БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ
МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ
Кафедра высшей алгебры

В.В. Беняш-Кривец, О.В. Мельников

ЛЕКЦИИ ПО АЛГЕБРЕ:

ГРУППЫ, КОЛЬЦА, ПОЛЯ

Курс лекций

МИНСК
2007

ВВЕДЕНИЕ

Предлагаемый ниже курс лекций предназначен для завершающего этапа алгебраического образования всех студентов математиков. Как это явствует из названия курса (и его оглавления), содержащийся в нем материал посвящен изложению ряда понятий и результатов, относящихся к теории абстрактных групп, колец и полей.

Необходимость знакомства с этими абстрактными алгебраическими объектами обусловлена тем, что в последнее время процесс, связанный с переходом математики на теоретико-множественную основу и выходом на передний план аксиоматических методов исследования, привел к изменению представления об алгебре как математической дисциплине.

Прежде, начиная с ее возникновения, алгебра понималась как наука о решении уравнений или систем уравнений сначала для чисел, позднее для некоторых других конкретных математических объектов. В настоящее время основным объектом исследования алгебры являются свойства операций, производимых над объектами произвольной природы. Возникающие на этом пути так называемые абстрактные алгебраические системы оказываются достаточно универсальными, чтобы конкретные их реализации можно было найти в самых разных областях как математики, так и некоторых других наук.

Отбор материала для курса лекций был основан на некоторых общих принципах. Прежде всего, мы ограничились изложением результатов лишь о классических алгебраических системах. Группы и поля были, пожалуй, первыми алгебраическими системами, возникшими в математике в связи с решением алгебраических уравнений. В настоящее время теория групп и теория полей являются наиболее развитыми в алгебре, а полученные в них результаты наиболее используемыми в других областях математики.

Отбирая материал из этих теорий в курс лекций, мы стремились включить по возможности достаточно широкий спектр результатов, которые можно было бы использовать как в общих, так и в специальных курсах по другим разделам математики. Кроме того, на отбор мате-

риала повлияла, разумеется, необходимость заложения базы алгебраических знаний как для чтения в дальнейшем специальных курсов по алгебре, так и для самостоятельного изучения студентами специальной литературы.

В основе представленного ниже курса лежат реальные лекции, читавшиеся на протяжении ряда последних лет для студентов 2-го курса механико-математического факультета БГУ. Поэтому у потенциальных читателей книги предполагается наличие определенных алгебраических знаний. К их числу относятся, прежде всего, теория делимости многочленов одной переменной, исчисление матриц и основные факты об определителях, ряд элементарных понятий и результатов линейной алгебры. Все это без труда можно найти в учебниках из списка литературы, приведенного в конце курса лекций.

Предлагаемый курс содержит две главы. Первая глава посвящена основам теории групп. Рассматриваются основные теоретико-групповые понятия: группы, подгруппы, факторгруппы, гомоморфизма и изоморфизма, прямого произведения групп, коммутанта. Доказываются классические теоремы Лагранжа и Кэли. Подробно изучаются два специальных класса групп — циклические группы и конечно порожденные абелевы группы.

Во второй главе изучаются кольца и поля. В теории колец вводятся такие понятия, как кольцо, подкольцо, идеал, факторкольцо, прямое произведение колец, гомоморфизм и изоморфизм колец. Изучается кольцо многочленов от нескольких переменных и доказывается основная теорема о симметрических многочленах. §§20–27 посвящены теории полей. Вводятся основные понятия теории: поле, характеристика поля, расширение полей, степень расширения, простое поле, алгебраический и трансцендентный элемент. Изучаются простые алгебраические и трансцендентные расширения полей. Значительное внимание уделяется конечным полям.

Глава 1
ОСНОВЫ ТЕОРИИ ГРУПП

§1. Множества с алгебраическими операциями.

Определение 1.1. *Пусть X — произвольное множество.* ***Бинарной алгебраической операцией*** *на X называется некоторое отображение $\tau : X \times X \to X$ декартова квадрата $X \times X$ в X.*

Таким образом, любой упорядоченной паре (a, b) элементов $a, b \in X$ ставится в соответствие однозначно определённый элемент $\tau(a, b)$ того же множества X. Часто вместо $\tau(a, b)$ пишут $a\tau b$, а ещё чаще бинарную операцию на X обозначают каким-нибудь специальным символом, например $a \circ b$ (или используют какой-либо другой специальный символ вместо $\circ$: $*$, $\cdot$, $\otimes$, $\oplus$, $+$, $-$ и т.д.). Наиболее часто используются две формы записи операции: **аддитивная** и **мультипликативная**. При аддитивной форме записи операцию называют сложением и вместо $c = a \circ b$ пишут $c = a + b$. При мультипликативной форме записи операцию называют умножением и вместо $c = a \circ b$ пишут $c = a \cdot b$ (или вообще опускают точку и пишут $c = ab$). В дальнейшем при изложении теории мы в основном будем использовать мультипликативную форму записи операции и лишь в некоторых случаях — аддитивную.

На X может быть задано, вообще говоря, много разных операций. Желая выделить одну из них, используют скобки: $(X, \circ)$, и говорят, что операция $\circ$ определяет на X алгебраическую структуру или что $(X, \circ)$ — **алгебраическая структура** (алгебраическая система). В направлении конструирования разных бинарных операций на множестве X также, очевидно, открывается неограниченный простор для фантазии. Но задача изучения произвольных алгебраических структур слишком обща, чтобы представлять реальную ценность. По этой причине рассматривают различные естественные ограничения на алгебраические операции.

Определение 1.2. *Бинарная операция $\circ$ на множестве X называется* ***ассоциативной****, если*

$$(a \circ b) \circ c = a \circ (b \circ c)$$

для всех $a, b, c \in X$; она называется ***коммутативной****, если*

$$a \circ b = b \circ a$$

для всех $a, b \in X$. Те же названия присваиваются и соответствующей алгебраической структуре $(X, \circ)$.

Требования ассоциативности и коммутативности независимы. В самом деле, операция $*$ на $\mathbb{Z}$, заданная правилом $n * k = -n - k$, очевидно, коммутативна, но

$$(1 * 2) * 3 = (-1 - 2) * 3 = -(-1 - 2) - 3 = 0 \neq 4 = 1 * (2 * 3),$$

так что условие ассоциативности не выполняется. Далее, на множестве $M_n(\mathbb{R})$ всех вещественных квадратных матриц порядка $n > 1$ определена операция умножения — ассоциативная, но некоммутативная.

Определение 1.3. *Элемент $e \in X$ называется* ***нейтральным*** *относительно рассматриваемой бинарной операции $\circ$, если*

$$e \circ x = x \circ e = x$$

для всех $x \in X$.

