, b \in \mathbf{P}$;

2) операция ассоциативна, т.е. $a \circ (b \circ c) = (a \circ b) \circ c$ для любых $a, b, c \in \mathbf{P}$.

Теорема 1.2.1. В полугруппе может быть не более одного нейтрального элемента. Если в полугруппе имеется нейтральный элемент, то каждый элемент обладает не более, чем одним симметричным.

В математике, в основном, используются две формы записи операции: аддитивная и мультипликативная. При аддитивной записи операцию называют сложением и вместо $\circ$ пишут $+$. Элемент $a+b$ называют суммой элементов a и b. Нейтральный элемент называют нулевым, а симметричный – противоположным.

При мультипликативной записи операцию называют умножением, а знак $\circ$ опускают. Элемент ab называют произведением элементов a и b. Вместо нейтрального элемента говорят о единичном, а вместо симметричного — об обратном.

В дальнейшем будем использовать мультипликативную запись, а при необходимости обращаться к аддитивной.

Пусть $a_1, a_2, \ldots, a_n$ — упорядоченная последовательность элементов из полугруппы $\mathbf{P}$. Не меняя порядка, мы можем многими разными способами составлять произведения длины n. Для $n = 3$ и 4 можно составить следующие произведения

$n = 3:$ $\quad (a_1a_2)a_3,\ a_1(a_2a_3)$

$n = 4:$ $\quad ((a_1a_2)a_3)a_4,\ (a_1(a_2a_3)a_4),\ a_1((a_2a_3)a_4),\ a_1(a_2(a_3a_4)),\ (a_1a_2)(a_3a_4).$

Поскольку операция ассоциативна, то при $n = 3$ имеем равенство $(a_1a_2)a_3 = a_1(a_2a_3)$. Для $n = 4$, используя ассоциативность, легко проверить, что все пять произведений совпадают. Далее, используя индукцию, получаем следующую теорему.

Теорема 1.2.2. Если алгебраическая операция (умножение) на множестве $\mathbf{P}$ ассоциативна, то результат ее последовательного применения к n элементам не зависит от расстановки скобок.

Эта теорема позволяет в полугруппах использовать знак кратного умножения без расстановки скобок:

$a_1a_2 = \prod\limits_{i=1}^{2} a_i$; $a_1a_2a_3 = \prod\limits_{i=1}^{3} a_i$; $a_1a_2\dots a_n = \prod\limits_{i=1}^{n} a_i$.

В частности, при $a_1 = a_2 = \dots = a_n = a$ произведение $aa\dots a$ обозначают a^n, называя его $n-$ степенью элемента a.

Следствие 1.2.1. Если $\mathbf{P}$ — полугруппа и $a \in \mathbf{P}$, то $a^n a^m = a^{n+m}, (a^n)^m = a^{nm}$ для любых натуральных n и m.

Для полугруппы с аддитивной записью вместо произведения $\prod\limits_{i=1}^{n} a_i$ надо рассматривать сумму $\sum\limits_{i=1}^{n} a_i = a_1+a_2+\dots+a_n$, а вместо степени a^n кратное $na = a+a+\dots+a$. Следствие 1.2.1 в аддитивной записи примет вид

$$na + ma = (n+m)a, m(na) = (mn)a,\ m, n \in \mathbb{N}.$$

Определение 1.2.2. ***Группой*** называется непустое множество G с бинарной алгебраической операцией $\circ$, удовлетворяющей следующим требованиям:

1) операция $\circ$ определена;

2) операция $\circ$ ассоциативна;

3) в G существует нейтральный элемент относительно операции $\circ$;

4) для каждого элемента множества G в этом множестве G существует симметричный элемент.

Если в качестве операции $\circ$ взято умножение, то более кратко, полугруппа с единицей, в которой каждый элемент обладает обратным, называется группой.

Когда говорят, что G – группа, то всегда имеют в виду определённую алгебраическую операцию, относительно которой множество G является группой. На том же множестве G могут быть заданы и другие алгебраические операции, и относительно каждой из них G может быть, а может и не быть группой. Например, множество всех целых чисел является группой относительно сложения, но не является группой относительно умножения. Алгебраическая операция, относительно которой множество G – группа, называется *групповой операцией*. Естественно называть групповую операцию умножением или сложением, ибо ей присущи многие формальные свойства умножения и сложения чисел. Группу, в которой операция – *умножение*, называют *мультипликативной*. Если же групповая операция – *сложение*, то группу называют *аддитивной*.

1. Группу всех подстановок множества X обозначают символом $Sym\ X$ и называют *симметрической группой множества* X. Если X – конечное множество n элементов, то для $Sym\ X$ употребляют ещё обозначение S_n.

2. Множество всех чётных подстановок n чисел также является группой относительно умножения подстановок. Его обозначают символом A_n и называют *знакопеременной группой*.

3. Множество всех отличных от нуля действительных чисел – группа относительно умножения. Это *мультипликативная группа действительных чисел*.

4. Множество всех действительных чисел является группой и относительно сложения. Это *аддитивная группа действительных чисел*.

5. Множество всех вращений плоскости вокруг неподвижной точки – группа относительно умножения преобразований. Произведение поворотов на угол α и на угол β есть поворот на угол $\alpha + \beta$. Единицей служит поворот на нулевой угол. Для поворота на угол α обратным является поворот на угол, дополняющий α до целого кратного числа 2π.

Отметим простые свойства групп. Когда мы говорим «свойства группы G», то имеем в виду свойства групповой операции. Само название этой операции (сложе-

ние, умножение и пр.), как и соответствующие обозначения, являются просто кодом, языком, на котором мы эти свойства излагаем. И, конечно, утверждение, полученное на одном языке, имеют аналог на любом другом.

Ниже мы считаем, что G – мультипликативная группа.

Свойства группы.

1. В группе лишь одна единица и для каждого элемента есть лишь один обратный элемент.

Это свойство непосредственно следует из определения группы и теорем (1.1.1) и (1.1.2).

Будем обозначать единицу группы буквой e, а элемент, обратный элементу g, – символом g^{-1}.

2. *Для любых элементов g и h группы G каждое из уравнений*

$$gx = h \tag{1.2.1}$$

и

$$yg = h \tag{1.2.2}$$

имеет в G единственное решение:

$$x = g^{-1}h, \qquad y = hg^{-1}. \tag{1.2.3}$$

Доказательство. Если x определяется равенством (1.2.3), то

$$gx = g(g^{-1}h) = (gg^{-1})h = eh = h,$$

поэтому x – решение уравнения (1.2.1). Если, с другой стороны, элемент f группы G является решением уравнения (1.2.1), то

$$gf = h \Longrightarrow g^{-1}(gf) = g^{-1}h \Longrightarrow f = g^{-1}h,$$

поэтому f – единственное решение этого уравнения. Доказательство существования и единственности решения уравнения (1.2.2) оставлено читателю. □

3. *Для любых элементов g и h группы G*

$$(gh)^{-1} = h^{-1}g^{-1}.$$

Доказательство. $(gh)(h^{-1}g^{-1}) = g(hh^{-1})g^{-1} = (ge)g^{-1} = gg^{-1} = e.$
Аналогично

$$(h^{-1}g^{-1})(gh) = e.$$

□

4. *В мультипликативной группе для любого элемента $a \in \mathbf{G}$ положим $a^0 = e$ и $a^{-n} = (a^n)^{-1}$, где $n \in \mathbb{N}$. Тем самым мы определили степени элемента группы с произвольным целым показателем.*

5. *Если $\mathbf{G}$ — группа и $a \in \mathbf{G}$, то $a^s a^t = a^{s+t}$ и $(a^s)^t = a^{st}$ для любых целых s и t.*

Если групповая операция коммутативна, то группу называют *коммутативной* или *абелевой*.

Всюду ниже, если не оговорено иное, мы называем групповую операцию *умножением*.

Определение 1.2.3. Пусть G – группа. Непустое подмножество H множества G называется ***подгруппой группы*** G, если оно *замкнуто относительно умножения* и *обращения (взятия обратного элемента)*, т.е. удовлетворяет следующим двум условиям:

1) для любых элементов a и b множества H $\quad ab \in H$;

2) для любого элемента a множества H $\quad a^{-1} \in H$.

Из этих условий вытекает, очевидно, что $e \in H$, где e — единица группы G. Поэтому можно сказать, что непустое подмножество группы G называется ***подгруппой*** группы G, если оно является группой относительно групповой операции, определённой в G. В дальнейшем $H \leqslant G$ обозначает, что H — подгруппа группы G.

Теорема 1.2.3. Непустое подмножество H группы G тогда и только тогда является подгруппой, когда для любых элементов g и h множества H следует, что $gh^{-1} \in H$.

Доказательство. Необходимость условия теоремы очевидна. Докажем достаточность. Итак, пусть H удовлетворяет условию теоремы и $h \in H$. Тогда

$$e = hh^{-1} \in H, \qquad h^{-1} = eh^{-1} \in H.$$

Если ещё $g \in H$, то

$$gh = g(h^{-1})^{-1} \in H.$$

Доказано, что $H \leqslant G$. □

1. Для любой группы G сама она и множество E, содержащее лишь единицу e этой группы, являются подгруппами.

2. Мультипликативная группа положительных чисел – подгруппа мультипликативной группы всех отличных от нуля чисел.

1.3. Гомоморфизмы и изоморфизмы групп

Определение 1.3.1. Пусть G_1 и G_2 – мультипликативные группы, а $f : G_1 \to G_2$ – такое отображение, при котором для любых элементов a и b группы G_1

$$f(ab) = f(a)f(b). \tag{1.3.4}$$

Тогда f называется ***гомоморфным отображением*** или ***гомоморфизмом*** группы G_1 в группу G_2. Если гомоморфизм f биективен, то он называется ***изоморфизмом*** групп G_1 и G_2. Если существует изоморфизм групп G_1 и G_2, то пишут $G_1 \cong G_2$ и говорят, что группа G_1 *изоморфна группе* G_2. Гомоморфизм группы в

себя называется её ***эндоморфизмом***. Изоморфизм группы на себя называется ***автоморфизмом***.

Теорема 1.3.1. Совокупность $\mathrm{Aut}G$ всех автоморфизмов группы G является группой относительно последовательного выполнения автоморфизмов: $(\varphi\psi)(g) = \varphi(\psi(g))$ для любых $\varphi, \psi \in \mathrm{Aut}G$ и всех $g \in G$.

Определение 1.3.2. Если M — подмножество G_1, то $f(M)$ называется ***образом*** M ***при гомоморфизме*** f, а $f(G_1)$ называется ***образом гомоморфизма*** φ и обозначается через Imf.

Определение 1.3.3. ***Ядром гомоморфизма*** f называется множество $Kerf = \{x \in G_1 | f(x) = \varepsilon\}$, где ε – нейтральный элемент группы G_2. Другими словами, в ядре собраны все элементы x группы G_1, переходящие при отображении f в нейтральный элемент группы G_2.

Если G_1 и G_2 — аддитивные группы, то (1.3.4) принимает вид:

$$f(x+y) = f(x) + f(y).$$

Если G_1 — мультипликативная группа, а G_2 — аддитивная, то (1.3.4) выглядит так:

$$f(xy) = f(x) + f(y).$$

В дальнейшем мы будем предпочитать мультипликативную запись.

Лемма 1.3.1. (**Свойства гомоморфизма**) Пусть $f : G_1 \to G_2$ — гомоморфизм мультипликативной группы G_1 в мультипликативную группу G_2. Тогда справедливы следующие утверждения:

1) единица e группы G_1 переходит в единицу ε группы G_2, т.е.

$$f(e) = \varepsilon;$$

2) обратный элемент переходит в обратный, т.е

$$f(a^{-1}) = f(a)^{-1}$$

для всех $a \in G_1$;

3) образ гомоморфизма является подгруппой группы G_2, т.е.

$$Imf \leq G_2;$$

4) ядро гомоморфизма является подгруппой в G_1, т.е.

$$Kerf \leq G_1.$$

Доказательство. 1. Пусть $a \in G$. Тогда

$$f(a)f(e) = f(ae) = f(a). \tag{1.3.5}$$

Так как в группе G_2 решением уравнения $f(a)x = f(a)$ является только единица, то из (1.3.5) следует, что $f(e)$ – единица группы G_2.

2.

$$f(a^{-1})f(a) = f(a^{-1}a) = f(e), \tag{1.3.6}$$

$$f(a)f(a^{-1}) = f(e). \tag{1.3.7}$$

Согласно свойству 1, $f(e) = \varepsilon$ – единица группы G_2, поэтому равенства (1.3.6) и (1.3.7) указывают на то, что $f(a^{-1})$ – элемент, обратный элементу $f(a)$. □

Определение 1.3.4. Гомоморфизм $f : G_1 \to G_2$ называется ***мономорфизмом***, если $Kerf = \{e\}$. Легко говорить, что гомоморфизм f является мономорфизмом тогда и только тогда, когда отображение f — инъекция.

Если $Imf = G_2$, то гомоморфизм $f : G_1 \to G_2$ называется ***эпиморфизмом***. Ясно, что в этом случае f — сюръекция.

Пример 1.3.1. 1. Тождественное отображение e_G является изоморфизмом, т.е. $G \simeq G$ для любой группы G.

2. Отображение произвольной группы G в себя, ставящее в соответствие каждому элементу этой группы её единицу, является эндоморфизмом группы G.

3. Симметрическая группа S_n гомоморфно отображается на мультипликативную группу $\mathbb{Z}^* = \mathbb{Z}\backslash\{0\}$, если каждой чётной подстановке поставить в соответствие число 1, а нечётной -1.

4. Если G – группа, а H – её подгруппа, то отображение $i : G \to H$ — гомоморфизм групп.

5. Если $f : G_1 \to G_2$ – изоморфизм, то и

$$f^{-1} : G_2 \to G_1 \tag{1.3.8}$$

является изоморфизмом.

6. Если $f : G_1 \to G_2$ и $g : G_2 \to G_3$ — гомоморфизмы групп, то и $gf : G_1 \to G_3$ — гомоморфизм. Если при этом f и g являются изоморфизмами, то и gf – изоморфизм.

Доказательство. 5. Для биективного отображения f существует обратное биективное отображение (1.3.8). Покажем, что (1.3.8) – изоморфизм групп. Нужно доказать, что для любых a и b из G_2

$$f^{-1}(ab) = f^{-1}(a)f^{-1}(b). \tag{1.3.9}$$

Так как f – биекция, то равенство (1.3.9) равносильно равенству

$$f(f^{-1}(ab)) = f(f^{-1}(a)f^{-1}(b)). \tag{1.3.10}$$

Левая часть равенства (1.3.10) равна ab. Правая его часть также равна ab, так как f – изоморфизм. Следовательно, равентсво (1.3.10) верно. Вместе с ним верно и равентсво (1.3.9).

Таким образом, если $G \cong H$, то и $H \cong G$, так что можно просто говорить, что *группы G и H изоморфны.*

6. Для любых элементов a и b группы G_1 справедливо $(gf)(ab) = g(f(ab)) = g(f(a)f(b)) = (gf)(a)(gf)(b)$. Таким образом, доказано, что gf – гомоморфизм групп. Кроме того, произведение биекций также биективно. □

Таким образом, справедлива следующая

Теорема 1.3.2. Отношение изоморфизма является отношением эквивалентности на множестве всех групп.

Из этой теоремы следует, что множество всех групп разбивается на непересекающиеся классы изоморфных групп. Две изоморфные группы могут различаться лишь природой своих элементов, а не алгебраическими свойствами. Грубо говоря, в этих группах «одинаковы операции», нужно только каждый элемент одной из групп заменить его образом при изоморфизме на другую группу. Те свойства, которые могут быть выражены в терминах групповой операции, у изоморфных групп одинаковы и, если нас интересуют именно эти свойства, мы можем изоморфные группы не различать.

1.4. Кольцо

В алгебре часто изучают множества с несколькими, например с двумя, алгебраическими операциями. Обычно между этими операциями существуют определённые связи. В этом параграфе мы вводим одно важное понятие алгебры – понятие кольца.

Определение 1.4.1. Непустое множество K с двумя бинарными алгебраическими операциями (*сложение* и *умножение*) называется ***кольцом***, если выполняются следующие условия:

1) относительно сложения K является абелевой группой;

2) умножение определено на K и ассоциативно;

3) умножение дистрибутивно относительно сложения, т. е. $k(l+m) = kl + km$ и $(l+m)k = lk + mk$ для любых элементов k, l и m из множества K.

По определению кольца относительно сложения множество всех его элементов является группой. Эта группа называется *аддитивной группой кольца*.

1. Множество всех целых, всех рациональных, всех действительных чисел (относительно обычных сложения и умножения чисел) являются кольцами.

2. Множество всех полиномов (многочленов) от одной переменной с действительными коэффициентами – кольцо.

3. Обозначим буквой F множество всех действительных функций одной переменной. Сумму и произведение функций f и g определим для каждого действительного числа x формулам

$$(f+g)(x) = f(x) + g(x), \quad fg(x) = f(x)g(x),$$

т. е. так, как это делается обычно в математическом анализе (здесь вводится новое умножение функций fg, отличное от произведения отображений f и g!). Легко убедится в том, что множество F относительно так определённых сложения и умножения является кольцом. Нулём этого кольца служит функция $0(x) \equiv 0$.

Кольцо называется *коммутативным*, если в нём умножение коммутативно.

Все упомянутые выше кольца коммутативны, примеры некоммутативных колец возникнут ниже.

Рассмотрим **простейшие свойства колец**.

1. Так как элементы кольца составляют абелеву группу относительно сложения, то

1) *в кольце лишь один нуль 0;*

2) *для любого элемента k кольца K в K есть единственный противоположный элемент $-k$;*

3) *для любых элементов k и l кольца K уравнение*

$$k + x = l \tag{1.4.11}$$

имеем в K единственное решение $x = -k + l$.

Решение уравнения (1.4.11) называется *разностью* $l - k$. Таким образом в кольце определена операция *вычитания.*

Непосредственно из определения разности следует, что *для любого элемента k кольца* $k - k = 0$.

2. *Умножение дистрибутивно относительно вычитания, т. е. для любых элементов k, l и m кольца*

$$k(l - m) = kl - km, \qquad (l - m)k = lk - mk.$$

Доказательство. $l = (l - m) + m \Longrightarrow kl = k(l - m) + km \Longrightarrow kl - km = k(l - m)$. Первое из нужных равенств доказано, второе получается аналогично. □

3. $k0 = 0k = 0$ *для любого элемента $k \in K$.*

Доказательство. Так как $k - k = 0$, то $k0 = k(k - k) = k^2 - k^2 = 0$. Второе равенство доказывается аналогично. □

4. *В кольце произведение отличных от нуля элементов может быть равным нулю.*

Пример 1.4.1. В кольце F всех действительных функций одной переменной рассмотрим две функции f и g, определённые условиями:

$$f(x) = \begin{cases} x, & x \leqslant 0; \\ 0, & x > 0, \end{cases} \qquad g(x) = \begin{cases} 0, & x \leqslant 0; \\ x, & x > 0. \end{cases} \tag{1.4.12}$$

Очевидно, $f \neq g$, $\quad g \neq 0$, но $fg = 0$ ($f(x)g(x) = 0$ для любого x).

Если в кольце $kl = 0$, а k и l отличны от нуля, то k и l называются ***делителями нуля***.

Пример 1.4.2. В кольце F функции f и g (1.4.12) – делители нуля. В кольце целых чисел нет делителей нуля.

5. *Пусть k – отличный от нуля элемент кольца, не являющийся делителем нуля. Если*

$$kl = km, \tag{1.4.13}$$

или

$$lk = mk, \tag{1.4.14}$$

то $l = m$.

Доказательство. Из (1.4.13) следует $kl - km = 0$, $k(l - m) = 0$, $l - m = 0$, $l = m$. Аналогично для равенства (1.4.14). □

6. *Для любых элементов k и l кольца*

$$(-k)l = k(-l) = -(kl).$$

Доказательство. $kl + (-k)l = (k + (-k))l = 0 \cdot l = 0$. Поэтому $(-k)l = -(kl)$. Второе равенство получается аналогично. □

Существуют кольца с единицей и без неё. Например, в кольце всех целых чисел есть единица, а в кольце всех целых чисел, делящихся на 2, единицы нет. *Однако кольцо не может иметь более одной единицы* (см. теорему (1.1.1)).

Ясно, что существует такое кольцо, в котором содержится лишь один элемент. Например, множество $\{0\}$, содержащее лишь число 0, является кольцом относительно сложения и умножения чисел. *Если K – произвольное одноэлементное кольцо, а — его элемент, то a является нулём этого кольца.*

7. *Если кольцо содержит более одного элемента, то в нём нуль не является единицей.*

Доказательство. Пусть a – произвольный элемент, 1 – единица кольца K и $0 = 1$. Тогда $0 \cdot a = 1 \cdot a$. Последнее невозможно для любого a, так как в кольце K более одного элемента. □

Единственное исключение, когда нуль и единица кольца совпадают, имеет место, если в этом кольце только один элемент.

Определение 1.4.2. Пусть K – кольцо с единицей 1. Если для элемента k кольца K в K существует обратный элемент, то k называется ***обратимым элементом кольца*** K.

1 сама себе обратна, поэтому 1 – обратимый элемент; 0 необратим, если только 0 не есть 1. Если элемент k обратим, то обратим и элемент k^{-1} – обратным для него является k.

8. *В кольце K с единицей 1 множество K^* всех обратимых элементов является группой относительно умножения.*

Доказательство. $1 \in K^*$. Если $k \in K^*$, то и k^{-1} обратим, поэтому

$$k^{-1} \in K^*.$$

Наконец, если $k \in K^*$ и $l \in K^*$, то рассмотрим произведение $l^{-1}k^{-1}$.

$$(kl)(l^{-1}k^{-1}) = k(ll^{-1})k^{-1} = (ke)k^{-1} = kk^{-1} = 1.$$

Точно так же

$$(l^{-1}k^{-1})(kl) = 1,$$

поэтому

$$l^{-1}k^{-1} = (kl)^{-1}, \quad kl \in K^*.$$

□

Группу K^* называют **мультипликативной группой** кольца K.

Пример 1.4.3. Для кольца Z всех целых чисел $Z^* = \{1, -1\}$.

Определение 1.4.3. Пусть K – кольцо. Непустое подмножество L кольца K называется ***подкольцом кольца*** K, если оно является подгруппой аддитивной группы K и замкнуто относительно умножения.

Иными словами, непустое подмножество L кольца K называется ***подкольцом кольца*** K, если оно является кольцом относительно операций кольца K.

Теорема 1.4.1. ***(критерий подкольца)*** Непустое подмножество L кольца K является подкольцом тогда и только тогда, когда $a - b \in L$ и $ab \in L$ для любых элементов a и b множества L.

Пример 1.4.4. $\mathbb{Z}$ подкольцо в $\mathbb{Q}$, $\mathbb{Q}$ подкольцо в $\mathbb{R}$, $2\mathbb{Z}$ *(множество целых чисел, кратных 2)* подкольцо в $\mathbb{Z}$.

1.5. Гомоморфизмы и изоморфизмы колец

Определение 1.5.1. Пусть K и L – кольца, $f : K \to L$ — отображение, при котором для любых элементов a и b кольца K

$$f(a+b) = f(a) + f(b), \qquad f(ab) = f(a)f(b). \tag{1.5.15}$$

Тогда f называется ***гомоморфным отображением*** или ***гомоморфизмом*** кольца K в кольцо L. Если гомоморфизм f биективен, то он называется ***изоморфизмом*** колец K и L. Гомоморфизм кольца в себя называется его ***эндоморфизмом***. Изоморфизм кольца на себя называется его ***автоморфизмом***.

Если существует изоморфизм колец K и L, то пишут $K \cong L$ и говорят, что *кольцо K изоморфно кольцу L.*

Согласно определению, гомоморфизм кольца K в кольцо L — это гомоморфизм аддитивных групп этих колец, который сохраняет умножение (образ произведения

элементов равен произведению из образов). Поэтому гомоморфизмы колец обладают свойствами, аналогичными изложенным в предыдущем параграфе 1.3 свойствам гомоморфизмов групп. Перечислим без доказательств простейшие свойства гомоморфизмов колец.

1. *$K \simeq K$ для любого кольца K.*

2. *Если $f : K \to L$ – изоморфизм колец, то $f^{-1} : L \to K$ — также изоморфизм. Следовательно, если $K \cong L$, то $L \cong K$.*

3. *Если $f : K \to L$, $g : L \to M$ – гомоморфизмы колец, то и $gf : K \to M$ — также гомоморфизм колец. Если при этом f и g являются изоморфизмами, то и gf — изоморфизм.*

Из этих трёх свойств вытекает

Теорема 1.5.1. Отношение изоморфизма является отношением эквивалентности на множестве всех колец.

4. *Пусть $f : K \to L$ — гомоморфизм. Если 0 – нуль кольца K и a — произвольный элемент кольца K, то $f(0)$ – нуль кольца L и $f(-a) = -f(a)$.*

5. *Пусть K – кольцо с единицей 1. Тогда:*

5.1) *$f(1)$ – единица кольца L;*

5.2) если *a – обратимый элемент кольца K, то $f(a)$ – обратимый элемент кольца L и*

$$f(a^{-1}) = (f(a))^{-1};$$

6. *Если K – коммутативно, то L также коммутативно;*

7. *Если K^* – мультипликативная группа кольца K, то $f(K^*)$ – мультипликативная группа кольца L.*

1.6. Поле.

Определение 1.6.1. Непустое множество P с двумя бинарными алгебраическими операциями (*сложение* и *умножение*) называется ***полем***, если выполняются следующие условия:

1) P — абелева аддитивная группа;

2) $P^* = P \setminus \{0\}$ — абелева мультипликативная группа;

3) умножение дистрибутивно относительно сложения, т. е. $k(l+m) = kl + km$ и $(l+m)k = lk + mk$ для любых элементов k, l и m из множества K.

Утверждение 1.6.1. Всякое поле является кольцом.

Определение 1.6.2. ***Поле*** – это коммутативное кольцо с единицей, в котором все ненулевые элементы обратимы.

Пример 1.6.1. Полями являются множество всех действительных чисел, множество всех рациональных чисел.

Утверждение 1.6.2. В поле нет делителей нуля.

Доказательство. Пусть P – поле, p и q – делители нуля в поле P, т.е. $p \neq 0$, $q \neq 0$ и $pq = 0$. Умножая обе части последнего равенства на элемент p^{-1}, получаем

$$p^{-1}(pq) = p^{-1} \cdot 0, \quad q = p^{-1} \cdot 0.$$

Учитывая соответствующее свойства колец, имеем $q = 0$, противоречие. □

Так как все отличные от нуля элементы поля составляют группу относительно умножения, то

1) *в поле лишь одна единица;*

2) *для любого отличного от нуля элемента поля в этом поле есть единственный обратный элемент;*

3) *для любого элемента a поля P и отличного от нуля элемента b из P уравнение*

$$bx = a \tag{1.6.16}$$

имеет в этом поле единственное решение $x = b^{-1}a$.

(При $a \neq 0$ свойство группы, при $a = 0$ это следует из соответствующего свойства кольца.)

Решение уравнения (1.6.16) обозначается символом $\frac{a}{b}$ и называется ***частным элементов*** a и b. Таким образом, в поле определено *деление* на любой отличный от нуля элемент.

Отмеченные выше свойства полей и аксиомы, входящие в определение поля, указывают на то, что в поле можно производить следующие четыре операции: сложение, умножение, вычитание и деление.

РАЗДЕЛ 2
Поле $\mathbb{C}$

2.1. Построение поля комплексных чисел

Действительные (вещественные числа) играют огромную роль в математике и естествознании, в частности при измерении длин, обьёмов, при узучении движения материальных тел и т. д. Однако есть задачи, для решения которых действительных чисел не хватает. Простейшей из таких задач является решение уравнения $x^2+1=0$. Поставим цель расширить поле R действительных чисел до такого поля, в котором уравнение $x^2+1=0$ уже имело бы решение.

Пусть $\mathbb{C}=\mathbb{R}^2=\{(a,b)|\quad a,b\in\mathbb{R}\}$.

Дадим обозначение сумме и произведению пар из множества $\mathbb{C}$:

$$(a,b)+(c,d)\stackrel{df}{=}(a+c,b+d); \tag{2.1.1}$$

$$(a,b)(c,d)\stackrel{df}{=}(ac-bd,ad+bc); \tag{2.1.2}$$

Теорема 2.1.1. Множество $\mathbb{C}$ пар действительных чисел со сложением и умножением является полем.

Доказательство. Покажем сначала, что множество $\mathbb{C}$ со сложением и умножением — коммутативное кольцо с единицей.

1) на $\mathbb{C}$ определены бинарные операции – сложение и умножение (очевидно);

2) $\mathbb{C}$ — абелева аддитивная группа:

1. Сложение на $\mathbb{C}$ коммутативно и ассоциативно (очевидно);
2. $\exists(0,0)\in\mathbb{C}\ \ \forall(a,b)\in\mathbb{C}\ \ (a,b)+(0,0)=(a,b)$;
3. $\forall(a,b)\in\mathbb{C}\ \ \exists-(a,b)=(-a,-b)\in\mathbb{C}\ \ (a,b)+(-a,-b)=(0,0)$.

3) умножение на $\mathbb{C}$ коммутативно, ассоциативно и дистрибутивно относительно сложения (очевидно).

Таким образом, $\mathbb{C}$ – коммутативное кольцо.
По свойству произвольного кольца $\forall (a,b),(c,d) \in \mathbb{C}$ в $\mathbb{C}$ существует единственное решение уравнения $(c,d)+(x,y)=(a,b)$. Решением является пара $(x,y)=(a,b)+(-(c,d))=(a,b)+(-c,-d)=(a-c,b-d) \in \mathbb{C}$, которая называется разностью пар (a,b) и (c,d) и обозначается $(a,b)-(c,d)$. Значит, на множестве $\mathbb{C}$ определена бинарная операция вычитания:

$$(a,b)-(c,d)=(a-c,b-d). \tag{2.1.3}$$

4) в $\mathbb{C}$ есть единица — пара $(1,0)$, так как $\forall (a,b) \in \mathbb{C}$ $(a,b)(1,0)=(a,b)$.

Покажем теперь, что в кольце $\mathbb{C}$ всякая ненулевая пара (c,d) обратима, т.е. $\forall (c,d) \neq (0,0) \quad \exists (x,y) \in \mathbb{C}$

$$(c,d)(x,y)=(1,0). \tag{2.1.4}$$

$(2.1.4) \Leftrightarrow (cx-dy,cy+dx)=(1,0) \Leftrightarrow \begin{cases} cx-dy=1 \\ dx+cy=0 \end{cases} \Leftrightarrow \begin{cases} x=\frac{c}{c^2+d^2} \\ y=\frac{d}{c^2+d^2} \end{cases}$.
Таким образом, для $\forall (c,d) \neq (0,0)$ обратной будет пара $(\frac{c}{c^2+d^2}, \frac{d}{c^2+d^2})$. □

Свойство поля позволяет утверждать, что $\forall (a,b),(c,d) \in \mathbb{C}, (c,d) \neq (0,0)$ уравнение $(c,d)(x,y)=(a,b)$ имеет в поле $\mathbb{C}$ единственное решение $(x,y)=(a,b)(c,d)^{-1}=(a,b)\cdot\left(\frac{c}{c^2+d^2}, \frac{d}{c^2+d^2}\right)=\left(\frac{ac+bd}{c^2+d^2}, \frac{bc-ad}{c^2+d^2}\right)$, которое называется *частным пар* (a,b) и (c,d) и обозначается $\frac{(a,b)}{(c,d)}$. Значит в поле $\mathbb{C}$ однозначно выполняется деление на любой ненулевой элемент:

$$\frac{(a,b)}{(c,d)}=\left(\frac{ac+bd}{c^2+d^2}, \frac{bc-ad}{c^2+d^2}\right). \tag{2.1.5}$$

Теорема 2.1.2. Поле $\mathbb{C}$ является расширением поля $\mathbb{R}$ действительных чисел и содержит элемент, квадрат которого равен -1.

Доказательство. Пусть $\mathbb{R}'=\{(a,0), a \in \mathbb{R}\}$. Тогда:

1) множество $\mathbb{R}'$ со сложением и умножением, определённым на $\mathbb{C}$, есть подполе поля $\mathbb{C}$ (очевидно).

2) отображение $f : \mathbb{R} \to \mathbb{R}' \big| f(a) = (a, 0)$ – изоморфизм поля $\mathbb{R}$ на поле $\mathbb{R}'$. Действительно, f – биекция множества $\mathbb{R}$ на множество $\mathbb{R}'$, поскольку каждый элемент $(a, 0) \in \mathbb{R}'$ имеет единственный прообраз $a \in \mathbb{R}$. Кроме того, f – гомоморфизм поля $\mathbb{R}$, это значит $(\forall a, b \in \mathbb{R})\ f(a + b) = (a + b, 0) = (a, 0) + (b, 0) = f(a) + f(b)$, $f(ab) = (ab, 0) = (a, 0)(b, 0) = f(a) \cdot f(b)$.

Таким образом, $\mathbb{R} \simeq \mathbb{R}'$. Поэтому когда $\mathbb{R}$ и $\mathbb{R}'$ мы не различаем, а вместо пары $(a, 0)$ будем писать число a. В частности, $(1, 0) = 1$, $(0, 0) = 0$. Значит поле $\mathbb{R}$ является подполем поля $\mathbb{C}$. Заметим, что $(0, 1)^2 = (0, 1)(0, 1) = (-1, 0) = -1$, это значит $(0, 1)$ — один из корней уравнения $x^2 + 1 = 0$. Очевидно, $(0, -1)$ является вторым корнем этого уравнения. Обоначим пару $(0, 1)$ символом i : $\quad i = (0, 1)$. Тогда пара $(0, -1) = -(0, 1)$ будет обозначаться символом $-i$. Значит, $i^2 = (-i)^2 = -1$. $\square$

Теорема 2.1.3. Поле $\mathbb{C}$ является минимальным расширением поля $\mathbb{R}$ действительных чисел, содержащем элемент, квадрат которого равен -1, это значит, что нет отличного от поля $\mathbb{C}$ его подполя, которое было бы расширением поля $\mathbb{R}$ и содержало бы элемент i, $i^2 = -1$.

Кроме построенного поля $\mathbb{C}$ есть и другие минимальные расширения поля $\mathbb{R}$, которые содержат корень уравнения $x^2 + 1 = 0$.

Элементами этих расширений являются не пары действительных чисел, а объекты совсем другой природы, например, векторы на плоскости, матрицы второго порядка.

Однако, можно доказать, что всякое минимальное расширение поля $\mathbb{R}$, содержащее элемент, квадрат которого равен -1, изоморфно полю $\mathbb{C}$. Отсюда следует, что все такие минимальные расширения поля $\mathbb{R}$ изоморфны между собой.

Определение 2.1.1. Всякое минимальное расширение поля $\mathbb{R}$ действительных чисел, содержащее элемент i, квадрат которого равен -1, называется ***полем комплексных чисел.***

Далее под полем комплексных чисел будем подразумевать построенное нами поле $\mathbb{C}$, а его элементы будем называть ***комплексными числами***. Комплексное число i назовём ***мнимой единицей поля*** $\mathbb{C}$.

2.2. Числовые поля. Поле рациональных чисел

Ранее было доказано, что кроме поля комплексных чисел и его подполей никаких других полей, элементами которых являются числа, не существует. Поэтому ***числовым полем*** называют любое подполе поля комплексных чисел.

Теорема 2.2.1. ***(о минимальном числовом поле)*** Поле $\mathbb{Q}$ рациональных чисел является минимальным числовым полем, т.е. содержится в любом числовом поле.

Доказательство. Пусть F – любое числовое поле. Тогда:

1) $0, 1 \in F$;

2) любое натуральное число принадлежит F;

3) любое целое число принадлежит F;

4) любая дробь $\frac{m}{n}, m \in \mathbb{Z}, n \in \mathbb{N}$, принадлежит F. □

2.3. Алгебраическая форма комплексного числа. Сопряжённые комплексные числа. Действия над комплексными числами в алгебраической форме. Решение квадратичных уравнений

Пусть $z = (a, b)$ — произвольное комплексное число. Тогда

$$z = (a, 0) + (0, b) = a + (b, 0)(0, 1) = a + bi$$

– ***алгебраическая форма комплексного числа*** $z = (a, b)$, в которой $a \in \mathbb{R}$ называют ***действительной частью*** z, $b \in \mathbb{R}$ — мнимой частью z и обозначают: $a = Re\ z$ (лат. *realis* — действительный), $b = Im\ z$. Когда $Im\ z = 0$, то z — ***действительное число***; когда же $Im\ z \neq 0$, то z называется **мнимым числом**. Мнимое число z называется ***чисто мнимым***, когда $Re\ z = 0$.