Предложение 1.4. *В алгебраической структуре $(X, \circ)$ может существовать не более одного нейтрального элемента.*

Доказательство. Пусть e_1, e_2 — два нейтральных элемента. Тогда, как следует из определения, $e_1 e_2 = e_1$, поскольку e_2 — нейтральный элемент, и $e_1 e_2 = e_2$, поскольку e_1 — нейтральный элемент. Поэтому $e_1 = e_2$. □

Определение 1.5. *Пусть $(X, \circ)$ — алгебраическая структура с нейтральным элементом e. Элемент $a \in X$ называется* ***обратимым****, если найдётся элемент $b \in X$, для которого*

$$ab = ba = e.$$

Элемент b называется ***симметричным*** *к a.*

Ясно, что если b — симметричный элемент к a, то и a — симметричный элемент к b.

Предложение 1.6. *Пусть $(X, \circ)$ — ассоциативная алгебраическая структура с нейтральным элементом e. Тогда для любого элемента $a \in X$ может существовать не более одного симметричного элемента.*

Доказательство. Пусть $b_1,\ b_2$ — два симметричных элемента к a. Тогда, как следует из определения,

$$(b_1 \circ a) \circ b_2 = e \circ b_2 = b_2 = b_1 \circ (a \circ b_2) = b_1 \circ e = b_1. \quad \square$$

Пусть $(X, \circ)$ — произвольная алгебраическая структура с бинарной операцией $\circ$. Пусть, далее, $x_1, \ldots, x_n$ — упорядоченная последовательность элементов из X. Не меняя порядка, мы можем многими разными способами составлять произведения длины n. Пусть l_n — число таких способов:

$$\begin{aligned}
l_2 = 1 &: \ x_1 \circ x_2; \\
l_3 = 2 &: \ (x_1 \circ x_2) \circ x_3,\ x_1 \circ (x_2 \circ x_3); \\
l_4 = 5 &: \ ((x_1 \circ x_2) \circ x_3) \circ x_4,\ (x_1 \circ x_2) \circ (x_3 \circ x_4),\ x_1 \circ (x_2 \circ (x_3 \circ x_4)), \\
&\qquad (x_1 \circ (x_2 \circ x_3)) \circ x_4,\ x_1 \circ ((x_2 \circ x_3) \circ x_4).
\end{aligned}$$

Очевидно, что, перебирая всевозможные произведения $x_1 \circ \cdots \circ x_k$, $x_{k+1} \circ \cdots \circ x_n$ длин k и $n-k$, $1 \le k \le n-1$, а затем соединяя их нашей бинарной операцией в данном порядке, мы исчерпаем все l_n возможностей.

Замечательно, что для ассоциативной алгебраической операции расстановка скобок оказывается излишней.

Теорема 1.7. *Если бинарная операция на X ассоциативна, то результат ее последовательного применения к n элементам множества X не зависит от расстановки скобок.*

Доказательство. При $n = 1,\ 2$ доказывать нечего. При $n = 3$ утверждение теоремы совпадает с законом ассоциативности. Далее рассуждаем индукцией по n. Предположим, что $n > 3$ и что для числа

элементов $< n$ справедливость утверждения установлена. Нам достаточно лишь показать, что

$$(x_1 \circ \cdots \circ x_k) \circ (x_{k+1} \circ \cdots \circ x_n) = (\ldots (x_1 \circ x_2) \circ x_3) \circ \cdots \circ x_{n-1}) \circ x_n$$

при любом k, $1 \leq k \leq n-1$. В левой части мы выписали только внешние пары скобок, поскольку по предположению индукции расстановка внутренних скобок несущественна. В частности, при $k < n$ независимо от расстановки скобок в левой части имеем

$$x_1 \circ x_2 \circ \cdots \circ x_k = (\ldots (x_1 \circ x_2) \circ x_3) \circ \cdots \circ x_{k-1}) \circ x_k.$$

Рассмотрим два случая:

а) $k = n-1$; тогда имеем очевидное равенство

$$(x_1 \circ \cdots \circ x_{n-1}) \circ x_n = (\ldots (x_1 \circ x_2) \circ x_3) \circ \cdots \circ x_{n-1}) \circ x_n.$$

б) $k < n-1$; ввиду ассоциативности и учитывая предположение индукции, имеем

$$(x_1 \circ \cdots \circ x_k) \circ (x_{k+1} \circ \cdots \circ x_{n-1} \circ x_n) = (x_1 \circ \cdots \circ x_k) \circ ((x_{k+1} \circ \cdots \circ x_{n-1}) \circ x_n) =$$
$$= ((x_1 \circ \cdots \circ x_k) \circ (x_{k+1} \circ \cdots \circ x_{n-1})) \circ x_n = (\ldots (x_1 \circ x_2) \circ x_3) \circ \cdots \circ x_{n-1}) \circ x_n. \square$$

Упражнения

1. Ассоциативна ли операция $*$ на множестве M, если

а) $M = \mathbb{N}$, $x * y = x^y$; б) $M = \mathbb{N}$, $x * y = \text{НОД}(x, y)$;

в) $M = \mathbb{N}$, $x * y = 2xy$; г) $M = \mathbb{Z}$, $x * y = x - y$;

д) $M = \mathbb{Z}$, $x * y = x^2 + y^2$; е) $M = \mathbb{R}$, $x * y = \sin x \cdot \sin y$.

2. На множестве M определена операция $\circ$ по правилу $x \circ y = x$. Ассоциативна ли эта операция? Что можно сказать о нейтральном и обратимых элементах M?

3. На множестве M^2, где M — некоторое множество, определена операция $\circ$ по правилу $(x, y) \circ (z, t) = (x, t)$. Ассоциативна ли эта операция? Существует ли в M^2 нейтральный элемент?

§2. Понятие группы, подгруппы, примеры.

Определение 2.1. *Непустое множество G с определенной на нем бинарной операцией $\circ$ называется* ***группой****, если*

1) *операция* $\circ$ *ассоциативна;*

2) *существует нейтральный элемент* e*;*

3) *любой элемент* a *из* G *имеет симметричный элемент* $b \in G$*.*

Группа с коммутативной операцией называется, естественно, коммутативной, а ещё чаще — абелевой (в честь норвежского математика Абеля).

Для обозначения групповой операции чаще всего используют два символа:

1) точку; тогда вместо $a \cdot b$ пишут просто ab и говорят об умножении элементов из группы; группу называют *мультипликативной*, для обозначения нейтрального элемента используют символ 1, а элемент, симметричный к a, называют обратным к a и обозначают a^{-1};

2) знак сложения $+$; тогда говорят о сложении элементов из группы, группу называют *аддитивной*, для обозначения нейтрального элемента используют символ 0, а элемент, симметричный к a, называют противоположным к a и обозначают $-a$.

Мы в дальнейшем будем использовать (если не оговорено противное) мультипликативную запись.

Удивительно, что одна из старейших и богатейших по результатам область алгебры, играющая фундаментальную роль в геометрии и в приложениях математики к вопросам естествознания, основывается на столь простых аксиомах. Идеи теории групп "носились в воздухе"(как это часто бывает с основополагающими математическими идеями) задолго до Галуа, и некоторые из её теорем в наивной форме были доказаны еще Лагранжем. Гениальные работы Галуа оказались непонятыми, и возрождение интереса к ним началось только после книги К. Жордана "Курс теории перестановок и алгебраических уравнений"(1870 г.).

Порядком группы G называется мощность $|G|$ множества G.

Благодаря ассоциативности в группе, произведение любых ее элементов $a_1, a_2, \ldots, a_n$ в заданном порядке не зависит от расстановки скобок и поэтому может быть записано как $a_1 a_2 \ldots a_n$.

Определение 2.2. *Пусть a — элемент группы G. Для произвольного целого числа n положим*

$$a^n = \begin{cases} 1, & \text{если } n = 0, \\ a \dots a, & \text{если } n > 0 \ (n \text{ множителей}), \\ (a^{-n})^{-1}, & \text{если } n < 0. \end{cases}$$

Предложение 2.3. *Пусть a — элемент некоторой группы и $n, m \in \mathbb{Z}$. Тогда $a^{n+m} = a^n a^m$ и $(a^n)^m = a^{nm}$.*

Определение 2.4. *Непустое подмножество H группы G называется* ***подгруппой*** *группы G (пишут $H \leq G$), если H является группой относительно той же операции, которая определена на G.*

Теорема 2.5 (Критерий подгруппы). *Непустое подмножество H группы G является подгруппой группы G тогда и только тогда, когда выполнены следующие условия:*

1) *если $a, b \in H$, то $ab \in H$;*
2) *если $a \in H$, то $a^{-1} \in H$.*

Доказательство. Пусть H — подгруппа в G, т.е. H — группа относительно той же операции, которая определена на G. На H определена алгебраическая операция, поэтому $ab \in H$ для все $a, b \in H$.

Проверим, совпадает ли единица 1_H подгруппы H с единицей 1_G группы G. Ясно, что

$$1_H 1_G = 1_G 1_H = 1_H,$$

поскольку 1_H — элемент группы G. В G для 1_H имеется обратный элемент 1_H^{-1}, т.е. $1_H^{-1} 1_H = 1_H 1_H^{-1} = 1_G$. Так как 1_H — единица в H, то $1_H 1_H = 1_H$.Умножив обе части последнего равенства на 1_H^{-1}, получим

$$1_H^{-1}(1_H 1_H) = 1_H^{-1} 1_H = 1_G = (1_H^{-1} 1_H) 1_H = 1_G 1_H = 1_H.$$

Поскольку H — подгруппа, то для любого $a \in H$ существует обратный элемент $a^{-1} \in H$, т.е. такой, что $a^{-1}a = aa^{-1} = 1$, где 1 — единичный элемент в группе G и подгруппе H. Это означает, что элемент a^{-1} является обратным к a в группе G.

Докажем обратное утверждение. Пусть $ab \in H$ и $a^{-1} \in H$ для всех $a, b \in H$. Тогда на H определена алгебраическая операция $\tau : H \times H \to H$, где $\tau(h_1, h_2) = h_1 h_2$. Она ассоциативна, так как ассоциативность справедлива для всех элементов из G. Так как $a, a^{-1} \in H$, то $aa^{-1} = 1_G \in H$ и H содержит единичный элемент. Значит, H — подгруппа в G. □

Если $H \leq G$ и $H \neq G$, то подгруппу H называют *собственной подгруппой* группы G и пишут $H < G$. Любая группа G содержит подгруппы $\{1\}$ и G; их называют *тривиальными*. В случае $\{1\} < H < G$ подгруппу H называют *нетривиальной подгруппой* группы G.

Приведем примеры групп и их подгрупп. Далее мы используем следующее определение композиции двух отображений:

$$(fg)(x) = f(g(x)).$$

Таким образом, подстановки перемножаются справа налево.

1. Множества $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ — абелевы группы относительно сложения. При этом $\mathbb{Z} < \mathbb{Q} < \mathbb{R} < \mathbb{C}$. Множество классов вычетов $\mathbb{Z}_n$ по модулю n — абелева группа порядка n относительно сложения.

2. Множества $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$, $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$, $T = \{z \in \mathbb{C} \mid |z| = 1\}$, $\mathbb{C}_n = \{z \in \mathbb{C} \mid z^n = 1\}$ — абелевы группы относительно умножения. При этом $\mathbb{Q}^* < \mathbb{R}^* < \mathbb{C}^*$, $C_n < T < \mathbb{C}^*$.

3. Множество всех подстановок на множестве $X = \{1, 2, \ldots, n\}$ относительно умножения подстановок является группой. Она называется *симметрической группой* степени n и обозначается S_n. Все четные подстановки в S_n образуют подгруппу, которая обозначается A_n и называется *знакопеременной группой* степени n. Порядок группы S_n равен $n!$, а порядок группы A_n равен $n!/2$ при $n \geq 2$.

Этот пример можно обобщить на бесконечное множество X. Пусть $S(X)$ — множество всех биективных отображений $f : X \to X$. Тогда $S(X)$ — группа с естественной бинарной операцией, являющейся композицией отображений. Сама по себе группа $S(X)$ и различные её подгруппы, называемые *группами преобразований* множества X, — стартовая площадка, с которой начинаются всевозможные применения

теории групп. Достаточно упомянуть о знаменитой "Эрлангенской программе"Ф. Клейна (1872 г.), положившей понятие группы преобразований в основу классификации различных типов геометрий.

4. Множество $\mathrm{GL}_n(K)$ всех невырожденных матриц размера $n \times n$ над полем K является группой относительно умножения матриц. Она называется *общей линейной группой*. Ее подгруппа $\mathrm{SL}_n(K)$, состоящая из всех матриц с определителем 1, называется *специальной линейной группой*. Группа $\mathrm{SL}_n(K)$ содержит подгруппу $\mathrm{T}_n(K)$, состоящую из всех матриц с нулями под главной диагональю, и подгруппу $\mathrm{UT}_n(K)$, состоящую из всех матриц с единицами на главной диагонали и нулями под ней.