Два комплексных числа в алгебраической форме равны тогда и только тогда, когда равны их действительные и мнимые части:

$$a + bi = c + di \Leftrightarrow a = c \wedge b = d.$$

В частности,

$$a + bi = 0 \Leftrightarrow a = b = 0.$$

Определение 2.3.1. Комплексные числа $z = a + bi$ и $\overline{z} = a - bi$ называются ***сопряжёнными***.

Рассмотрим действия над комплексными числами в алгебраической форме.

Сложение, умножение, вычитание и деление комплексных чисел выполняют по формулам (2.1.1), (2.1.2), (2.1.3),(2.1.5) соответственно.

$$(a + bi) + (c + di) = (a + c) + (b + d)i;$$

$$(a + bi) - (c + di) = (a - c) + (b - d)i;$$

$$(a+bi)(c+di) = (ac-bd)+(ad+bc)i;$$

$$\frac{a+bi}{c+di} = \frac{ac+bd}{c^2+d^2} + \frac{bc-ad}{c^2+d^2}i, \quad c+di \neq 0.$$

Отметим, что формулы умножения и деления нет необходимости запоминать. Первую из них мы получим по правилу умножения суммы на сумму, вторую — умножив числитель и знаменатель на число $c-di$, сопряжённое со знаменателем.

Пример 2.3.1. 1. $(1+3i)(3-2i) = 1\cdot 3+3\cdot 3i-1\cdot 2i-3i\cdot 2i = (3+6)+(9-2)i = 9+7i$.
2.

$$\frac{11+7i}{2-3i} = \frac{(11+7i)(2+3i)}{(2-3i)(2+3i)} = \frac{1+47i}{13} = \frac{1}{13} + \frac{47}{13}i.$$

Отметим, что $i^1 \stackrel{df}{=} i$, $i^2 = -1$, $i^3 = i^2 \cdot i = -i$, $i^4 = 1$. Тогда

$$(\forall k \in \mathbb{Z}) \quad i^{4k} = 1, \; i^{4k+1} = i, \quad i^{4k+2} = -1, \quad i^{4k+3} = -i.$$

Для возведения любого комплексного числа в алгебраической форме в степень с натуральным показателем можно применить формулу бинома Ньютона:

$$(a+b)^n = \sum_{i=0}^{n} C_n^i a^{n-i} b^i,$$

$n \in \mathbb{N}$, $C_n^i = \frac{n!}{i!(n-i)!}$ (число сочетаний из n элементов по i, то есть количество различных i-подмножеств n-множества).

Определение 2.3.2. ***Корнем n-ой степени*** (n – произвольное натуральное число) из комплексного числа z, называется такое комплексное число u, что $u^n = z$. Обозначается $\sqrt[r]{z}$.

Операция нахождения квадратного корня из комплексного числа в алгебраической форме всегда выполняется:

$\sqrt{a+bi} = \pm\left(\sqrt{\frac{\sqrt{a^2+b^2}+a}{2}} + i\sqrt{\frac{\sqrt{a^2+b^2}-a}{2}}\right)$, когда $b > 0$;

$\sqrt{a+bi} = \pm\left(\sqrt{\frac{\sqrt{a^2+b^2}+a}{2}} - i\sqrt{\frac{\sqrt{a^2+b^2}-a}{2}}\right)$, когда $b > 0$;

$\sqrt{a} = \pm\sqrt{-a}i$, $a < 0$ (знак $\sqrt{}$ справа обозначает арифметический квадратный корень).

Извлечение корня более высокой степени из комплексного числа в алгебраической форме в общем случае невозможно.

Пример 2.3.2.

1. $\sqrt{-5-12i} = \pm\left(\sqrt{\frac{\sqrt{169}-5}{2}} - i\sqrt{\frac{\sqrt{169}+5}{2}}\right) = \pm(2-3i)$.
2. $\sqrt{-4} = \pm\sqrt{4}i = \pm 2i$.

Аналогично, как и в школьном курсе математики, доказывается, что корни квадратичного уравнения $ax^2+bx+c=0$ с комплексными коэффициентами находятся по формуле: $x_{1,2} = \frac{-b\pm\sqrt{b^2-4ac}}{2a}$.

Свойства сопряжённых комплексных чисел.

1. Всякое действительное число сопряжено само с собой: $(\forall a \in \mathbb{R})\ \overline{a} = a$.
2. Сумма и произведение сопряжённых комплексных чисел — числа действительные.
3. $(\forall z_1, z_2 \in \mathbb{C})\ \ \overline{z_1+z_2} = \overline{z_1} + \overline{z_2};\ \ \overline{z_1-z_2} = \overline{z_1} - \overline{z_2}$.
4. $(\forall z_1, z_2 \in \mathbb{C}, z_2 \neq 0)\ \overline{\left(\frac{z_1}{z_2}\right)} = \frac{\overline{z_1}}{\overline{z_2}}$.
5. $(\forall z \in \mathbb{C}, z \neq 0\ \ \forall n \in \mathbb{Z})\ \overline{z^n} = (\overline{z})^n$.

2.4. Геометрическая интерпретация комплексных чисел

Возьмём на плоскости прямоугольную систему координат. Условимся комплексное число $z = a + bi$ показывать точкой (a, b). Этим самым мы задали биекцию множества $\mathbb{C}$ комплексных чисел на множество точек координатной плоскости. Поэтому сама плоскость называется ***комплексной***. Очевидно, что действительные числа показывают точками оси абсцисс, в связи с чем эту ось называют ***действительной осью***. Чисто мнимые числа показывают точками оси ординат. Поэтому ось ординат называют ***мнимой осью***.
Комплексное число 0 показывается началом координат. Сопряжённым комплексным числам z и $\overline{z}$ отвечают точки, симметричные относительно действительной оси, а противоположным числам z и $-z$ – точки, симметричные относительно начала координат. Интерпретация комплексных чисел с помощью точек плоскости довольно простая,но она неудобна для геометрической иллюстрации операции умножения и деления комплексных чисел. Поэтому мы дадим другую геометрическую интерпретацию комплексных чисел. Произвольное комплексное число $z = a + bi$ будем показывать радиус-вектором (a, b) координатной плоскости. Такое представление комплексных чисел задаёт биекцию множества $\mathbb{C}$ на множество радиус-векторов комплексной плоскости.

Вместо выражения «точка(радиус-вектор), которая(-ый) отвечает комплексному числу z» будем говорить просто: «точка z (радиус-вектор $\overline{z}$)».

2.5. Тригонометрическая форма комплексного числа

Рассмотрим произвольное комплексное число $z = a + bi$ и соответствующий ему радиус-вектор $\overline{z}$ (a, b). Длину r радиус-вектора $\overline{z}$ (расстояние от точки z до начала координат) назовём ***модулем комплексного числа*** z и обозначим символом $|z|$, а угол φ между положительной полуосью абцисс и радиус-вектором $\overline{z}$, отличным от

положительной полуоси Ox, – ***аргументом комплексного числа*** z и обозначим $Arg\ z$.

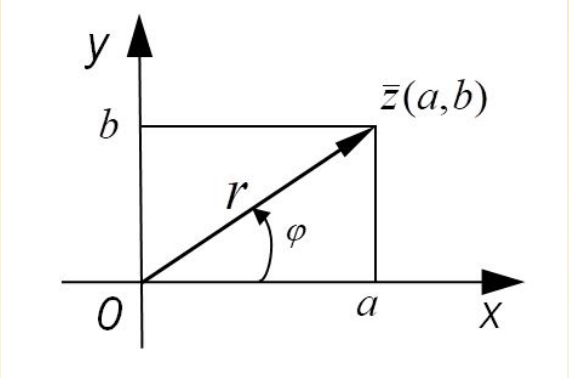


Рис. 2.1:

Аргумент не определён для числа 0, $|0| = 0$. Когда декартовые координаты точки z выражены через полярные координаты (считая, что полюс совпадает с началом координат, а полярная ось – с положительной поуосью Ox), то получаем $a = r\cos\varphi$, $b = \sin\varphi$.

Таким образом, $z = a + bi = r(\cos\varphi + i\sin\varphi)$, $r, \varphi \in R, r > 0$, — ***тригонометрическая форма комплексного числа*** $z = a + bi \neq 0$. Очевидно, $|z| = r = \sqrt{a^2 + b^2}$, а $Arg\ z = \varphi$ определяется из системы:

$$\cos\varphi = \frac{a}{\sqrt{a^2 + b^2}}, \quad \sin\varphi = \frac{b}{\sqrt{a^2 + b^2}}. \tag{2.5.6}$$

И в связи с периодичностью sin и cos имеет бесконечное множество решений, поэтому и $Arg\ z$ определяется неоднозначно. Одно из значений $Arg\ z$, которое берут из

промежутка $[0, 2\pi)$ (наименьшее неотрицательное) или $(-\pi, \pi]$ (наименьшее по абсолютной величине) называют ***главным значением аргумента*** z и обозначают $arg\ z$. Тогда $Arg\ z = arg\ z + 2\pi k, k \in \mathbb{Z}$.

Пусть $a \neq 0$. В этом случае $arg\ z$ является ещё и решением уравнения

$$\operatorname{tg}\varphi = \frac{b}{a}. \tag{2.5.7}$$

Но не всякое решение уравнения (2.5.7) является решением системы (2.5.6). Поэтому при нахождении $arg\ z$ из (2.5.7) необходимо учитывать положение точки z на комплексной плоскости.

Замечание 2.5.1. Иногда тригонометрической формой 0 считают выражение $0(\cos\varphi + i\sin\varphi)$ при любом $\varphi \in \mathbb{R}$.

Пример 2.5.1. Запишем комплексное число $z = 1 - i$ в тригонометрической форме. $a = 1$, $b = -1$:

$$|z| = \sqrt{2}, \quad \operatorname{tg}\varphi = -1. \tag{2.5.8}$$

$\varphi = -\frac{\pi}{4} + \pi k$, $k \in \mathbb{Z}$ – все решения уравнения (2.5.8).

Отсюда, $arg\ z = \frac{7}{4}\pi$ или $-\frac{\pi}{4}$, так как $\frac{7}{4}\pi \in [0, 2\pi)$, $-\frac{\pi}{4} \in (-\pi, \pi]$ и эти числа отвечают расположению точки z на комплексной плоскости. Отметим, что $arg\ z$ можно было найти как решение системы $\cos\varphi = \frac{\sqrt{2}}{2}$, $\sin\varphi = -\frac{\sqrt{2}}{2}$.
Таким образом, $z = \sqrt{2}(\cos\frac{7}{4}\pi + i\sin\frac{7}{4}\pi)$ – тригонометрическая форма числа $1 - i$.

Утверждение 2.5.1. Два отличных от нуля комплексных числа равны тогда и только тогда, когда равны их модули, а значения аргументов отличаются на $2\pi k$, $k \in \mathbb{Z}$.

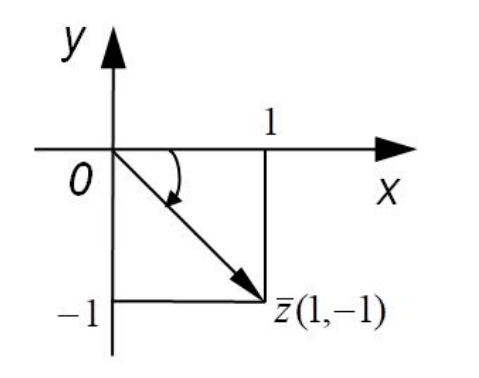


Рис. 2.2:

2.6. Действия над комплексными числами в тригонометрической форме. Двучленные уравнения

Тригонометрическая форма комплексных чисел очень удобна при их делении и умножении. Действительно, пусть даны два числа: $z_1 = r_1(\cos\varphi_1 + i\sin\varphi_1)$, $z_2 = r_2(\cos\varphi_2 + i\sin\varphi_2)$. Тогда

$$z_1 z_2 = r_1 r_2(\cos\varphi_1\cos\varphi_2 + i\cos\varphi_1\sin\varphi_2 + i\sin\varphi_1\cos\varphi_2 - \sin\varphi_1\sin\varphi_2) =$$

$$= r_1 r_2(\cos(\varphi_1+\varphi_2) + i\sin(\varphi_1+\varphi_2))-$$

тригонометрическая форма $z_1 z_2$, $|z_1 z_2| = r_1 r_2 = |z_1||z_2|$, $Arg\ (z_1 z_2) = \varphi_1 + \varphi_2 = Arg\ z_1 + Arg\ z_2$ (равенство нужно понимать с точностью до слагаемого $2\pi k, k \in Z$). Таким образом, модуль произведения двух комплексных чисел равен произведению их модулей, а аргумент произведения двух комплексных чисел равен сумме их аргументов. Эти правила распространяются на любое конечное число множителей: $|z_1 z_2 \dots z_n| = Arg\ z_1 + Arg\ z_2 + \dots + Arg\ z_n$.

Пусть теперь $z_2 \neq 0$. Разделим z_1 на z_2:

$$\frac{z_1}{z_2} = \frac{r_1(\cos\varphi_1 + i\sin\varphi_1)(\cos\varphi_2 + i\sin\varphi_2)}{r_2(\cos^2\varphi_2 - i^2\sin^2\varphi_2)} = \frac{r_1}{r_2}(\cos\varphi_1 + i\sin\varphi_1)(\cos(-\varphi_2) + i\sin(-\varphi_2)) =$$

$$= \frac{r_1}{r_2}(\cos(\varphi_1 - \varphi_2) + i\sin(\varphi_1 - \varphi_2)).$$

Отсюда $\left|\frac{z_1}{z_2}\right| = \frac{r_1}{r_2} = \frac{|z_1|}{|z_2|}$, $Arg\left(\frac{z_1}{z_2}\right) = \varphi_1 - \varphi_2 = Arg\ z_1 - Arg\ z_2$. Таким образом модуль частного двух комплексных чисел равен частному их модулей, а аргумент частного двух комплексных чисел равен разности их аргументов (с точностью до слагаемого $2\pi k, k \in \mathbb{Z}$).

Возведение в степень с целым показателем так же, как и при умножении и делении, удобно выполнять, исходя из тригонометрической формы комплексного числа.

Теорема 2.6.1. ***(формула Муавра)***

$$(\forall n \in \mathbb{Z}) \quad (r(\cos\varphi + i\sin\varphi))^n = r^n(\cos n\varphi + i\sin n\varphi). \tag{2.6.9}$$

Доказательство. Методом математической индукции докажем формулу (2.6.9) для натуральных n.

1) При $n = 1$ формула (2.6.9), очевидно, истинная.

2) Докажем, что из истинности (2.6.9) при $n = k$, где k – любое фиксированное натуральное число, вытекает истинность (2.6.9) при $n = k + 1$. Действительно,

$$(r(\cos\varphi + i\sin\varphi))^{k+1} = (r(\cos\varphi + i\sin\varphi))^k \cdot r(\cos\varphi + i\sin\varphi) =$$

$$= r^n(\cos k\varphi + i\sin k\varphi) \cdot r(\cos\varphi + i\sin\varphi) = r^{k+1}(\cos(k+1)\varphi + i\sin(k+1)\varphi).$$

Значит, по основной форме принципа математической индукции формула (2.6.9) правильная для любого натурального показателя n.

Пусть $n = -m (m \in \mathbb{N})$. Тогда

$$(r(\cos\varphi + i\sin\varphi))^n = \frac{1(\cos 0 + i\sin 0)}{r^m(\cos m\varphi + i\sin m\varphi)} =$$

$$= r^{-m}(\cos(-m\varphi) + i\sin(-m\varphi)) = r^n(\cos n\varphi + i\sin n\varphi).$$

Значит, и при любом целом произвольном показателе n формула справедлива. При $n = 0$ справедливость формулы (2.6.9) очевидна. □

Пример 2.6.1.

$$\frac{\left(\frac{-2-i}{1-2i}\right)^{65} - 31i}{(1-\sqrt{3}i)^5(\cos\frac{\pi}{6} - i\sin\frac{\pi}{6})^{40}} = \frac{\left(\frac{-i(1-2i)}{1-2i}\right)^{65} - 31i}{\left(2(\cos\frac{4\pi}{3} + i\sin\frac{4\pi}{3})\right)^5\left(\cos\left(-\frac{\pi}{6}\right) + i\sin\left(-\frac{\pi}{6}\right)\right)^{40}} =$$

$$= \frac{(-i)^{65} - 31i}{2^5(\cos\frac{20\pi}{3} + i\sin\frac{20\pi}{3})\left(\cos\left(-\frac{20\pi}{3}\right) + i\sin\left(-\frac{20\pi}{3}\right)\right)} = -i.$$

С алгебраической точки зрения поле $\mathbb{C}$ имеет существенное преимущество в сравнении с полем $\mathbb{R}$: из любого комплексного числа z можно извлечь корни любой степени n. Действительно, когда $z = 0$, то $\sqrt[n]{z} = 0$, так как 0 — единственное число, n-ая степень которого равна 0.

Вопрос извлечения корня любой степени из произвольного комплексного числа $z \neq 0$ полностью решается только при использовании тригонометрической формы z.

Теорема 2.6.2. Существует ровно n различных корней n-й степени $(n \in \mathbb{N})$ из произвольного числа $z = r(\cos\varphi + i\sin\varphi)$:

$$\sqrt[n]{r(\cos\varphi + i\sin\varphi)} = \sqrt[n]{r}\left(\cos\frac{\varphi + 2\pi k}{n} + i\sin\frac{\varphi + 2\pi k}{n}\right), \quad k = \overline{0, n-1}. \qquad (2.6.10)$$

($\sqrt[n]{r}$ обозначает арифметический корень n-й степени из положительного числа r).

Доказательство. Будем искать $\sqrt[n]{z}$ в тригонометрической форме: $\rho(\cos\psi + i\sin\psi)$. Тогда $(\rho(\cos\psi + i\sin\psi))^n = r(\cos\varphi + i\sin\varphi)$. Применив формулу Муавра, получим:

$$\rho^n(\cos n\psi + i\sin n\psi) = r(\cos\varphi + i\sin\varphi).$$

Отсюда $\rho^n = r$, $n\psi = \varphi + 2\pi k$, k – любое целое число. Значит, $\rho = \sqrt[n]{r}$, $\psi = \frac{\varphi+2\pi k}{n}$, где $\sqrt[n]{r}$ – арифметический корень n-й степени из r, так как $\rho > 0$.

Таким образом,

$$\sqrt[n]{r(\cos\varphi + i\sin\varphi)} = \sqrt[n]{r}\left(\cos\frac{\varphi+2\pi k}{n} + i\sin\frac{\varphi+2\pi k}{n}\right),$$

$k \in \mathbb{Z}$. Покажем, что количество различных корней равно n. Действительно, при $k = \overline{0, n-1}$ получим n различных корней, так как разность любых двух корней не кратна 2π:

$$\frac{\varphi+2\pi l}{n} - \frac{\varphi+2\pi s}{n} = 2\pi\frac{l-s}{n} \neq 2\pi p,$$

$p \in \mathbb{Z}$.

$$0 \leqslant s < l \leqslant n-1, \quad 0 < \frac{l-s}{n} < 1.$$

Если же $k = m$, где m – любое целое число, отличное от $1, 2, \ldots, n-1$, то разделим с остатком m на n: $m = nq + r$, $q, r \in Z$, $0 \leqslant r \leqslant n-1$. Тогда

$$\frac{\varphi+2\pi m}{n} = \frac{\varphi+2\pi(nq+r)}{n} = \frac{\varphi+2\pi r}{n} + 2\pi q,$$

т. е. аргумент при $k = m$ отличается от аргумента при $k = r$ слагаемым, кратным 2π. Значит, при $k = m$ мы получим такой же корень, как и при $k = r$. □

Пример 2.6.2. Найдём $\sqrt[4]{-4}$.

Запишем число -4 в тригонометрической форме: $-4 = 4(\cos\pi + i\sin\pi)$. По формуле (2.6.10):

$$u_k = \sqrt[4]{-4} = \sqrt[4]{4}\left(\cos\frac{\pi+2\pi k}{4} + i\sin\frac{\pi+2\pi k}{4}\right),$$

$k = \overline{0,3}$. Отсюда

$$u_0 = \sqrt{2}\left(\cos\frac{\pi}{4} + i\sin\frac{\pi}{4}\right) = 1+i,$$

$$u_1 = \sqrt{2}\left(\cos\frac{3\pi}{4} + i\sin\frac{3\pi}{4}\right) = -1+i,$$

$$u_2 = \sqrt{2}\left(\cos\frac{5\pi}{4} + i\sin\frac{5\pi}{4}\right) = -1-i,$$

$$u_3 = \sqrt{2}\left(\cos\frac{7\pi}{4} + i\sin\frac{7\pi}{4}\right) = 1-i.$$

Упражнение 2.6.1. Выясните, как расположены на комплексной плоскости все n корней n-й степени из $z \neq 0$.

Утверждение 2.6.1. Если v – какой-нибудь корень n-й степени из комплексного числа $z_1 \neq 0$ и $u_0, u_1, \ldots, u_{n-1}$ – все корни n-й степени из комплексного числа $z_2 \neq 0$, то $vu_0, vu_1, \ldots, vu_{n-1}$ – все корни n-й степени произведения $z_1 z_2$.

Доказательство. Действительно, все числа vu_k, $k = \overline{0,n-1}$, различны, их количество равно n и каждый из них является корнем n-й степени из $z_1 z_2$, поскольку $(vu_k)^n = v^n u_k^n = z_1 z_2$. □

Утверждение 2.6.2. Если $u_0, u_1, \ldots, u_{n-1}$ – все корни n-й степени из комплексного числа $z \neq 0$, то $\overline{u_0}, \overline{u_1}, \ldots, \overline{u_{n-1}}$ – все корни n-й степени из сопряжённого комплексного числа $\overline{z}$.

Докажите самостоятельно.

Рассмотрим частный случай извлечения корня n-й степени из единицы. Тригонометрическая форма числа 1: $1 = 1(\cos 0 + i \sin 0)$. Поэтому по формуле (2.6.10) получатся следующие корни n-й степени из 1: $\varepsilon_k = \cos \frac{2\pi k}{n} + i \sin \frac{2\pi k}{n}$ $(k = \overline{0, n-1})$.

Упражнение 2.6.2. Дайте геометрическую интрепретацию корней n-й степени из 1.

Утверждение 2.6.3. Если υ – какой-нибудь корень n-й степени из комплексного числа $z \neq 0$, то $\upsilon\varepsilon_0, \upsilon\varepsilon_1, \ldots, \upsilon\varepsilon_{n-1}$ – все корни n-й степени из z.

Докажите самостоятельно.

Теорема 2.6.3. Множество всех корней n-й степени из 1 с умножением является абелевой мультипликативной группой.

Докажите самостоятельно.

Отметим, что существует хотя бы один корень n-й степени из 1, а именно $\varepsilon_1 = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}$, при возведении которого в степени $0, 1, \ldots, n-1$ получаем все корни n степени из 1: $\varepsilon_1^k = \cos \frac{2\pi k}{n} + i \sin \frac{2\pi k}{n} = \varepsilon_k$ $(k = \overline{0, n-1})$. Среди корней ε_k могут встретиться и другие, которые обладают таким же свойством.

Определение 2.6.1. Корень ε n-й степени из 1 называется первообразным корнем n-й степени из 1, если его степени $\varepsilon^0 = 1, \varepsilon^1, \varepsilon^2, \ldots, \varepsilon^{n-1}$ являются всеми корнями n-й степени из 1.

Согласно утверждению (2.6.3), числа $\upsilon\varepsilon^0, \upsilon\varepsilon^1, \ldots, \upsilon\varepsilon^{n-1}$ – все корни n-й степени из комплексного числа $z \neq 0$.

Следующие утверждения характеризуют первообразные корни:

Теорема 2.6.4.

1. Если ε – первообразный корень n-й степени из 1 и $\varepsilon^l = 1$, то l делится на n (в $\mathbb{Z}$).

2. Число ε является первообразным корнем n-й степени из 1 тогда и только тогда, когда n – наименьшее натуральное число, для которого $\varepsilon^n = 1$.

3. Число ε_k $(0 \leqslant k \leqslant n-1)$ является превообразным корнем n-й степени из 1 тогда и только тогда, когда числа k и n взаимно простые.

Пример 2.6.3. 1. Первообразными корнями 6-й степени из 1 является:

$$\varepsilon_1 = \cos\frac{2\pi}{6} + i\sin\frac{2\pi}{6} = \frac{1}{2} + \frac{\sqrt{3}}{2}i,$$

$$\varepsilon_5 = \cos\frac{10\pi}{6} + i\sin\frac{10\pi}{6} = \frac{1}{2} - \frac{\sqrt{3}}{2}i,$$

т. к. среди чисел $0, 1, 2, 3, 4, 5$ только числа 1 и 5 взаимно просты с 6.

2. Одним из корней 6-й степени из числа $-8i$ является число $\upsilon = 1+i$, поскольку $(1+i)^6 = (2i)^3 = -8i$. Тогда $\sqrt[6]{-8i} = \upsilon\varepsilon_1^k$ $(k = \overline{0,5})$ и аналогично через первообразный корень ε_5.

С извлечением корней из комплексных чисел тесно связано решение двучленных уравнений n-й степени:

$$ax^n + b = 0, \tag{2.6.11}$$

где $a, b \in \mathbb{C}$, $a \neq 0$, $n \in \mathbb{N}$. (2.6.11) $\Leftrightarrow x^n = -\frac{b}{a}$. Если $b = 0$, то (2.6.11) имеет один корень 0; если же $b \neq 0$, то (2.6.11) имеет n разных корней, а именно, n корней n-й степени из числа $-\frac{b}{a}$.

Пример 2.6.4. Решим уравнение $x^4 - 16 = 0$.

Имеем $x^4 = 16$. Тогда $x_k = \sqrt[4]{16} = 2\left(\cos\frac{\pi k}{2} + i\sin\frac{\pi k}{2}\right)$ $(k = 0, 1, 2, 3)$, т. е. $x_0 = 2$, $x_1 = 2i$, $x_2 = -2$, $x_3 = -2i$.

Замечание 2.6.1. Отдельные двучленные уравнения можно решать разложением левой части уравнения на множители.

2.7. Геометрический смысл модуля разности двух комплексных чисел. Геометрическая интерпретация действий над комплексными числами.

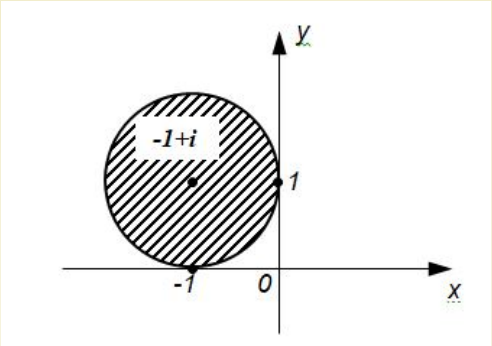
Покажем, что модуль разности двух комплексных чисел z_1 и z_2 есть расстояние между точками z_1 и z_2 на комплексной плоскости. Действительно, если $z_1 = x_1 + y_1 i$, $z_2 = x_2 + y_2 i$, то $z_1 - z_2 = (x_1 - x_2) + (y_1 - y_2)i$ и $|z_1 - z_2| = \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2}$ — растояние между точками (x_1, y_1) и (x_2, y_2).

Пример 2.7.1. Определим, какое множество точек комплексной плоскости задаётся условием:

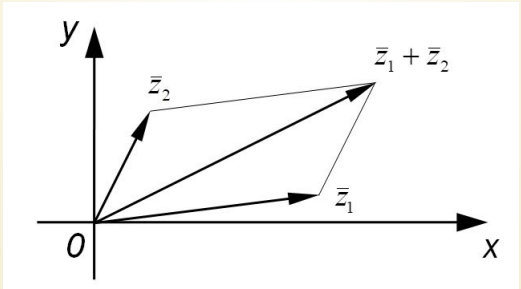
$$|z + 1 - i| \leqslant 1. \tag{2.7.12}$$

Запишем сумму $z + 1 - i$ в виде разности двух комплексных чисел: $z + 1 - i = z - (-1 + i)$. Тогда неравенство (2.7.12) примет вид: $|z - (-1 + i)| \leqslant 1$. Значит, нам нужно найти все точки z, расстояние от которых до точки $-1 + i$ не превышает 1. Искомое множество – круг с центром в точке $-1 + i$ и радиусом 1.

При помощи векторной интерпретации наглядно иллюстрируются сложение и вычитание комплексных чисел. Покажем числа $z_1 = x_1 + y_1 i$ и $z_2 = x_2 + y_2 i$ соответственно векторами $\overline{z_1}(x_1, y_1)$ и $\overline{z_2}(x_2, y_2)$. Тогда сумма $z = z_1 + z_2 = (x_1 + x_2) +$

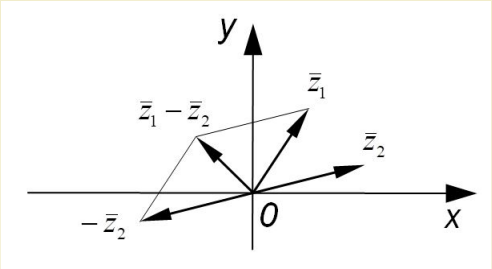


$(y_1 + y_2)i$ — вектор $\overline{z}(x_1 + x_2, y_1 + y_2) = \overline{z_1} + \overline{z_2}$. Таким образом, сложение комплексных чисел геометрически обозначает сложение соответствующих векторов и выполняется по правилу сложения векторов (в частности, если точки O, z_1, z_2 не лежат на одной прямой, по правилу параллелограмма). Очевидно, что разность

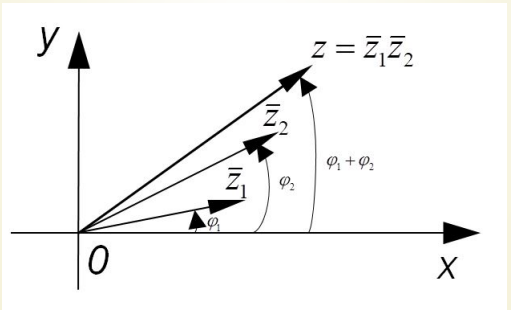


$z = z_1 - z_2 = (x_1 - x_2) + (y_1 - y_2)i$ — вектор $\overline{z}(x_1 - x_2, y_1 - y_2) = \overline{z_1} - \overline{z_2}$. Значит, вычитание комплексных чисел геометрически сводится к вычитанию соответствующих векторов.

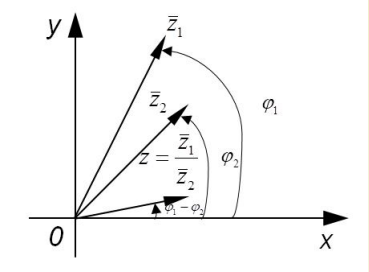
Геометрический смысл умножения и деления комплексных чисел легко выяснить, используя их запись в тригонометрической форме. Действительно, если



$z_1 = r_1(\cos\varphi_1 + i\sin\varphi_1)$, $z_2 = r_2(\cos\varphi_2 + i\sin\varphi_2)$, то вектор $\overline{z}$, который показывает произведение $z = z_1 z_2$, согласно формуле произведения чисел в тригонометрической форме, можно получить из z_1, повернув его вокруг начала координат на угол φ_2, а затем растянув (или сжав) в r_2 раз, если $r_2 > 1$ (или $0 < r_1 < 1$). Для построения



вектора $\overline{z}$, который показывает частное $z = \frac{z_1}{z_2}$ нужно, в соответствии с формулой частного чисел в тригонометрической форме, вектор $\overline{z_1}$ повернуть вокруг точки 0 на угол φ_2, а затем сжать (или растянуть) в r_2 раз, если $r_2 > 1$ (или $0 < r_2 < 1$).



РАЗДЕЛ 3
Теория групп

3.1. Порядок элемента группы. Циклические группы.

Определение 3.1.1. ***Порядком конечной группы*** называют число её элементов. Бесконечную группу называют группой бесконечного порядка.

Пример 3.1.1. Группами порядка n являются:

а) группа вращений правильного n-угольника;

б) R_n - группа корней n-ой степени из единицы (это единственная группа n-го порядка, элементами которой являются числа).

Пример 3.1.2. Группами бесконечного порядка являются:

а) аддитивные группы $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$;

б) полная линейная группа $GL_n(P) = \{A \in P_{n\times n} \big| \, |A| \neq 0\}$;

в) специальная линейная группа $SL_n(P) = \{A \in P_{n\times n} \big| \, |A| = 1\}$.

Порядок группы G обозначается $|G|$.
Пусть G — мультипликативная группа.

Определение 3.1.2. ***Порядком элемента*** $a \in G$ называется такое наименьшее натуральное число n, при котором $a^n = e$. Если такого n не существует, то a называется ***элементом бесконечного порядка***. Обозначают $n = |a|$.

Пример 3.1.3. В мультипликативной группе $\mathbb{C}^* = \mathbb{C}\backslash\{0\}$ порядки элементов
а) i, б) $\cos\frac{2\pi}{9} + i\sin\frac{2\pi}{9}$, в) 5
соответственно равны $4, 9, \infty$.

Утверждение 3.1.1. 1. Если a — элемент n-го порядка группы G и $s = ng+r, r < n$, то $a^s = a^r$.

2. Если a — элемент n-го порядка группы G, то $a^s = e \Leftrightarrow s \vdots n$.

3. Если a — элемент n-го порядка группы G, то порядок a^k равен $\frac{n}{d}$, где $d = $НОД$(n, k)$. В частности порядок a^k равен n тогда и только тогда, когда НОД$(n, k) = 1$.

Рассмотрим порядок произведения двух перестановочных элементов. В этом случае имеет место следующая лемма.

Лемма 3.1.1. Пусть a и b перестановочные элементы группы G, порядки n и k которых взаимно просты. Тогда:
1) $|ab| = nk$;
2) $(ab)^s = e \Rightarrow s \vdots n$ и $s \vdots k$;
3) $s \vdots nk \Rightarrow (ab)^s = e$.

Доказательство. 1. Пусть s_1 — порядок элемента ab. Тогда из

$$(ab)^{nk} = \underbrace{(ab)\ldots(ab)}_{nk} = a^{nk}\cdot b^{nk} = (a^n)^k\cdot(b^k)^n = e\cdot e = e.$$

$((ab)^{nk} = a^{nk} \cdot b^{nk}$ в силу перестановочности элементов) следует, что $nk \vdots s_1$. Поскольку $(ab)^{s_1} = 1$, то $(ab)^{s_1 k} = 1$ и $a^{s_1 k} = 1$. Тогда $s_1 k \vdots n$. Учитывая, что НОД$(n, k) = 1$, имеем $s_1 \vdots n$. Аналогично $s_1 \vdots k$. Так как НОД$(n, k) = 1$, то $s_1 \vdots nk$. Поэтому $s_1 = nk$.

2. Так как $(ab)^s = e$, то $s \vdots nk$. Поэтому $s \vdots n$ и $s \vdots k$.
3. Если $s : nk$, то $s = nkq$, тогда

$$(ab)^s = a^{nkq} \cdot b^{nkq} = (a^n)^{kq} \cdot (b^k)^{nq} = e.$$

□

Теорема 3.1.1. Если a и b перестановочные элементы группы G, порядков n и k соответственно, то порядок элемента ab равен НОК(n, k).

Однако, если элементы a и b конечного порядка неперестановочны, то их произведение может быть элементом бесконечного порядка. Например, в группе $GL_2(\mathbb{Q})$ элементы $A = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$ и $B = \begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix}$ второго порядка, но $AB = \begin{bmatrix} -1 & -1 \\ 0 & -1 \end{bmatrix}$ — элемент бесконечного порядка.

Определение 3.1.3. Мультипликативная группа G называется ***циклической***, если существует такой элемент $a \in G$, что каждый элемент из G может быть записан в виде $a^s, s \in \mathbb{Z}$.

Элемент a называют ***образующим группы*** G, а группа обозначается $G =< a >$. Говорят ещё, что группа порождается элементом a.

Если a — элемент конечного порядка n, то в этом случае $G =< a >= \{e, a, a^2, ..., a^{n-1}\}$. В самом деле, все элементы G различны. Если предположить, что $a^k = a^s$, $0 \leqslant k \leqslant n-1$, $0 \leqslant s \leqslant n-1$ и $k > s$, то $a^{k-s} = e$, $0 < k-s < n$. Последнее противоречит тому, что порядок a равен n.

Перемножаются элементы следующим образом: $a^k \cdot a^l = a^r$, где r — остаток от деления $k + l$ на n, $0 \leqslant r < n$ и $a^r \in G$. Обратным для a^n будет элемент $a^{n-k} \in G$.

Если же a — элемент бесконечного порядка, то группа G состоит из всевозможных целых степеней элемента a, которые попарно различны и перемножаются по обычному правилу умножения степеней.

Теорема 3.1.2. Все конечные циклические группы одного порядка изоморфны между собой. Все бесконечные циклические группы изоморфны между собой.

Доказательство. Пусть $G =< a >= \{e, a, a^2, ..., a^{n-1}\}$. Построим отображение

$$f : G \to R_n,\ f\left(a^k\right) = \xi_1^k,\ R_n = \{e, \xi_1, \xi_1^2, ..., \xi_1^{n-1}\}.$$

Так как $f\left(a^k \cdot a^l\right) = f\left(a^{k+l}\right) = \xi_1^{k+l} = \xi_1^k \cdot \xi_1^l = f\left(a^k\right) \cdot f\left(a^l\right)$. Отображение f биективно, а значит, f — изоморфно. Итак, любая циклическая группа порядка n изоморфна R_n, следовательно, циклические группы порядка n изоморфны между собой.

Если $G =< a >$ — бесконечная циклическая группа порождённая элементом a, то легко проверить, что отображение $f : G \longrightarrow \mathbb{Z}$, $f\left(a^k\right) = k$ является изоморфизмом. Значит, любая бесконечная циклическая группа изоморфна аддитивной группе целых чисел $\mathbb{Z}$. Значит, все бесконечные циклические группы изоморфны между собой. □

Напомним, что подмножество H группы G, которое образует группу относительно групповой операции G, называют ***подгруппой группы*** G. Любая мультипликативная группа G имеет тривиальные подгруппы: саму группу G и так называемую единичную подгруппу. Но в группе G могут быть и другие подгруппы. Например, множество матриц, определитель которых равен 1, является подгруппой полной линейной группы $GL_n(P)$. Т. е. $SL_n(P)$ подгруппа $GL_n(P)$. Важным примером подгрупп являются циклические группы.

Теорема 3.1.3. Любая подгруппа H циклической группы G является циклической группой.

Доказательство. Так как $H \leq G =< a >$, то H состоит из степеней элемента a. Пусть a^k - наименьшая положительная степень элемента a в H. Возьмём любой элемент $a^s \in H$. По теореме о делении с отстатком в $\mathbb{Z}$ имеем: $s = kq + r$, $0 \leqslant r \leqslant k$. Тогда $a^s = a^{kq} \cdot a^r$. Так как $a^s \in H$ и $(a^{kq})^{-1} \in H$, то $a^r = (a^{kq})^{-1} a^s \in H$.

Но $r < k$ и в силу выбора a^k следует, что $r = 0$. Следовательно, любой элемент $a^s = (a^k)^q$ и $H =< a^k >$. □

Следствие 3.1.1. Подгруппы аддитивной группы целых чисел $\mathbb{Z}$ исчерпываются группами $m\mathbb{Z} = \{mk | k \in \mathbb{Z}\}$.

Теорема 3.1.4. Если $< a >$ — циклическая группа порядка n, то число образующих этой группы равно $\varphi(n)$.

Доказательство. Если НОД$(k, n) = 1$, то, согласно 3.1.1 (3), порядок a^k равен n и a^k является образующим группы $< a >$. Так как таких k всего $\varphi(n)$, то число образующих группы $< a >$ есть $\varphi(n)$. □

Упражнение 3.1.1. Докажите, что при любых элементах a и b из группы G порядки элементов ab и ba совпадают.

Упражнение 3.1.2. Пусть G — циклическая группа порядка 15. Определите число порождающих её элементов.

Упражнение 3.1.3. В $GL_2(\mathbb{C})$ определите порядки элементов:

а) $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$; б) $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$; в) $\begin{bmatrix} i & 0 \\ 0 & i \end{bmatrix}$;

г) $\begin{bmatrix} -2+2i & -2+3i \\ 1-i & 3-2i \end{bmatrix}$; д) $\begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$.

Упражнение 3.1.4. Пусть x — элемент бесконечного порядка некоторой группы. Докажите, что $\forall n, m \in \mathbb{Z}$ $n \neq m$ имеет место $x^m \neq x^n$.

Упражнение 3.1.5. Укажите все подгруппы:

а) циклической группы 12-го порядка;

б) группы R_6;

в) аддитивной группы $\mathbb{Z}$.

Теорема 3.1.5. 1. Пусть $G =< a >$ — конечная циклическая подгруппа порядка n и d — натуральный делитель n. Пусть $H_d = \{a^d, a^{2d}, a^{3d}, ..., a^{\frac{n}{d}d} = a^n = e\}$. Тогда:

1) H_d - подгруппа группы G порядка $\frac{n}{d}$;

2) если $d_1 \neq d_2$, то $H_{d_1} \neq H_{d_2}$;

3) G не имеет других подгрупп, кроме H_d.

Таким образом, все подгруппы конечной циклической группы $< a >$ порядка n исчерпываются циклическими подгруппами $< a^d >$ порядка $\frac{n}{m}$ для каждого натурального m, делящего n.

2) Все подгруппы бесконечной циклической группы $< a >$ исчерпываются единичной подгруппой и бесконечными циклическими подгруппами $< a^m >$ для каждого $m \in \mathbb{N}$.

Упражнение 3.1.6. Докажите, что пересечение любого множества подгрупп группы само является её подгруппой.

Упражнение 3.1.7. Докажите, что если все неединичные элементы группы имеют порядки равные 2, то группа абелева.

Упражнение 3.1.8. Докажите, что $K = \{1, -1, i, j, k, -i, -j, -k\}$ является группой относительно действия, заданного следующим образом:

$$ij = k \qquad jk = i \qquad ki = j$$
$$ji = -k \qquad kj = -i \qquad ik = -j$$
$$(-i)k = -(ik) = -(-j) = j \text{ и т. д.}$$

Эту группу называют **группой кватернионов.**

Поскольку у элементов конечного порядка обратные элементы нужно искать среди натуральных степеней. Поэтому в критерии подгруппы (см. теорему 1.2.3) можно сократить число требований.

Теорема 3.1.6. Пусть H — подмножество произвольной группы и предположим, что каждый элемент из H имеет конечный порядок. Если $h_1h_2 \in H$ для всех h_1 и $h_2 \in H$, то H — подгруппа.

Следствие 3.1.2. Если H — подмножество конечной группы G и $h_1h_2 \in H$ для всех $h_1, h_2 \in H$, то H — подгруппа.

3.2. Группы подстановок

В этом параграфе мы изучим ещё один важный пример групп — группу подстановок.

Пусть M — непустое множество, $S(M)$ — совокупность всех биективных отображений M на себя. Легко проверить, что $S(M)$ относительно композиции отображений есть группа.

Если M — конечное множество, состоящее из n элементов, то $S(M)$ называется ***симметрической группой степени*** n.

Поскольку природа элементов множества M не имеет значения, то будем считать $M = \{1, 2, ..., n\}$, а симметрическую группу n-й степени обозначать символом S_n.

Элементы S_n называют ***подстановками*** и обозначают $\varphi = \begin{pmatrix} 1 & 2 & \dots & n \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \end{pmatrix}$.

Такая запись показывает, что $\varphi(i) = \alpha_i$, $i = \overline{1,n}$. Подстановка

$$\varphi^{-1} = \begin{pmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_n \\ 1 & 2 & \dots & n \end{pmatrix}, \; e = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix} -$$

единичная подстановка.

Пример 3.2.1. $S_3 = \left\{ e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \varphi_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \varphi_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \right.$
$\left. \varphi_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \varphi_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \varphi_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\}$.

Композиция отображений из S_3 задаётся следующей таблицей:

	e	φ_1	φ_2	φ_3	φ_4	φ_5
e	e	φ_1	φ_2	φ_3	φ_4	φ_5
φ_1	φ_1	e	φ_4	φ_5	φ_2	φ_3
φ_2	φ_2	φ_3	e	φ_1	φ_5	φ_4
φ_3	φ_3	φ_2	φ_5	φ_4	e	φ_1
φ_4	φ_4	φ_5	φ_1	e	φ_3	φ_2
φ_5	φ_5	φ_4	φ_3	φ_2	φ_1	e

Заметим, что второй ряд подстановки является перестановкой из n чисел $1, 2, \dots, n$. Поскольку из n элементов можно составить $n!$ перестановок, отсюда следует, что порядок S_n равен $n!$, т. е. $|S_n| = n!$

Следующая теорема объясняет значение групп подстановок.

Теорема 3.2.1. ***(Кэли)*** Любая конечная группа G порядка n изоморфна некоторой подгруппе симметрической группы S_n.

Доказательство. Каждому элементу a из группы G поставим в соответствие преобразование φ_a множества G: $\varphi_a(x) = ax$ для $\forall x \in G$. Таким образом, если $G = \{a_1, a_2, \ldots, a_n\}$ и $aa_1 = a_{s_1}, aa_2 = a_{s_2}, \ldots, aa_n = a_{s_n}$, то $\varphi_a = \begin{pmatrix} a_1 & a_2 & \ldots & a_n \\ a_{s_1} & a_{s_2} & \ldots & a_{s_n} \end{pmatrix}$ или проще $\varphi_a = \begin{pmatrix} 1 & 2 & \ldots & n \\ s_1 & s_2 & \ldots & s_n \end{pmatrix}$. Поскольку $G = \{a_{s_1}, a_{s_2}, \ldots, a_{s_n}\}$, то для произвольного $b \in G$ справедливо

$$\begin{gathered} ba_{s_1} = a_{t_1} \\ ba_{s_2} = a_{t_2} \\ \ldots\ldots\ldots \\ ba_{s_n} = a_{t_n} \end{gathered}$$

и $\varphi_b = \begin{pmatrix} s_1 & s_2 & \ldots & s_n \\ t_1 & t_2 & \ldots & t_n \end{pmatrix}$. Так как $ba \in G$, то

$$\begin{gathered} (ba)a_1 = b(aa_1) = ba_{s_1} = a_{t_1} \\ (ba)a_2 = b(aa_2) = ba_{s_2} = a_{t_2} \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ (ba)a_n = b(aa_n) = ba_{s_n} = a_{t_n} \end{gathered}$$

и $\varphi_{ba} = \begin{pmatrix} 1 & 2 & \ldots & n \\ t_1 & t_2 & \ldots & t_n \end{pmatrix}$. Заметим, что $\varphi_{ba} = \varphi_b \cdot \varphi_a$. Легко проверить, что множество $f(G) = \{\varphi_a \big| a \in G\}$ является группой относительно композиции преобразований, а следовательно, $f(G) \leq S_n$.

Рассмотрим отображение $f : G \to f(G)$, $f(a) = \varphi_a$. Так как $f(ba) = \varphi_{ba} = \varphi_b \cdot \varphi_a = f(b) \cdot f(a)$ и f — биективное отображение, то $f : G \to f(G)$ — изоморфизм. Поэтому $G \simeq f(G) \leq S_n$. □

Следствие 3.2.1. Число неизоморфных между собой групп конечного порядка n конечно.

Определение 3.2.1. ***Циклом*** называется подстановка $\varphi \in S_n$ такая, что на некотором подмножестве $\{i_1, i_2, \ldots, i_k\}$ множества $\{1, 2, \ldots, n\}$ выполняются соотношения:

$$\varphi(i_1) = i_2, \varphi(i_2) = i_3, \ldots, \varphi(i_{k-1}) = i_k, \varphi(i_k) = i_1$$

и $\varphi(j) = j$, если $j \notin \{i_1, i_2, \ldots, i_k\}$. Другими словами цикл есть подстановка вида

$$\begin{pmatrix} i_1 & i_2 & \ldots & i_k & j_1 & j_2 & \ldots & j_{n-k} \\ i_2 & i_3 & \ldots & i_1 & j_1 & j_2 & \ldots & j_{n-k} \end{pmatrix}.$$

Цикл кратно записывают в виде $\varphi = (i_1\ i_2\ \ldots\ i_k)$ или $\varphi = (i_2\ i_3\ \ldots\ i_k\ i_1)$ и т. д. Число k называют **длиной цикла**.

Пример 3.2.2. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 4 & 2 & 5 & 6 \end{pmatrix} = (2\ 3\ 4).$

Два цикла $s = (i_1\ \ i_2\ \ \ldots\ \ i_k)$ и $(j_1\ \ j_2\ \ \ldots\ \ j_l)$ называются независимыми, если множества $\{i_1\ \ i_2\ \ \ldots\ \ i_k\}$ и $\{j_1\ \ j_2\ \ \ldots\ \ j_l\}$ не пересекаются.

Непосредственной проверкой легко убедиться, что если s и t — независимые циклы, то $st = ts$.

Теорема 3.2.2. Любая подстановка $\varphi \neq \varepsilon$ является произведением независимых циклов длиной $\geqslant 2$. Это разложение однозначно с точностью до порядка сомножителей.

Пример 3.2.3.

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

Учитывая, что независимые циклы перестановочны, получаем: порядок подстановки равен наименьшему общему кратному длин независимых циклов. Циклы длины 2 называются **транспозициями**.

Теорема 3.2.3. Всякая подстановка $\tau \in S_n$ является произведением $n-c$ транспозиций, где c — число независимых циклов подстановки τ .

В самом деле, по теореме (3.2.2) любая подстановка есть произведение независимых циклов, а цикл

$$(i_1\ i_2\ \ldots\ i_k) = (i_1\ i_k)(i_1\ i_{k-1})\ldots(i_1\ i_2)$$

есть произведение транспозиций.

Определение 3.2.2. Если подстановка $\varphi = \begin{pmatrix} 1 & 2 & \ldots & n \\ \beta_1 & \beta_2 & \ldots & \beta_n \end{pmatrix}$ и t - число инверсий в перестановке $(\beta_1\ \ \beta_2\ \ \ldots\ \ \beta_n)$, то чётностью подстановки φ называется ***чётность числа*** t.

Теорема 3.2.4. Множество A_n всех чётных подстановок n-й степени является подгруппой группы S_n. Порядок группы $A_n = \frac{n!}{2}$. Группу A_n называют знакопеременной группой степени n.

3.3. Разложение группы по подгруппе. Теорема Лагранжа.

Пусть A и B подмножества группы G, тогда $AB = \{ab \mid a \in A, b \in B\}$. Если одно из подмножеств одноэлементно, например, $A = \{a\}$, то записывают $aB = \{ab \mid b \in B\}$.

Пусть H — подгруппа группы G. Определим на G бинарное отношение $\rho : a\rho b \Leftrightarrow a^{-1}b \in H$. Легко показать, что ρ — отношение эквивалентности на G, а, значит, ρ порождает разбиение множества G.

Пусть K_a — одно из подмножеств разбиения, то есть $K_a = \{x \in G \mid a\rho x\} = \{x \in G \mid a^{-1}x \in H\}$.

Тогда $a^{-1}x = h \in H \Longrightarrow x = ah \Longrightarrow x \in aH$. Последнее означает, что

$$K_a \subset aH \qquad (3.3.1)$$

С другой стороны, если $y \in aH$, то $y = ah$ и $a^{-1}y \in H$, значит $a\rho y, y \in K_a$ и

$$aH \subset K_a \tag{3.3.2}$$

.

Из (3.3.1) и (3.3.2) следует, что $K_a = aH$ и $G = \bigcup\limits_{a \in G} aH$.

Аналогично можно получить $G = \bigcup\limits_{a \in G} Ha$, если ρ определить следующим образом: $a\rho b \Leftrightarrow ba^{-1} \in H$.

Определение 3.3.1. Множество aH называют ***левым смежным классом***, а Ha — ***правым смежным классом*** группы G по подгруппе H. Каждый элемент смежного класса называется **представителем** этого класса.

Например, если $S_3 = \left\{\varphi_1 = \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}, \varphi_2 = \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}, \varphi_3 = \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}, \right.$ $\left. \varphi_4 = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}, \varphi_5 = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}, \varphi_6 = \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}\right\}$, то $H_1 = \{\varphi_1, \varphi_2\}$, $H_2 = \{\varphi_1, \varphi_4, \varphi_5\}$ являются подгруппами, $\varphi_2 H_2 = \{\varphi_2, \varphi_6, \varphi_3\}$, $H_2\varphi_2 = \{\varphi_2, \varphi_3, \varphi_6\}$, $\varphi_3 H_1 = \{\varphi_3, \varphi_4\}$, $H_1\varphi_3 = \{\varphi_3, \varphi_5\}$.

Как видим $\varphi_2 H_2 = H_2\varphi_2$, $\varphi_3 H_1 \neq H_1\varphi_3$. Очевидно, что смежный класс в общем случае подгруппой группы G не является.

Если $b \in aH$, то $bH = aH$, так как каждый класс эквивалентности однозначно определяется любым своим представителем. Разумеется, это справедливо и для правых смежных классов.

Пример 3.3.1. Найти множества левых и правых смежных классов группы S_3 по подгруппе $H_1 = \{\varphi_1, \varphi_2\}$.

Решение. $\varphi_1 H_1 = eH_1 = \{\varphi_1, \varphi_2\}$, $\varphi_3 H_1 = \{\varphi_3, \varphi_4\}$, $\varphi_5 H_1 = \{\varphi_5, \varphi_6\}$ — левые смежные классы; $H_1\varphi_1 = \{\varphi_1, \varphi_2\}$, $H_1\varphi_3 = \{\varphi_3, \varphi_5\}$, $H_1\varphi_5 = \{\varphi_4, \varphi_6\}$ — правые смежные классы разложения группы G по подгруппе H_1.

Как видно из примера, разложения группы на левые и правые смежные классы различны. Однако количество смежных классов в обоих разложениях одинаково.

Рассмотренные ранее свойства смежных классов можно собрать воедино в следующей лемме.

Лемма 3.3.1. Пусть H — подгруппа группы G. Тогда справедливы следующие утверждения:

1) $eH = H$; $a \in aH$;

2) если $a \in H$, то $aH = H$; если $b \in aH$, то $bH = aH$;

3) $aH = bH$ тогда и только тогда, когда $b^{-1}a \in H$;

4) два левых смежных класса либо совпадают, либо их пересечение пусто;

5) G является обьединением непересекающихся левых смежных классов группы G по подгруппе H.

6) если H — конечная группа, то $\mid H \mid = \mid aH \mid$ для всех $a \in G$.

Аналогичную лемму можно сформулировать и доказать для правых смежных классов G по H.

Определение 3.3.2. Количество смежных классов группы G по подгруппе H называют ***индексом подгруппы H в группе G*** и обозначают $|G : H|$.

В предыдущем примере $|S_3 : H_1| = 3$.

Для конечных групп справедлива следующая зависимость между порядком группы и порядком подгруппы.

Теорема 3.3.1. ***(Лагранжа)*** Порядок и индекс подгруппы H конечной группы G являются делителями порядка группы, причём $|G| = |H| \cdot |G : H|$.

Доказательство. Пусть H — подгруппа группы G, причём $|H| = k$ и $G = \bigcup\limits_{a \in G} aH$. В каждом классе aH содержится k элементов. В самом деле:

$$aH = \{ah_i \big| h_i \in H \quad i = \overline{1,k}\}$$

и если предположить, что $ah_s = ah_e$, то, умножив равенство на a^{-1} слева, получим $h_s = h_e$, противоречие. Так как классы не пересекаются, то $n = k \cdot |G : H|$, что и требовалось доказать. □

Следствие 3.3.1. Порядок любого элемента группы G является делителем порядка группы.

Доказательство. Пусть a — произвольный элемент группы G. Рассмотрим $H =< a >$. Порядок цикличной подгруппы, порождённой элементом a, совпадает с порядком элемента a, и, по теореме Лагранжа, является делителем порядка группы. □

Следствие 3.3.2. Каждая группа простого порядка является циклической и любой её элемент, отличный от единицы, является её образующим.

Доказательство. Пусть $|G| = p$, где p — простое число. Возьмём любой элемент $a \in G, a \neq e$. Порядок подгруппы $H =< a >$ является делителем порядка группы G. Так как число p имеет лишь два натуральных делителя 1 и p и $a \neq e$, то $|H| = p$ и, следовательно, $H =< a >= G$. □

Замечание 3.3.1. Легко видеть, что подгруппы конечной циклической группы n-го порядка находятся во взаимно однозначном соответствии с делителем числа n, поэтому теорему Лагранжа в случае циклических групп можно обратить. Однако, в общем случае теорема Лагранжа необратима. Так, например, доказано, что знакопеременная группа $A_4(|A_4| = 12)$ не имеет подгрупп 6-го порядка.

Упражнение 3.3.1. Найдите левые и правые разложения группы S_3 по всем её подгруппам.

Упражнение 3.3.2. Найдите левые (правые) смежные классы аддитивной группы $\mathbb{Z}$ по подгруппе $m\mathbb{Z} \quad (m > 0)$.

Упражнение 3.3.3. Найдите левые (правые) смежные классы полной линейной группы $GL_n(\mathbb{C})$ по специальной подгруппе $SL_n(\mathbb{C})$.

Упражнение 3.3.4. Найдите разложение циклической подгруппы 12-го порядка по всем её подгруппам.

Упражнение 3.3.5. Найдите правое и левое разложение группы кватернионов K по подгруппе $H = \{1, -1\}$. Сравните их и объясните результат сравнения.

Упражнение 3.3.6. Найдите разложение бесконечной циклической группы, порождённой элементом x, по подгруппе, порождённой элементом x^3.

3.4. Нормальные подгруппы.

Из предыдущих примеров видно, что левый и правый смежные классы aH и Ha группы G по подгруппе H могут, вообще говоря, не совпадать. Если группа G абелева, то $aH = Ha$ всегда. Однако в неабелевой группе G возможно, что $aH = Ha$ при любом $a \in G$.

Определение 3.4.1. Подгруппа H группы G называется ***нормальной подгруппой (нормальным делителем, инвариантной подгруппой)***, если $aH = Ha$ для любого $a \in G$. Обозначают $H \lhd G$ (H нормальна в G).

Напомним, что равенство $aH = Ha$ обозначает: для любого $h_1 \in H$ существует $h_2 \in H$ такой, что $ah_1 = h_2a$.

Пример 3.4.1. Подгруппа $A_3 = \{e, \varphi_4, \varphi_5\}$ является нормальной подгруппой группы S_3.

Пример 3.4.2. Подгруппы G и $\{e\}$ являются нормальными подгруппами любой группы G.

Пример 3.4.3. $SL_n(\mathbb{C}) \lhd GL_n(\mathbb{C})$.

Определение 3.4.2. Элемент y группы G называют ***сопряжённым элементу*** x, если существует $a \in G$, что $y = a^{-1}xa$.

Очевидно, что если y сопряжён элементу x, то x будет сопряжён элементу y, так как $x = (a^{-1})^{-1}\, y\, (a^{-1})$. Поэтому элементы x и y называют **сопряжёнными**.

Теорема 3.4.1. Подгруппа H группы G нормальна в G тогда и только тогда, когда $a^{-1}xa \in H$ для любого $x \in H$ и любого $a \in G$.

Доказательство. Пусть $H \lhd G$. Тогда по определению, $\forall a \in G\ aH = Ha$, значит, $a^{-1}H = Ha^{-1}$ и для любого $h \in H$ существует $h_1 \in H$ такой, что $a^{-1}h = h_1a^{-1}$. Отсюда $h_1 = a^{-1}ha \in H$.

Если $\forall h \in H\ \forall a \in G \quad a^{-1}ha \in H$, то $a^{-1}ha = h_1$, $ha = ah_1$, следовательно $Ha \subset aH$ и, наоборот, $aH \subset Ha$. Значит $aH = Ha$. □

Теорема 3.4.2. Пересечение любого множества нормальных подгрупп группы G является нормальной подгруппой группы G.

Теорема 3.4.3. Произведение нормальных подгрупп группы G является нормальной подгруппой группы G.

Доказательство. Пусть $H \lhd G$, $F \lhd G$. Рассмотрим $HF = \{hf \,|\, h \in H, f \in F\}$. Для любых $h_1f_1 \in HF$ и $h_2f_2 \in HF \quad (h_1f_1)(h_2f_2) = h_1(f_1h_2)f_2 = h_1(h_3f_3)f_2 = (h_1h_3)(f_3f_2) \in HF$. Для любого элемента $hf \in HF\ (hf)^{-1} = f^{-1}h^{-1} = h_4f_4$ (так как группа $H \lhd G$). Значит $(hf)^{-1} \in HF$ и HF — подгруппа группы G.

Покажем, что $HF \lhd G$. Возьмём любой элемент $hf \in HF$. Так как $h \in H$ и $H \lhd G$, то для любого $a \in G \quad a^{-1}ha \in H$. Аналогично $a^{-1}fa \in F$. Тогда $a^{-1}hfa = (a^{-1}ha)\,(a^{-1}fa) \in HF$, значит $HF \lhd G$. □

Вместо $x^{-1}bx$ удобно писать b^x.

Лемма 3.4.1. Для любых элементов a, b, x, y в группе G справедливы следующие равенства:

1) $a^{xy} = (a^x)^y$;
2) $(ab)^x = a^x b^x$;
3) $(a^x)^{-1} = (a^{-1})^x$.

Через a^G обозначим класс всех элементов, сопряженных с a, т. е. $a^G = \{a^x \mid x \in G\}$. Легко проверить, что любая группа G разбивается на непересекающиеся классы сопряженных элементов.

Теорема 3.4.4. Следующие два утверждения эквивалентны:

1) $xH = Hx$ для всех $x \in G$;
2) если $h \in H$ и $x \in H$, то $h^x \in H$.

Другими словами, подгруппа H нормальна в G тогда и только тогда, когда H вместе с каждым своим элементом содержит и все с ним сопряженные.

Если H — подгруппа группы G, то $H^x = \{h^x \mid h \in H\}$ также является подгруппой, которая называется **подгруппой, сопряженной с H посредством элемента x.**

Теорема 3.4.5. Подгруппа H нормальна в группе G тогда и только тогда, когда она совпадает с каждой своей сопряженной подгруппой.

Определение 3.4.3. ***Простой*** называется группа, у которой нет нормальных подгрупп, отличных от всей группы и единичной подгруппы.

Теорема 3.4.6. Абелева простая группа является циклической группой простого порядка. Обратно: каждая группа простого порядка будет простой абелевой группой.

Существуют неабелевы простые группы. Например, все знакопеременные группы A_n при $n \geq 5$ являются простыми неабелевыми группами.

Теорема 3.4.7. Пусть $H \lhd G$, $a, b \in G$. Тогда:
1) $(aH) \cdot (bH) = (ab)H$; 2) $(aH) \cdot H = H \cdot (aH) = aH$;
3) $(a^{-1}H) \cdot (aH) = (aH)(a^{-1}H) = H$.

То есть множество смежных классов группы G по нормальной подгруппе H (безразлично каких, поскольку $H \lhd G$) является группой относительно операции умножения подмножеств.

Эту группу называют ***фактор-группой группы*** G по нормальной подгруппе H и обозначают $\overline{G} = {}^{G}\!/_{H}$.

Доказательство. 1) $(aH)(bH) = a(Hb)H = a(bH) \cdot H = (ab)H \cdot H$ (в силу ассоциативности операции в группе и того, что $H \lhd G$). Покажем, что $H \cdot H = H$. В самом деле $H \subset HH$, так как $H = He = eH$ $(e \in H)$. Если $h_1 \in H$ и $h_2 \in H$, то $h_1 h_2 \in H \Longrightarrow H \cdot H \subset H$. Значит, $HH = H$. Тогда $(aH) \cdot bH = (ab)H$.

2) $(aH)H = a(H \cdot H) = aH$

$H(aH) = (Ha)H = (aH)H = aH \cdot H = aH$, т. е. $(aH)H = H(aH) = aH$ и подгруппа H выполняет роль нейтрального элемента относительно умножения подмножеств.

3) $(a^{-1}H) \cdot (aH) = (a^{-1}a)H = H$. Значит, $a^{-1}H$ является обратным для aH. Так как умножение подмножеств ассоциативно, то множество смежных классов группы G по нормальной подгруппе H является группой. Таким образом, $\overline{G} = {}^{G}\!/_{H} = \{aH \,|\, a \in G\}$. □

Упражнение 3.4.1. Докажите, что подгруппа H группы G индекса 2 является нормальной в G.

Упражнение 3.4.2. Возможно ли, что $F \lhd H$, $H \lhd G$, но F не является нормальной подгруппой группы G.

Упражнение 3.4.3. Пусть $B_4 = \{e, (12)(34), (13)(24), (14)(23)\}$. Докажите, что:
1) B_4 — подгруппа группы S_4 (её называют четвертой группой Клейна);

2) $B_4 \lhd S_4$; 3) $A_4 \lhd G$; 4) никаких других нормальных подгрупп, кроме A_4 и B_4 в S_4 нет.

Упражнение 3.4.4. Пусть K - группа кватернионов. Докажите, что любая подгруппа этой группы является её нормальной подгруппой. *(Пример неабелевой группы, каждая подгруппа которой нормальна).*

Упражнение 3.4.5. Докажите, что фактор-группа циклической группы по любой её подгруппе — циклическая группа.

Упражнение 3.4.6. Найдите фактор-группы циклической группы 12-го периода по всем её подгруппам.

Упражнение 3.4.7. Что представляет собой фактор-группа G/G и $G/\{e\}$?

Упражнение 3.4.8. Найдите фактор-группы:
1) S_4/A_4; 2) S_4/B_4.

Упражнение 3.4.9. Докажите, что если элементы x и y сопряжены в G, то их порядки равны.

Упражнение 3.4.10. Пусть $G = GL_n(\mathbb{R})$. Докажите, что $H = SL_n(\mathbb{R})$ является нормальной подгруппой группы G.

Упражнение 3.4.11. Пусть A и B — нормальные подгруппы группы G и $A \cap B = \{e\}$ — единичная подгруппа. Докажите, что $xy = yx$ для любых $x \in A$, $y \in B$.

Упражнение 3.4.12. Найдите фактор-группы:
а) $\mathbb{Z}/n\mathbb{Z}$; б) $4\mathbb{Z}/12\mathbb{Z}$.

Упражнение 3.4.13. Пусть P^n — аддитивная группа n-мерного линейного пространства над полем P и H — аддитивная подгруппа k-мерного векторного подпространства. Опишите фактор-группу P^n/H.

Лемма 3.4.2. Порядок фактор-группы G/H равен индексу нормальной подгруппы H, т.е. $|\, G/H \,| = |\, G : H \,|$.

3.5. Гомоморфизмы групп.

В параграфе 1.3 изложена базовая информация о гомоморфизмах групп.

Пусть $\varphi : G_1 \to G_2$ — гомоморфизм мультипликативной группы G_1 в мультипликативную группу G_2.

Теорема 3.5.1. Ядро гомоморфизма φ является нормальной подгруппой группы G_1.

Доказательство. По лемме 1.3.1 $Ker\varphi$ — подгруппа группы G_1. Если $x \in Ker\varphi$, то для любого элемента $a \in G_1$ $\varphi(a^{-1}xa) = \varphi(a^{-1}) \cdot \varphi(x) \cdot \varphi(a) = \varphi(a^{-1}) \cdot \varphi(a) = \varphi(a^{-1}a) = \varphi(e) = e$. Следовательно $a^{-1}xa \in Ker\varphi$. По теореме 3.4.1 $Ker\varphi \lhd G_1$. □

Пример 3.5.1. Ядром гомоморфизма $\varphi : S_n \to G = \{-1, 1\}$ является множество всех чётных подстановок, т.е. группа A_n.

Пример 3.5.2. Ядром гомоморфизма φ аддитивной группы $\mathbb{Z}$ на фактор-группу $\mathbb{Z}/m\mathbb{Z}$, определяемое $\varphi(z) = \overline{z}$, ($\overline{z}$ — класс вычетов, которому принадлежит z), является множество целых чисел кратных m.

Пусть G — группа и $H \lhd G$. Пусть μ — отображение, которое ставит элементу $g \in G$ смежный класс gH фактор-группы G/H. Отображение μ является гомоморфизмом G на G/H. Действительно, $\mu(g_1g_2) = (g_1g_2)H = g_1H \cdot g_2H = \mu(g_1) \cdot \mu(g_2)$. Гомоморфизм μ называют **естественным или каноническим**.

Теорема 3.5.2. Пусть $K \lhd G$ и f — естественный гомоморфизм группы G на фактор-группу G/K. Тогда справедливы следующие утверждения:

1) если U — подгруппа группы G, то $f(U) = UK/K$ — подгруппа группы G/K;

2) подгруппа U, содержащая K, нормальна в G тогда и только тогда, когда U/K нормальна в G/K;

3) если U нормальна в $G, K \leq U$, то $G/U \cong (G/K)/(U/K)$.

Теорема 3.5.3. Пусть φ — гомоморфизм группы G на G' и $Ker\varphi = H$. Тогда группа G' изоморфна фактор-группе G/H, причём существует такой изоморфизм $\psi : G/H \to G'$, что $\varphi = \psi\mu$, где μ — естественный гомоморфизм ($\mu : G \to G/H$).

Доказательство. Пусть g' — произвольно выбранный элемент группы G', а g — такой элемент G, что $\varphi(g) = g'$. Пусть $h \in H(\varphi(h) = e)$. Тогда $\varphi(gh) = \varphi(g)\varphi(h) = g'$. Значит, любой элемент смежного класса gH отображается в g'. С другой стороны, если $q \in G$ при гомоморфизме φ отображается в $g' \in G'$, то

$$\varphi(g^{-1}q) = \varphi(g^{-1})\varphi(q) = (\varphi(g))^{-1} \cdot g' = (g')^{-1} \cdot g^{-1} = e.$$

Т. е. $g^{-1}q \in H$, а это значит, что $g^{-1}q = h$ и $q = gh \in gH$.

Таким образом, множество всех элементов группы G, которые при гомоморфизме φ отображаются в $g' \in G'$ составляет смежный класс $\overline{g} = gH$ группы G по нормальной подгруппе H. Пусть ψ — отображение, которое каждому смежному классу $\overline{g} = gH$ ставит в соответствие $g' \in G$, $g' = \varphi(g)$, т. е. $\psi(\overline{g}) = \varphi(g)$.

Покажем, что ψ — изоморфное отображение фактор-группы G/H на G'. Действительно, пусть $\overline{g_1} = g_1H$ и $\overline{g_2} = g_2H$ — произвольные элементы G/H. Поскольку $\overline{g_1} \cdot \overline{g_2} = g_1H \cdot g_2H = (g_1g_2)H$, то

$$\psi(\overline{g_1g_2}) = \varphi(g_1 \cdot g_2) = \varphi(g_1) \cdot \varphi(g_2) = \psi(\overline{g_1})\psi(\overline{g_2}).$$

Кроме того отображение ψ биективно, т.е. $\overline{g_1} \neq \overline{g_2} \Rightarrow \psi(\overline{g_1}) \neq \psi(\overline{g_2})$, поскольку

$$\psi(\overline{g_1}) = \psi(\overline{g_2}) \Rightarrow \varphi(g_1) = \varphi(g_2) \Rightarrow g_1' = g_2' \Rightarrow g_1H = g_2H \Rightarrow \overline{g_1} = \overline{g_2}.$$

Таким образом, ψ — изоморфное отображение G/H на G'.

Рассмотрим теперь отображение $\psi\mu$. Поскольку μ — естественный гомоморфизм G на G/H, а ψ — изоморфизм фактор-группы G/H на G', то $\psi\mu$ есть отображение

G на G'. Докажем, что $\psi\mu = \varphi$. По определению естественного гомоморфизма μ $\mu(g) = \overline{g}$, а $\psi(\overline{g}) = \varphi(g)$. Следовательно, $\psi\mu(g) = \psi(\mu(g)) = \psi(\overline{g}) = \varphi(g)$ для любого элемента $g \in G$, т. е. $\forall g \in G \quad \psi\mu(g) = \varphi(g)$, значит $\varphi = \psi\mu$. □

Следствие 3.5.1. Изоморфные группы с алгебраической точки зрения неразличимы. Следовательно, теорема о гомоморфизмах показывает, что все группы на которые может гомоморфно отображаться группа G, фактически исчерпываются её фактор-группами, а все гомоморфизмы группы G исчерпываются естественными гомоморфизмами μ на её фактор-группы. Однако гомоморфное отображение группы G на группу G' не определяется однозначно ядром.

Например, гомоморфизм группы корней 3-ей степени из единицы на себя, заданное формулой $f(u) = u^2$, имеет то же ядро, что и тождественное отображение $(Ker f = e)$.

Теорема 3.5.4. ***(Основная теорема о гомоморфизме)***
Если $\varphi : G \to G_1$ — гомоморфизм, то $G/Ker\varphi \simeq Im\varphi$, т. е. при гомоморфизме групп фактор-группа по ядру изоморфна образу.