Надо сказать, что группа $\mathrm{GL}_n(K)$, будучи вместилищем многих интересных групп, является для математиков как бы нескончаемым источником новых идей и нерешённых задач.

4. Множество $O_n(\mathbb{R})$ всех ортогональных матриц порядка n (т.е. таких матриц $A \in \mathrm{GL}_n(\mathbb{R})$, что $AA^\top = E$) образует подгруппу в $\mathrm{GL}_n(\mathbb{R})$, которая называется *ортогональной группой*.

Действительно, если $A, B \in O_n(\mathbb{R})$, то $AB(AB)^\top = A(BB^\top)A^\top = AA^\top = E$. Значит, $AB \in O_n(\mathbb{R})$. Далее, по определению $A^\top = A^{-1}$, поэтому, транспонируя обе части последнего равенства, получаем $A = (A^{-1})^\top$. Следовательно, $A^{-1}(A^{-1})^\top = A^{-1}A = E$ и $A^{-1} \in O_n(K)$.

Множество $SO_n(\mathbb{R})$ всех ортогональных матриц порядка n с определителем 1, очевидно, образует подгруппу в $O_n(\mathbb{R})$, которая называется *специальной ортогональной группой*.

5. Множество $U_n(\mathbb{C})$ всех унитарных матриц порядка n (т.е. таких матриц $A \in \mathrm{GL}_n(\mathbb{C})$, что $AA^* = E$) образует подгруппу в $\mathrm{GL}_n(\mathbb{C})$, которая называется *унитарной группой*. Множество $\mathrm{SU}_n(\mathbb{C})$ всех унитарных матриц порядка n с определителем 1, очевидно, образует подгруппу в $\mathrm{U}_n(\mathbb{C})$, которая называется *специальной унитарной группой*.

6. Целочисленные матрицы с определителем 1 образуют подгруппу в группе $\mathrm{SL}_n(\mathbb{R})$, обозначаемую через $\mathrm{SL}_n(\mathbb{Z})$.

7. Множество невырожденных диагональных матриц порядка n является абелевой подгруппой группы $\mathrm{GL}_n(K)$.

8. Движением евклидовой плоскости называется любое отображение этой плоскости на себя, сохраняющее расстояния между точками. Пусть F — произвольная фигура на евклидовой плоскости. Множество всех движений евклидовой плоскости, переводящих F на себя, с операцией "композиция двух движений", является группой. Эта группа называется группой симметрии фигуры F. Аналогично, можно рассматривать группы симметрий фигур в пространстве.

В группе симметрии правильного n-угольника имеется ровно $2n$ элементов: n вращений по часовой стрелке на углы $\frac{2\pi k}{n}$, $k = 0, \ldots, n-1$, вокруг его центра и n отражений относительно прямых, проходящих через центр и одну из его вершин или середину одной из его сторон (в зависимости от четности n). Эта группа называется *группой диэдра* D_n порядка $2n$. Все вращения в группе D_n образуют подгруппу, которая называется *группой вращений* данного n-угольника.

9. Пусть f — какой-либо многочлен от n переменных. Тогда

$$\mathrm{Sym}(f) = \{\boldsymbol{\sigma} \in S_n \mid f(x_{\boldsymbol{\sigma}(1)}, \ldots, x_{\boldsymbol{\sigma}(n)}) = f(x_1, \ldots, x_n)\}.$$

есть подгруппа группы S_n. В самом деле, пусть $\boldsymbol{\sigma}, \boldsymbol{\tau} \in \mathrm{Sym}(f)$. Положим $x_{\boldsymbol{\sigma}(i)} = y_i$. Тогда

$$f(x_{\boldsymbol{\tau\sigma}(1)}, \ldots, x_{\boldsymbol{\tau\sigma}(n)}) = f(y_{\boldsymbol{\tau}(1)}, \ldots, y_{\boldsymbol{\tau}(n)}) = f(y_1, \ldots, y_n) = f(x_{\boldsymbol{\sigma}(1)}, \ldots, x_{\boldsymbol{\sigma}(n)}) = f(x_1, \ldots, x_n),$$

значит $\boldsymbol{\tau\sigma} \in \mathrm{Sym}(f)$. Другая аксиома подгруппы выполнена очевидным образом.

В частности, многочлен f является симметрическим тогда и только тогда, когда $\mathrm{Sym}(f) = S_n$. В качестве примера многочлена с менее богатой, но не тривиальной симметрией рассмотрим многочлен $f = x_l x_2 + x_3 x_4$ (от 4 переменных). Легко видеть, что группа $\mathrm{Sym}(f)$ состоит из 8 подстановок, сохраняющих разбиение множества $\{1, 2, 3, 4\}$ на два подмножества $\{1, 2\}$ и $\{3, 4\}$. (Допускается перестановка этих подмножеств и перестановка элементов в каждом из них).

Определение 2.6. *Группы G и G_1 называют изоморфными и пишут $G \simeq G_1$, если существует биективное отображение $f : G \to$*

G_1, *которое называют* изоморфизмом, *которое обладает свойством*

$$f(ab) = f(a)f(b) \quad \textit{для любых } a, b \textit{ из } G.$$

Пример. Из курса линейной алгебры известно, что имеется взаимно однозначное соответствие между квадратными матрицами порядка n над полем K и линейными преобразованиями n-мерного векторного пространства V над полем K при выборе в V фиксированного базиса. При этом невырожденным матрицам отвечают обратимые линейные преобразования, а умножению матриц соответствует умножение линейных преобразований. Следовательно, группа $\mathrm{GL}_n(K)$ изоморфна группе $\mathrm{GL}(V)$ невырожденных линейных преобразований пространства V.

Упражнения

1. Докажите, что для любого элемента a из группы G отображения $l_a : G \to G$, $r_a : G \to G$, заданные правилами $l_a(g) = ag$, $r_a(g) = ga$ $(g \in G)$, являются биекциями. Отображение l_a называется **левым сдвигом**, а r_a — **правым сдвигом**.

2. Доказать предложение 2.3.

3. Доказать, что а) в любой группе$(ab)^{-l} = b^{-1}a^{-l}$, $(a^{-1})^{-1} = a$; б) для любых элементов a, b из группы G уравнение $ax = b$ имеет единственное решение, равное $a^{-1}b$, а уравнение $xa = b$ имеет единственное решение, равное ba^{-1}.

4. Доказать, что группа симметрии правильного треугольника изоморфна группе S_3.

5. Доказать, что группа вращений правильного n-угольника изоморфна группе $\mathbb{Z}_n$.

6. Если H_i, $i \in I$, — подгруппы группы G, то $H = \bigcap\limits_{i \in I} H_i$ — подгруппа группы G.