Доказательство. Пусть $K = Ker\varphi$. Поставим в соответствие элементу $aK \in {}^{G}/_{K}$ элемент $\varphi(a) \in Im\varphi$, т.е. положим $f(aK) = \varphi(a)$. Если $aK = bK$, то $b^{-1}a \in K$ и $\varphi(b^{-1}a) = \varepsilon$. Поэтому $\varphi(a) = \varphi(b)$ и $f(aK) = f(bK)$. Таким образом, соответствие f не зависит от выбора представителя смежного класса и каждому aK ставится в соотвествие единственный элемент $\varphi(a)$. Следовательно, $f : aK \mapsto \varphi(a)$ является отображением группы ${}^{G}/_{K}$ в группу $Im\varphi$. Так как

$$f((aK)(bK)) = f(abK) = \varphi(ab) = \varphi(a)\varphi(b) = f(aK)f(bK),$$

то f — гомоморфизм. Если $\varphi(a)$ — произвольный элемент из $Im\varphi$, то $\varphi(a) = f(aK)$, т.е. f — сюръекция. Если $f(aK) = f(bK)$, то $\varphi(a) = \varphi(b)$, поэтому $\varphi(a^{-1}b) = \varepsilon$ и $a^{-1}b \in Ker\varphi = K$, т. е. $aK = bK$. Следовательно, f — инъекция и f — изоморфизм групп ${}^{G}/_{K}$ и $Im\varphi$. □

Теорема 3.5.5. ***(Теорема об изоморфизме)***

Пусть H — нормальная в G подгруппа. Тогда для любой подгруппы A пересечение $A \cap H$ является нормальной в A подгруппой, а отображение $f : aH \mapsto a(A \cap H)$ — изоморфизмом групп AH/H и $A/A \cap H$.

РАЗДЕЛ 4
Идеалы кольца

4.1. Кольцо. Область целостности.

Элементарные сведения о кольцах содержатся в параграфе 1.4.

Распространяя терминологию, которая применяется для целых чисел, на элементы произвольного кольца, примем следующее определение.

Определение 4.1.1. Элемент $b \in K$ называют ***левым (соответсвенно правым) делителем элемента*** $a \in K$, если существует элемент $c \in K$ такой, что $a = bc$ (соответственно $a = cb$); при этом говорят также, что a является **левым (соответственно правым) кратным** элемента b.

Если кольцо K коммутативно, то эти понятия совпадают и говорят о делителе и кратном элемента.

Напомним, что если в кольце K есть единичный элемент, т.е. такой элемент e, что $\forall a \in K \quad ae = ea = a$, то кольцо K называют кольцом с единицей. Заметим, что когда в кольце K нет единицы, то элемент a может не быть делителем самого себя. Так в кольце $2\mathbb{Z}$ ни одно из отличных от нуля чисел не является делителем самого себя. Также, если в K нет единицы e, то элемент na, где $a \in K$, а n — некоторое целое число, не будет, вообще говоря, кратным элемента a в смысле определения, приведенного выше.

Так в кольце $3\mathbb{Z}$ элемент $5 \cdot 3 = 15$ не является кратным элемента 3, поскольку число $5 \notin 3\mathbb{Z}$.

Если K кольцо с единицей e, то для любого $a \in K$ $na = n(ea) = \underbrace{ea + ea + \cdots + ea}_{n} = \underbrace{(e + e + \cdots + e)}_{n} a$, то есть na является кратным элемента a.

Напомним, что подмножество K' кольца K называется ***подкольцом кольца*** K, если K' является кольцом относительно операций сложения и умножения, определённых в кольце K. Так, кольцо $2\mathbb{Z}$ является подкольцом кольца $\mathbb{Z}$, а последнее является подкольцом кольца $\mathbb{Q}$. Кольцо $\mathbb{Q}$ и кольцо чисел вида $a+b\sqrt{2}$, где $a, b \in \mathbb{Q}$, являются подкольцами кольца $\mathbb{R}$.

В каждом кольце K, очевидно, есть следующие подкольца: само кольцо K и нулевое подкольцо, которое состоит только из нуля кольца K. Эти кольца называют тривиальными.

Пусть K — произвольное кольцо с единицей. Так как для всякого отличного от нуля элемента $a \in K$ справедливы равенства $a \cdot 0 = 0 \cdot a = 0$ и $a \cdot e = e \cdot a = a$, то e и 0 являются различными элементами кольца, т. е. $e \neq 0$.

Раньше доказано, что если для элемента $a \in K$ в кольце существует обратный элемент a^{-1}, то он только один. Элемент e является обратным для самого себя. Так как $(-e)(-e) = e$, то $-e$ также является обратным для самого себя.

Элемент 0 не имеет обратного элемента, поскольку $a \cdot 0 = 0 \cdot a = 0 \neq e$ для любого элемента $a \in K$.

Определение 4.1.2. Элемент $a \in K$, для которого в кольце существует обратный элемент a^{-1}, называют ***обратимым*** или ***делителем единицы***.

Определение 4.1.3. Элементы a и b кольца K называются ***делителями нуля***, если $a \neq 0$, $b \neq 0$, но $ab = 0$. При этом a называют левым, а b — правым делителем нуля.

В коммутативных кольцах понятия левого и правого делителей нуля, очевидно, совпадают. Например, если m — составное число, т.е. $m = p \cdot q$, то в кольце $\mathbb{Z}_m$ $\overline{p} \cdot \overline{q} = \overline{0}$. Если $n \geqslant 2$, то матрицы n-го порядка

$\begin{bmatrix} 100\ldots00 \\ 000\ldots00 \\ \ldots\ldots\ldots \\ 000\ldots00 \end{bmatrix}$ и $\begin{bmatrix} 000\ldots00 \\ 000\ldots00 \\ \ldots\ldots\ldots \\ 000\ldots01 \end{bmatrix}$ являются делителями нуля в кольце $\mathbb{Q}_{n\times n}$.

Определение 4.1.4. Коммутативное кольцо с единицей, в котором нет делителей нуля, называют ***областью целостности***.

Упражнение 4.1.1. Выяснить, какие из следующих числовых множеств образуют кольцо относительно обычных операций сложения и умножения:

а) множество неотрицательных целых чисел;

б) множество рациональных чисел, в несократимой записи которых знаменатели являются степенями фиксированного простого числа P;

в) множество действительных чисел вида $a + b\sqrt{3}$, где $a, b \in Q$;

г) множество действительных чисел вида $a + b\sqrt[3]{2}$, где $a, b \in Q$;

д) множество действительных чисел вида $x + y\sqrt[3]{2} + z\sqrt[3]{4}$, где $x, y, z \in Q$;

е) множество комплексных чисел вида $a + bi$, $a, b \in Z$.

Упражнение 4.1.2. Какие из указанных множеств матриц образуют кольцо относительно матричного сложения и умножения:

а) множество действительных симметрических матриц порядка n;

б) множество действительных ортогональных матриц порядка n;

в) множество матриц порядка $n \geqslant 2$, у которых две последние строки нулевые;

г) множество матриц вида $\begin{bmatrix} a & b \\ kb & a \end{bmatrix}$ $a, b \in Z$ k — фиксированное целое число;

д) множество матриц вида $\begin{bmatrix} x & y \\ my & x \end{bmatrix}$, где m — фиксированное целое число некоторого кольца $K, x, y \in K$;

е) множество матриц вида $\frac{1}{2}\begin{bmatrix} x & y \\ my & x \end{bmatrix}$, где m — фиксированное целое число, не делящееся на квадрат простого числа, x, y — целые числа одинаковой четности.

Упражнение 4.1.3. Какие из следующих множеств функций образуют кольцо относительно обычных операций сложения и умножения функций:

а) множество функций действительного переменного, непрерывных на отрезке $[a, b]$;

б) множество функций, имеющих вторую производную на интервале (a, b).

Упражнение 4.1.4. В множестве многочленов от переменного t с обычным сложением в качестве умножения рассматривается операция, заданная правилом $(f \circ g)(t) = f(g(t))$. Является ли это множество кольцом относительно заданных операций?

Упражнение 4.1.5. Пусть K — конечное кольцо. Докажите что:

а) если K не содержит делителей нуля, то оно имеет единицу и все его ненулевые элементы обратимы;

б) если K содержит единицу, то всякий левый делитель единицы является правым делителем единицы.

4.2. Идеалы кольца. Действия над идеалами.

В теории колец особую роль, аналогичную роли нормальных подгрупп, играют подкольца, которые получили название идеалов.

Определение 4.2.1. ***Левым (правым) идеалом кольца*** K называется такое непустое подмножество I, что:

1) $a, b \in I \Rightarrow a - b \in I$;

2) $\forall a \in K$ и $\forall i \in I \quad ai \in I \quad (ia \in I)$.

В кольце $M_n(K)$ всех матриц n-го порядка левый идеал образуют множество матриц, у которых все столбцы, кроме s-го, нулевые.

В самом деле:

1) разность матриц такого вида – матрица такого вида;

2) например, при $n = 3$ и $s = 3$

$$\begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix} \begin{bmatrix} 0 & 0 & \alpha \\ 0 & 0 & \beta \\ 0 & 0 & \gamma \end{bmatrix} = \begin{bmatrix} 0 & 0 & \alpha a_{11} + \beta a_{12} + \gamma a_{13} \\ 0 & 0 & \alpha a_{21} + \beta a_{22} + \gamma a_{23} \\ 0 & 0 & \alpha a_{31} + \beta a_{32} + \gamma a_{33} \end{bmatrix}.$$

Определение 4.2.2. Подмножество I кольца K, которое одновременно является левым и правым идеалом, называется ***двусторонним идеалом***, или просто **идеалом кольца**.

В коммутативном кольце каждый левый и правый идеал, очевидно, является двусторонним идеалом. Из определения следует, что каждый левый, правый и двусторонний идеал является подкольцом кольца K. Очевидно, в произвольном кольце K идеалами являются $\{0\}$ и K. Эти идеалы называются ***тривиальными***.

Пример 4.2.1. Подкольцо $2\mathbb{Z}$ — идеал кольца $\mathbb{Z}$.

Пример 4.2.2. В кольце $M_2(\mathbb{C})$ всех комплексных матриц 2-го порядка подкольцо $I = \left\{ \begin{bmatrix} ak & al \\ bk & bl \end{bmatrix} \middle| a, b, k, l \in \mathbb{C} \right\}$ является идеалом.

Пример 4.2.3. В кольце $\mathbb{C}[a, b]$ функций, непрерывных на отрезке $[a, b]$ подкольцо $I = \{f \in C[a, b] \big| f(c) = 0, c \in [a, b]\}$ является идеалом.

Упражнение 4.2.1. Докажите, что в кольце Z_8 необратимые элементы образуют идеал, а в кольце Z_{12} — нет.

Упражнение 4.2.2. Докажите, что при $n = p^k$ (p — простое число) все необратимые элементы кольца Z_n образуют идеал.

Перейдём к рассмотрению некоторых операций над идеалами кольца. Первой операцией, которую мы рассмотрим, является операция теоретико-множественного пересечения.

Теорема 4.2.1. Пересечение $I_1 \cap I_2$ идеалов I_1 и I_2 кольца K является идеалом этого кольца.

Доказательство. Если $a, b \in I_1 \cap I_2 \Longrightarrow a, b \in I_1$ и $a, b \in I_2$, тогда $a - b \in I_1$ и $a - b \in I_2 \Longrightarrow a - b \in I_1 \cap I_2$.

Пусть $i \in I_1 \cap I_2 \Longrightarrow i \in I_1$ и $i \in I_2$, а, следовательно, $\forall k \in I \quad ki \in I_1 \quad ki \in I_2$ и $ki \in I_1 \cap I_2$.

Теорема легко распространяется на любое конечное или бесконечное число идеалов. □

Определение 4.2.3. ***Суммой конечного числа идеалов*** $I_1, I_2, \ldots, I_s$ называется множество $I_1 + I_2 + \cdots + I_s = \{i_1 + i_2 + \cdots + i_s \big| i_j \in I_j \quad j = \overline{1, s}\}$.

Определение 4.2.4. ***Произведением идеалов*** I_1 и I_2 называют множество $I_1 I_2 = \{x_1 y_1 + x_2 y_2 + \cdots + x_n y_n \big| n \in \mathbb{N}, \quad x_i \in I_i, \quad y_i \in I_2\}$.

Теорема 4.2.2. Сумма $I_1 + I_2 + \cdots + I_s$ идеалов кольца K является идеалом кольца K.

Теорема 4.2.3. Произведение $I_1 I_2$ идеалов I_1 и I_2 кольца K является идеалом этого кольца.

Доказательство. Разность

$$\sum_{i=1}^{n} x_i y_i - \sum_{j=1}^{m} x'_j y'_j = \sum_{i=1}^{n} x_i y_i + \sum_{j=1}^{m} (-x'_j) y'_j$$

является элементом произведения $I_1 I_2$. Далее для произвольного $k \in K$ прозведения

$$k \cdot \left(\sum_{i=1}^{n} x_i y_i \right) = \sum_{i=1}^{n} (k x_i) y_i \in I_1 I_2$$

$$\left(\sum_{i=1}^{n} x_i y_i \right) \cdot k = \sum_{i=1}^{n} x_i (y_i k) \in I_1 I_2,$$

т.к. $x_i \in I_1 \Longrightarrow k x_i \in I_1$, $y_i \in I_2 \Longrightarrow y_i k \in I_2$. □

Теорема 4.2.4. Операции умножения и сложения идеалов кольца K связаны дистрибудивными законами. Т. е. для любых идеалов I_1, I_2, I_3 кольца K имеем $(I_1 + I_2) I_3 = I_1 I_3 + I_2 I_3$, $\quad I_3 (I_1 + I_2) = I_3 I_1 + I_3 I_2$.

4.3. Сравнения и классы вычетов по идеалу. Фактор-кольцо.

Пусть K — некоторое кольцо и I — произвольный идеал этого кольца. Так как K — аддитивная абелева группа, то идеал I — его подгруппа. Поскольку в абелевой

группе все подгруппы нормальны, то $I \lhd K$. Следовательно, существует фактор-группа $K/I = \{0+I, \quad a+I \quad b+I, \dots\}$. Покажем, что в фактор-группе K/I можно так определить операцию умножения, что она будет кольцом относительно определённых в ней операций сложения и умножения. Но сначала определим одно важное понятие — понятие сравнения.

Определение 4.3.1. Элементы $x, y \in K$ называются ***сравнимыми элементами по идеалу*** I ***или по модулю*** I, если x и y принадлежат одному и тому же смежному классу фактор-группы K/I.

Высказывание «x сравним с y по модулю I» коротко записывают $x \equiv y(\mod I)$. Значит, $x \equiv y(\mod I) \Leftrightarrow x - y \in I$.

Отношение сравнимости является отношением эквивалентности на K. Классы эквивалентности отношения сравнимости на K называют ***классами вычетов кольца*** K ***по идеалу*** I, ***или по модулю*** I. Мы будем обозначать их символами $\overline{a}, \overline{b}, \overline{c}, \dots$.

Соотношения вида $x \equiv y(\mod I)$ называют **сравнениями**. Вернёмся теперь к фактор-группе $K/I = \{\overline{a}, \overline{b}, \overline{c}, \dots\}$. Напомним, что $\overline{a} + \overline{b} = \overline{a+b}$.

Определим умножение классов следующим образом $\overline{a} \cdot \overline{b} = \overline{ab}$. Покажем, что определённое так произведение классов не зависит от выбора представителей этих классов. Действительно, если $a, a' \in \overline{a}, \quad b, b' \in \overline{b}$, то $a \equiv a'(\mod I), \quad b \equiv b'(\mod I)$, т. е. $a - a' \in I$, $b - b' \in I$. Значит $a - a' = i_1, \quad b - b' = i_2$ или $a = a' + i_1$, $b = b' + i_2$. Тогда $ab = a'b' + a'i_2 + b'i_1 + i_1 i_2 = a'b' + i$, где $i = a'i_2 + b'i_1 + i_1 i_2 \in I$ и $ab \equiv a'b'(\mod I) \quad \overline{ab} = \overline{a'b'}$.

Теорема 4.3.1. Множество K/I классов вычетов кольца K по идеалу I с определёнными в нём операциями сложения и умножения является кольцом. Это кольцо называют **фактор-кольцом кольца** K **по идеалу** I.

Доказательство. Множество K/I — аддитивная абелева группа (обосновано раньше). Определённая в этой группе операция умножения является ассоциативной и

связана дистрибутивным законом с операцией сложения. Действительно,

$$\forall \overline{a}, \overline{b}, \overline{c} \in {}^{K}\!/_{I} \qquad (\overline{a}\overline{b})\overline{c} = \overline{a}\overline{b}\overline{c} = \overline{(ab)c} = \overline{a(bc)} = \overline{a}\overline{bc} = \overline{a}(\overline{b}\cdot\overline{c}).$$

$$(\overline{a}+\overline{b})\overline{c} = \overline{a+b}\cdot\overline{c} = \overline{(a+b)c} = \overline{ac+bc} = \overline{ac}+\overline{bc} = \overline{a}\cdot\overline{c}+\overline{b}\cdot\overline{c}.$$

$$\overline{c}(\overline{a}+\overline{b}) = \overline{c}\cdot\overline{a+b} = \overline{c(a+b)} = \overline{ca+cb} = \overline{ca}+\overline{cb} = \overline{c}\cdot\overline{a}+\overline{c}\cdot\overline{b}.$$

Следовательно, ${}^{K}\!/_{I}$ — кольцо. Заметим, что фактор-кольцо ${}^{K}\!/_{I}$ называют ещё **кольцом классов вычетов K по I.** □

Пример 4.3.1. В кольце $\mathbb{Z}$ возьмём идеал I, состоящий из всех целых чисел, кратных m (m — некоторое отличное от 1 натуральное число). Тогда $\overline{k} = \{k + ms \big| 0 \leqslant k \leqslant m\}$ и ${}^{\mathbb{Z}}\!/_{I} = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{m-1}\}$. Это кольцо называют ***кольцом классов вычетов по модулю*** m.

Упражнение 4.3.1. Докажите, что фактор-кольцо ${}^{\mathbb{Z}[i]}\!/_{I}$, где $I = \{3k \big| k \in \mathbb{Z}[i]\}$ является полем, состоящим из девяти элементов.

Упражнение 4.3.2. Докажите, что фактор-кольцо ${}^{\mathbb{Z}[i]}\!/_{I}$, где $I = \{nk \big| k \in \mathbb{Z}[i]\}$ является полем тогда и только тогда, когда n — простое число, не равное сумме квадратов целых чисел.

4.4. Гомоморфизмы колец.

В параграфе 1.5 рассмотрены основные определения и свойства гомоморфизма колец.

Напомним, что отображение f кольца K в кольцо L называется ***гомоморфным (или гомоморфизмом)***, если для любых $a, b \in K$ $\quad f(a+b) = f(a)+f(b); \quad f(ab) = f(a)\cdot f(b)$.

Теорема 4.4.1. Образ Imf кольца K при гомоморфизме $f : K \to L$ является подкольцом кольца L.

Доказательство. Доказательство заключается в непосредственной проверке аксиом кольца для Imf. □

Определение 4.4.1. Множество элементов кольца K отображающихся при гомоморфизме f в нуль кольца L называют ***ядром гомоморфизма*** f и обозначают $Kerf$. Таким образом, $Kerf = \{x \in K \big| f(x) = 0, \quad 0 \in L\}$.

Теорема 4.4.2. $Kerf$ — идеал кольца K.

Следующая теорема даёт важнейший пример гомоморфного отображения.

Теорема 4.4.3. Пусть I — идеал кольца K и $\overline{K} = {}^{K}\!/_{I}$. Тогда отображение кольца K на $\overline{K}$, заданное формулой $f(a) = \overline{a}$ является гомоморфизмом ($\overline{a}$ — класс вычетов, содержащий a). Идеал I является ядром этого гомоморфизма.

Доказательство. Для любых элементов a и b из K имеем:

$$f(a+b) = \overline{a+b} = \overline{a} + \overline{b} = f(a) + f(b); \quad f(ab) = \overline{ab} = \overline{a} \cdot \overline{b} = f(a) \cdot f(b).$$

Значит, f — гомоморфизм K на $\overline{K}$ (т. к. любой класс является образом какого-нибудь элемента из K). Найдём ядро этого гомоморфизма. По определению

$$Kerf = \left\{x \in K \big| f(x) = \overline{0}\right\} = \{x \in K \big| f(x) = 0 + I\}.$$

Значит $x \in I$ и $Kerf \subset I$. Наоборот, если $i \in I$, то $f(i) = \overline{i} = i + I = I = 0 + I = \overline{0}$, следовательно, $I \subset Kerf$. Откуда $Kerf = I$. □

Определение 4.4.2. Отображение $f : K \to {}^{K}\!/_{I}$ называют ***естественным*** или ***каноническим гомоморфизмом***.

Итак, каждому идеалу I кольца K соответствует гомоморфизм f, ядром которого служит этот идеал. Следующая теорема о гомоморфизмах обращает эту связь.

Теорема 4.4.4. Пусть f — гомоморфизм кольца K на кольцо L и I — ядро этого гомоморфизма. Тогда I — идеал кольца K и отображение φ фактор-кольца $\overline{K} = {}^{K}\!/_{I}$ на L, заданное формулой $\varphi(\overline{a}) = f(a)$ является изоморфизмом.

Доказательство. Докажем, что $I = Ker f$ — идеал кольца K.

Пусть $i_1, i_2 \in I$, т.е. $f(i_1) = 0 \quad f(i_2) = 0$, тогда

$$f(i_1 - i_2) = f(i_1) - f(i_2) = 0 - 0 = 0$$

и $i_1 - i_2 \in I$. Для любого $i \in I$ и $k \in I$ имеем

$$f(ik) = f(i) \cdot f(k) = 0 \cdot f(k) = 0;$$

аналогично $f(ik) = 0$. Значит, $ik \in I$ и $ki \in I$ и I — идеал кольца K.

Докажем, что φ — инъекция. Для этого покажем, что $\overline{a} = \overline{b} \Leftrightarrow f(a) = f(b)$. В самом деле, $\overline{a} = \overline{b} \Longrightarrow a + I = b + I$. Следовательно, для любого элемента $a + i$ из множества $a + I$ в множестве $b + I$ найдётся элемент $b + i_1$ такой, что $a + i = b + i_1$. Отсюда

$$f(a + i) = f(b + i_1) \Longrightarrow f(a) = f(b).$$

Наоборот, если $f(a) = f(b)$, то $f(a - b) = f(a) - f(b) = 0$ и $a - b \in I$, т. е.

$$a - b = i \in I \Longrightarrow a = b + i \Longrightarrow a \in b + I \Longrightarrow \overline{a} = \overline{b}.$$

Покажем, что φ — сюръекция, т. е., что всякий элемент из L является образом какого-нибудь элемента из $\overline{K}$. В самом деле, $\forall y \in L \quad y = f(x), \quad x \in K$. Но $x \in \overline{x} \in {}^{K}\!/_{I}$, тогда $\varphi(\overline{x}) = f(x)$.

Покажем, что φ — гомоморфизм.

$$\varphi(\overline{a}+\overline{b}) = \varphi(\overline{a+b}) = f(a+b) = f(a)+f(b) = \varphi(\overline{a})+\varphi(\overline{b}).$$

$$\varphi(\overline{a}\cdot\overline{b}) = \varphi(\overline{ab}) = f(ab) = f(a)\cdot f(b).$$

Следовательно, φ — биективный гомоморфизм, то есть φ — изоморфизм. Тогда $K/_I \simeq L$. □

4.5. Характеристика кольца с единицей.

Пусть K — кольцо с единицей e. Тогда $ne = e+e+e+\cdots+e \in K$ для любого $n \in \mathbb{N}$. В аддитивной группе кольца элемент e имеет либо конечный порядок $|e| = n$, либо бесконечный порядок $|e| = \infty$. В первом случае $n \cdot e = \underbrace{e+e+\cdots+e}_{n} = 0$, во втором – $ne = 0 \Leftrightarrow n = 0$.

Определение 4.5.1. Говорят, что кольцо K имеет **характеристику** n, если в аддитивной группе кольца единица кольца имеет конечный порядок n $(ne = 0)$.

Говорят, что кольцо K имеет **характеристику нуль**, если единица кольца K имеет бесконечный порядок $(ne = 0 \Leftrightarrow n = 0)$.

Пример 4.5.1. В кольце $\mathbb{Z}$ для любого целого положительного числа n выполняется условие $n \cdot 1 \neq 0$. Следовательно, кольцо $\mathbb{Z}$ имеет нулевую характеристику.

Пример 4.5.2. Пусть m — любое натуральное число. Фактор-кольцо $\mathbb{Z}_m = \mathbb{Z}/_{m\mathbb{Z}}$ имеет характеристику m, так как

$$m \cdot \overline{1} = \overline{1}+\overline{1}+\cdots+\overline{1} = \overline{m} = \overline{0}.$$

Упражнение 4.5.1. Докажите, что любое числовое кольцо имеет характеристику 0.

Теорема 4.5.1. Характеристикой области целостности является либо 0, либо простое число.

Доказательство. Пусть K — область целостности и e — единица кольца K. Если $|e| = \infty$, то K — имеет характеристику 0. Если же $|e| = 1$, то $e = 0$. Однако $e \neq 0$ в области целостности.

Пусть $|e| = n$, n — составное натуральное число $n = st$, $1 < s, 1 < n$. Следовательно $0 = ne = (st)e = (se) \cdot (te)$, $se \neq 0$, $te \neq 0$. А это противоречит тому, что K — область целостности. Следовательно, n — простое число. □

Пример 4.5.3. Пусть K – коммутативное кольцо с единицей e. Тогда:

1) отображение $f : \mathbb{Z} \to K$, заданное формулой $f(n) = ne$, является гомоморфизмом.

2) $Ker f = m\mathbb{Z}$ при некотором неотрицательном m.

3) $Im f = \mathbb{Z}/_{m\mathbb{Z}}$.

Пример 4.5.4. Пусть K — область целостности характеристики p. Тогда:

1) $\forall a \in K \quad a \neq 0 \quad$ и $\quad k, l$ — целых $\quad ka = la \Leftrightarrow k \equiv l(\mod p)$.

2) $\forall a, b \in K \quad$ и $\quad k \equiv 0(\mod p) \quad ka = kb \Leftrightarrow a = b$.

Пример 4.5.5. Пусть K – область целостности характеристики p. Тогда:
1) $\forall a, b \in K \quad (a+b)^p = a^p + b^p$; 2) $\forall a, b \in K \quad (a-b)^p = a^p - b^p$.

4.6. Кольцо главных идеалов.

В теории колец особого внимания заслуживают кольца, которые по своим свойствам достаточно близки к кольцу целых чисел. Развивая дальше теорию делимости, можно ввести следующие понятия.

Определение 4.6.1. Элементы a, b области целостности K называют ***взаимно простыми***, если они не имеют общих делителей, отличных от делителей единицы, т. е., если $\text{НОД}(a, b) = 1$.

Замечание 4.6.1. Пусть u — любой делитель единицы, a – произвольный элемент K. Тогда $a = a \cdot u \cdot u^{-1}$. Из этого равенства вытекает, что все элементы, ассоциированные с элементом a и все делители единицы являются делителями элемента a. Их называют ***тривиальными*** или ***несобственными делителями элемента*** a. Все другие делители, отличные от au, и от u, если такие существуют, называются нетривиальными или собственными. Например, в кольце $\mathbb{Z}$ тривиальными делителями числа 15 являются числа $\pm 1, \pm 15$ и нетривиальными (собственными) $\pm 3, \pm 5$.

Определение 4.6.2. Элемент $a \in K$ называется ***неразложимым*** или ***простым***, если он не является делителем единицы и не имеет нетривиальных делителей; элемент $a \in K$ называется **разложимым или составным**, если он имеет нетривиальные делители.

Свойства простых элементов.

1. если элемент $p \in K$ простой, то и любой ассоциированный с ним элемент также простой.

2. Если a — любой элемент кольца K, а p — простой элемент из K, то или a делится на p, или a и p взаимно просты.

Пусть K — область целостности. В области целостности K подкольцо $aK = \{ak \mid k \in K\}$, где $a \in K$, является идеалом.

Идеал aK кольца K называют **главным идеалом кольца K, порождённым элементом** a и обозначают (a).

Определение 4.6.3. ***Кольцом главных идеалов*** называют область целостности, в которой каждый идеал является главным.

Простейшим примером кольца главных идеалов является кольцо $\mathbb{Z}$. Конечно, не всякая область целостности является кольцом главных идеалов. Изучим свойства колец главных идеалов.

Легко проверит, что множество $(a, b) = \{ax + by \big| x, y \in K\}$, где a, b – фиксированные элементы K, являются идеалом области целостности K.

Теорема 4.6.1. Пусть p – простой элемент кольца K главных идеалов и $a \in K$. Если p не делит a, то $(p, a) = (1)$.

Доказательство. По условию каждый идеал K главный. Следовательно, существует в K такой элемент b, что $(p, a) = (b)$. Так как $p \in (p, a)$ и $a \in (p, a)$, то $p \vdots b, \quad a \vdots b$. Из того, что $p \vdots b$ следует, что или b ассоциирован с p или b – делитель единицы K.

Если b ассоциирован с p, то $b \vdots p$ и так как $a \vdots b$, то $a \vdots p$, что противоречит условию.

Следовательно, b – делитель единицы. Но b – делитель единицы тогда и только тогда, когда $(b) = (1)$. В самом деле: если b – делитель единицы, то $(1) \subset (b)$, так как $1 \vdots b \Longrightarrow \exists c \qquad 1 = bc$. Тогда $1 \in (b)$

$$(1) = \{m \cdot 1 \big| m \in K\} = \{mcb \big| m \in K\} \subset \{lb \big| l \in K\} = (b).$$

Поскольку $K = (1)$, то $(b) \subset (1)$. Значит $(b) = (1)$. Тогда $(p, a) = (1)$. $\square$

Теорема 4.6.2. Пусть p – простой элемент кольца K главных идеалов и $a, b \in K$. Если $ab \vdots p$, то $a \vdots p$ или $b \vdots p$.

Доказательство. Если a не делится на p, то по теореме (4.6.1) $(a,p)=(1)$. Значит в K существуют такие элементы x и y, что $ax+py=1$. Умножим последнее равенство на b: $axb+pyb=b$ или $abx+pby=b$. Так как $ab\vdots p \Longrightarrow b\vdots p$. □

Определение 4.6.4. Последовательность $(a_1),(a_2),(a_3),\ldots$ главных идеалов кольца называется ***возрастающей цепочкой идеалов***, если $(a_1)\subset(a_2)\subset(a_3)\subset\ldots$.

Теорема 4.6.3. В кольце главных идеалов возрастающая цепочка идеалов не может быть бесконечной.

Нашей целью теперь будет доказательство утверждения о возможности разложения каждого элемента кольца главных идеалов в произведение простых сомножителей.

Определение 4.6.5. Говорят, что элемент a области целостности K обладает однозначным разложением на простые множители, если выполняются условия:

1) существуют в K такие простые элементы p_i, что $a=\prod\limits_{i=1}^{m}p_i$;

2) если $a=\prod\limits_{i=1}^{n}q_i$ – другое разложение, в котором q_i – простые элементы K, то $m=n$ и при соответствующей нумерации p_i ассоциирован с q_i, $i=\overline{1,m}$.

Определение 4.6.6. Кольцо K называется ***факториальным***, если оно есть область целостности и всякий отличный от нуля необратимый элемент кольца обладает однозначным разложением на простые множители.

Теорема 4.6.4. Кольцо главных идеалов факториально.

Доказательство. Для простого элемента кольца K теорема справедлива: для простого элемента произведение, о котором говорится в теореме, состоит из одного сомножителя.

Предположим, что в кольце K есть отличный от нуля необратимый элемент a, который нельзя разложить в произвдение простых сомножителей. Тогда элемент a является составням, то есть $a = a_1 \cdot b_1$. Тогда главный идеал (a) включён в главный идеал (a_1), т. е. $(a) \subseteq (a_1)$. По крайней мере один из сомножителей a_1, b_1, например a_1, не обладает разложением на простые множители. Следовательно, $a_1 = a_2 \cdot b_2$ и $(a_1) \subseteq (a_2)$ и т. д. Таким образом образуется бесконечная возрастающая цепочка $(a) \subseteq (a_1) \subseteq (a_2) \subseteq \ldots$ – идеалов кольца K, что противоречит теореме (4.6.3). Следовательно, предположение неверно.

Докажем теперь единственность разложения на простые множители. Если a – простой элемент, то теорема верна. Предположим, что теорема верна для элементов, представимых в виде произведения n простых множителей, и докажем, чо теорема верна для элементов, представимых в виде произведения $n+1$ простых множителей. Пусть даны два разложения элемента a на простые множители:

$$a = p_1 p_2 \ldots p_n p_{n+1} = q_1 q_2 \ldots q_s q_{s+1}. \tag{4.6.1}$$

Простой элемент p_{n+1} делит произведение $q_1 q_2 \ldots q_s q_{s+1}$. Следовательно, он делит хотя бы один из сомножителей $q_1, q_2, \ldots, q_s, q_{s+1}$, например, q_{s+1}. Так как p_{n+1} и q_{s+1} – простые элементы, то $q_{s+1} = u p_{n+1}$, где u - обратимый элемент кольца. Сокращая обе части равенства (4.6.1) на p_{n+1} имеем

$$p_1 p_2 \ldots p_n = q_1 q_2 \ldots q_s u \qquad \text{или}$$

$$p_1 p_2 \ldots p_n = q_1 q_2 \ldots (u q_s) \tag{4.6.2}$$

По предположению индукции $n = s$ и при соответствующей нумерации p_i ассоциирован с $q_i \quad i = \overline{1, n}$. Кроме того, p_{n+1} ассоциировано с q_{n+1}. Следовательно, единственность разложения доказана. □

Замечание 4.6.2. Теорема об однозначном разложении на простые множители может нарушаться в двух разных смыслах: или в кольце существуют необратимые элементы, отличные от нуля, которые не разлагаются на простые множители, или нарушается однозначность разложения. Приведём примеры на оба случая.

Пример 4.6.1. ***(Кольцо с нарушением существования разложения на простые множители).***

Пусть $K = \{a_1 \cdot 2^{x_1} + a_2^{x_2} + \cdots + a_n^{x_n} \mid \quad n$ – любое натуральное число, $a_1, a_2, \ldots, a_n \in Z, \quad x_i$ – числа вида $\frac{m}{2^k}, \quad m, k$ – целые неотрицательные числа$\}$. В этом кольце число 2 разлагается на множители

$$2 = 2^{\frac{1}{2}} \cdot 2^{\frac{1}{2}} = 2^{\frac{1}{2}} \cdot 2^{\frac{1}{4}} \cdot 2^{\frac{1}{4}} = 2^{\frac{1}{2}} \cdot 2^{\frac{1}{4}} 2^{\frac{1}{8}} \cdot 2^{\frac{1}{8}} = \ldots$$

Таким образом, 2 разлагается на множители, но не разлагается на простые множители. Причём доказывается, что 2 и все числа вида $2^{\frac{1}{2^k}}$, k – целое неотрицательное, не являются делителями единицы.

Пример 4.6.2. ***(Кольцо с нарушением однозначности разложения на простые множители).***

Пусть $\{a + b\sqrt{-3} \mid a, b \in Z\} = \{a + bi\sqrt{3} \mid a, b \in Z\}$.

Назовём нормой $N(z)$ числа z из K квадрат его модуля, т. е. $N(z) = \overline{z}z = (a + bi\sqrt{3})(a - bi\sqrt{3}) = a^2 + 3b^2$. Очевидно, $(\forall k \in K) \quad N(z) > 0$, причём $N(z) = 0 \Leftrightarrow z = 0$. Если x – делитель единицы в K, т. е. $xy = 1$, то $N(x) \cdot N(y) = 1$. Но так как $N(x) \geqslant 1$ и $N(y) \geqslant 1$ следует, что $N(x) = N(y) = 1$. Пусть $x + di\sqrt{3}$, то $N(x) = c^2 + 3d^2 = 1 \Longrightarrow c \pm 1, d = 0$ или $x \pm 1$, т. е. делителями единицы в K являются только $+1$ и -1. Любое число из K, отличное от 0 и делителей единицы имеет норму большую 1. Поэтому, если t – собственый делитель z, то $N(t) < N(z)$. Отсюда легко доказать, разложимость на простые множители любого числа из K, отличного от 0 и ± 1. Однако единственность такого разлоения не имеет места.

В самом деле, $4 = 2 \cdot 2 = (1 + i\sqrt{3})(1 - i\sqrt{3})$, причём число 2 не ассоциировано

ни с одним из чисел $1 \pm \sqrt{3}$. Покажем, что 2 и $1 \pm \sqrt{3}$ – простые элементы кольца K. Если $2 = xy$, то $4 = N(z) = N(x) \cdot N(y)$. Но $4 = 2 \cdot 2 = 1 \cdot 4$. Если $N(x) \neq 2$ ($x = c + di\sqrt{3}$, $N(x) = c^2 + 3d^2$ и $c^2 + 3d^2 = 2 \Longrightarrow d^2 < 1 \Longrightarrow d = 0$ $c^2 = 2$, что невозможно). Значит, либо $N(x) = 4$ и тогда $N(y) = 1$, т.е. одно из чисел x, y будет делителем единицы. Следовательно, 2 – простое число. Так как $N(1 \pm i\sqrt{3}) = 4$, то простота чисел $1 \pm i\sqrt{3}$ доказывается аналогично. Тогда 4 обладает двумя различными разложениями на простые множители.