7. Пусть

$$I = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad J = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad K = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}.$$

Доказать, что

а) $I^2 = J^2 = K^2 = -E$, $IJ = K$, $JK = I$, $KI = J$, $JI = -K$, $KJ = -I$, $IK = -J$;

б) 8 матриц $\pm E$, $\pm I$, $\pm J$, $\pm K$ образуют подгруппу *кватернионов* Q_8 в группе $\mathrm{SL}_2(\mathbb{C})$.

8. Пусть G — группа относительно операции $\circ$. Операцию $*$ определим так: $a*b = b\circ a$. Доказать, что относительно операции $*$ множество G также является группой.

9. Доказать, что непрерывные строго возрастающие вещественные функции f, определенные на на отрезке $[0, 1]$ и имеющие значения $f(0) = 0$ и $f(1) = 1$, образуют группу относительно суперпозиции.

10. Доказать, что если в мультипликативно записанной группе квадрат любого элемента равен 1, то эта группа — абелева.

11. Обозначим через G множество матриц вида

$$\begin{pmatrix} a & -3b \\ b & a \end{pmatrix}, \qquad \text{где } a, b \in \mathbb{R},\ a^2 + b^2 \neq 0.$$

Доказать, что G — группа относительно матричного умножения.

12. Доказать, что квадратные матрицы n-го порядка, у которых в каждой строке и в каждом столбце ровно один элемент равен 1, а остальные равны 0, образуют группу относительно умножения.

13. Доказать, что непустое подмножество конечной группы, произведение любых элементов которого снова содержится в нем, является подгруппой.

15. Пусть $F, H \leq G$. Доказать, что $F \cup H \leq G$ тогда и только тогда, когда либо $F \subset H$, либо $H \subset F$.

16. Группа V_4 из четырёх элементов задана таблицей Кэли

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

(*четверная группа Клейна*). Найти все её подгруппы.

17. Для произвольного подмножества M группы G обозначим че-

рез $N_G(M)$ множество всех тех $g \in G$, для которых $gmg^{-1} \in M$ для любого элемента $m \in M$. Доказать, что $N_G(M)$ — подгруппа G (*нормализатор множества M в G*).

18. Найти все подгруппы симметрической группы S_3.

§3. Системы порождающих. Циклические группы.

Пусть S — какое-либо подмножество группы G. Обозначим через $\langle S \rangle$ совокупность всевозможных произведений вида

$$g_1^{\varepsilon_1} \dots g_k^{\varepsilon_k} \quad (g_1, \dots, g_k \in S, \varepsilon_1, \dots, \varepsilon_k = \pm 1). \tag{3.1}$$

Предложение 3.1. *Множество $\langle S \rangle$ — наименьшая подгруппа группы G, содержащая S.*

Доказательство. Если какая-либо подгруппа H содержит S, то она содержит и все указанные произведения, т.е. $H \supset \langle S \rangle$. С другой стороны, само множество $\langle S \rangle$ является подгруппой, как показывают следующие равенства:

$$(g_1^{\varepsilon_1} \dots g_k^{\varepsilon_k})(g_{k+1}^{\varepsilon_{k+1}} \dots g_{k+l}^{\varepsilon_{k+l}}) = g_1^{\varepsilon_1} \dots g_k^{\varepsilon_k} g_{k+1}^{\varepsilon_{k+1}} \dots g_{k+l}^{\varepsilon_{k+l}},$$
$$(g_1^{\varepsilon_1} \dots g_k^{\varepsilon_k})^{-1} = g_k^{-\varepsilon_k} \dots g_1^{-\varepsilon_1}.$$

Следовательно, $\langle S \rangle$ — наименьшая подгруппа группы G, содержащая S. □

Говорят, что $\langle S \rangle$ — подгруппа, *порожденная подмножеством S*. В частности, если $G = \langle S \rangle$, то говорят, что группа G порождается своим подмножеством S или что S — система порождающих (элементов) группы G.

Обычно для сокращения записи вместо $\langle \{a_1, a_2, \dots, a_n\} \rangle$ пишут $\langle a_1, a_2, \dots, a_n \rangle$ и говорят, что эта подгруппа порождается элементами $a_1, a_2, \dots, a_n$. Допустимы и другие вольности в обозначениях. Например, если A и B — подмножества группы G, c — ее элемент, то вместо $\langle A \cup BU\{c\} \rangle$ пишут $\langle A, B, c \rangle$.

Группа называется *конечно порожденной*, если она может быть порождена конечным множеством элементов.

Определение 3.2. *Пусть S состоит из одного элемента $a \in G$, тогда подгруппа $\langle a \rangle$ называется* ***циклической подгруппой****, порожденной элементом a. Если в группе G существует такой элемент a, что $G = \langle a \rangle$, то группа G называется* ***циклической****.*

Конечно, любая группа G порождается подмножеством $S = G$, однако представляет интерес найти возможно меньшую систему порождающих.

Пример 1. Группа диэдра D_n порождается поворотом φ на угол $2\phi/n$ и (любым) отражением $\psi \in D_n$. В самом деле, φ порождает циклическую подгруппу C_n всех поворотов, содержащихся в группе D_n; умножая элементы этой подгруппы на ψ, мы получим все отражения, входящие в группу D_n.

Пример 2. Группа S_n порождается транспозициями. В самом деле, поскольку каждая транспозиция обратна сама себе, то это утверждение эквивалентно тому, что любая подстановка разлагается в произведение транспозиций.

Пример 3. Напомним, что *элементарной матрицей* называется матрица вида $E + cE_{ij}$, где $c \neq -1$ при $i = j$, E_{ij} — матрица, у которой на позиции (i, j) находится 1, а все остальные элементы равны нулю. Справедливо следующее предложение.

Предложение 3.3. *Группа* $\mathrm{GL}_n(K)$ *порождается элементарными матрицами.*

Доказательство. Отметим, что матрица, обратная к элементарной, также элементарна. Поэтому утверждение предложения означает, что любая невырожденная матрица разлагается в произведение элементарных матриц. Умножение матрицы $A \in \mathrm{GL}_n(K)$ слева на элементарную матрицу вызывает соответствующее элементарное преобразование ее строк. Мы знаем, что с помощью элементарных преобразований строк любую невырожденную матрицу можно привести к единичной матрице. Таким образом, существуют такие элементарные матрицы $U_1, U_2, \ldots, U_s$, что

$$U_s \ldots U_2 U_1 A = E.$$

Значит,

$$A = U_1^{-1}U_2^{-1}...U_s^{-1} -$$

произведение элементарных матриц, что и требовалось доказать. $\square$

Рассмотрим более подробно циклические подгруппы данной группы G. Пусть $\langle a\rangle \leq G$. Возможны два принципиально разных случая: либо все степени элемента a различны (в частности, $a^k \neq 1$ при $k \neq 0$), либо нет.

Определение 3.4. *Наименьшее из натуральных чисел n, для которых $a^n = 1$, называется* ***порядком*** *элемента $a \in G$ и обозначается через* $\operatorname{ord} a$. *В том случае, когда не существует такого натурального m, что $a^m = 1$, полагают* $\operatorname{ord} a = \infty$ *и говорят, что элемент a имеет бесконечный порядок.*

ПРИМЕР 1. Найдем порядок матрицы $A = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$ как элемента группы $\mathrm{GL}_2(\mathbb{R})$. Имеем

$$A^2 = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}, \qquad A^3 = -E,$$

откуда

$$A^4 = -A, \quad A^5 = -A^2, \quad A^6 = -A^3 = E,$$

так что $\operatorname{ord} A = 6$. Конечно, этот пример специально подобран: вероятность того, что порядок наудачу выбранной матрицы $A \in \mathrm{GL}_2(\mathbb{R})$ будет конечен, равна нулю.

ПРИМЕР 2. Порядок комплексного числа a в группе $\mathbb{C}^*$ конечен тогда и только тогда, когда это число есть корень некоторой степени из единицы.

В случае $\operatorname{ord} a = \infty$ подгруппа $\langle a\rangle$ бесконечна. Рассмотрим более подробно случай $\operatorname{ord} a = n < \infty$.

Предложение 3.5. *Если* $\operatorname{ord} a = n$, *то*

1) $a^m = 1 \Leftrightarrow n \mid m$;

2) $a^k = a^l \Leftrightarrow k \equiv l \pmod{n}$.

Доказательство. 1) Разделим m на l остатком:

$$m = nq + r, \qquad 0 \leq r < n.$$

Тогда в силу определения порядка

$$a^m = (a^n)^q a^r = a^r = 1 \Leftrightarrow r = 0.$$

2) В силу пункта 1

$$a^k = a^l \Leftrightarrow a^{k-l} = 1 \Leftrightarrow n \mid (k-l) \Leftrightarrow k \equiv l \pmod{n},$$

что и требуется. □

Следствие 3.6. *Если* $\operatorname{ord} a = n$, *то подгруппа* $\langle g \rangle$ *содержит* n *элементов.*

Доказательство. Действительно,

$$\langle a \rangle = \{1, a, a^2, \ldots, a^{n-1}\},$$

причем все перечисленные элементы различны. Действительно, если бы $a^k = a^s$ при некоторых k, s, $0 \leq k < s < n$, то тогда, умножая обе части этого равенства на a^{-k}, мы имели бы $a^{s-k} = 1$ и $0 < s - k < n$. Это противоречит тому, что $\operatorname{ord} a = n$ по условию. □

Предложение 3.7. *Если* $\operatorname{ord} g = n$, *то*

$$\operatorname{ord} g^k = \frac{n}{(n,k)}.$$

Доказательство. Пусть

$$(n,k) = d, \quad n = n_1 d, \quad k = k_1 d.$$

Тогда $(n_1, k_1) = 1$ и

$$(g^k)^m = 1 \Leftrightarrow n \mid km \Leftrightarrow n_1 \mid k_1 m \Leftrightarrow n_1 \mid m.$$

Следовательно, $\operatorname{ord} g^k = n_1$. □

Отметим, что $\operatorname{ord} e = 1$; порядки же всех остальных элементов группы больше 1. В аддитивной группе говорят не о степенях элемента a, а о его *кратных*, которые обозначают через ka, т.е. ka — аддитивный аналог для a^k. В соответствии с этим порядок элемента a аддитивной группы G — это наименьшее из натуральных чисел n (если такие су-

ществуют), для которых

$$na = \underbrace{a + a + \cdots a}_{n} = 0.$$

Пусть $G = \langle a \rangle$ — циклическая группа, порожденная элементом a. Тогда G состоит из всех степеней элемента a, т.е. $G = \{a^n \mid n \in \mathbb{Z}\}$.

Если $\operatorname{ord} a = \infty$, то в циклической группе $\langle a \rangle$ элементы a^n и a^m различны при $n \neq m$ (иначе мы имели бы $a^{n-m} = 1$) и, следовательно, группа $\langle a \rangle$ бесконечна. Если же $\operatorname{ord} a = n$, то по следствию 3.6 $\langle a \rangle = \{1 = a^0, a, a^2, \ldots, a^{n-1}\}$, порядок группы $\langle a \rangle$ равен n и $a^k = a^l \Leftrightarrow k \equiv l \pmod{n}$.

Циклические группы — это наиболее простые группы, которые можно себе представить. (В частности, они абелевы.) Примером бесконечной циклической группы является группа $\mathbb{Z}$ всех целых чисел относительно обычной операции сложения (в качестве образующей a можно взять 1 или -1). Примером конечной циклической группы порядка n является группа $\mathbb{Z}_n$ классов вычетов по модулю n (в качестве образующей a можно взять класс вычетов $\overline{1}$). Оказывается, с точностью до изоморфизма этими группами исчерпываются все циклические группы.

Теорема 3.8. *Любая бесконечная циклическая группа изоморфна группе $\mathbb{Z}$, а любая конечная циклическая группа порядка n изоморфна группе $\mathbb{Z}_n$.*

Доказательство. Если $\langle a \rangle$ — бесконечная циклическая группа, то отображение $f : \mathbb{Z} \to \langle a \rangle$, заданное правилом $f(k) = a^k$, является изоморфизмом. Если $\langle a \rangle$ — циклическая группа порядка n, то отображение $f : \mathbb{Z}_n \to \langle a \rangle$, заданное тем же правилом $f(\overline{k}) = a^k$, является изоморфизмом. Сюръективность f очевидна. Проверим инъективность f. Предположим противное: $f(\overline{k}) = f(\overline{l})$, т.е. $a^k = a^l$ при некоторых $0 \leq k < l \leq n - 1$. Но тогда мы должны иметь $k \equiv l \pmod{n}$, что невозможно. □

Легко видеть, что в бесконечной циклической группе $\langle a \rangle$ порождающими элементами являются только a и a^{-1}. Поскольку порядок

конечной циклической группы равен порядку ее порождающего элемента, то из предложения 3.7 следует

Предложение 3.9. *Элемент g^k циклической группы $G = \langle g \rangle$ порядка n является порождающим тогда и только тогда, когда n и k взаимно просты, т.е. $(n, k) = 1$.*

Пример. Мультипликативная группа C_n комплексных корней n-й степени из 1 является циклической. В самом деле, эти корни являются числами

$$\alpha_k = \cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n}, \qquad (k = 0, 1, \ldots, n-1).$$

Ясно, что $\alpha_k = (\alpha_1)^k$. Следовательно, группа C_n циклическая и порождается элементом α_1. В частности, $C_n \simeq \mathbb{Z}_n$. Порождающие элементы группы C_n называются *первообразными* корнями n-й степени из 1. Это корни вида α_k, где $(n, k) = 1$. Например, первообразные корни 12-й степени из 1 — это $\alpha_1, \alpha_5, \alpha_7, \alpha_{11}$.