РАЗДЕЛ 5
Задания к практическим занятиям

5.1. Практикум по теме «Алгебры»

5.1.1. Примеры решения задач

Пример 5.1.1. Четыре функции, определенные на множестве $\mathbb{R}^*$,

$$f_1(x) = x, \quad f_2(x) = -x, \quad f_3(x) = \frac{1}{x}, \quad f_4(x) = -\frac{1}{x}$$

с операцией умножения образуют группу. Составим таблицу умножения этих функций.

	f_1	f_2	f_3	f_4
f_1	f_1	f_2	f_3	f_4
f_2	f_2	f_1	f_4	f_3
f_3	f_3	f_4	f_1	f_2
f_4	f_4	f_3	f_2	f_1

Произведение $f_i f_j$ указывается на пересечении строки f_i и столбца f_j. Например,

$$f_2 f_3 : x \overset{f_3}{\mapsto} \frac{1}{x} \overset{f_2}{\mapsto} -\frac{1}{x},$$

поэтому $f_2 f_3 = f_4$.

Из таблицы видно, что умножение определено на множестве $\{f_1, f_2, f_3, f_4\}$ и коммутативно. Поскольку умножение отображений ассоциативно, то выполняется второе требование определения группы. Функция f_1 является единичным элементом, а $f_i^{-1} = f_i$, т.е. каждый элемент является обратным для себя. Таким образом, множество $\{f_1, f_2, f_3, f_4\}$ с умножением является конечной абелевой группой порядка 4. ⊠

Пример 5.1.2. Является ли группой множество $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ ненулевых действительных чисел с операцией $a \circ b = 2ab$?

Доказательство. Для любых чисел $a, b \in \mathbb{R}^*$ элемент $a \circ b = 2ab$ также принадлежит $\mathbb{R}^*$, поэтому операция $\circ$ на множестве $\mathbb{R}^*$ определена. Проверим выполнение других условий в определении группы.

Ассоциативность операции:

$$(a \circ b) \circ c = (2ab) \circ c = 2(2ab)c = 4abc,$$

$$a \circ (b \circ c) = a \circ (2bc) = 2a(2bc) = 4abc,$$

т. е. $(a \circ b) \circ c = a \circ (b \circ c)$ и операция ассоциативна. Ясно, что

$$a \circ b = (2ab) = 2ba = b \circ a$$

и операция коммутативна. Поэтому множество $\mathbb{R}^*$ с операцией $\circ$ является коммутативной полугруппой.

Единичный элемент n должен удовлетворять равенствам:

$$a = a \circ n = 2an, \;\; a = n \circ a = 2na.$$

Очевидно, этим равенствам удовлетворяет число $\frac{1}{2}$, поэтому $\frac{1}{2}$ — единичный элемент.

Обратный элемент b к элементу a должен удовлетворять равенствам:

$$\frac{1}{2} = a \circ b = 2ab, \;\; \frac{1}{2} = b \circ a = 2ba.$$

Очевидно этим равенствам удовлетворяет элемент $\frac{1}{4a}$, поэтому $\frac{1}{4a}$ — обратный элемент к элементу a.

Таким образом, множество $\mathbb{R}^*$ с операцией $\circ$ является абелевой группой с единичным элементом $\frac{1}{2}$ и обратным к a элементом $\frac{1}{4a}$.

Ответ: Множество $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ с операцией $a \circ b = 2ab$ является абелевой группой. □

Пример 5.1.3. Будет ли множество

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$$

с обычными операциями сложения и умножения действительных чисел кольцом, полем?

Доказательство. Покажем прежде всего, что на множестве $\mathbb{Q}(\sqrt{2})$ сложение и умножение определено.

$$(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2} \in \mathbb{Q}(\sqrt{2}),$$

$$(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2} \in \mathbb{Q}(\sqrt{2})$$

для любых чисел $(a + b\sqrt{2}), (c + d\sqrt{2}) \in \mathbb{Q}(\sqrt{2})$.

Проверим выполнение условий определения кольца и поля. Ассоциативность сложения во множестве $\mathbb{Q}(\sqrt{2})$ следует из ассоциативности сложения во множестве $\mathbb{R}$ всех действительных чисел.

Нулевым элементом во множестве $\mathbb{Q}(\sqrt{2})$ будет число $0 + 0\sqrt{2} \in \mathbb{Q}(\sqrt{2})$.

Элементом, противоположным элементу $a + b\sqrt{2}$, во множестве $\mathbb{Q}(\sqrt{2})$ будет элемент $-a - b\sqrt{2}$.

Коммутативность сложения во множестве $\mathbb{Q}(\sqrt{2})$ следует из коммутативности сложения во множестве $\mathbb{R}$ всех действительных чисел.

Ассоциативность умножения во множестве $\mathbb{Q}(\sqrt{2})$ следует из ассоциативности умножения во множестве $\mathbb{R}$ всех действительных чисел.

Коммутативность умножения и выполнение законов дистрибутивности также следуют из выполнения соответствующих свойств во множестве $\mathbb{R}$ всех действительных чисел.

Тем самым доказано, что множество $\mathbb{Q}(\sqrt{2})$ является кольцом.

Единичным элементом во множестве $\mathbb{Q}(\sqrt{2})$ является число $1+0\sqrt{2}$ поскольку

$$(a+b\sqrt{2})(1+0\sqrt{2}) = a+b\sqrt{2}$$

для любого элемента $a+b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$.

Пусть $a+b\sqrt{2} \in \mathbb{Q}(\sqrt{2})^*$. Это означает, что $a^2+b^2 \neq 0$, т.е. a и b одновременно не равны нулю. Пусть $x+y\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ и является элементом, обратным для элемента $a+b\sqrt{2}$. Тогда

$$(a+b\sqrt{2})(x+y\sqrt{2}) = 1+0\sqrt{2},$$

$$(a+b\sqrt{2})(x+y\sqrt{2}) = 1,$$

откуда

$$x+y\sqrt{2} = \frac{1}{a+b\sqrt{2}} = \frac{a-b\sqrt{2}}{(a+b\sqrt{2})(a-b\sqrt{2})} = \frac{a-b\sqrt{2}}{a^2-2b^2} =$$

$$= \frac{a}{a^2-2b^2} + \frac{b}{2b^2-a^2}\sqrt{2} \in \mathbb{Q}(\sqrt{2}),$$

так как

$$\frac{a}{a^2-2b^2}, \quad \frac{b}{2b^2-a^2} \in \mathbb{Q}, \quad a^2-2b^2 \neq 0.$$

Таким образом, каждый ненулевой элемент $a+b\sqrt{2}$ имеет в $\mathbb{Q}(\sqrt{2})$ обратный элемент $\frac{a}{a^2-2b^2} + \frac{b}{2b^2-a^2}\sqrt{2}$.

Ответ: Множество $\mathbb{Q}(\sqrt{2})$ является полем. □

Пример 5.1.4. Множество всех перестановок на множестве из n элементов относительно умножения перестановок образует группу, которая обозначается S_n и называется симметрической группой n-ой степени. При $n > 2$ группа S_n неабелева.

Составим таблицу умножения для S_3. В группе S_3 шесть элементов: $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = e$, $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (12)$, $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (13)$, $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (23)$, $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (123)$, $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (132)$. Таким образом, $S_3 = \{e, (12), (13), (23), (123), (132)\}$.

Заполним следующую таблицу умножения для S_3. Например, на пересечении строки (12) и столбца (13) ставим произведение $(12)(13) = (132)$.

S_3	e	(12)	(13)	(23)	(123)	(132)
e	e	(12)	(13)	(23)	(123)	(132)
(12)	(12)	e	(132)	(123)	(123)	(132)
(13)	(13)	(123)	e	(132)	(123)	(132)
(23)	(23)	(132)	(123)	(23)	(123)	(132)
(123)	(123)	(13)	(23)	(23)	(123)	(132)
(132)	(132)	(23)	(12)	(23)	(123)	(132)

Пример 5.1.5. Пусть $G = S_n$ — симметрическая группа степени n, а $H = \{-1; 1\}$ — мультипликативная группа. Доказать, что отображение $f : S_n \to H$, $f(\tau) = sgn\tau$ является гомоморфизмом. Найти ядро и образ.

Решение. По условию, четным перестановкам ставится в соответствие 1, а нечетным — -1. Поскольку знак произведения перестановок равен произведению знаков, т. е.

$$f(\tau\sigma) = sgn(\tau\sigma) = sgn(\tau) \cdot sgn(\sigma) = f(\tau) \cdot f(\sigma),$$

то условие гомоморфизма выполняется и f — гомоморфизм. Ядро $Ker\ f$ состоит из четных перестановок, поэтому $Ker\ f = A_n$ — знакопеременная группа. Легко видеть, что f – эпиморфизм, поэтому $Im\ f = H$.

5.1.2. Индивидуальные задания

1. Будет ли множество A с операцией $*$ полугруппой? Существует ли здесь единичный элемент?

1.1. $A = \mathbb{N}$, $a * b = 2(a + b)$, $\forall a, b \in \mathbb{N}$.
1.2. $A = \mathbb{Z}$, $a * b = a - b + 1$, $\forall a, b \in \mathbb{Z}$.
1.3. $A = \mathbb{Q}$, $a * b = 2a + b$, $\forall a, b \in \mathbb{Q}$.
1.4. $A = \mathbb{R}$, $a * b = 4ab$, $\forall a, b \in \mathbb{R}$.
1.5. $A = \mathbb{N}$, $a * b = a^b$, $\forall a, b \in \mathbb{N}$.
1.6. $A = \mathbb{Z}$, $a * b = a + b - 2$, $\forall a, b \in \mathbb{Z}$.
1.7. $A = \mathbb{Q}$, $a * b = 3(a + b)$, $\forall a, b \in \mathbb{Q}$.
1.8. $A = \mathbb{R}$, $a * b = \frac{a+b}{3}$, $\forall a, b \in \mathbb{R}$.
1.9. $A = \mathbb{N}$, $a * b = \sqrt{ab}$, $\forall a, b \in \mathbb{N}$.
1.10. $A = \mathbb{Z}$, $a * b = -(a + b)$, $\forall a, b \in \mathbb{Z}$.
1.11. $A = \mathbb{Q}$, $a * b = (a + b)^2$, $\forall a, b \in \mathbb{Q}$.
1.12. $A = \mathbb{R}$, $a * b = -2ab$, $\forall a, b \in \mathbb{R}$.
1.13. $A = \mathbb{N}$, $a * b = a^2 + b^2$, $\forall a, b \in \mathbb{N}$.
1.14. $A = \mathbb{Z}$, $a * b = a + b^2$, $\forall a, b \in \mathbb{Z}$.
1.15. $A = \mathbb{Q}$, $a * b = \frac{ab}{2}$, $\forall a, b \in \mathbb{Q}$.

2. Будет ли множество M с указанной операцией $*$ группой? Операция $*$ коммутативна или нет?

2.1. $M = \mathbb{Q}^*$, $a * b = 5ab$, $\forall a, b \in M$.
2.2. $M = \{-1; 1\}$, $a * b = ab$, $\forall a, b \in M$.
2.3. $M = \{2k \mid k \in \mathbb{Z}\}$, $a * b = a + b$, $\forall a, b \in M$.
2.4. $M = \{2k + 1 \mid k \in \mathbb{Z}\}$, $a * b = ab$, $\forall a, b \in M$.
2.5. $M = \{\frac{m}{2^{k-1}} \mid m \in \mathbb{Z}, k \in \mathbb{N}\}$,
$a * b = a + b$, $\forall a, b \in M$.
2.6. $M = \{\frac{m}{2^{k-1}} \mid m \in \mathbb{Z}^*, k \in \mathbb{N}\}$,

$a * b = ab, \quad \forall a, b \in M.$

2.7. $M = \{c + d\sqrt{3} \mid c, d \in \mathbb{Z}\}$,
$a * b = a + b, \quad \forall a, b \in M.$

2.8. $M = \mathbb{Q}^*, \quad a * b = 3ab, \quad \forall a, b \in M.$

2.9. $M = \{c + d\sqrt{3} \mid c \in \mathbb{Q}^*, d \in \mathbb{Q}\}$,
$a * b = ab, \quad \forall a, b \in M.$

2.10. $M = \mathbb{Z}^2 = \{(a, b) \mid a, b \in \mathbb{Z}\}$,
$(a, b) * (c, d) = (a + c, b + d), \quad \forall (a, b), (c, d) \in M.$

2.11. $M = \{(a, b) \mid a \in \mathbb{R}^*, b \in \mathbb{R}\}$,
$(a, b) * (c, d) = (ac, bd), \quad \forall (a, b), (c, d) \in M.$

2.12. $M = \mathbb{Q}^*, \quad a * b = -2ab, \quad \forall a, b \in M.$

2.13. $M = \{3k \mid k \in \mathbb{Z}\}, \quad a * b = a + b, \quad \forall a, b \in M.$

2.14. $M = \{c - d\sqrt{2} \mid c, d \in \mathbb{Z}\}$,
$a * b = a + b, \quad \forall a, b \in M.$

2.15. $M = \{c - d\sqrt{2} \mid c \in \mathbb{Q}^*, d \in \mathbb{Q}\}$,
$a * b = ab, \quad \forall a, b \in M.$

3. Является ли следующее множество аддитивной или мультипликативной группой?

3.1. $M = \{\frac{a}{2^{k-1}} \mid a \in \mathbb{Z}, k \in \mathbb{N}\}.$

3.2. $M = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}.$

3.3. $M = \{a + b\sqrt{3} \mid a \in \mathbb{Q}^*, b \in \mathbb{Q}\}.$

3.4. $M = \{\frac{a}{3^{k-1}} \mid a \in \mathbb{Z}, k \in \mathbb{N}\}.$

3.5. $M = \{2k - 1 \mid k \in \mathbb{Z}\}.$

3.6. $M = \{2k \mid k \in \mathbb{Z}\}.$

3.7. $M = \{\frac{a}{2^{k-1}} \mid a \in \mathbb{Z}^*, k \in \mathbb{N}\}.$

3.8. $M = \{a - b\sqrt{3} \mid a, b \in \mathbb{Z}\}.$

3.9. $M = \{-\frac{a}{3^{k-1}} \mid a \in \mathbb{Z}^*, k \in \mathbb{N}\}.$

3.10. $M = \{-a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}.$

3.11. $M = \{2k+1 \mid k \in \mathbb{Z}\}$.
3.12. $M = \{3k \mid k \in \mathbb{Z}\}$.
3.13. $M = \{-a + b\sqrt{3} \mid a \in \mathbb{Q}^*, b \in \mathbb{Q}\}$.
3.14. $M = \{2k+1 \mid k \in \mathbb{R}\backslash\{-\frac{1}{2}\}\}$.
3.15. $M = \{2k-1 \mid k \in \mathbb{R}\backslash\{\frac{1}{2}\}\}$.

4. Будет ли множество K с указанными операциями сложения и умножения кольцом?

4.1. $K = \{a + b\sqrt{5} \mid a, b \in \mathbb{Q}\}$, сложение и умножение действительных чисел.
4.2. $K = \{(a,b) \mid a, b \in \mathbb{R}\}, (a,b) + (c,d) = (a+c, b+d), (a,b)(c,d) = (ac, bd)$.
4.3. $K = \{\frac{a}{2^{k-1}} \mid a \in \mathbb{Z}, k \in \mathbb{N}\}$, сложение и умножение действительных чисел.
4.4. $K = \mathbb{R}$, сложение действительных чисел, умножение: $a * b = 2ab$.
4.5. $K = \{a + b\sqrt{3} \mid a, b \in \mathbb{Q}\}$, сложение и умножение действительных чисел.
4.6. $K = \{a - b\sqrt{2} \mid a, b \in \mathbb{Q}\}$, сложение и умножение действительных чисел.
4.7. $K = \{(a,b) \mid a, b \in \mathbb{Q}\}, (a,b) + (c,d) = (a,d), (a,b)(c,d) = (ac, bd)$.
4.8. $K = \{\frac{a}{3^{k-1}} \mid a \in \mathbb{Z}, k \in \mathbb{N}\}$, сложение и умножение действительных чисел.
4.9. $K = \{(a,0) \mid a \in \mathbb{R}\}, (a,0) + (b,0) = (a+b, 0), (a,0)(b,0) = (ab, 0)$.
4.10. $K = \{-\frac{a}{4^{k-1}} \mid a \in \mathbb{Z}, k \in \mathbb{N}\}$, сложение и умножение действительных чисел.
4.11. $K = \{a - b\sqrt{3} \mid a, b \in \mathbb{Q}\}$, сложение и умножение действительных чисел.
4.12. $K = \{a - b\sqrt{5} \mid a, b \in \mathbb{Q}\}$, сложение и умножение действительных чисел.
4.13. $K = \{(0,b) \mid b \in \mathbb{R}\}, (0,a) + (0,b) = (0, a+b), (0,a)(0,b) = (0, ab)$.
4.14. $K = \{\frac{a}{5^{k-1}} \mid a \in \mathbb{Z}, k \in \mathbb{N}\}$, сложение и умножение действительных чисел.
4.15. $K = \{-\frac{a}{2^{k-1}} \mid a \in \mathbb{Z}, k \in \mathbb{N}\}$, сложение и умножение действительных чисел.

5. Является ли множество P с указанными операциями полем?

5.1. $P = \{(a,b) \mid a, b \in \mathbb{R}\}, (a,b) + (c,d) = (a+c, b+d), (a,b)(c,d) = (ac, bd)$.
5.2. $P = \{\frac{a}{2^{k-1}} \mid a \in \mathbb{Z}, k \in \mathbb{N}\}$, сложение и умножение действительных чисел.
5.3. $P = \mathbb{R}$, сложение действительных чисел, умножение: $a * b = 2ab$.
5.4. $P = \{a + b\sqrt{5} \mid a, b \in \mathbb{Q}\}$, сложение и умножение действительных чисел.
5.5. $P = \{(a,0) \mid a \in \mathbb{R}\}, (a,0) + (b,0) = (a+b, 0), (a,0)(b,0) = (ab, 0)$.

5.6. $P = \{(0, b) \mid b \in \mathbb{R}\}, (0, a) + (0, b) = (0, a + b), (0, a)(0, b) = (0, ab)$.

5.7. $P = \mathbb{Q}$, сложение рациональных чисел, умножение: $a * b = -3ab$.

5.8. $P = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$, сложение и умножение действительных чисел.

5.9. $P = \{\frac{a}{4^{k-1}} \mid a \in \mathbb{Z}, k \in \mathbb{N}\}$, сложение и умножение действительных чисел.

5.10. $P = \{a + b\sqrt{3} \mid a, b \in \mathbb{Q}\}$, сложение и умножение действительных чисел.

5.11. $P = \{\frac{a}{3^{k-1}} \mid a \in \mathbb{Z}, k \in \mathbb{N}\}$, сложение и умножение действительных чисел.

5.12. $P = \{\frac{a}{5^{k-1}} \mid a \in \mathbb{Z}, k \in \mathbb{N}\}$, сложение и умножение действительных чисел.

5.13. $P = \{-\frac{a}{2^{k-1}} \mid a \in \mathbb{Z}, k \in \mathbb{N}\}$, сложение и умножение действительных чисел.

5.14. $P = \{(a, b) \mid a, b \in \mathbb{R}\}, (a, b) + (c, d) = (a, d), (a, b)(c, d) = (ac, bd)$.

5.15. $P = \{a - b\sqrt{3} \mid a, b \in \mathbb{Q}\}$, сложение и умножение действительных чисел.

6. Пусть G — мультипликативная группа, e – единичный элемент, $a, b, c \in G$. Доказать следующие свойства групп:

6.1. $(a^{-1})^{-1} = a$, $(abc)^{-1} = c^{-1}b^{-1}a^{-1}$;

6.2. если $ab = ba$, то $(ab)^k = a^k b^k$ для всех $k \in Z$;

6.3. уравнение $ax = b$ имеет единственное решение $x = a^{-1}b$;

6.4. если $ac = ab$, то $c = b$; если $ca = ba$, то $c = b$.

7. Сформулировать и доказать свойства аддитивных групп, аналогичные свойствам задачи 6.

8. Доказать, что группа G абелева в каждом из следующих случаев:

8.1. $(gh)^2 = g^2h^2$ для всех $g, h \in G$;

8.2. $g^2 = e$ для всех $g \in G$;

8.3. $(gh)^{-1} = g^{-1}h^{-1}$ для всех $g, h \in G$.

9. Сформулировать и доказать утверждения задачи 8 для аддитивной абелевой группы.

10. Пусть $G = \{g_i \mid i \in I\}$ — множество функций. На множестве G введем операцию умножения $(g_i g_j)(x) = g_i(g_j(x))$. Составить таблицу умножения и выяснить, будет ли G группой.

10.1. $g_1(x) = x$; $g_2(x) = \frac{x-1}{x+1}$; $g_3(x) = -\frac{1}{x}$; $g_4(x) = -\frac{x+1}{x-1}$;

10.2. $g_1(x) = x$; $g_2(x) = -x$; $g_3(x) = \frac{1}{x}$; $g_4(x) = -\frac{1}{x}$;

10.3. $g_1(x) = x$; $g_2(x) = \frac{1}{x}$; $g_3(x) = -x$; $g_4(x) = -\frac{1}{x}$; $g_5(x) = \frac{x-1}{x+1}$; $g_6(x) = -\frac{x+1}{x-1}$.

11. Пусть $f : G_1 \to G_2$ — изоморфизм групп G_1 и G_2. Доказать, что:

11.1. если e_1 — единица в G_1, то $f(e_1) = e_2$ — единица в G_2;

11.2. если a^{-1} — обратный к элементу a в G_1, то $f(a^{-1}) = (f(a))^{-1}$ — обратный к $f(a)$ в группе G_2;

11.3. если G_1 абелева, то и G_2 абелева;

11.4. если G_1 конечна, то и G_2 конечна.

12. Сформулировать и доказать свойства, аналогичные свойствам 1 – 4 задачи 11, если:

12.1. G_1 — аддитивная группа, G_2 — мультипликативная группа;

12.2. G_1 и G_2 — аддитивные группы;

12.3. G_1 — мультипликативная, а G_2 — аддитивная группы.

13. Доказать, что группы $(m\mathbb{Z}, +)$ и $(nZ, +)$ изоморфны для любых m и n, принадлежащих $\mathbb{N}$.

14. Доказать, что мультипликативные группы $G_1 = \{-1, 1\}$ и

$$G_2 = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\}$$

изоморфны.

15. Установить изоморфизм между мультипликативной группой $\mathbb{R}_+$ положительных действительных чисел и аддитивной группой $\mathbb{R}$ всех действительных чисел.

16. Пусть a — фиксированный элемент в мультипликативной группе $(G, \cdot)$. На множестве G определим операцию $*$, считая $x * y = xay$. Доказать, что $(G, *)$ — группа и $\varphi : x \mapsto xa^{-1}, x \in G$ — изоморфизм $(G, \cdot)$ на $(G, *)$.

17. Доказать изоморфизм мультипликативных групп:

18.1. $G_1 = \left\{ a + b\sqrt{3} \mid a, b \in \mathbb{Q}, a^2 + b^2 > 0 \right\}$;

$G_2 = \left\{ \begin{pmatrix} a & 3b \\ b & a \end{pmatrix} \mid a, b \in \mathbb{Q}, a^2 + b^2 > 0 \right\}$;

18.2. $G_1 = \{z \in \mathbb{C} \mid \mid z \mid = 1\}$, $G_2 = \left\{ \begin{pmatrix} cos\varphi & sin\varphi \\ -sin\varphi & cos\varphi \end{pmatrix} \mid 0 < \varphi < 2\pi \right\}$

19. Пусть G — конечная группа, на которой действует автоморфизм φ, обладающий следующими свойствами: $\varphi(g) \neq g$ для каждого $g \in G$, $g \neq e, \varphi(\varphi(g)) = g$ для каждого $g \in G$. Доказать, что G абелева.

20. Доказать, что отображение f аддитивной группы комплексных чисел в аддитивную группу действительных чисел такое, что $f : a + bi \mapsto b$ является гомоморфизмом. Найти ядро и образ гомоморфизма.

21. Пусть φ — отображение аддитивной группы $\mathbb{Z}$ в мультипликативную группу $\mathbb{R}^*$ такое, что $\varphi : k \mapsto (-1)^k$. Показать, что φ — гомоморфизм. Найти $Im\varphi$ и $Ker\varphi$.

22. Доказать, что отображение f мультипликативной группы $\mathbb{C}^*$ в мультипликативную группу положительных действительных чисел, такое, что $f : a + bi \mapsto \sqrt{a^2 + b^2}$ является гомоморфизмом. Найти ядро и образ f.

23. Пусть G — абелева группа. Показать, что отображение $f : x \mapsto x^n, x \in G, n$ — фиксированное целое число, является гомоморфизмом. Этот гомоморфизм называется степенным. Показать, что все гомоморфизмы циклической группы G в себя являются степенными.

24. Пусть $f : (n\mathbb{Z}, +) \mapsto (m\mathbb{Z}, +)$ такое отображение, что $f : nk \mapsto rk, k \in \mathbb{Z}$, n, m, r — фиксированные натуральные числа. Доказать, что f — гомоморфизм. Найти ядро и образ f. Будет ли f мономорфизмом, эпиморфизмом, изоморфизмом?

24.1. $n = 1, m = 2, r = 4$; 24.2. $n = 2, m = 3, r = 3$;

24.3. $n = 3.m = 6, r = 12$; 24.4. $n = 1, m = 4, r = 4$;

24.5. $n = 3, m = 2, r = 4$; 24.6. $n = 2, m = 2, r = 6$.

25. Пусть φ — отображение группы $(M, *)$ в группу $(N, \circ)$. Будет ли φ гомоморфизмом? Если φ гомоморфизм, то найти $Im\varphi$ и $Ker\varphi$. Будет ли φ мономорфизмом, эпиморфизмом, изоморфизмом?

25.1. $M = \left\{ \begin{pmatrix} a & 3b \\ b & a \end{pmatrix} \mid a, b \in \mathbb{Q}, a^2 + b^2 > 0 \right\}$,
$N = \{a + b\sqrt{3} \mid a, b \in \mathbb{Q}, a^2 + b^2 > 0\}$,
$*$ и $\circ$ — умножение,
$\varphi : \begin{pmatrix} a & 3b \\ b & a \end{pmatrix} \mapsto a + b\sqrt{3}$;

25.2. $M = \left\{ \begin{pmatrix} a & 2b \\ b & a \end{pmatrix} \mid a, b \in \mathbb{Q} \right\}, N = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}, a^2 + b^2 > 0\}$,
$*$ — сложение, $\circ$ — умножение,
$\varphi : \begin{pmatrix} a & 2b \\ b & a \end{pmatrix} \mapsto a + b\sqrt{2}$;

25.3. $M = \left\{ \begin{pmatrix} a & b \\ b & a \end{pmatrix} \mid a, b \in \mathbb{Q} \right\}, N = 3\mathbb{Z}$,
$*$ и $\circ$ — сложение,
$\varphi : \begin{pmatrix} a & b \\ b & a \end{pmatrix} \mapsto 3a + 3b$;

25.4. $M = \left\{ \begin{pmatrix} a & 2b \\ b & a \end{pmatrix} \mid a, b \in \mathbb{Q}, a^2 + b^2 > 0 \right\}, N = \mathbb{Q}$,
$\circ$ — сложение, $*$ — умножение,
$\varphi : \begin{pmatrix} a & 2b \\ b & a \end{pmatrix} \mapsto a - b$;

25.5. $M = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \mid a, b \in \mathbb{R}^* \right\}, N = \mathbb{R}^*$,
$*$ и $\circ$ — умножение,
$\varphi : \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \mapsto ab$.

26. Какие из отображений $f : \mathbb{C}^* \to \mathbb{R}^*$ являются гомоморфизмами:

26.1. $f(z) = |z|$; $\quad g(z) = 3|z| - 1$;

26.2. $f(z) = \frac{1}{|z|}$; $\quad g(z) = 4$;

26.3. $f(z) = 1 + |z|; \qquad g(z) = |z|^2;$

26.4. $f(z) = \frac{|z|+1}{2}; \qquad g(z) = 1;$

26.5. $f(z) = |z| - 3; \qquad g(z) = 2|z|;$

26.6. $f(z) = \frac{1}{|z|+1}; \qquad g(z) = 3|z|;.$

27. Для каких групп G отображение $f : G \to G$, определенное правилом

27.1. $f(x) = x^2;$ 27.2. $f(x) = x^{-1};$

является гомоморфизмом?

28. При каком условии отображение f группы G в группу G, определенное правилом

28.1. $f(x) = x^2;$ 28.2. $f(x) = x^{-1};$

является изоморфизмом?

29. Докажите, что данные отображения являются гомоморфизмами групп. Найдите ядро и образ.

29.1. $f : (\mathbb{R}, +) \to (\mathbb{R}^*, \cdot), \quad f(a) = e^a, \forall a \in \mathbb{R}$. Здесь e — основание натурального логарифма.

29.2. $f : (\mathbb{R}+, \cdot) \to (\mathbb{R}, +), \quad f(a) = lna, \forall a \in \mathbb{R}^*.$

29.3. $f : (\mathbb{R}^*, \cdot) \to (\mathbb{R}^*, \cdot), f(a) = signa, \forall a \in \mathbb{R}^*.$

29.4. $f : (\mathbb{R}^*, \cdot) \to (\mathbb{R}^*, \cdot), f(a) = |a|, \forall a \in \mathbb{R}^*.$

29.5. $f : (\mathbb{C}^*, \cdot) \to (\mathbb{R}^*, \cdot), f(a) = |a|, \forall a \in \mathbb{C}^*.$

30. Найдите все пары (m, n) целых чисел, при которых отображение

$$x \mapsto mx^n, \quad \forall x \in \mathbb{Q}^*,$$

является эндоморфизмом мультипликативной группы $\mathbb{Q}^*$.

31. Докажите, что аддитивная группа целых чисел не является эпиморфным образом аддитивной группы рациональных чисел.

32. Докажите изоморфизм мультипликативных групп

$$\mathbb{C}^* \simeq \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} | a, b \in \mathbb{R}, a^2 + b^2 > 0 \right\},$$

33. Следующий набор групп разбейте на классы попарно изоморфных групп: $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$, $(\mathbb{C}^*, \cdot)$, $(\mathbb{Z}, +)$, $(m\mathbb{Z}, +)$, $m \in \mathbb{N}$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$.

34. Докажите, что группа автоморфизмов группы S_3 изоморфна S_3.

35. Докажите, что группа автоморфизмов группы S_4 изоморфна S_4.

36. Пусть G — абелева группа и $f(a) = a^2$, $\forall a \in G$. Будет ли $f : G \to G$ гомоморфизмом, мономорфизмом, автоморфизмом?

37. Пусть G и H — группы взаимно простых порядков и отображение $f : G \to H$ — гомоморфизм. Докажите, что $Kerf = G$.

38. Пусть $(G, \cdot)$ — мультипликативная группа и $t \in G$ — фиксированный элемент. На множестве G введем новую операцию $*$ полагая $a*b = atb$. Докажите, что $(G, *)$ — группа, изоморфная группе $(G, \cdot)$.

39. Найдите все изоморфизмы групп $(\mathbb{Z}_4, +)$ и $(\mathbb{Z}_5, \cdot)$.

40. Зафиксируем рациональное число $t \neq 0$. Докажите, что отображение $f : x \mapsto xt$, $\forall x \in \mathbb{Q}$, является автоморфизмом аддитивной группы $(\mathbb{Q}, +)$.

5.2. Практикум по теме «Поле С»

5.2.1. Примеры решения задач

Пример 5.2.1. Даны комплексные числа $z_1 = 2 - 3i$ и $z_2 = -1 - i$. Вычислите $z_1 + z_2$, $z_1 - z_2$, $z_1 \cdot z_2$, z_1/z_2.

Доказательство. При сложении комплексных чисел в алгебраической форме складываются их действительные части и коэффициенты при i:

$$z_1 + z_2 = (2 - 3i) + (-1 - i) = (2 - 1) + (-3 - 1)i = 1 - 4i.$$

При вычитании комплексных чисел в алгебраической форме вычитаются их действительные части и коэффициенты при i:

$$z_1 - z_2 = (2 - 3i) - (-1 - i) = (2 + 1) + (-3 + 1)i = 3 - 2i.$$

Для того чтобы перемножить два комплексных числа, надо перемножить их как двучлены, а затем заменить i^2 на -1:

$$z_1 \cdot z_2 = (2-3i)(-1-i) = -2+3i-2i+3i^2 =$$
$$= (-2-3)+(3-2)i = -5+i.$$

Для вычисления частного умножим делимое и делитель на число, сопряженное делителю:

$$\frac{z_1}{z_2} = \frac{2-3i}{-1-i} = \frac{(2-3i)(-1+i)}{(-1-i)(-1+i)} =$$
$$= \frac{-2+3i+2i-3i^2}{(-1)^2-i^2} = \frac{1+5i}{2} = \frac{1}{2}+\frac{5}{2}i.$$

О т в е т: $z_1+z_2 = 1-4i$, $z_1-z_2 = 3-2i$, $z_1 \cdot z_2 = -5+i$, $z_1/z_2 = 1/2+(5/2)i$. □

Пример 5.2.2. Вычислите $(3+2i)/(7-2i)$, $\big((1-2i)/(1+2i)\big)^3$.

Доказательство. Для вычисления $(3+2i)/(7-2i)$ умножим числитель и знаменатель на число, сопряженное знаменателю:

$$\frac{3+2i}{7-2i} \cdot \frac{7+2i}{7+2i} = \frac{(21-4)+(6+14)i}{7^2-(2i)^2} = \frac{17}{53}+\frac{20}{53}i.$$

Для возведения в куб числа $(1-2i)/(1+2i)$ вначале вычислим:

$$\frac{1-2i}{1+2i} \cdot \frac{1-2i}{1-2i} = \frac{(1-2i)^2}{1^2-(2i)^2} = \frac{1-4i-4}{1+4} = \frac{-3}{5}-\frac{4}{5}i.$$

Теперь имеем:

$$\left(\frac{1+2i}{1-2i}\right)^3 = \left(\frac{-3}{5}-\frac{4}{5}i\right)^3 = \frac{-1}{5^3}(3+4i)^3 = \frac{-1}{5^3}(27+108i-$$

$$-144-64i) = \frac{-1}{5^3}(-117+44i) = \frac{117}{125}-\frac{44}{125}i.$$ □

Пример 5.2.3. Вычислите $\sqrt{6+8i}$.

Доказательство. По определению (2.3.2) имеем $\sqrt{6+8i} = \pm(\sqrt{8}+i\sqrt{2})$.

П р о в е р к а: $\left(\pm(\sqrt{8}+i\sqrt{2})\right)^2 = 8-2+2\sqrt{8}\sqrt{2}i = 6+8i$.

О т в е т: $\pm(\sqrt{8}+i\sqrt{2})$. □

Пример 5.2.4. Вычислите $\sqrt{1-i}$.

Доказательство. Пусть $\sqrt{1-i} = x+yi$, где $x, y \in \mathbb{R}$. Возводя обе части равенства в квадрат, получим $1-i = (x^2-y^2)+2xyi$. Из условия равенства комплексных чисел имеем:

$$\begin{cases} x^2-y^2 = 1 \\ 2xy = -1. \end{cases}$$

Возводя оба уравнения в квадрат и складывая их, получим:

$$x^4+2x^2y^2+y^4 = 2,$$

откуда $(x^2+y^2)^2 = 2$ или $x^2+y^2 = \sqrt{2}$. Теперь из системы

$$\begin{cases} x^2+y^2 = \sqrt{2} \\ x^2-y^2 = 1, \end{cases}$$

находим $x^2 = (\sqrt{2}+1)/2$, $y^2 = (\sqrt{2}-1)/2$. Второе уравнение $2xy = -1$ первоначальной системы указывает, что числа x и y имеют разные знаки. Поэтому исходная система имеет два решения:

$$x_1 = \sqrt{\frac{\sqrt{2}+1}{2}},\ y_1 = -\sqrt{\frac{\sqrt{2}-1}{2}},$$

$$x_2 = -\sqrt{\frac{\sqrt{2}+1}{2}},\ y_2 = \sqrt{\frac{\sqrt{2}-1}{2}}.$$

О т в е т: $\sqrt{1-i} = \pm\left(\sqrt{\frac{\sqrt{2}+1}{2}} - i\sqrt{\frac{\sqrt{2}-1}{2}}\right)$. □

Пример 5.2.5. Найдите действительные решения уравнения

$$(5-8i)x+(7+3i)y=2-i.$$

Доказательство. Преобразуя левую часть уравнения и используя условие равенства комплексных чисел $(5x+7y)+(-8x+3y)i=2-i$, получим систему

$$\begin{cases} 5x+7y=2 \\ -8x+3y=-1, \end{cases}$$

откуда находим $x=13/71$, $y=11/71$.

О т в е т: $x=13/71$, $y=11/71$. □

Пример 5.2.6. В поле $\mathbb{C}$ решите уравнение $x^2+x+1=0$.