Для понимания строения какой-либо группы важную роль играет знание ее подгрупп. Все подгруппы циклической группы могут быть легко описаны.

Теорема 3.10. 1. *Любая подгруппа циклической группы — циклическая.*

2. *В циклической группе $G = \langle a \rangle$ порядка n для любого натурального делителя d числа n существует ровно одна подгруппа H порядка d. Подгруппа H порождается элементом $a^{\frac{n}{d}}$.*

Доказательство. 1. Очевидно, единичная подгруппа — циклическая. Пусть H — неединичная подгруппа циклической группы $\langle a \rangle$, и пусть k — наименьшее натуральное число с условием $a^k \in H$. Очевидно, $\langle a^k \rangle \subset H$. Докажем, что $\langle a^k \rangle = H$. Возьмем в H произвольный элемент, он имеет вид a^t. Поделим t на k с остатком: $t = kq + r$, $0 \le r < k$. Тогда $a^r = a^{t-kq} = a^t(a^k)^{-q} \in H$. В силу минимальности k отсюда следует, что $r = 0$. Тогда $a^t = (a^k)^q \in \langle a^k \rangle$.

2. Пусть $n = dn_1$. Тогда элемент a^{n_1} имеет порядок d (проверить!) и порождает циклическую подгруппу порядка d. Покажем, что любая

подгруппа $H \leq \langle a \rangle$ порядка d совпадает с $\langle a^{n_1} \rangle$. В силу пункта 1, H — циклическая подгруппа в $\langle a \rangle$, порожденная элементом a^t. Нам достаточно показать, что $a^t \in \langle a^{n_1} \rangle$. Так как a^t имеет порядок d, то $a^{td} = 1$. По условию, a имеет порядок n, следовательно, по предложению 3.5 $n|td$, т.е. $td = ns = dn_1 s$. Отсюда немедленно получаем, что $t = n_1 s$ и $a^t = (a^{n_1})^s \in \langle a^{n_1} \rangle$. □

Следствие 3.11. *В циклической группе простого порядка любая неединичная подгруппа совпадает со всей группой.*

Упражнения

1. Доказать, что число решений уравнения $x^k = 1$ в циклической группе порядка n равно наибольшему общему делителю чисел n и k.

2. Если a и b — перестановочные элементы группы G, т. е. $ab = ba$, и их порядки взаимно просты, то $\operatorname{ord} ab = \operatorname{ord} a \operatorname{ord} b$.

3. Найти порядки элементов $\begin{pmatrix} 0 & i \\ 1 & 0 \end{pmatrix}$, $\begin{pmatrix} i & i \\ i & -i \end{pmatrix}$ и $\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$ группы $GL_2(\mathbb{C})$.

4. Выписать все элементы группы $GL_2(\mathbb{Z}_2)$ и указать их порядки.

5. Доказать, что порядки $\operatorname{ord}(g)$ и $\operatorname{ord}(hgh^{-1})$ сопряженных при помощи элемента h элементов g и hgh^{-1} одинаковы.

6. Доказать, что для любого элемента g группы G $\operatorname{ord}(g) = \operatorname{ord}(g^{-1})$.

7. Доказать, что для любых элементов g_1 и g_2 группы G $\operatorname{ord}(g_1 g_2) = \operatorname{ord}(g_2 g_1)$.

8. Пусть G — неединичная группа, в которой все неединичные элементы имеют один и тот же порядок p. Доказать, что p — простое число.

9. В группе $GL_2(\mathbb{R})$ найти две матрицы a и b, имеющие конечные порядки, для которых произведение ab было бы элементом бесконечного порядка. Доказать, что в абелевой группе такое невозможно, т.е. элементы конечного порядка в абелевой группе образуют подгруппу (т.н. *подгруппу кручения*).

10. Доказать, что в абелевой группе множество тех элементов, порядки которых делят фиксированное число n, является подгруппой. Привести пример неабелевой группы, для которой это утверждение неверно.

11. Обозначим через G множество всех ненулевых вещественных чисел a, для каждого из которых a^n — рациональное число при некотором натуральном n. Доказать, что G — подгруппа $\mathbb{R}^*$. Является ли она циклической?

12. Пусть G — группа порядка n. Доказать, что группа G циклическая тогда и только тогда, когда в G существует элемент порядка n.

13. Пусть $\mathbb{Z}_n$ — циклическая группа порядка n. Найти количество элементов порядка p^m в $\mathbb{Z}_{p^n}$ $(0 < m < n$, p — простое).

14. Доказать, что любая бесконечная группа имеет бесконечно много подгрупп.

§4. Смежные классы и теорема Лагранжа.

Определение 4.1. *Пусть H — подгруппа в группе G, и $g \in G$.* ***Левым смежным классом*** *gH называется подмножество $\{gh \mid h \in H\}$ в G.* ***Правым смежным классом*** *Hg называется подмножество $\{hg \mid h \in H\}$ в G.*

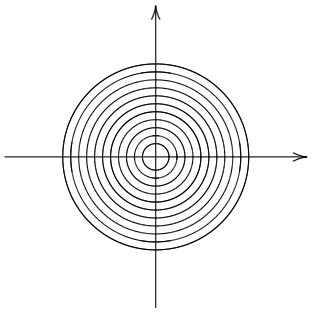
Пример 1. Смежными классами группы $\mathbb{C}^*$ по подгруппе $T = \{z \in \mathbb{C} \mid |z| = 1\}$ являются множества

$$r(\cos\varphi + i\sin\varphi)T = \{r(\cos\varphi + i\sin\varphi)z \mid |z| = 1\}.$$

Так как любое комплексное число z, $|z| = 1$, можно записать в виде $z = \cos\alpha + i\sin\alpha$, то

$$r(\cos\varphi + i\sin\varphi)T = \{r(\cos(\varphi+\alpha) + i\sin(\varphi+\alpha)) \mid \alpha \in \mathbb{R}\}.$$

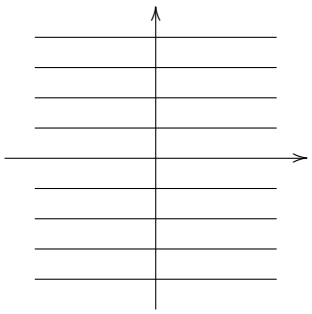
Эти смежные классы изображаются на комплексной плоскости окружностями с центром в начале координат.