Доказательство. Уравнение $x^2+x+1=0$ не имеет действительных корней, поскольку дискриминант $D=1^2-4\cdot 1\cdot 1=-3<0$. Но оно имеет комплексные корни:

$$x_1=\frac{-1+i\sqrt{3}}{2},\ x_2=\frac{-1-i\sqrt{3}}{2}.$$

О т в е т: $x_{1,2}=(-1\pm i\sqrt{3})/2$. □

Пример 5.2.7. В поле $\mathbb{C}$ решите квадратное уравнение

$$z^2-(2+4i)z+(-9/2+2i)=0.$$

Доказательство. Находим дискриминант $D=v^2-4uw=6+8i$. Получаем:

$$z_1=\frac{2+4i+\sqrt{8}+i\sqrt{2}}{2}=1+\sqrt{2}+(2+\sqrt{2}/2)i,$$

$$z_2=\frac{2+4i-(\sqrt{8}+i\sqrt{2})}{2}=1-\sqrt{2}+(2-\sqrt{2}/2)i.$$

О т в е т: $z_{1,2}=1\pm\sqrt{2}+(2\pm\sqrt{2}/2)i$. □

Пример 5.2.8. Решите уравнение

$$(2+i)x^2-(5-i)x+(2-2i)=0.$$

Доказательство. По формуле корней квадратного уравнения находим:

$$x_{1,2}=\frac{(5-i)\pm\sqrt{(5-i)^2-4(2+i)(2-2i)}}{2(2+i)}=$$

$$=\frac{(5-i)\pm\sqrt{-2i}}{4+2i}.$$

Так как $\sqrt{-2i}=\pm(1-i)$, то

$$x_1=\frac{(5-i)+(1-i)}{4+2i}=\frac{6-2i}{4+2i}=1-i,$$

$$x_2=\frac{(5-i)-(1-i)}{4+2i}=\frac{4}{4+2i}=\frac{2}{2+i}=\frac{4}{5}-\frac{2}{5}i.$$

О т в е т: $x_1=1-i$, $x_2=4/5-(2/5)i$. □

Пример 5.2.9. Представьте в тригонометрической форме числа: $z_1=\sqrt{3}-i$, $z_2=-5$, $z_3=-3(\cos(\pi/5)-i\sin(\pi/5))$.

Доказательство. Изобразим числа z_1, z_2 на плоскости (см. рис. 1). Для комплексного числа $z_1=\sqrt{3}-i$ согласно формулам 2.5.6 имеем:

$$|z_1|=\sqrt{(\sqrt{3})^2+(-1)^2}=2,\ \sin\varphi=-\frac{1}{2},\ \cos\varphi=\frac{\sqrt{3}}{2},\ \varphi=-\frac{\pi}{6}.$$

Значит

$$z_1=\sqrt{3}-i=2\left(\cos\left(-\frac{\pi}{6}\right)+i\sin\left(-\frac{\pi}{6}\right)\right).$$

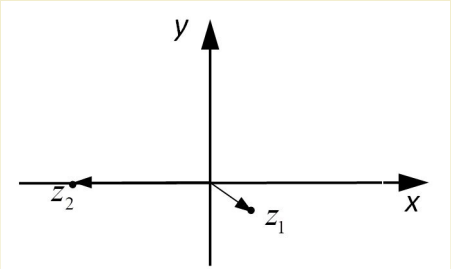


Рис. 1

Для комплексного числа $z_2 = -5$ имеем: $|z_2| = 5$, $\varphi = \pi$ и

$$z_2 = -5 = 5(\cos\pi + i\sin\pi).$$

Комплексное число $z_3 = -3(\cos(\pi/5) - i\sin(\pi/5))$ записано не в тригонометрической форме, так как отрицательное число -3 нельзя считать модулем z_3. Кроме того, коэффициент при i равен $-\sin(\pi/5)$, а в тригонометрической форме мнимая часть должна быть записана так: $i\sin\varphi$. Представим число z_3 в виде $z_3 = 3(-\cos(\pi/5) + i\sin(\pi/5))$. Отсюда заключим, что аргументом комплексного числа z_3 является такой угол φ, для которого $\cos\varphi = -\cos(\pi/5)$, а $\sin\varphi = \sin(\pi/5)$. Этот угол легко найти: $\varphi = \pi - (\pi/5) = (4/5)\pi$. Итак, искомое представление в тригонометрической форме: $z_3 = 3(\cos(4/5)\pi + i\sin(4/5)\pi)$.

О т в е т: $z_1 = 2(\cos(-\pi/6) + i\sin(-\pi/6))$, $z_2 = 5(\cos\pi + i\sin\pi)$, $z_3 = 3(\cos(4/5)\pi + i\sin(4/5))$. □

Пример 5.2.10. Изобразите на плоскости и запишите в тригонометрической форме числа

$$z_1 = -2i,\ z_2 = -1 + i\sqrt{3},\ z_3 = 1 - i.$$

Доказательство. Откладывая действительную часть комплексного числа на оси OX, а коэффициент при i — на оси OY, получим точки на координатной плоскости, соответствующие числам z_1, z_2, z_3 (см. рис. 2).

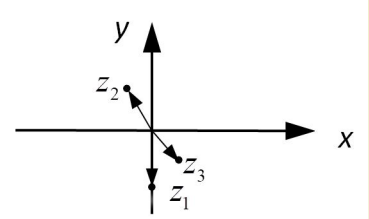


Рис. 2

Так как точка, соответствующая числу z_1, лежит на координатной оси OY, то модуль и аргумент числа z_1 легко определить по рис. 3: $|z_1| = 2$, $\arg z_1 = (3/2)\pi$. Следовательно, тригонометрическая форма числа z_1 имеет вид:

$$z_1 = 2\left(\cos\frac{3\pi}{2} + i\sin\frac{3\pi}{2}\right).$$

Для нахождения тригонометрической формы комплексного числа $z_2 = a + bi$ воспользуемся формулами модуля и аргумента комплексного числа. Определяем $|z_2| = \sqrt{(-1)^2 + (\sqrt{3})^2} = 2$. Так как точка, соответствующая комплексному числу z_2, лежит во второй четверти, то $x < 0$ и

$$\arg z_2 = \pi + \operatorname{arctg}(-\sqrt{3}) = \pi - \frac{\pi}{3} = \frac{2\pi}{3}.$$

Получаем следующую тригонометрическую форму:

$$z_2 = 2\left(\cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3}\right).$$

Определяем $|z_3| = \sqrt{1^2 + (-1)^2} = \sqrt{2}$. Так как точка, соответствующая комплексному числу z_3, лежит в четвертой четверти, то $x > 0$ и

$$\arg z_3 = \operatorname{arctg}(-1) = -\frac{\pi}{4}.$$

Тригонометрическая форма принимает вид:

$$z_3 = \sqrt{2}\left(\cos\left(-\frac{\pi}{4}\right) + i\sin\left(-\frac{\pi}{4}\right)\right).$$

О т в е т: $z_1 = 2(\cos(3\pi/2) + i\sin(3\pi/2))$, $z_2 = 2(\cos(2\pi/3) + i\sin(2\pi/3))$, $z_3 = \sqrt{2}(\cos(-\pi/4) + i\sin(-\pi/4))$. □

Пример 5.2.11. Изобразите на плоскости множество решений системы неравенств

$$\begin{cases} 1 \le |z| \le 3 \\ -\frac{\pi}{4} < \arg z < \frac{\pi}{2}. \end{cases}$$

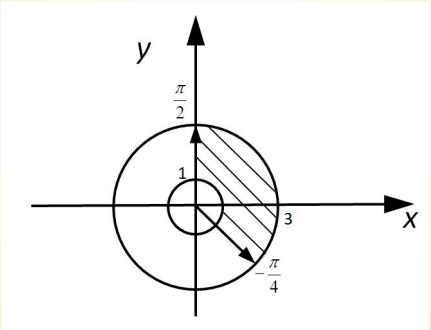


Рис. 3

Доказательство. Точки, изображающие решения первого неравенства, лежат между окружностями радиусов 1 и 3 с центром в начале координат, включая сами окружности. Точки, изображающие решения второго неравенства, лежат между лучами OA и OB, не включая эти лучи. Искомая область является пересечением этих двух фигур и выделена на рис. 3. □

Пример 5.2.12. Вычислите $z_1z_2z_3$, $(z_1z_2)/z_3$ и z_1^{-1}, где z_1, z_2 и z_3 — комплексные числа из примера 5.2.9.

Доказательство.

$$z_1z_2z_3 = 2\cdot 5\cdot 3(\cos(-\frac{\pi}{6}+\pi+\frac{4\pi}{5})+i\sin(-\frac{\pi}{6}+\pi+\frac{4\pi}{5}) =$$

$$= 30(\cos(\tfrac{49\pi}{30})+i\sin(\tfrac{49\pi}{30}),$$

$$(z_1z_2)/z_3 = ((2\cdot 5)/3)(\cos(-\pi/6+\pi-(4/5)\pi)+i\sin(-\pi/6+\pi-(4/5)\pi)) =$$

$$= (10/3)(\cos(\pi/30)+i\sin(\pi/30)),$$

$$z_1^{-1} = (1/2)(\cos(\pi/6)+i\sin(\pi/6)).$$

□

Пример 5.2.13. Вычислите

$$A = \frac{3(\cos 20^\circ - i\sin 20^\circ)\cdot 2(\cos 230^\circ - i\sin 130^\circ)}{-\sin 210^\circ - i\cos 210^\circ}.$$

Доказательство. Используя формулы приведения и свойства тригонометрических функций, преобразуем комплексные числа к тригонометрической форме:

$$A = \frac{3(\cos(-20^\circ)+i\sin(-20^\circ))2(\cos 230^\circ + i\sin(360^\circ-130^\circ))}{-\sin(270^\circ-60^\circ)-i\cos(270^\circ-60^\circ)} =$$

$$= \frac{3(\cos(-20^\circ)+i\sin(-20^\circ))2(\cos 230^\circ + i\sin 230^\circ)}{\cos 60^\circ + i\sin 60^\circ}.$$

Теперь, применяя правила умножения и деления комплексных чисел в тригонометрической форме, вычислим:

$$A = \frac{3 \cdot 2(\cos(-20^\circ + 230^\circ) + i\sin(-20^\circ + 230^\circ))}{\cos 60^\circ + i\sin 60^\circ} =$$

$$= 6(\cos(210^\circ - 60^\circ) + i\sin(210^\circ - 60^\circ)) = 6(\cos 150^\circ + i\sin 150^\circ) =$$

$$= 6(\cos(180^\circ - 30^\circ) + i\sin(180^\circ - 30^\circ)) = 6(-\cos 30^\circ + i\sin 30^\circ) =$$

$$= 6\left(-\frac{\sqrt{3}}{2} + i\frac{1}{2}\right) = -3\sqrt{3} + 3i.$$

О т в е т: $A = -3\sqrt{3} + 3i$. □

Пример 5.2.14. Вычислите $(z_1 z_3)^{30}$, где z_1 и z_3 — комплексные числа из примера 5.2.9.

Доказательство. Имеем: $(z_1 z_3)^{30} = (2 \cdot 3)^{30} \times (\cos 30(-\pi/6 + (4/5)\pi) + i\sin 30(-\pi/6 + (4/5)\pi)) = 6^{30}(\cos 19\pi + i\sin 19\pi) = 6^{30}(\cos\pi + i\sin\pi) = -6^{30}$. □

Пример 5.2.15. *Вычислите* $\sqrt[3]{-5}$.

Доказательство. Число (-5) в тригонометрической форме записывается так: $-5 = 5(\cos\pi + i\sin\pi)$. По формуле (2.6.10) имеем:

$$c_k = \sqrt[3]{-5} = \sqrt[3]{5}\left(\cos\frac{\pi + 2\pi k}{3} + i\sin\frac{\pi + 2\pi k}{3}\right), \quad k = 0, 1, 2.$$

Отсюда $c_0 = \sqrt[3]{5}\left(\cos(\pi/3) + i\sin(\pi/3)\right) = (\sqrt[3]{5}/2)(1 + i\sqrt{3})$,

$$c_1 = \sqrt[3]{5}(\cos\pi + i\sin\pi) = -\sqrt[3]{5},$$

$$c_2 = \sqrt[3]{5}(\cos(5/3)\pi + i\sin(5/3)\pi) = (\sqrt[3]{5}/2)(1 - i\sqrt{3}).$$ □

Пример 5.2.16. Вычислите $(-1+i\sqrt{3})^6$, $\sqrt[4]{-1+i\sqrt{3}}$.

Доказательство. В примере (5.2.10) найдена тригонометрическая форма комплексного числа $-1+i\sqrt{3}$, а именно: $-1+i\sqrt{3}=2(\cos(2\pi/3)+i\sin(2\pi/3))$. Из формулы Муавра 2.6.9 при $n=6$ имеем:

$$(-1+i\sqrt{3})^6=\Big(2\Big(\cos\frac{2\pi}{3}+i\sin\frac{2\pi}{3}\Big)\Big)^6=$$

$$=2^6\Big(\cos\frac{6\cdot 2\pi}{3}+i\sin\frac{6\cdot 2\pi}{3}\Big)=64(\cos 4\pi+i\sin 4\pi)=$$

$$=64(\cos 0+i\sin 0)=64.$$

Для извлечения корня из комплексного числа используем формулу

$$\sqrt[n]{r(\cos\varphi+i\sin\varphi)}=\sqrt[n]{r}\Big(\cos\frac{\varphi+2\pi k}{n}+i\sin\frac{\varphi+2\pi k}{n}\Big),$$

где $k=0,1,\ldots,n-1$. Поскольку $n=4$, то

$$z_k=\sqrt[4]{-1+i\sqrt{3}}=\sqrt[4]{2(\cos\frac{2\pi}{3}+i\sin\frac{2\pi}{3})}=$$

$$=\sqrt[4]{2}\Big(\cos\frac{2\pi/3+2\pi k}{4}+i\sin\frac{2\pi/3+2\pi k}{4}\Big).$$

Полагая $k=0,1,2,3$, получим:

$$z_0=\sqrt[4]{2}\Big(\cos\tfrac{\pi}{6}+i\sin\tfrac{\pi}{6}\Big)=\tfrac{\sqrt[4]{2}\cdot\sqrt{3}}{2}+i\tfrac{\sqrt[4]{2}}{2},$$

$$z_1=\sqrt[4]{2}\Big(\cos\tfrac{2\pi}{3}+i\sin\tfrac{2\pi}{3}\Big)=-\tfrac{\sqrt[4]{2}}{2}+i\tfrac{\sqrt[4]{2}\cdot\sqrt{3}}{2},$$

$$z_2=\sqrt[4]{2}\Big(\cos\tfrac{7\pi}{6}+i\sin\tfrac{7\pi}{6}\Big)=-\tfrac{\sqrt[4]{2}\cdot\sqrt{3}}{2}-i\tfrac{\sqrt[4]{2}}{2},$$

$$z_3=\sqrt[4]{2}\Big(\cos\tfrac{5\pi}{3}+i\sin\tfrac{5\pi}{3}\Big)=\tfrac{\sqrt[4]{2}}{2}-i\tfrac{\sqrt[4]{2}\cdot\sqrt{3}}{2}.$$

□

Пример 5.2.17. Вычислите $\sqrt[n]{1}$ при $n \leq 4$.

Доказательство. При $n = 2$ имеем два корня: $\varepsilon_0 = 1$, $\varepsilon_1 = -1$. Множество $\{-1, 1\}$ с умножением является циклической группой $\langle -1 \rangle$ порядка 2.

При $n = 3$ имеем три корня:

$$\varepsilon_0 = 1,\ \varepsilon_1 = \cos\frac{2}{3}\pi + i\sin\frac{2}{3}\pi = -\frac{1}{2} + i\frac{\sqrt{3}}{2},$$

$$\varepsilon_2 = \cos\frac{4}{3}\pi + i\sin\frac{4}{3}\pi = -\frac{1}{2} - i\frac{\sqrt{3}}{2}.$$

Множество

$$\left\{-\frac{1}{2} + i\frac{\sqrt{3}}{2},\ -\frac{1}{2} - i\frac{\sqrt{3}}{2},\ 1\right\}$$

с умножением является циклической группой $\langle -1/2 + \sqrt{3}i/2 \rangle$ порядка 3, порожденной элементом $-1/2 + \sqrt{3}i/2$. Составим таблицу умножения для этих корней.

	1	$-\frac{1}{2} + i\frac{\sqrt{3}}{2}$	$-\frac{1}{2} - i\frac{\sqrt{3}}{2}$
1	1	$-\frac{1}{2} + i\frac{\sqrt{3}}{2}$	$-\frac{1}{2} - i\frac{\sqrt{3}}{2}$
$-\frac{1}{2} + i\frac{\sqrt{3}}{2}$	$-\frac{1}{2} + i\frac{\sqrt{3}}{2}$	$-\frac{1}{2} - i\frac{\sqrt{3}}{2}$	1
$-\frac{1}{2} - i\frac{\sqrt{3}}{2}$	$-\frac{1}{2} - i\frac{\sqrt{3}}{2}$	1	$-\frac{1}{2} + i\frac{\sqrt{3}}{2}$

В частности,

$$\left(-\frac{1}{2} - i\frac{\sqrt{3}}{2}\right)^{-1} = -\frac{1}{2} + i\frac{\sqrt{3}}{2},$$

$$\left(-\frac{1}{2} + i\frac{\sqrt{3}}{2}\right)^{-1} = -\frac{1}{2} - i\frac{\sqrt{3}}{2}.$$

При $n = 4$ имеем четыре корня:

$$\varepsilon_0 = 1, \quad \varepsilon_1 = \cos\frac{2}{4}\pi + i\sin\frac{2}{4}\pi = i,$$

$$\varepsilon_2 = \cos\pi + i\sin\pi = -1, \quad \varepsilon_3 = \cos\frac{6}{4}\pi + i\sin\frac{6}{4}\pi = -i.$$

Множество $\{i, -1, -i, 1\}$ с умножением является циклической группой $\langle i \rangle$ порядка 4, порожденной элементом i. Составим таблицу умножения для этих корней.

	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	i
$-i$	$-i$	1	i	-1

В частности, $i^{-1} = -i$, $(-1)^{-1} = -1$, $(-i)^{-1} = i$. □

Пример 5.2.18. Укажите первообразные корни четвертой степени из единицы.

Доказательство. Преобразными корнями четвертой степени из единицы будут корни: $\varepsilon_1 = i$ и $\varepsilon_3 = -i$. □

5.2.2. Индивидуальные задания

1. Найдите $z_1 + z_2$, $z_1 - z_2$, $z_1 \cdot z_2$, z_1/z_2.
   - 1.1. $z_1 = 2 + i$, $z_2 = -3 - 2i$.
   - 1.2. $z_1 = -1 + 3i$, $z_2 = 2 - i$.
   - 1.3. $z_1 = 4 - i$, $z_2 = 1 + 3i$.
   - 1.4. $z_1 = -1 + 4i$, $z_2 = 2 - 3i$.
   - 1.5. $z_1 = 3 - i$, $z_2 = -2 + 3i$.
   - 1.6. $z_1 = -4 + i$, $z_2 = 2 - i$.

1.7. $z_1 = 1 - 3i$, $z_2 = -2 + i$.
1.8. $z_1 = 4 - 3i$, $z_2 = -2 + 5i$.
1.9. $z_1 = 2 - 4i$, $z_2 = 3 + i$.
1.10. $z_1 = -3 + 2i$, $z_2 = 5 - i$.
1.11. $z_1 = -2 - 5i$, $z_2 = -1 + i$.
1.12. $z_1 = -4 + 3i$, $z_2 = 6 - i$.
1.13. $z_1 = 5 - 2i$, $z_2 = 3 + 4i$.
1.14. $z_1 = -1 - 2i$, $z_2 = 4 + 3i$.
1.15. $z_1 = 6 - 4i$, $z_2 = 4 + i$.

2. Найдите действительные значения x и y из уравнения $z_1 \cdot x + z_2 \cdot y = 2 - 5i$, где z_1 и z_2 — числа из задания 1.

3. Вычислите $\sqrt{z_1}$ и $\sqrt{z_2}$ в алгебраической форме для чисел z_1 и z_2 из задания 1.

4. Решите уравнения.

4.1. $x^2 - (2+i)x + 7i - 1 = 0$, $x^2 - 4x + 5 = 0$.
4.2. $x^2 - (3-2i)x + 5 - 5i = 0$, $x^2 - 3x + 4 = 0$.
4.3. $x^2 - (5-3i)x + 2 - 6i = 0$, $2x^2 - 3x + 5 = 0$.
4.4. $x^2 + (2i-7)x + 13 - i = 0$, $x^2 + 3x + 6 = 0$.
4.5. $x^2 - (1+i)x + 6 + 3i = 0$, $3x^2 - 2x + 3 = 0$.
4.6. $x^2 - 5x + 4 + 10i = 0$, $-2x^2 + x - 1 = 0$.
4.7. $(1-i)x^2 + (5-i)x + 4 + 2i = 0$, $-x^2 + 2x - 2 = 0$.
4.8. $(3+i)x^2 + (1-i)x - 6i = 0$, $x^2 + x + 2 = 0$.
4.9. $x^2 - (7+i)x + 16 + 11i = 0$, $3x^2 - 2x + 4 = 0$.
4.10. $x^2 - (3+2i)x + 5i + 5 = 0$, $-2x^2 + 3x - 2 = 0$.
4.11. $x^2 + (5i-1)x - 8 - i = 0$, $3x^2 + 5x + 3 = 0$.
4.12. $x^2 + (4i-3)x - 7 - i = 0$, $2x^2 - 4x + 5 = 0$.
4.13. $x^2 - (3-3i)x + 6 - 2i = 0$, $x^2 - 2x + 5 = 0$.
4.14. $x^2 - (5-6i)x + 1 - 13i = 0$, $x^2 + 3x + 5 = 0$.
4.15. $x^2 - 3x + 11 - 3i = 0$, $x^2 + 5x + 7 = 0$.

5. Изобразите на плоскости и запишите в тригонометрической форме числа z_1 и z_2.

5.1. $z_1 = 1 - i$, $z_2 = -2i$.
5.2. $z_1 = 3i$, $z_2 = -1 + i\sqrt{3}$.
5.3. $z_1 = 2 + 2i$, $z_2 = -3$.
5.4. $z_1 = -\sqrt{3} + i$, $z_2 = -i$.
5.5. $z_1 = \sqrt{12} - 2i$, $z_2 = 2i$.
5.6. $z_1 = -4$, $z_2 = 1 + i$.
5.7. $z_1 = 1$, $z_2 = -\sqrt{12} + 2i$.
5.8. $z_1 = -1 + i$, $z_2 = -i$.
5.9. $z_1 = -1 - i$, $z_2 = 6i$.
5.10. $z_1 = 1 + i\sqrt{3}$, $z_2 = -2$.
5.11. $z_1 = -3i$, $z_2 = -\sqrt{3} - i$.
5.12. $z_1 = -2 - i\sqrt{12}$, $z_2 = -1$.
5.13. $z_1 = 2$, $z_2 = -1 - i\sqrt{3}$.
5.14. $z_1 = \sqrt{12} + 2i$, $z_2 = -6i$.
5.15. $z_1 = 5i$, $z_2 = -\sqrt{3} - i$.

6. Вычислите.

6.1. $5(\cos 350^\circ - i\sin(-10^\circ)) \cdot 2(\cos 80^\circ - i\sin 280^\circ)$.
6.2. $3(\cos 50^\circ - i\sin 670^\circ) \cdot 4(\cos 290^\circ + i\sin 70^\circ)$.
6.3. $\dfrac{2(\cos 220^\circ + i\sin 140^\circ)}{\sin 40^\circ - i\cos 220^\circ}$.
6.4. $3(\cos 230^\circ - i\sin 130^\circ) \cdot 4(\sin 50^\circ + i\cos(-50^\circ))$.
6.5. $\dfrac{2(\cos(-13\pi/7) + i\sin(6\pi/7))}{6(\cos(-13\pi/7) - i\sin(6\pi/7))}$.
6.6. $3(\cos\frac{3\pi}{4} - i\sin\frac{7\pi}{4}) \cdot (\cos\frac{7\pi}{4} - i\cos\frac{3\pi}{4})$.
6.7. $\dfrac{5(\cos 49^\circ - i\sin 229^\circ)}{3(\cos 41^\circ - i\cos 49^\circ)}$.

6.8. $3(\cos 340^\circ - i\sin 20^\circ) \cdot 2(-\sin 70^\circ - i\sin 160^\circ)$.

6.9. $\dfrac{2(\cos 430^\circ + i\cos 160^\circ)}{5(\cos 110^\circ - i\sin 250^\circ)}$.

6.10. $5(-\cos\frac{\pi}{3} - i\sin\frac{4\pi}{3}) \cdot 4(\cos\frac{5\pi}{3} - i\sin\frac{\pi}{3})$.

6.11. $\dfrac{6(\cos 42^\circ + i\sin 222^\circ)}{5(\sin 42^\circ + i\sin 132^\circ)}$.

6.12. $(\cos\frac{7\pi}{4} - i\sin\frac{\pi}{4}) \cdot 3(\cos\frac{7\pi}{4} - i\sin\frac{3\pi}{4})$.

6.13. $\dfrac{3(-\sin 20^\circ - i\sin 110^\circ)}{\cos(-220^\circ) - i\sin 140^\circ}$.

6.14. $7(-\sin 40^\circ - i\sin 130^\circ) \cdot 3(\cos 40^\circ - i\sin 320^\circ)$.

6.15. $\dfrac{3(\cos 190^\circ - i\sin 170^\circ)}{-\sin 40^\circ + i\sin 50^\circ}$.

7. Изобразите на плоскости множество комплексных чисел, удовлетворяющих системе неравенств.

7.1. $\begin{cases} 2 \le |z| \le 4 \\ \frac{\pi}{2} \le \arg\left(\frac{z}{1+i}\right) \le \pi. \end{cases}$

7.2. $\begin{cases} 1 < \left|\frac{z}{1+i\sqrt{3}}\right| < 2 \\ -\frac{\pi}{4} \le \arg z \le \frac{\pi}{2}. \end{cases}$

7.3. $\begin{cases} 1 < |z| < 3 \\ \frac{\pi}{4} \le \arg\left(\frac{z}{1-i}\right) \le \frac{3\pi}{4}. \end{cases}$

7.4. $\begin{cases} 1 \le \left|\frac{z}{\sqrt{12}-2i}\right| \le 2 \\ -\frac{\pi}{2} \le \arg z \le \pi. \end{cases}$

7.5. $\begin{cases} 2 \le |z| + 1 \le 3 \\ \frac{\pi}{3} \le \arg\left(\frac{z}{1-i\sqrt{3}}\right) \le \frac{5\pi}{6}. \end{cases}$

7.6. $\begin{cases} 2 < \left|\frac{z}{-1-i\sqrt{3}}\right| < 3 \\ \frac{\pi}{3} \le \arg z - \frac{\pi}{6} \le \frac{\pi}{2}. \end{cases}$

7.7. $\begin{cases} 3 \le |z| \le 5 \\ \frac{\pi}{4} < \arg\left(\frac{z}{-1-i}\right) < \frac{\pi}{2}. \end{cases}$

7.8. $\begin{cases} 1 \le \left|\frac{z}{2-i\sqrt{12}}\right| \le 3 \\ -\frac{\pi}{6} < \arg z < \frac{\pi}{2}. \end{cases}$

7.9. $\begin{cases} 1 \le \left|\frac{z}{1+\sqrt{3}}\right| \le 3 \\ -\frac{\pi}{4} < \arg z < \frac{3\pi}{4}. \end{cases}$

7.10. $\begin{cases} 1 < |z| < 5 \\ -\frac{\pi}{4} \le \arg\left(\frac{z}{\sqrt{12}-2i}\right) \le \frac{\pi}{3}. \end{cases}$

7.11. $\begin{cases} 2 < \left|\frac{z}{-1-i\sqrt{3}}\right| < 3 \\ -\frac{\pi}{3} \le \arg z \le \frac{\pi}{3}. \end{cases}$ 7.12. $\begin{cases} 2 \le |z| \le 6 \\ \frac{\pi}{2} < \arg\left(\frac{z}{1-i\sqrt{3}}\right) < \pi. \end{cases}$

7.13. $\begin{cases} 1 \le \left|\frac{z}{\sqrt{3}-i}\right| \le 4 \\ -\frac{\pi}{4} < \arg z < \frac{3\pi}{4}. \end{cases}$ 7.14. $\begin{cases} 2 < |z| < 3 \\ -\frac{\pi}{4} \le \arg\left(\frac{z}{1-i}\right) \le \pi. \end{cases}$

7.15. $\begin{cases} 2 \le \left|\frac{z}{\sqrt{3}-i}\right| \le 4 \\ -\frac{\pi}{3} < \arg\left(\frac{z}{2-i\sqrt{12}}\right) < \frac{\pi}{4}. \end{cases}$

8. Вычислите.

8.1. $(-1-i\sqrt{3})^{30}$, $\sqrt[5]{-\sqrt{12}+2i}$, $\sqrt[3]{-8}$.

8.2. $(1-i)^{40}$, $\sqrt[4]{-\sqrt{12}-2i}$, $\sqrt[4]{-16}$.

8.3. $(-\sqrt{3}+i)^{36}$, $\sqrt[6]{-2-i\sqrt{12}}$, $\sqrt[4]{i}$.

8.4. $(-1-i)^{24}$, $\sqrt[5]{1-i\sqrt{3}}$, $\sqrt[3]{-1}$.

8.5. $(-1+i\sqrt{3})^{30}$, $\sqrt[4]{-16-16i}$, $\sqrt[3]{-2}$.

8.6. $(-\sqrt{3}-i)^{42}$, $\sqrt[5]{-2+i\sqrt{12}}$, $\sqrt[3]{3i}$.

8.7. $(1-i)^{24}$, $\sqrt[6]{-1-i\sqrt{3}}$, $\sqrt[4]{-2i}$.

8.8. $(-\frac{1}{2}-i\frac{\sqrt{3}}{2})^{36}$, $\sqrt[4]{\sqrt{12}+2i}$, $\sqrt[5]{-4}$.

8.9. $(-\sqrt{12}+2i)^{48}$, $\sqrt[5]{3-i3\sqrt{3}}$, $\sqrt[4]{-81}$.

8.10. $(-4-4i)^{20}$, $\sqrt[6]{-\sqrt{12}+2i}$, $\sqrt[3]{-8i}$.

8.11. $(1-i\sqrt{3})^{54}$, $\sqrt[4]{-5+5i}$, $\sqrt[6]{64}$.

8.12. $(\sqrt{12}+2i)^{48}$, $\sqrt[5]{1-i}$, $\sqrt[4]{-4}$.

8.13. $(-1+i)^{28}$, $\sqrt[6]{\sqrt{3}-i}$, $\sqrt[3]{8i}$.

8.14. $(\frac{\sqrt{3}}{3}-\frac{1}{3}i)^{30}$, $\sqrt[4]{-\sqrt{3}-i}$, $\sqrt[6]{-1}$.

8.15. $(2-i\sqrt{12})^{36}$, $\sqrt[5]{3-3i}$, $\sqrt[4]{-9}$.

9. Для чисел $z, z_1, z_2 \in \mathbb{C}$ докажите следующие равенства:

9.1. $\bar{z}_1 + \bar{z}_2 = \overline{z_1 + z_2}$. 9.2. $\bar{z}_1 \cdot \bar{z}_2 = \overline{z_1 z_2}$.

9.3. $|z|^2 = z\bar{z}$. 9.4. $z_1/z_2 = (z_1\overline{z_2})/(|z_2|^2)$.

9.5. $\bar{z}_1^k = (\bar{z}_1)^k$ для любого $k \in \mathbb{N}$.

9.6. $|z_1 + z_2| \le |z_1| + |z_2|$, для каких комплексных чисел z_1, z_2 имеет место равенство?

9.7. $|z_1| - |z_2| \le |z_1 - z_2|$, для каких комплексных чисел z_1, z_2 имеет место равенство?

10. Докажите, что для любых комплексных чисел z_1 и z_2 выполняется равенство

$$|z_1 + z_2|^2 + |z_1 - z_2|^2 = 2(|z_1|^2 + |z_2|^2).$$

В чем заключается геометрический смысл этого равенства?

11. Для любого натурального n вычислите: $(1+i)^n/(1-i)^n$; i^n; $(1+i)^{n+2}/(1-i)^n$.

12. Найдите $z^{1990} + z^{-1990}$, если $z^2 - z + 1 = 0$.

13. Вычислите

$$\sqrt[4]{\frac{(-1+i\sqrt{3})^{17} \cdot (\cos\frac{19\pi}{12} + i\sin\frac{19\pi}{12})}{32\sqrt{2}(1-i)^7}}.$$

14. Решите уравнения.

14.1. $x^8 - 5x^4 - 6 = 0$, $x \in \mathbb{R}$.

14.2. $x^4 + 1 + i\sqrt{3} = 0$, $x \in \mathbb{R}$.

14.3. $(x+i)^4 + (x-i)^4 = 0$, $x \in \mathbb{R}$.

14.4. $z^3 = -z$, $z \in \mathbb{C}$.

14.5. $(1-i)\overline{z} - 3iz = 2 - i$, $z \in \mathbb{C}$.

14.6. $z\overline{z} + 2\overline{z} = 3 + 2i$, $z \in \mathbb{C}$.

14.7. $z\overline{z} + 3(z - \overline{z}) = 4 + 3i$, $z \in \mathbb{C}$.

14.8. $z\overline{z} + 3(z + \overline{z}) = 3i$, $z \in \mathbb{C}$.

15. Решите системы уравнений:

$$\begin{cases} ix + (1+i)y = 3 - i \\ (1-i)x - (6-i)y = 4, \end{cases} \qquad \begin{cases} (2+i)x - (3+i)y = i \\ (3-i)\overline{x} + (2+i)\overline{y} = -i. \end{cases}$$

16. Изобразите на плоскости множество решений системы

$$\begin{cases} |2z - 4 - 2i| \le 6 \\ |iz + 2| \ge 2 \\ -\frac{5\pi}{6} \le \arg\left(\frac{2z}{i-\sqrt{3}}\right) \le \frac{\pi}{6}. \end{cases}$$

17. Докажите, что если z_1, z_2, z_3, z_4 — различные комплексные числа и число

$$\frac{z_1 - z_3}{z_2 - z_3} \Big/ \frac{z_1 - z_4}{z_2 - z_4}$$

действительное, то числа z_1, z_2, z_3, z_4 лежат на одной окружности или на одной прямой.

18. Изобразите на плоскости множество комплексных чисел, удовлетворяющих системе неравенств

$$\begin{cases} 2 \le |z - 2i| \le 3 \\ \frac{\pi}{2} \le \arg z_i \le \pi. \end{cases}$$

19. Пусть a и b — фиксированные различные комплексные числа. На комплексной плоскости найдите все точки, изображающие комплексные числа z, для которых

$$\frac{z-a}{z-b} = \cos\varphi + i\sin\varphi,$$

где φ принимает произвольные действительные значения.

20. Выразите через $\cos\alpha$ и $\sin\alpha$ с помощью формулы Муавра: $\cos 4\alpha$; $\sin 4\alpha$; $\sin 5\alpha + \cos 3\alpha$.

21. Докажите, что для любых целых чисел a, b, c, d произведение $(a^2+b^2)(c^2+d^2)$ можно представить как сумму квадратов k^2+l^2 целых чисел k и l.

22. Докажите, что если m и n взаимно просты, то все корни степени mn из единицы получаются умножением корней n-й степени из единицы на корни m-й степени из единицы.

23. Среди комплексных чисел, удовлетворяющих условию $|z-25i| \leq 15$, найдите число с наименьшим положительным аргументом.

24. Докажите, что бинарное отношение ρ на множестве всех комплексных чисел является отношением эквивалентности. Изобразите классы эквивалентности на плоскости:

24.1. $z_1 \rho z_2$ тогда и только тогда, когда $|z_1| = |z_2|$;

24.2. $z_1 \rho z_2$ тогда и только тогда, когда $z_1/z_2 \in \mathbb{R}$;

24.3. $z_1 \rho z_2$ тогда и только тогда, когда $z_1/z_2 \in \mathbb{R}^+$. Здесь $\mathbb{R}^+$ — множество всех положительных действительных чисел.

25. Докажите, что объединение всех корней n-й степени из комплексных чисел z и $-z$ совпадает с множеством всех корней $2n$-й степени из z^2.

26. Пусть $n, s \in \mathbb{N}$, $s \geq 2$. Верно ли равенство $\sqrt[ns]{z^s} = \sqrt[n]{z}$?

27. Решите следующие уравнения: $(z+1)^n + (z-1)^n = 0$; $(z+1)^n - (z-1)^n = 0$; $(z+i)^n + (z-i)^n = 0$.

28. Пусть z — первообразный корень нечетной степени n из единицы. Докажите, что $(-z)$ — первообразный корень степени $2n$ из единицы.

28. Пусть z — первообразный корень степени $2n$ из единицы. Докажите, что z или $(-z)$ — первообразный корень степени n из единицы.

30. Обозначим через $\sigma(n)$ сумму всех первообразных корней степени $n > 1$ из единицы. Докажите следующие утверждения:

30.1. $\Sigma_{d|n}\sigma(d) = 0$;

30. 2. Если p — простое число, то $\sigma(p) = -1$;

30. 3. Если p — простое число, $k > 1$, то $\sigma(p^k) = 0$;

30. 4. Если r и s — взаимно простые натуральные числа, $r > 1$, $s > 1$, то $\sigma(rs) = \sigma(r)\sigma(s)$.

31. Является ли число $(2+i)/(2-i)$ корнем некоторой степени из единицы?

32. Найдите комплексные числа, соответствующие противоположным вершинам квадрата, если двум другим вершинам соответствуют комплексные числа z и w.

33. Найдите комплексные числа, соответствующие вершинам правильного n-угольника, если двум смежным вершинам соответствуют комплексные числа z_0 и z_1.

5.3. Практикум по теме «Теория групп»

5.3.1. Примеры решения задач

Пример 5.3.1. Найти разложение циклической группы $G =< g >$ порядка 12 по подгруппе, порожденной элементом g^8.

Решение. По утверждению 3.1.1 порядок элемента g^8 равен $|g^8| = \frac{12}{(12,8)} = \frac{12}{4} = 3$. Найдем элементы циклической группы, порожденной элементом g^8 и состоящей, как мы выяснили, из трех элементов.

$(g^8)^2 = g^{16} = g^{12} \cdot g^4, (g^8)^3 = g^{24} = g^{12} \cdot g^{12}$.

Таким образом, $< g^8 >= \{e, g^4, g^8\}$.

Обозначим эту подгруппу через H. Число левых смежных классов G по H равно $|G : H| = |G|/|H| = 4$.

$gH = \{g, g^5, g^8\}; \quad g^2H = \{g^2, g^6, g^{10}\};$

$g^3H = \{g^3, g^7, g^{11}\}; \quad g^4H = \{g^4, g^8, g^{12} = e\}.$

Нетрудно заметить, что

$g^5H = g^9H = gH; \quad g^6H = g^{10}H = g^2H;$

$g^7H = g^{11}H = g^3H; \quad g^8H = g^{12}H = g^4H = H.$

Таким образом,

$$G = H \cup gH \cup g^2H \cup g^3H.$$

Пример 5.3.2. Составить таблицу сложения для фактор-группы аддитивной группы $5\mathbb{Z}$ по подгруппе $15\mathbb{Z}$. Указать образующие элементы этой фактор-группы.

Решение. Так как $5\mathbb{Z} = \{5k \mid k \in \mathbb{Z}\}$, то любой элемент $5k$ из $5\mathbb{Z}$ можно представить в одном из следующих видов: $5k = 15t$, $5k = 5 + 15t$, $5k = 10 + 15t$, где t — некоторое целое число. Поскольку $15t + 15\mathbb{Z} = 15\mathbb{Z}$, то $5k + 15\mathbb{Z}$ может быть одного из следующих видов: $15\mathbb{Z}$, $5 + 15\mathbb{Z}$, $10 + 15\mathbb{Z}$.

Эти множества — левые смежные классы аддитивной группы $5\mathbb{Z}$ по подгруппе $15\mathbb{Z}$, они образуют фактор-группу $5\mathbb{Z}/15\mathbb{Z}$ со следующей таблицей сложения

	$15\mathbb{Z}$	$5 + 15\mathbb{Z}$	$10 + 15\mathbb{Z}$
$15\mathbb{Z}$	$15\mathbb{Z}$	$5 + 15\mathbb{Z}$	$10 + 15\mathbb{Z}$
$5 + 15\mathbb{Z}$	$5 + 15\mathbb{Z}$	$10 + 15\mathbb{Z}$	$15\mathbb{Z}$
$10 + 15\mathbb{Z}$	$10 + 15\mathbb{Z}$	$15\mathbb{Z}$	$5 + 15\mathbb{Z}$

Напомним, что следующие классы $a + H$ и $b + H$ складываются так:
$(a + H) + (b + H) = (a + b) + H$. В нашей таблице
$(5 + 15\mathbb{Z}) + (5 + 15\mathbb{Z}) = 10 + 15\mathbb{Z}$;
$(10 + 15\mathbb{Z}) + (5 + 15\mathbb{Z}) = 15 + 15\mathbb{Z} = 15\mathbb{Z}$;
$(10 + 15\mathbb{Z}) + (10 + 15\mathbb{Z}) = 20 + 15\mathbb{Z} = 5 + 15\mathbb{Z}$ и т.д.

Так как $|5\mathbb{Z}/15\mathbb{Z}| = 3$, то фактор-группа циклическая, и каждый ее ненулевой элемент будет образующим, т.е.

$5\mathbb{Z}/15\mathbb{Z} =< 5 + 15\mathbb{Z} >=< 10 + 15\mathbb{Z} >$.

Пример 5.3.3. Пусть G — множество корней степени n из единицы, т.е.

$$G = \left\{ \varepsilon_k = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n} \mid k = 0, 1, \ldots, n-1 \right\}.$$

По формуле Муавра 2.6.9 $\varepsilon_k = \varepsilon_1^k$, поэтому $G =< \varepsilon_1 >$ – циклическая группа порядка n, порожденная элементом $\varepsilon_1 = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$.

Корень n – ой степени из 1 называется примитивным или первообразным, если он не является корнем из единицы меньшей степени. Известно, что корень n-ой степени из единицы будет примитивным тогда и только тогда, когда m и n взаимно просты. В частности, ε_1 и ε_{n-1} — примитивные корни n-ой степени из единицы. Поэтому $G =< \varepsilon_1 >=< \varepsilon_{n-1} >=< \varepsilon_m >$ для любого m взаимно простого с n.

Пример 5.3.4. Перечислить в S_3 все классы сопряженных элементов и все сопряженные подгруппы.

Решение. $S_3 = \{e, (12), (13), (23), (123), (132)\}$. Вычислим $(12)^x$, где x пробегает элементы из S_3. Ясно, что $(12)^e = (12)^{12} = (12)$. Далее,

$(12)^{13} = (13)^{-1}(12)(13) = (31)(12)(13) = (23)$;

$(12)^{23} = (32)(12)(23) = (13)$;

$(12)^{123} = (321)(12)(123) = (13)$;

$(12)^{132} = (231)(12)(132) = (23)$.

Итак, $(12)^{S_3} = \{(12), (23), (13)\}$. Вычислив x^y для всех x и y из S_3, получаем, что в S_3 имеется три класса сопряженных элементов:

$e^{S_3} = \{e\}$;

$(12)^{S_3} = (13)^{S_3} = (23)^{S_3} = \{(12), (23), (13)\}$;

$(123)^{S_3} = (132)^{S_3} = \{(123), (132)\}$.

Поэтому, $S_3 = e^{S_3} \cup (12)^{S_3} \cup (123)^{S_3}$. Подгруппы группы S_3 исчерпываются следующими шестью подгруппами (см. пример (5.3.6)):

$H_1 =< e >= \{e\}$; $\quad H_2 =< (12) >= \{e, (12)\}$;

$H_3 =< (13) >= \{e, (13)\}$; $\quad H_4 =< (23) >= \{e, (23)\}$;

$H_5 =< (123) >= \{e, (123), (132)\} =< (132) >$; $\quad H_6 = S_3$.

Так как элементы $(12), (13), (23)$ сопряжены в S_3, то подгруппы H_2, H_3 и H_4 сопряжены, причем ${H_2}^{(23)} = H_3$, ${H_2}^{(123)} = H_4$. Следовательно, S_3 содержит четыре класса сопряженных подгрупп: $\{H_1\}$, $\{H_2, H_3, H_4\}$, H_5, H_6.

Пример 5.3.5. Найти все фактор-группы группы S_3.

Решение. Среди подгрупп группы S_3 со своими сопряженными сов- падают подгруппы $E = H_1$, $H = H_5$ и $S_3 = H_6$. Поэтому по теореме (3.4.5) они нормальны в S_3.

E — единичная подгруппа, поэтому

$S_3/E = \{E, (12)E, (13)E, (23)E, (123)E, (132)E\}$

изоморфна с S_3.

Так как $S_3/H_6 = S_3/S_3 = \{S_3\}$, то S_3/H_6 — группа, изоморфная единичной группе.

Осталось рассмотреть нормальную подгруппу $H = H_5$. Ее порядок равен 3, а порядок S_3/H равен 2 по лемме (3.4.2). Поэтому S_3/H — циклическая группа порядка 2 (см. следствие теоремы Лагранжа). Смежные классы S_3 по H исчерпываются двумя классами: H и $(12)H$.

Таким образом, группа S_3 имеет три фактор-группы: $S_3/E \ncong S_3$, $S_3/S_3 \ncong E$ и $S_3/H = \{H, (12)H\}$, где E — единичная подгруппа, $H =< (123) >= \{e, (123), (132)\}$.

Пример 5.3.6. Найти все подгруппы симметрической группы S_3 степени 3.

Решение. Порядок $\mid S_3 \mid = 6$, поэтому по теореме Лагранжа 3.3.1 ее подгруппы могут быть только следующих порядков: 1, 2, 3, 6. Подгруппы порядков 1 и 6 — это единичная подгруппа $H_1 =< e >$ и вся группа $H_2 = S_3$. Подгруппы порядков 2 и 3, согласно следствию 3.3.2 теоремы Лагранжа, циклические, поэтому для их отыскания надо найти все подгруппы, порожденные неединичными элементами группы S_3:

$H_3 =< (12) >= \{e, (12)\}$,
$H_4 =< (13) >= \{e, (13)\}$,
$H_5 =< (23) >= \{e, (23)\}$,
$H_6 =< (123) >= \{e, (123), (132)\}$,
$H_7 =< (132) >= \{e, (132), (123)\}$.

Так как $H_6 = H_7$, то S_3 имеет в точности шесть подгрупп: H_1, H_2, H_3, H_4, H_5, H_6.

Пример 5.3.7. Найти разложение группы S_3 в левые смежные классы по подгруппе $H =< (12) >$.

Решение. Так как $S_3 = \{e, (12), (13), (23), (123), (132)\}$, то левыми смежными классами по H будут множества:

$eH = (12)H = H = \{e, (12)\}$,

$(13)H = (13)\{e, (12)\} = \{(13), (123)\}$,

$(23)H = (23)\{e, (12)\} = \{(23), (132)\}$,

$(123)H = (123)\{e, (12)\} = \{(123), (13)\}$,

$(132)H = (132)\{e, (12)\} = \{(132), (23)\}$.

Легко заметить, что различными левыми смежными классами будут множества H, $(13)H$, $(23)H$. Искомое разложение имеет вид

$S_3 = H \cap (13)H \cap (23)H$.

Пример 5.3.8. Выяснить, будет ли подгруппой произведение групп $A =< (12) >$ и $B =< (13) >$ группы S_3?

Рещение. Подгруппы A и B состоят из следующих элементов:

$A = \{e, (12)\}, B = \{e, (13)\}$.

Найдем произведения AB и BA:

$AB = \{e, (12)\} \cdot \{e, (13)\} = \{e, (12), (13), (132)\}$,

$BA = \{e, (13)\} \cdot \{e, (12)\} = \{e, (13), (12), (123)\}$.

Так как $AB \neq BA$, то AB не является подгруппой группы S_3.

Пример 5.3.9. Пусть G - циклическая группа порядка 12, порожденная элементом a. Пусть $A =< a^2 >$ и $B =< a^3 >$. Определить число элементов в произведении AB.

Решение. Хорошо известно, что

$$| AB | = \frac{| A | \cdot | B |}{| A \cap B |}.$$

Найдем элементы подгрупп A и B:

$$A = \left\{a^2, a^4, a^6, a^8, a^{10}, a^{12} = e\right\}, B = \left\{a^3, a^5, a^9, a^{12} = e\right\}.$$

Тогда $\mid A \mid = 6$, $\mid B \mid = 4$. Так как $A \cap B = \{e, a^6\}$, то $\mid A \cap B \mid = 2$. Следовательно, $\mid AB \mid = \frac{6 \cdot 4}{2} = 12$. Так как $\mid AB \mid = 12$, то легко заметить, что $AB = G$.

Пример 5.3.10. Пусть $\mathbb{Z}$ — аддитивная группа целых чисел, а H — произвольная мультипликативная группа. Зафиксируем элемент $g \in H$. Доказать,что $< g >$ — гомоморфный образ группы $\mathbb{Z}$.

Доказательство. Зададим отображение $\varphi : k \mapsto g^k$ для каждого $k \in \mathbb{Z}$. Так как $\varphi(k+l) = g^{k+l} = g^k \cdot g^l = \varphi(k)\varphi(l)$, то φ — гомоморфизм аддитивной группы $\mathbb{Z}$ в мультипликативную группу H. Образ

$$Im\varphi = \{\varphi(k) \mid k \in \mathbb{Z}\} = \left\{g^k \mid k \in \mathbb{Z}\right\} =< g >,$$

т. е. $Im\varphi =< g >$ — циклическая подгруппа в группе H, порожденная элементом g. Ядро $Ker\varphi = \{k \in Z \mid \varphi(k) = e\} = \left\{k \in \mathbb{Z} \mid g^k = e\right\}$ состоит из целых чисел k, для которых $g^k = e$. Поэтому заключаем, что ядро состоит из целых чисел, кратных порядку элемента g, т. е. $Ker\varphi = |g|\mathbb{Z}$. Тогда $\mathbb{Z}/|g|\mathbb{Z}$ изоморфна $< g >$. □

Пример 5.3.11. Показать, что факор-группа $GL(n,P)/SL(n,P)$ изоморфна мультипликативной группе P^* поля P.

Доказательство. Определим отображение $f : GL(n,P) \to P^*$, $f(A) = det\, A$, которое каждой матрице A из полной линейной группы $GL(n,P)$ степени n над полем P ставит в соответствие ее определитель. Так как определитель произведения двух матриц равен произведению определителей, т. е. $f(AB) = det\,(AB) = det\, A \cdot det\, B$, то отображение f — гомоморфизм. Каждый элемент $a \in P^*$ будет определителем матрицы

$$\mathbf{A} = \begin{pmatrix} a & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \dots\dots\dots & \dots\dots\dots & \dots\dots\dots & \\ 0 & 0 & \dots & 1 \end{pmatrix},$$

поэтому $Imf = P^*$, т. е. f — эпиморфизм. Ядро f состоит из матриц с единичным определителем, поэтому $Kerf = SL(n,P)$ — специальная линейная группа. По лемме 1.3.1 подгруппа $SL(n,P)$ нормальна в $GL(n,P)$. По теореме 3.5.4 фактор-группа $GL(n,P)/SL(n,P)$ изоморфна мультипликативной группе P^* поля P. □

5.3.2. Индивидуальные задания

1. Найти все элементы циклической подгруппы $H =< g >$ группы $(C^*, \cdot)$:

1.1. $g = \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i$;

1.2. $g = \frac{\sqrt{2}}{2} - \frac{1}{\sqrt{2}}i$;

1.3. $g = \frac{\sqrt{-3}}{2} + \frac{1}{2}i$;

1.4. $g = \frac{1}{2} - \frac{\sqrt{3}}{2}i$;

1.5. $g = -\frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}}i$.

2. Доказать, что порядки указанных элементов группы равны

2.1. ab и ba; 2.2. abc и bca; 2.3. a и $b^{-1}ab$;

2.4. ab^{-1} и ba^{-1}; 2.5. bca и cab.

3. Найти все подгруппы мультипликативной циклической группы порядка n. Указать все ее образующие элементы:

3.1. $n = 20$; 3.2. $n = 24$;

3.3. $n = 12$; 3.4. $n = 18$;

3.5. $n = 16$.

4. Найти все подгруппы аддитивной циклической группы порядка m по подгруппе порядка n. Указать все ее образующие элементы:

4.1. $m = 6, n = 2$; 4.2. $m = 15, n = 5$;
4.3. $m = 12, n = 4$; 4.4. $m = 16, n = 4$;
4.5. $m = 18, n = 6$.

5. Составить таблицу сложения для фактор-группы аддитивной группы $\mathbb{Z}$ по подгруппе $m\mathbb{Z}$. Указать образующие элементы $m\mathbb{Z}$ и $\mathbb{Z}_m$:
5.1. $m = 5$; 5.2. $m = 4$; 5.3. $m = 3$; 5.4. $m = 6$; 5.5. $m = 7$.

6. Найти все гомоморфизмы циклической группы порядка n в группу порядка m:
6.1. $n = 6, m = 5$; 6.2. $n = 8, m = 3$;
6.3. $n = 9, m = 5$; 6.4. $n = 10, m = 3$;
6.5. $m = 12, m = 7$.

7. Найти разложения циклической группы $G =< a >$ порядка n по всем ее подгруппам:
7.1. $n = 10$; 7.2. $n = 6$;
7.3. $n = 9$; 7.4. $n = 15$;
7.5. $n = 4$; 7.6. $n = 14$.

8. Пусть $G =< g >$ — циклическая группа порядка n. Найти порядок элемента g^m:
8.1. $n = 1023, m = 120$; 8.2. $n = 2132, m = 58$;
8.3. $n = 564, m = 124$; 8.4. $n = 332, m = 60$;
8.5. $n = 1551, m = 21$; 8.6. $n = 786, m = 153$.

9. Пусть A и B — нормальные подгруппы группы G, $A \cap B = 1$. Доказать,что $ab = ba$ для любых $a \in A$ и $b \in B$.

10. Доказать,что множество матриц с определителем, равным единице,образует нормальную подгруппу в группе $GL(n, P)$.

11. Доказать,что подгруппа $H =< (132) >$ — нормальная подгруппа группы S_3.

12. Доказать, что множество матриц вида $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$, где $a \in \mathbb{R}$, образует нормальную подгруппу группы $GL(2, \mathbb{R})$.

13. Доказать,что отношение сопряженности элементов в группе является отношением эквивалентности.

14. Элементы знакопеременной группы A_4 распределить по классам сопряженных элементов в A_4.

15. Определить число классов сопряженных элементов в A_5 и A_6.

16. Доказать,что множество $V_4 = \{e, (12)(34), (13)(24), (14)(23)\}$ является нормальной подгруппой группы A_4.

17. Пусть $G = \{y = ax + b \mid a, b \in \mathbb{R}, a \neq 0\}$ — группа функций с операцией $(y_1y_2)(x) = y_1(y_2(x))$. Доказать, что множество $H = \{y = x + c \mid c \in \mathbb{R}\}$ является нормальной подгруппой группы G.

18. В множестве пар целых чисел (n, m) действие определяется по правилу:

$$(n_1, m_1)(n_2, m_2) = (n_1 + n_2, (-1)^{n_2}m_1 + m_2).$$

Доказать, что относительно этого действия множество пар образует группу. Будет ли множество пар $\{(n, 0) \mid n \in \mathbb{Z}\}$ нормальной подгруппой этой группы?

19. Пусть G — мультипликативное множество всевозможных троек целых чисел, действие в котором определено следующим образом:

$$(k_1, k_2, k_3)(l_1, l_2, l_3) = (k_1 + (-1)^{k_3}l_1, k_2 + l_2, k_3 + l_3).$$

Проверить, что G группа и доказать, что подгруппа $H =< (1, 0, 0) >$ является нормальной в G.

20. В $GL(2, \mathbb{R})$ указать хотя бы один элемент(если он существует),посредством которого сопряжены данные матрицы:

20.1. $A = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$ и $B = \begin{pmatrix} 3 & 1 \\ 1 & 1 \end{pmatrix}$;

20.2. $A = \begin{pmatrix} 2 & 1 \\ -2 & 0 \end{pmatrix}$ и $B = \begin{pmatrix} 4 & 2 \\ 1 & 1 \end{pmatrix}$;

20.3. $A = \begin{pmatrix} 3 & 1 \\ 1 & 1 \end{pmatrix}$ и $B = \begin{pmatrix} 2 & 1 \\ -2 & 0 \end{pmatrix}$;

20.4. $A = \begin{pmatrix} 0 & -2 \\ 1 & 3 \end{pmatrix}$ и $B = \begin{pmatrix} 1 & -1 \\ 1 & -1 \end{pmatrix}$;

20.5. $A = \begin{pmatrix} 1 & 2 \\ 1 & 4 \end{pmatrix}$ и $B = \begin{pmatrix} 3 & 1 \\ 1 & 1 \end{pmatrix}$;

20.6. $A = \begin{pmatrix} -5 & 1 \\ 3 & 1 \end{pmatrix}$ и $B = \begin{pmatrix} 0 & -2 \\ 1 & 3 \end{pmatrix}$;

21. В A_4 найти класс элементов, сопряженных с элементом a:

21.1. $a = (123)$; 21.2. $a = (234)$; 21.3. $a = (134)$;

21.4. $a = (12)(34)$; 21.5. $a = (13)(24)$; 21.6. $a = (14)(23)$.

22. Пусть M_1 и M_2 — подгруппы группы G и $M_1 = x^{-1}M_2x$. Доказать, что

$$|G : M_1| = |G : M_2|.$$

23. Найти фактор-группу циклической группы $G =< a >$ порядка n по подгруппе $H =< a^m >$:

23.1. $m = 2, n = 10$; 23.2. $m = 3, n = 12$; 23.3. $m = 4, n = 12$;

23.4. $m = 3, n = 9$; 23.5. $m = 5, n = 15$; 23.6. $m = 2, n = 8$.

24. Составить таблицу сложения для фактор-группы $k\mathbf{Z}$ по подгруппе $t\mathbf{Z}$.

24.1. $m = 3, n = 9$; 24.2. $m = 5, n = 15$; 24.3. $m = 2, n = 6$;

24.4. $m = 4, n = 12$; 24.5. $m = 6, n = 18$; 24.6 $m = 2, n = 8$.

25. Пусть G — группа, N и H — подгруппы группы G, причем $N \triangleleft G$ и $N \subseteq H$. Доказать, что $H \triangleleft G$ тогда и только тогда, когда $H/N \triangleleft G/N$.

26. Найти все нормальные подгруппы фактор-группы A_4/V_4, где V_4 — подгруппа из задания 16.

27. Доказать, что все конечные циклические группы одного порядка изоморфны.

28. Доказать, что любая бесконечная циклическая группа изоморфна аддитивной группе целых чисел.

29. Пусть $G =< a >$, H — подгруппа группы G и a^k — элемент в H с наименьшим положительным показателем. Доказать, что $H =< a^k >$, т.е. подгруппа циклической группы является циклической группой.

30. Пусть G — мультипликативная группа, $a \in G$ и $H = \left\{a^{nk} \mid k \in Z\right\}$. Будет ли H подгруппой группы G при указанном n?

30.1. $n = 1$, 30.2. $n = 2$, 30.3. $n = 3$, 30.4. $n = 4$, 30.5. $n = 5$.

31. С помощью критерия подгрупп доказать, что множество mZ является подгруппой аддитивной группы Z при указанном m. Найти разложение Z в правые смежные классы по mZ.

31.1. $n = 4$, 31.2. $n = 3$, 31.3. $n = 6$, 31.4. $n = 7$, 31.5. $n = 5$.

32. Найти все элементы подгруппы M группы S_n и индекс подгруппы M в группе S_n:

32.1. $n = 6$; $M =< (15)(3624) >$;

32.2. $n = 4$; $M =< (3214) >$;

32.3. $n = 6$; $M =< (135)(624) >$;

32.4. $n = 5$; $M =< (12)(345) >$;

32.5. $n = 5$; $M =< (153)(24) >$.

33.Найти все подгруппы циклической группы $G =< a >$ порядка n. Найти разложения G в левые смежные классы по этим подгруппам.

33.1. $n = 6$, 33.2. $n = 10$, 33.3. $n = 15$, 33.4. $n = 14$, 33.5 $n = 21$.

34.Найти порядок элемента g, принадлежащего мультипликативной группе G. Вычислить g^{100}.

34.1. $g = \frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}}i$, $G = \mathbb{C}^*$;

34.2. $g = -i$, $G = \mathbb{C}^*$;

34.3. $g = \begin{pmatrix} 1 & i \\ 0 & 1 \end{pmatrix}$, $G = GL(2, \mathbb{C})$;

34.4. $g = -\frac{\sqrt{3}}{2} + \frac{1}{2}i$, $G = \mathbb{C}^\sharp$;

34.5. $g = \begin{pmatrix} 1 & 0 \\ i & 1 \end{pmatrix}$, $G = GL(2, \mathbb{C})$.

35.Пусть A и B — подгруппы группы S_4. Будет ли подгруппой произведение AB? Найти число элементов множества AB:

35.1. $A =< (1234) >$, $B =< (234) >$;

35.2. $A =< (12)(34) >$, $B =< (142) >$;

35.3. $A =< (341) >$, $B =< (12) >$;

35.4. $A =< (3142) >$, $B =< (214) >$;

35.5. $A =< (14)(23) >$, $B =< (132) >$.

36.Пусть $G =< a >$ — группа порядка n. Найти все элементы a^k этой группы такие, что $< a^k >= G$:

36.1. $n = 6$, 36.2. $n = 7$, 36.3. $n = 8$, 36.4. $n = 9$, 36.5. $n = 5$.

37. Найдите порядок перестановки.

37.1. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix} \in S_5$. 38.2. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 5 & 1 & 6 \end{pmatrix} \in S_6$.

38.3. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix} \in S_5$. 38.4. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 7 & 6 & 5 & 1 & 2 & 3 \end{pmatrix} \in S_7$.

38.5. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{pmatrix} \in S_5$.

39. В группе $GL(2, \mathbf{C})$ найдите порядки элементов.

39.1. $\begin{pmatrix} i & 1 \\ 0 & -i \end{pmatrix}$, $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

39.2. $\begin{pmatrix} -i & 0 \\ 1 & i \end{pmatrix}$, $\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$, $\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$.

39.3. $\begin{pmatrix} -i & 1 \\ 0 & i \end{pmatrix}$, $\begin{pmatrix} 0 & i \\ 1 & 0 \end{pmatrix}$, $\begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$.

39.4 $\begin{pmatrix} i & 0 \\ 1 & -i \end{pmatrix}$, $\begin{pmatrix} -1 & a \\ 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}$.

39.5. $\begin{pmatrix} -i & 1 \\ 0 & i \end{pmatrix}$, $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $\begin{pmatrix} -2+3i & -2+2i \\ 1-i & 3-2i \end{pmatrix}$.

40. В группе $GL(2, \mathbf{Z}_p)$ найдите порядки элементов.

40.1. $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$, $p = 3$. 4.2. $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $p = 5$.

40.3. $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$, $p = 5$. 4.4. $\begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix}$, $p = 3$.

40.5. $\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$, $p = 3$.

41. Докажите, что порядки указанных элементов мультипликативной группы равны.

41.1. abc и bca. 41.2. a и $b^{-1}a^{-1}b$. 41.3. ab^{-1} и ba^{-1}.

41.4. a и $b^{-1}ab$. 41.5. ab и ba.

42. В циклической группе $< a >$ порядка n найдите все элементы g, удовлетворяющие условию $g^k = e$, и все элементы порядка n.

52.1. $n = 24$, $k = 6$. 52.2. $n = 100$, $k = 5$.

52.3. $n = 24$, $k = 4$. 52.4. $n = 100$, $k = 20$.

52.5. $n = 36$, $k = 4$.

53. Найдите циклическую подгруппу из S_5, содержащую точно пять элементов.

54. Найдите циклическую подгруппу из S_6, содержащую точно шесть элементов.

55. Найдите порядки всех элементов группы S_n, $n \leqslant 7$.

56. Докажите, что порядок нечетной перестановки есть четное число.

57. Элементов какого порядка в симметрической группе S_n больше, четного или нечетного?

58. Докажите, что существуют перестановки любого порядка.

59. Докажите, что группа абелева, если в ней все неединичные элементы имеют порядок 2. Кроме того, если группа конечна, то ее порядок равен 2^n.

60. Могут ли в группе существовать точно два элемента порядка 2?

61. Докажите, что в абелевой группе множество элементов, порядки которых делят фиксированное число n, является подгруппой.

62. Если a — элемент группы порядка 5, то сколько различных элементов находится в группе $< a >$? Каковы порядки каждого из этих элементов?

63. Если a — элемент группы порядка 6, то сколько различных элементов находится в группе $< a >$? Каковы порядки каждого из этих элементов?

64. Если a — элемент группы порядка 6, найдите все подгруппы из $< a >$. Из них все циклические?

65. Если a и b — элементы циклической группы, то следует ли равенство $ab = ba$?

66. Если a — элемент группы и a имеет порядок n, что тогда можно сказать о порядке элемента a^{-1}?

67. Аддитивная группа $\mathbb{Z}$ циклическая, порождённая элементом 1. Если H — подгруппа группы $\mathbb{Z}$ и a — наименьшее положительное целое число в H, то докажите, что $H =< a >$.

68. Если a и b — элементы группы, и $ab = ba$, то докажите, что $a^n b = ba^n$ для всех $n \in \mathbf{Z}$.

69. Если a и b — элементы группы, и $ab = ba$, то докажите, что $a^n b^2 = b^2 a^n$ для всех $n \in \mathbf{Z}$.

70. Если a и b — элементы группы, и $ab = ba$, то докажите, что $a^m b^n = b^n a^m$ для любых $m, n \in Z$.

71. Если a и b — элементы группы, и $(ab)^2 = a^2 b^2$, то докажите, что $ab = ba$.

72. Докажите, что всякая конечная подгруппа мультипликативной группы $\mathbb{C}^*$ циклическая.

73. Найдите число элементов порядка p^m в циклической группе порядка p^n, где p — простое число, $0 < m \leqslant n$.

74. В мультипликативной группе $\mathbb{C}^*$ найдите все элементы 5-го порядка, 6-го порядка.

75. Докажите, что в абелевой группе нечетного порядка каждый элемент явля-

ется квадратом некоторого элемента.

76. Докажите, что абелева группа порядка, не делящегося на квадрат простого числа, является циклической.

77. Пусть в абелевой группе G все неединичные элементы имеют один и тот же порядок p. Докажите, что:

77.1. число p простое;

77.2. группа G разложима в прямое произведение подгрупп порядка p;

77.3. порядок группы G равен p^n, где n — число сомножителей в прямом произведении;

77.4. любая неединичная подгруппа является прямым произведением подгрупп порядка

78.1. Пусть $SL \pm (2, \mathbb{Q})$ — множество всех 2×2-матриц над полем $\mathbb{Q}$ с определителем ± 1, а $(\mathbb{Q}_+, \cdot)$ — мультипликативная группа положительных рациональных чисел. Проверьте, что $SL\pm(2, \mathbb{Q})$ является нормальной подгруппой группы $GL(2, \mathbb{Q})$. Докажите изоморфизм

$$GL(2, \mathbb{Q})/SL \pm (2, \mathbb{Q}) \simeq (\mathbb{Q}_+, \cdot).$$

78.2. Пусть K — множество всех 2×2-матриц над полем $\mathbb{R}$ с положительным определителем. Проверьте, что K является нормальной подгруппой группы $GL(2, \mathbb{R})$. Докажите изоморфизм

$$GL(2, \mathbb{R})/K \simeq (\{1, -1\}, \cdot).$$

78.3. Пусть L — множество всех 2×2-матриц над полем $\mathbb{C}$ с определителем, по модулю равным 1, а $(\mathbb{R}_+, \cdot)$ — мультипликативная группа положительных действительных чисел. Проверьте, что L является нормальной подгруппой группы $GL(2, \mathbb{C})$. Докажите изоморфизм

$$GL(2, \mathbb{C})/L \simeq (\mathbb{R}_+, \cdot)$$

78.4. Пусть S — множество всех 2×2-матриц над полем $\mathbb{C}$ с положительным действительным определителем, а $\mathbb{C}_1$ — множество всех комплексных чисел, по модулю равных единице. Проверьте, что S является нормальной подгруппой группы $GL(2, \mathbb{C})$, а $\mathbb{C}_1$ с умножением — группа. Докажите изоморфизм

$$GL(2, \mathbb{C})/S \simeq (\mathbb{C}_1, \cdot).$$

79. Пусть $\varphi : G \mapsto H$ — гомоморфизм группы G в группу H, K и N — подгруппы группы G, a, b — элементы из G. Доказать следующие утверждения:

79.1. $|\varphi(H)|$ делит $|H|$;

79.2. $|\varphi(a)|$ делит $|a|$;

79.3. $\varphi(a) = \varphi(b)$ тогда и только тогда, когда a и b принадлежат одному смежному классу G по $Ker\varphi$;

79.4. если $H \cap K \supseteq Ker\varphi$, то $\varphi(H \cap K) = \varphi(H) \cap \varphi(K)$;

79.5. $Ker\varphi$ — нормальная подгруппа группы G и $|G| = |Ker\varphi| \cdot |Im\varphi|$;

79.6. если G —циклическая группа порядка n, то $Im\varphi$ — циклическая группа и $|Im\varphi|$ делит n.

80. Найдите группы автоморфизмов циклической группы порядка 5, циклической группы порядка 6.

81. Докажите, что группа всех автоморфизмов циклической группы абелева.

82. Докажите, что группа автоморфизмов конечной циклической группы простого порядка p является конечной циклической группой порядка $p - 1$.

83. Докажите, что группа H тогда и только тогда является гомоморфным образом конечной циклической группы G, когда H также циклическая и $|H|$ делит $|G|$.

84. Докажите, что не существует группы, у которой группа автоморфизмов является конечной циклической группой нечетного порядка.

85. Докажите, что группа автоморфизмов бесконечной циклической группы является конечной группой порядка 2.

86. Докажите, что группа автоморфизмов конечной абелевой нециклической группы не является абелевой группой.

87. Докажите, что группа автоморфизмов неабелевой группы не может быть циклической группой.

5.4. Практикум по теме «Идеалы кольца»

5.4.1. Примеры решения задач

Пример 5.4.1. Доказать, что алгебраическая система $(\{a+b\sqrt{2}|a,b\in\mathbb{Z}\},+,\cdot)$ является кольцом. Указать его подкольца, идеалы и соответствующие гомоморфизмы, фактор-кольца.

Доказательство. Проверим замкнутость обеих операций:

$$(a+b\sqrt{2})+(c+d\sqrt{2})=(a+c)+(b+d)\sqrt{2},$$
$$(a+b\sqrt{2})(c+d\sqrt{2})=(ac+2bd)+(ad+bc)\sqrt{2}.$$

Так как числа $a+c$, $b+d$, $ac+2bd$, $ad+bc$ целые, то операции сложения и умножения замкнуты. Сложение и умножение любых действительных чисел коммутативны и ассоциативны, умножение дистрибутивно относительно сложения. Нуль и единица содержатся среди этих чисел. Каждое число $a+b\sqrt{2}$, $a,b\in\mathbb{Z}$ обладает противоположным числом того же вида. Следовательно, указанная алгебра является кольцом.

Обозначим это кольцо $\mathbb{Z}[\sqrt{2}]$. При $b=0$ получаем, что кольцо целых чисел является подкольцом кольца $\mathbb{Z}[\sqrt{2}]$. Но $\mathbb{Z}$ не является идеалом в $\mathbb{Z}\sqrt{2}$, ибо произведение целого числа на число $a+b\sqrt{2}$, $a,b\in\mathbb{Z}$, не есть целое число. Любое подкольцо кольца $\mathbb{Z}$ является подкольцом в $\mathbb{Z}[\sqrt{2}]$, но не является идеалом в $\mathbb{Z}[\sqrt{2}]$, хотя является идеалом в $\mathbb{Z}$.

Очевидно, что $\{a+b\sqrt{2}|a,b\in 2\mathbb{Z}\}$ замкнуто по сложению, умножению и взятию противоположного числа, то есть является подкольцом в $\mathbb{Z}[\sqrt{2}]$. Более того,

это подкольцо есть идеал, ибо если a и b четные числа, то при любых целых c и d числа $ac+2db$, $ad+bc$ являются чётными. Аналогично, при любом натуральном m $I=\{a+b\sqrt{2}\big|a,b\in m\mathbb{Z}\}$ есть идеал в кольце $\mathbb{Z}[\sqrt{2}]$.

Рассмотрим смежные классы по идеалу I. Для того чтобы числа $a+b\sqrt{2}$ и $c+d\sqrt{2}$ принадлежали одному смежному классу, их разность должна принадлежать идеалу, то есть числа $a-c$, $b-d$ должны быть кратны m. В этом случае $a\equiv c(mod\ m)$, $b\equiv d(mod\ m)$. Если хотя бы одно из указанных сравнений ложно, то взятые числа принадлежат разным смежным классам. Отсюда следует, что взяв два экземпляра полной системы вычетов по модулю m и комбинируя каждый вычет с каждым, получим, m^2 чисел $a+b\sqrt{2}$, являющихся представителями различных смежных классов по идеалу I. Очевидно, что этим будут исчерпаны все смежные классы, то есть фактор-кольцо по идеалу I состоит из m^2 элементов. Например, при $m=2$ фактор-кольцо состоит из элементов I, $1+I$, $\sqrt{2}+I$, $1+\sqrt{2}+I$. Как обычно, отображение элемента кольца на содержащий его смежный класс задаёт гомоморфизм кольца $\mathbb{Z}[\sqrt{2}]$ на фактор-кольцо. □

Пример 5.4.2. Доказать, что фактор-кольцо $\mathbb{Z}[\sqrt{2}]/3Z[\sqrt{2}]$ есть поле порядка 9.

Доказательство. Решение задачи (5.4.1) при $m=3$ даёт фактор-кольцо порядка $3^2=9$.

В данном случае фактор-кольцо состоит из элементов

$$I=3\mathbb{Z}[\sqrt{2}],\ 1+I,\ 2+I,\ 1+\sqrt{2}+I,\ 2+\sqrt{2}+I,\ \sqrt{2}+I,\ 2\sqrt{2}+I,\ 1+2\sqrt{2}+I,\ 2+2\sqrt{2}+I.$$

Докажем, что любой ненулевой элемент фактор-кольца имеет себе обратный. Для того чтобы найти элемент обратный к $a+b\sqrt{2}+I$ требуется решить уравнение $(a+b\sqrt{2}+I)(x+y\sqrt{2}+I)=1+I$. Это уравнение равносильно сравнению $(a+$

$b\sqrt{2})(x+y\sqrt{2}) \equiv 1(mod\ I)$, которое равносильно системе двух сравнений:

$$\begin{cases} ax+2by \equiv 1(\mod 3) \\ bx+ay \equiv 0(\mod 3) \end{cases} \tag{5.4.1}$$

Требуется показать, что если a или b не сравнимы с нулём по модулю 3, т.е. $a+b\sqrt{2}$ не принадлежит идеалу I, то система (5.4.1) имеет решение.

Рассмотрим три возможных случая:

1. $a \equiv 0(\mod 3)$, $b \not\equiv 0(\mod 3)$
2. $a \not\equiv 0(\mod 3)$, $b \equiv 0(\mod 3)$
3. $a \not\equiv 0(\mod 3)$, $b \not\equiv 0(\mod 3)$

В первом случае второе сравнение системы принимает вид $bx \equiv (\mod 3)$, откуда $x \equiv 0(\mod 3)$. Тогда из первого сравнения получаем сравнение $2by \equiv 1(\mod 3)$, которое имеет решение, так как НОД $(2b,3)=1$. Аналогично рассматривается второй случай. Из второго сравнения получаем $y \equiv 0(\mod 3)$. Тогда из первого сравнения имеем $ax \equiv 1(\mod 3)$. Последнее сравнение имеет решение, так как НОД $(a,3)=1$. В третьем случае умножим первое сравнение системы на b, второе сравнение – на a и почленно вычтем, исключая x. Получим:

$$(2b^2-a^2)y \equiv b(\mod 3), \tag{5.4.2}$$

где пара (a,b) может принимать следующие значения $(1;1)$, $(1;2)$, $(2;1)$, $(2;2)$. При всех указанных значениях по теореме Ферма $a^2 \equiv 1(\mod 3)$, $b^2 \equiv 1(\mod 3)$. Следовательно, сравнение (5.4.2) сводится к сравнению $y \equiv b(\mod 3)$. Подставляя найденное значение во второе сравнение системы (5.4.1) получаем сравнение $bx+ab \equiv 0(\mod 3)$. Так как НОД $(b,3)=1$, то $x \equiv -a(\mod 3)$. □

Пример 5.4.3. Найти все идеалы кольца верхних треугольных матриц второго порядка с целыми элементами.

Решение. Так как все идеалы кольца целых чисел имеют вид $m\mathbb{Z}$, где m – натуральное число, то рассмотрим множество $I = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \middle| a, b, c \in m\mathbb{Z} \right\}$. Очевидно, что I замкнуто по сложению, умножению и взятию противоположного элемента, т. е. является подкольцом. При любых целых x, y, z и a, b, c кратных m, имеем:

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \times \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} = \begin{pmatrix} ax & ay + bz \\ 0 & cz \end{pmatrix} \in I,$$

$$\begin{pmatrix} x & y \\ 0 & z \end{pmatrix} \times \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = \begin{pmatrix} ax & bx + cy \\ 0 & cz \end{pmatrix} \in I,$$

Получим, что множество I замкнуто относительно умножения слева и справа на элементы кольца. Следовательно, I есть идеал кольца верхних треугольных матриц второго порядка с целыми элементами. Рассмотрим далее множество

$$I_1 = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \middle| a \in m\mathbb{Z}, b \in l\mathbb{Z}, c \in n\mathbb{Z} \right\},$$

где m, l, n – натуральные числа. Легко видеть, что множество I_1 также как и множество I, замкнуто по сложению, умножению и взятию противоположного элемента, то есть также является подкольцом. Пусть x, y, z – целые числа, $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in I_1$, тогда $ax \in m\mathbb{Z}$, $cz \in n\mathbb{Z}$. Если НОД$(m, l) = d$ и $d = l$, то $ay + bz$ всегда принадлежит множеству $l\mathbb{Z}$. Аналогично, если НОД$(n, l) = l$, то $bx + cy$ всегда принадлежит множеству $l\mathbb{Z}$. Следовательно I_1 является идеалом кольца верхних треугольных матриц второго порядка с целыми элементами при условии, что $m \vdots l$, $n \vdots l$.

Пример 5.4.4. Найти все обратимые элементы кольца целых гауссовых чисел $(\{a+bi \mid a,b \in \mathbb{Z}\},+,\cdot)$.

Решение. I способ.

Обозначим кольцо целых гауссовых чисел A. Пусть $a+bi \in A$. Элемент $x+iy$, принадлежащий кольцу A, будет обратным для $a+bi$, если $(a+bi)(x+iy)=1$. Приравнивая действительные и мнимые части комплексных чисел, стоящих в левой и правой частях последнего уравнения, получим систему уравнений

$$\begin{cases} ax-by=1, \\ ay+bx=0 \end{cases}$$

Решая её, получим

$$\begin{cases} x=\frac{a}{a^2+b^2}, \\ y=-\frac{b}{a^2+b^2} \end{cases}$$

Учитывая, что a и b целые числа заключаем, что x, y удовлетворяют неравенствам $-1 \leqslant x \leqslant 1$, $-1 \leqslant y \leqslant 1$. Так как x, y целые числа, то их возможные значения будут $-1, 0, 1$. Если $x=-1$, то $a=-1, b=0$ и, следовательно, $y=0$. Если $x=0$, то $a=0$ и $y=-\frac{1}{b}$. Откуда получаем, что $b=1$ и $y=-1$ или $b=-1, y=1$. Если $x=1$, то $a=1, b=0$ и, следовательно, $y=0$. Таким образом, обратимыми элементами кольца целых гауссовских чисел являются $1, -1, i, -i$.

II способ. Наиболее эффективным методом исследования свойств делимости в кольце является построение такого отображения кольца во множество натуральных чисел с нулём, при котором образ произведения равен произведению образов сомножителей. Такое отображение позволяет найти обратимые элементы кольца, а для факториальных колец и простые элементы кольца. Для любого элемента $a+bi$ кольца целых гауссовских чисел обозначим $N(a+bi)$ число a^2+b^2 и назовём нормой этого элемента. Проверим, что норма произведения равна произведению норм сомножителей. Действительно,

$$N((a+bi)(c+di)) = N(ac-bd+(ad+bc)i) = (ac-bd)^2+(ad+bc)^2 =$$
$$= a^2c^2 - 2abcd + b^2d^2 + a^2d^2 + 2abcd + b^2c^2 = a^2(c^2+b^2) + b^2(c^2+d^2) =$$
$$= (a^2+b^2)(c^2+d^2) = N(a+bi)N(c+di).$$

Пусть элемент $c+di \in A$ является обратным для элемента $a+bi \in A$. Тогда $(a+bi)(c+di) = 1$ и следовательно $N(a+bi)N(c+di) = 1$. Так как $N(a+bi)$, $N(c+di)$ принадлежат множеству натуральных чисел с нулем, то $N(a+bi) = 1$, $N(c+di) = 1$. Можно показать и обратное. Если $a+di \in A$ и $N(a+bi) = 1$, то $a+bi$ обратим в кольце A. Действительно $N(a+bi) = (a+bi)(a-bi) = 1$. Следовательно, элемент $a+bi$ имеет обратный $a-bi$, то есть, обратим в кольце A.

Таким образом, элемент $a+bi$ обратим в кольце целых гауссовских чисел тогда и только тогда, когда $a^2+b^2 = 1$. Последнее равенство возможно лишь при $a = 1$, $b = 0$; $a = 0$, $b = 1$; $a = 0$, $b = -1$. Следовательно, обратимыми элементами кольца целых гауссовских чисел будут $1, -1, i, -i$.

Пример 5.4.5. Доказать, что обратимый элемент коммутативного кольца с единицей не может быть делителем нуля.

Доказательство. Пусть $(K, +, \cdot)$ — коммутативное кольцо с единицей e и a — некоторый обратимый элемент кольца K. Следовательно существует элемент b, принадлежащий K, такой, что $a \cdot b = b \cdot a = e$. Предположим, что элемент a является делителем нуля в кольце K. Это означает, что $a \neq 0$ и существует элемент $c \neq 0$, принадлежащий кольцу K, такой, что

$$a \cdot c = 0. \tag{5.4.3}$$

Домножим обе части равенства (5.4.3) слева на b. Получим $ba \cdot c = b \cdot 0$ или $c = 0$. Но по предположению $c \neq 0$. Получили противоречие. Следовательно, наше предположение о том, что a является делителем нуля неверно, т.е. a не является делителем нуля. □

Пример 5.4.6. Выясните, какие из ниже приведенных колец являются кольцами с делителями нуля:

а) Кольцо матриц вида

$$\begin{pmatrix} a_1 & 0 & 0 & \dots & 0 \\ 0 & a_2 & 0 & \dots & 0 \\ 0 & 0 & a_3 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & a_n \end{pmatrix}$$

порядка $n \geqslant 2$ с действительными элементами относительно сложения и умножения матриц.

б) Кольцо непрерывных функций на $[-1;1]$ с обычными операциями сложения и умножения.

в) Кольцо классов вычетов по модулю n, $n \in \mathbb{N}$, $n \geqslant 2$.

г) Кольцо матриц вида $\begin{pmatrix} a & b \\ 2b & a \end{pmatrix}$ с рациональными a, b относительно операций сложения и умножения матриц.

д) Кольцо $(P, +, \cdot)$, где $p(M) = P$ – множество всех подмножеств некоторого множества M.

е) Кольцо многочленов одной переменной с целыми коэффициентами, имеющих чётные свободные члены относительно операций сложения и умножения многочленов.

ж) Кольцо матриц $\begin{pmatrix} a+bi & c+di \\ -c+di & a-bi \end{pmatrix}$ с действительными a, b, c, d, где $i^2 = -1$, относительно операций сложения и умножения матриц.

Какие из указанных колец являются областями целостности?

Решение. а) Рассмотрим матрицу A, у которой $a_1 = a_2 = ... = a_k = 0$, $k < n$, а элементы $a_{k+1}, a_{k+2}, ..., a_n$ отличны от нуля и матрицу B, у которой элементы $a_1, a_2, ..., a_k$ отличны от нуля, а $a_{k+1}, a_{k+2}, ..., a_n = 0$. Очевидно, что произведение $A \cdot B$ является нулевой матрицей n-го порядка, которая служит нулём данного кольца. Таким образом, матрицы A и B – делители нуля.

б) Нулём указанного кольца является непрерывная на $[-1; 1]$ функция, принимающая значение 0 при любом значении аргумента. Рассмотрим функции $f_1 = \begin{cases} 0, & x \leqslant 0 \\ x, & x > 0 \end{cases}$, $f_2 = \begin{cases} x, & x \leqslant 0 \\ 0, & x > 0 \end{cases}$. Произведение функций $f_1(x) \cdot f_2(x)$ принимает значение 0 при любом значении аргумента. Следовательно, функции $f_1(x)$, $f_2(x)$ являются делителями нуля.

в) Рассмотрим два возможных случая:

1. Число n является составным.

2. Число n является простым.

В первом случае $n = a \cdot b$, где $a, b \in \mathbb{N}$, $1 < a < n$, $1 < b < n$. Следовательно $\overline{a} \cdot \overline{b} = 0$ и классы $\overline{a}, \overline{b}$ отличны от класса $\overline{0}$. Таким образом классы $\overline{a}, \overline{b}$ – делители нуля. Покажем, что во втором случае любой ненулевой элемент кольца является обратимым. Единицей кольца класса вычетов является класс $\overline{1}$. Пусть $\overline{a}$ произвольный ненулевой класс вычетов. Рассмотрим уравнение

$$\overline{a} \cdot \overline{x} = \overline{1}, \qquad (5.4.4)$$

которое равносильно уравнению

$$ax \equiv 1(\mod n). \tag{5.4.5}$$

Так как НОД$(a, n) = 1$, то сравнение (5.4.5), а, следовательно, и уравнение (5.4.4) имеют решения. Учитывая, что кольцо классов вычетов коммутативно, и используя задачу (5.4.5) заключаем, что при простом n указанное кольцо не содержит делителей нуля.

г) Рассмотрим произвольную ненулевую матрицу $\begin{pmatrix} a & b \\ 2b & a \end{pmatrix}$ с рациональными a и b. Её определитель равен $a^2 - 2b^2$ и отличен от нуля. Нулём указанного кольца является нулевая матрица $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$. Так как определитель произведения матриц равен произведению определителей сомножителей, то произведение двух ненулевых матриц вида $\begin{pmatrix} a & b \\ 2b & a \end{pmatrix}$ с рациональными a и b является невырожденной матрицей и следовательно не может быть нулевой матрицей. Таким образом, указанное кольцо не содержит делителей нуля.

д) Нулём кольца $(P, +, \cdot)$ является $\varnothing$. Пусть A непустое собственное подмножество множества M, тогда его дополнение $\overline{A}$ также не пусто и $A \cdot \overline{A} = A \cap \overline{A} = \varnothing$. Следовательно, кольцо $(P, +, \cdot)$ обладает делителями нуля.

е) Пусть $f_1(x)$, $f_2(x)$ ненулевые многочлены одной переменной с целыми коэффициентами, имеющие четные свободные члены. Если степень хотя бы одного их многочленов $f_1(x)$ или $f_2(x)$ положительна, то многочлен $f_3(x) = f_1(x) \cdot f_2(x)$ имеет положительную степень и, следовательно, не может быть нулевым многочленом. Если же многочлеы $f_1(x)$ и $f_2(x)$ имеют нулевую степень, то, учитывая, что кольцо $(2\mathbb{Z}, +, \cdot)$ не содержит делителей нуля, также заключаем, что их произведение не является нулевым многочленом. Таким образом, указанное кольцо не обладает делителями нуля.

ж) Так как произвольная ненулевая матрица $\begin{pmatrix} a+bi & c+di \\ -c+di & a-bi \end{pmatrix}$, где $a, b, c, d \in \mathbb{R}$, $i^2 = -1$, является невырожденной, то, как и в пункте г) заключаем, что указанное кольцо матриц не содержит делителей нуля.

Поскольку кольца из пунктов а), б), д) и кольцо классов вычетов по составленному модулю содержат делители нуля, то они не являются областями целостности.

Кольцо классов вычетов по простому модулю коммутативно, поскольку коммутативно кольцо целых чисел. Единицей этого кольца является класс $\overline{1}$. Следовательно, кольцо классов вычетов по простому модулю является областью целостности.

Кольцо матриц вида $\begin{pmatrix} a & b \\ 2b & a \end{pmatrix}$ с рациональными a и b коммутативно. Действительно,

$$\begin{pmatrix} a & b \\ 2b & a \end{pmatrix} \cdot \begin{pmatrix} c & d \\ 2d & c \end{pmatrix} = \begin{pmatrix} ac+2bd & ad+bc \\ 2bc+2ad & 2bd+ac \end{pmatrix} = \begin{pmatrix} c & d \\ 2d & c \end{pmatrix} \cdot \begin{pmatrix} a & b \\ 2b & a \end{pmatrix}.$$

Единицей указанного кольца служит единичная матрица $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Следовательно, это кольцо является обсластью целостности.

Кольцо многочленов одной переменной с целыми коэффициентами, имеющих четные свободные члены с операциями сложения и умножения многочленов и кольцо матриц $\begin{pmatrix} a+bi & c+di \\ -c+di & a-bi \end{pmatrix}$, где a, b, c, d действительные числа, $i^2 = -1$ с операциями сложения и умножения матриц областями целостности не являются. Поскольку первое не содержит единиц, а второе – некоммутативно.

Пример 5.4.7. В кольце целых чисел найдите:

1) $< 4 > + < 4 >$; 2) $< 3 > \cap < 4 >$; 3) $< 3 > \cdot < 4 >$; 4) $< 4 > : < 6 >$.

Решение. 1) Идеал $< 3 >$ представляет собой множество целых чисел кратных 3, $< 3 > = \{3k \mid k \in Z\}$, аналогично $< 4 > = \{4t \mid t \in \mathbb{Z}\}$. Тогда $< 3 > + < 4 > = \{3k + 4t \mid k, t \in \mathbb{Z}\}$.

Так как единица принадлежит множеству $< 3 > + < 4 >$, то $< 3 > + < 4 >=< 1 >= \mathbb{Z}$.

2) Пересечением множеств $\{3k \big| k \in \mathbb{Z}\}$ и $\{4t \big| t \in \mathbb{Z}\}$ является множество $\{12n \big| n \in \mathbb{Z}\}$. Следовательно, $< 3 > \cap < 4 >=< 12 >$.

3) $< 3 > \cdot < 4 >= \{3k \cdot < 4 > \big| k, t \in \mathbb{Z}\} = \{12kt \big| k, t \in \mathbb{Z}\} = \{12n \big| n \in \mathbb{Z}\}$. Таким образом, $< 3 > \cdot < 4 >=< 12 >$.

4) $< 6 >= \{6l \big| l \in \mathbb{Z}\}$. Тогда

$$< 4 >:< 6 >= \{n \in \mathbb{Z} \big| n \cdot < 6 > \subset < 4 >\} = \{n \in \mathbb{Z} \big| n \cdot 6k = 4t, k, t \in \mathbb{Z}\}.$$

Следовательно, n любое четное число. Таким образом, $< 4 >:< 6 >=< 2 >$.

Пример 5.4.8. Проверить, являются ли в кольце многочленов с целыми коэффициентами $\mathbb{Z}[x]$ сравнимыми по идеалу $I =< x, 2 >$ элементы $f(x) = x^2 + 3x + 4$ и $g(x) = x + 2$.

Решение. Многочлены $f(x)$ и $g(x)$ сравнимы по идеалу I, если их разность принадлежит этому идеалу. Так как

$$I =< x, 2 >= \{x \cdot \varphi(x) + 2 \cdot h(x) \big| \varphi(x), h(x) \in \mathbb{Z}[x]\},$$

то

$$f(x) - g(x) = x^2 + 2x + 2 = (x + 2) \cdot x + 1 \cdot 2 \in I.$$

Следовательно, $x^2 + 3x + 4 \equiv x + 2 (\mod I)$.

Пример 5.4.9. Пусть $K = \{a + bi\sqrt{3} \big| a, b \in \mathbb{Z}\}$, $I_1 =< 2 >$, $I_2 =< 1 + i\sqrt{3}$ – идеалы кольца $(K, +, \cdot)$. Верно ли, что $I_1 + I_2 = K$?

Решение. Обозначим сумму $I_1 + I_2 = I$. Тогда

$$I = \{2(a + bi\sqrt{3}) + (1 + i\sqrt{3})(c + di\sqrt{3}) \big| a, b, c, d \in \mathbb{Z}\} =$$

$$= \{(2a + c - 3d) + (2b + c + d)i\sqrt{3} \big| a, b, c, d \in \mathbb{Z}\}.$$

Поскольку кольцо K можно рассматривать как идеал, порождённый числом 1, то выясним, принадлежит ли 1 идеалу I. Для этого решим в целых числах систему уравнений:

$$\begin{cases} 2a + c - 3d = 1 \\ 2b + c + d = 0 \end{cases} \tag{5.4.6}$$

Если система (5.4.6) имеет решение в целых числах, то $1 \in I$, если же не имеет, то $1 \notin I$.

От системы уравнений (5.4.6) перейдём к системе сравнений по модулю 2:

$$\begin{cases} c - 3d \equiv 1 (\mod 2) \\ c + d \equiv 0 (\mod 2) \end{cases} \tag{5.4.7}$$

Почленно вычитая из второго сравнения первое, получим:

$$4d \equiv -1 (\mod 2) \tag{5.4.8}$$

Сравнение (5.4.8) не иеет решений в целых числах и, следовательно, $1 \notin I$, т. е. равенство $I_1 + I_2 = K$ не верно.

Пример 5.4.10. Пусть I сумма идеалов I_1 и I_2. Причём любой элемент $x \in I$ единственным образом представляется в виде $x = x_1 + x_2$, где $x_1 \in I_1$, $x_2 \in I_2$. В этом случае сумма называется прямой. Докажите, что $I_1 \cap I_2 = \{0\}$.

Доказательство. Пусть $I_3 = I_1 \cap I_2$ и y – произвольный элемент из I_3. Так как I_3 является идеалом, то $-y \in I_3$. Следовательно, $0 = -y + y$. Учитывая, что сумма идеалов I_1 и I_2 прямая, имеем $y = 0$. В силу произвольности выбора y заключаем $I_1 \cap I_2 = \{0\}$. □

Пример 5.4.11. Выяснить, какие из идеалов в указанных кольцах являются главными.

а) Идеал $I = \{a + bi \big| a, b \in 3\mathbb{Z}\}$ в кольце целых гауссовских чисел A.

б) Идеал $I =< x, 2 >$ вкольце многочленов переменной x с целыми коэффициентами.

в) Идеал $I = \left\{ \begin{pmatrix} a & a \\ a & a \end{pmatrix} \Big| a \in \mathbb{Z} \right\}$ в кольце $(A, +, \cdot)$, где $A = \left\{ \begin{pmatrix} a & b \\ b & a \end{pmatrix} \Big| a, b \in \mathbb{Z} \right\}$.

г) Идеал $P(S)$ в кольце $(P(M), +, \cdot)$, $S \subset M$, где алгебра $(P(M), +, \cdot)$ определена в задаче 2.

Решение. а) Любой элемент идеала I может быть представлен в виде $3 \cdot (a + bi)$, где $a, b \in \mathbb{Z}$. Следовательно, I – главный идеал, порождённый элементом 3.

б) Так как элементы x и 2 неразложимы в кольце целочисленных многочленов, то их общим делителем в указанном кольце может быть только обратимый элемент. Следовательно, идеал I может быть главным идеалом только в том случае, когда I совпадает со всем кольцом.

Пусть $f(x)$ – произвольный многочлен идеала I, тогда

$$f(x) = x \cdot \varphi(x) + 2 \cdot g(x) \tag{5.4.9}$$

где $\varphi(x)$, $g(x)$ – целочисленные многочлены. Из (5.4.9) получаем, что многочлен $f(x)$ имеет четный свободный член. Следовательно, целочисленные многочлены, имеющие нечётные свободные члены, не принадлежат идеалу I, и идеал I не является главным.

в) Легко проверить, что кольцо A коммутативно. Тогда любой элемент $\begin{pmatrix} a & a \\ a & a \end{pmatrix}$, где $a \in \mathbb{Z}$, идеала I можно представить в виде $\begin{pmatrix} a & a \\ a & a \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$, $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \in A$. Следовательно, I – главный идеал, порождённый элементом $\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$.

г) Так как $S \subset M$, то любое подмножество S можно рассматривать как пересечение множества S и некоторого подмножества мнжества M. Следовательно, $P(S) = S \cdot P(M)$, любой идеал $P(S)$ является главным идеалом, порожденным множеством S.

Пример 5.4.12. Доказать, что кольцо $(\{a + bi\sqrt{5} \big| a, b \in \mathbb{Z}\}, +, \cdot)$ не является кольцом главных идеалов.

Доказателъство. I способ. Нетрудно заметить, что

$$(1 + i\sqrt{5}) \cdot (1 - i\sqrt{5}) = 2 \cdot 3 \tag{5.4.10}$$

Вводя для любого элемента $a + bi\sqrt{5}$ кольца K понятие нормы $N(a + bi\sqrt{5}) = a^2 + 5b^2$ можно доказать, что элементы $1 + i\sqrt{5}$, $1 - i\sqrt{5}$, 2, 3 неразложимы в кольце K и ни один из элементов $1 + i\sqrt{5}$, $1 - i\sqrt{5}$ неассоциирован с элементами 2 или 3. Тогда из равенства (5.4.10) следует, что кольцо K не является факториальным и, следовательно, не является кольцом главных идеалов.

II способ. Доказав, что элементы $1 + i\sqrt{5}$ и 2 неразложимы в кольце K, рассмотрим идеал, $I =< 2, 1 + i\sqrt{5} >$. Так как элементы $1 + i\sqrt{5}$ и 2 неразложимы в кольце K, то их общим делителем в K может быть только обратимый элемент этого кольца. Следовательно, I будет главным идеалом лишь в том случае, когда I совпадает со всем кольцом. Покажем, что I не содержит 1. По определению идеала, порождённого подмножеством, имеем:

$$I = \{2(a + bi\sqrt{5}) + (1 + i\sqrt{5}) \cdot (c + di\sqrt{5}) \big| a, b, c, d \in \mathbb{Z}\} =$$

$$= \{(2a + c - 5d) + (2b + c + d)i\sqrt{5} \big| a, b, c, d \in \mathbb{Z}\}.$$

1 не принадлежит I, если система уравнений

$$\begin{pmatrix} 2a + c - 5d = 1 \\ 2b + c + d = 0 \end{pmatrix} \tag{5.4.11}$$

не имеет решений в целых числах.

Вычитая из первого уравнения системы второе, получим уравнение

$$2a - 2b - 6d = 1 \tag{5.4.12}$$

Уравнение (5.4.12) не имеет решений в целых числах и, следовательно, 1 не принадлежит I. Таким образом кольцо K не является кольцом главных идеалов. □

5.4.2. Индивидуальные задания

1. Докажите, что идеалами являются:

1.1. в кольце $\mathbb{Z}$ множества $2\mathbb{Z}$, $m\mathbb{Z}$;

1.2. в кольце $\{a + b\sqrt{3} \big| a, b \in \mathbb{Z}\}$ подкольцо $\{a + b\sqrt{3} \big| a, b \in 2\mathbb{Z}\}$;

1.3. в кольце $\{a + bi \big| a, b \in \mathbb{Z}\}$ подкольцо $\{a + bi \big| a, b \in 3\mathbb{Z}\}$;

1.4. в кольце функций, непрерывных на отрезке $[-1; 1]$ множество таких функций g, что $g\left(\frac{1}{2}\right) = 0$;

1.5. в кольце $A = \left\{ \begin{bmatrix} a & b \\ b & a \end{bmatrix} \big| a, b \in \mathbb{Z} \right\}$ множество $J = \left\{ \begin{bmatrix} a & a \\ a & a \end{bmatrix} \big| a \in \mathbb{Z} \right\}$.

1.6. в кольце $A = \left\{ \begin{bmatrix} a & b & c \\ 0 & a & b \\ 0 & 0 & a \end{bmatrix} \big| a, b, c \in \mathbb{Z} \right\}$ множество $J = \left\{ \begin{bmatrix} 0 & b & c \\ 0 & 0 & b \\ 0 & 0 & 0 \end{bmatrix} \big| b, c \in \mathbb{Z} \right\}$.

2. Докажите, что в произвольном кольце A идеалами являются:

2.1. все A и $\{0\}$;

2.2. множество $(a) = aA = \{ax \big| x \in A\}$;

2.3. множество $(a_1, \cdots, a_s) = \{a_1x_1 + ... + a_sx_s \big| x_1, ..., x_s \in A\}$.

3. В кольце $\mathbb{Z}$ найдите:

3.1. $(3)+(4)$; 3.2. $(3)\cap(4)$; 3.3. $(3)\circ(4)$;
3.4. $(3):(4)$; 3.5. $(4):(3)$; 3.6. $(3)+(6)$;
3.7. $(3)\cap(6)$; 3.8. $(3)\circ(6)$; 3.9. $(3):(6)$;
3.10. $(6):(3)$; 3.11. $(4)+(6)$; 3.12. $(4)\cap(6)$;
3.13. $(4)\circ(6)$; 3.14. $(4):(6)$; 3.15. $(6):(4)$.

4. Докажите, что если a и b – ненулевые элементы кольца главных идеалов A, то:

4.1. d – НОД$(a,b) \Leftrightarrow (d)=(a)+(b)$;
4.2. m – НОК$(a,b) \Leftrightarrow (m)=(a)\cap(b)$.

5. Найдите образующие следующих идеалов кольца $\mathbb{Z}$:

5.1. $(6,9,15)+(10,25,30)$;
5.2. $(6,9,15)\cap(20,25,30)$;
5.3. $(6,9,15)\circ(20,25,30)$;
5.4. $(6,9,15):(20,15,30)$;
5.5. $(20,25,30):(6,9,15)$.

6. Докажите, что следующие множества являются идеалами кольца $\mathbb{Z}$, и найдите образующие этих идеалов:

6.1. $\{x \mid bx \vdots a\}$; 6.2. $\{x \mid x \vdots a \wedge x \vdots b\}$;
6.3. $\{x \mid x = 26u + 65v; \quad u,v \in \mathbb{Z}\}$;
6.4. $\{x \mid x \vdots 8 \wedge x \vdots 14 \wedge x \vdots 35\}$;
6.5. $\{x \mid x \vdots 5 \wedge x = 18u + 42v; \quad u,v \in \mathbb{Z}\}$.

7. Пусть J – идеал кольца A. Докажите, что:

7.1. отношение сравнения по модулю J есть отношение эквивалентности на A;
7.2. $a+J$ – это класс вычетов, содержащий a.

8. Пусть $A=\{a+b\sqrt{3} \mid a,b \in \mathbb{Z}\}$, $J=\{a+b\sqrt{3} \mid a,b \in 2\mathbb{Z}\}$. Опишите:

8.1. классы вычетов по модулю J;
8.2. кольцо A/J (составьте таблицы сложения и умножения).

9. Пусть $A = \{a + bi \big| a, b \in \mathbb{Z}\}$, $J = \{a + bi \big| a, b \in 3\mathbb{Z}\}$. Опишите:

9.1. классы вычетов по модулю J;

9.2. кольцо A/J (составьте таблицы сложения и умножения).

10. Пусть $\varphi : \mathbb{Z} \to \mathbb{Z}_2 : \varphi(x) = \begin{cases} \overline{0}, \text{ если } x \text{ чётное;} \\ \overline{1}, \text{ если } x \text{ нечётное.} \end{cases}$ Докажите, что φ – гомоморфизм.

11. Пусть $A = \left\{ \begin{bmatrix} a & b \\ b & a \end{bmatrix} \big| a, b \in \mathbb{Z} \right\}$. Докажите, что отображение

$$\varphi : A \to \mathbb{Z}, \varphi \begin{bmatrix} a & b \\ b & a \end{bmatrix} = a - b -$$

гомоморфизм. Укажите его ядро.

12. Пусть F — кольцо всех непрерывных функций на отрезке $[-1; 1]$. Докажите, что отображение $\varphi : F \to \mathbb{R}, \varphi(f) = f(\frac{1}{2})$ — гомоморфизм. Укажите его ядро.

Вопросы к экзамену и итоговый тест

1. Группы, простейшие свойства, примеры.

2. Подгруппы. Примеры. Критерий подгруппы.

3. Гомоморфизмы групп (определение, виды гомоморфизма, примеры).

4.Кольца, простейшие свойства кольца, примеры. Делители нуля. Область целостности.

5. Подкольца, примеры. Критерий подкольца.

6. Гомоморфизмы колец (определение, виды гомоморфизма, примеры).

7. Поле, простейшие свойства поля, примеры.

8. Поле, характеристики отличной от 0.

9. Построение поля комплексных чисел C. Теорема 1 (с д-вом).

10. Построение поля комплексных чисел C. Теорема 2 (с д-вом).

11. Алгебраическая форма комплексного числа. Сопряженные комплексные числа. Действия над комплексными числами в алгебраической форме.

12. Алгебраическая форма комплексного числа. Сопряженные комплексные числа. Извлечение квадратного корня из комплексного числа записанного в алгебраической форме.

13. Геометрическая интерпретация комплексных чисел, корней из них и модуля разности двух комплексных чисел.

14. Решение квадратных уравнений. Двучленные уравнения.

15. Тригонометрическая форма комплексного числа. Равенство комплексных чисел в тригонометрической форме. Действия над комплексными числами в тригонометрической форме (деление и умножение) (с д-вом).

16. Тригонометрическая форма комплексного числа. Формула Муавра (с док-вом).

17. Тригонометрическая форма комплексного числа. Теорема о корне n-ой степени из комплексного числа в тригонометрической форме (с док-вом).

18. Корни из единицы. Первообразные корни. Теорема 1 (с д-вом). Корни из единицы. Первообразные корни. Теорема 2 (с д-вом).

19. Группы. Пример. Порядок группы. Порядок элемента группы. Циклические группы. Подгруппы циклических групп (с д-вом).

20. Группы подстановок. Теорема Кэли (с д-вом). Разложение группы по подгруппе. Смежные классы, свойства смежных классов (с д-вом). Индекс подгруппы. Примеры.

21. Теорема Лагранжа (с д-вом). Следствия (с д-вом). Примеры.

21. Нормальная подгруппа. Примеры. Критерий нормальной подгруппы (с д-вом). Примеры.

22. Фактор-группа. Теорема (с д-вом). Примеры.

23. Ядро гомоморфизма группы. Теорема о нормальности ядра в группе (с д-вом).

24. Основная теорема о гомоморфизме групп (с д-вом). Примеры.

25. Кольцо. Подкольцо. Критерий подкольца. Идеалы кольца. Примеры.

26. Критерий идеала кольца K. Действия над идеалами (с д-вом).

27. Идеал, порожденный множеством S. Теорема о структуре идеала, порожденного множеством S (с док-вом).

28. Главный идеал. Пример кольца главных идеалов (с доказательством).

29. Фактор-кольцо по идеалу. Классы вычетов кольца K по идеалу I. Примеры. Критерий сравнимости по идеалу (с д-вом).

30. Ядро гомоморфизма колец. Теорема о ядре (с д-вом). Теорема об гомоморфизме колец.

К итоговому тесту можно перейти по следующей ссылке Тест.

Литература

[1] Артамонов, В.А. Сборник задач по алгебре / В.А. Артамонов. — М: Физмалит, 2001.‘— 464 с.

[2] Борбат, В.Н. Кольца: Методические указания и задачи для самостоятельного решения / В.Н. Борбат, Н.В. Сакович. — Могилев: МГУ им. А.А.Кулешова, 2002. — 32 с.

[3] Курош, А.Г. Курс высшей алгебры / А.Г. Курош. — М.: Наука, 1975.

[4] Милованов, М.В. Алгебра и аналитическая геометрия: учебное пособие: в 2 ч. / М.В. Милованов, Р.И. Тышкевич, А.С. Феденко. Ч. 1. — Минск, 2001. — 400 с.

[5] Милованов, М.В. Алгебра и аналитическая геометрия: учебное пособие: в 2 ч. / М.В. Милованов [и др.]. Ч. 2. — Минск, 2001. — 352 с.

[6] Монахов, В.С. Введение в теорию конечных групп и их классов / В.С. Монахов. — Минск: Вышэйшая школа, 2006. — 207 с.

[7] Монахов, В.С. Алгебра и теория чисел : учебное пособие / В.С. Монахов, А.В. Бузланов. — Минск : Изд. центр БГУ, 2007. — 264 с.

[8] Монахов, В.С. Числовые функции и классы вычетов : практикум / В.С. Монахов, А.А. Трофимук. — Брест : Изд-во БрГУ имени А.С. Пушкина 2012. — 88 с.

[9] Монахов, В.С. Теория групп: практическое пособие / В.С. Монахов, Д.А. Ходанович. — Гомель: ГГУ им.Ф. Скорины, 2014. — 40 с.

[10] Нечаев, В.А. Задачник-практикум по алгебре / В.А. Нечаев. — М. : Просвещение, 1983. — 121 с.

[11] Трофимук, А.А. Алгебра. Линейная алгебра. Часть 1 / А.А. Трофимук, В.С. Монахов // Электронный учебно-методический комплекс, Брест, объём — 1,8 Мб, 1 файл, 235 с., 2015 (при обязательной регистрации в университете — свидетельство №13/2015 от 24.09.2015).

[12] Шнеперман, Л.Б. Сборник задач по алгебре и теории чисел / Л.Б. Шнеперман. — Мн. : Выш. школа, 1982. — 223 с.