Пример 2. Смежными классами аддитивной группы $\mathbb{C}$ по подгруппе $\mathbb{R}$ являются множества

$$a + bi + \mathbb{R} = \{a + bi + x \mid x \in \mathbb{R}\}.$$

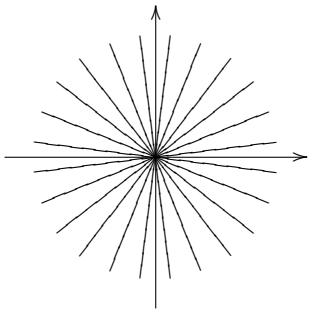
Эти смежные классы изображаются на комплексной плоскости прямыми, параллельными вещественной оси.



Пример 3. Смежными классами мультипликативной группы $\mathbb{C}^*$ по подгруппе $\mathbb{R}^{>0}$ положительных вещественных чисел являются множества

$$r(\cos\varphi + i\sin\varphi)\mathbb{R}^{>0} = \left\{rx(\cos\varphi + i\sin\varphi) \mid x \in \mathbb{R}^{>0}\right\}.$$

Эти смежные классы изображаются на комплексной плоскости лучами, исходящими из начала координат.



Предложение 4.2. *Пусть H — подгруппа в группе G и $x, y \in G$. Если $y \in xH$, то $yH = xH$. Аналогично, если $y \in Hx$, то $Hy = Hx$. В частности, если $x \in H$, то $xH = H = Hx$.*

Доказательство. Докажем предложение для левых смежных классов (для правых смежных классов доказательство проводится аналогично). По условию, $y = xh$ для некоторого $h \in H$. Тогда для любого элемента $h_1 \in H$ мы имеем $yh_1 = x(hh_1) \in xH$, значит, $yH \subset xH$. Поскольку $x = yh^{-1}$, то аналогично получаем $xH \subset yH$. Значит, $xH = yH$. □

Предложение 4.3 (О равенстве смежных классов). *Пусть H — подгруппа в группе G и $x, y \in G$. Тогда*

$$xH = yH \quad \Leftrightarrow \quad x^{-1}y \in H, \tag{4.1}$$

$$Hx = Hy \quad \Leftrightarrow \quad yx^{-1} \in H. \tag{4.2}$$

Доказательство. Если $xH = yH$, то $y = y \cdot 1 \in yH = xH$. Следовательно, $y = xh$ для некоторого $h \in H$, т.е. $x^{-1}y = h \in H$. Обратно, если $x^{-1}y = h \in H$, то $y = xh$ и в силу предложения 4.2 $xH = yH$. □

Пример 4. В случае $G = \mathrm{GL}_n(K)$, $H = \mathrm{SL}_n(K)$ условия равенства смежных классов 4.1 и 4.2 означают, что $\det g_1 = \det g_2$. Поэтому левые смежные классы в данном случае совпадают с правыми (хотя группа $\mathrm{GL}_n(K)$ не абелева); каждый из них представляет собой совокупность всех матриц с определителем, равным какому-либо фиксированному числу.

Следствие 4.4. *Пусть H — подгруппа в группе G. Тогда два левых (правых) смежных класса G по H либо совпадают, либо не пересекаются. В частности, группа G является объединением непересекающихся левых (правых) смежных классов G по H.*

Доказательство. Предположим, что $z \in xH \cap yH$. Тогда из предложения 4.2 следует, что $xH = zH = yH$. □

Представление конечной группы G в виде объединения непересекающихся левых (правых) смежных классов G по H называют **разложением Лагранжа**.

Определение 4.5. *Множество левых смежных классов группы G по подгруппе H обозначается через G/H. Мощность множества G/H называется* ***индексом*** *подгруппы H и обозначается через $[G : H]$.*

Мощность множества левых смежных классов группы G по подгруппе H совпадает с мощностью множества правых смежных классов (см. упражнение 1).

Теорема 4.6 (Лагранжа). *Если G — конечная группа и H — любая ее подгруппа, то $|G| = [G : H]|H|$*

Доказательство. Покажем, что $|xH| = |H|$. Действительно, если $H = \{h_1, \ldots, h_s\}$, то $xH = \{xh_1, \ldots, xh_s\}$ и ясно, что $xh_i \neq xh_j$ при $i \neq j$.

Разобьем G на левые смежные классы по H. Тогда каждый элемент $x \in G$ лежит в некотором классе, а именно, в xH. Поскольку различные смежные классы не пересекаются, то порядок группы G равен произведению их числа на H. □

Следствие 4.7. *Порядок любой подгруппы конечной группы делит порядок группы.*

Следствие 4.8. *Порядок любого элемента конечной группы делит порядок группы.*

Доказательство вытекает из следствия 4.7 и того, что порядок элемента равен порядку порождаемой им циклической подгруппы. □

Следствие 4.9. *Всякая конечная группа простого порядка является циклической.*

Доказательство. В силу следствия 4.7 такая группа должна совпадать с циклической подгруппой, порожденной любым элементом, отличным от единицы. □

Следствие 4.10. *Если $|G| = n$, то $g^n = 1$ для любого $g \in G$.*

Доказательство. Пусть $\operatorname{ord} g = m$. В силу следствия 4.8 имеем $m \mid n$. Значит, $g^n = (g^m)^{\frac{n}{m}} = 1$. □

Следствие 4.11. *Пусть A, B — подгруппы в G, причем $B \leq A$. Тогда*

$$[G : B] = [G : A][A : B].$$

Доказательство. По теореме Лагранжа

$$|G| = [G : A][A] = [G : B][B] \quad \text{и} \quad |A| = [A : B][B],$$

откуда и получаем требуемое равенство. □

Упражнения

1. Доказать, что соответствие $xH \leftrightarrow Hx^{-1}$ задает биекцию между множествами левых и правых смежных классов группы G по подгруппе H.

2. Взяв какую-нибудь подгруппу второго порядка в симметрической группе S_3, найти левое и правое разложение Лагранжа по этой подгруппе.

3. Найти левые и правые смежные классы симметрической группы S_4 по её подгруппе $H\,\{\boldsymbol{\sigma} \in S_4 \mid \boldsymbol{\sigma}(1) = 1\}$.

4. Пусть K — правый смежный класс группы G по подгруппе H. Доказать, что для любых $x, y, z \in K$ имеем $xy^{-1}z \in K$.

5. Доказать, что верно и обратное утверждение: если K — непустое подмножество группы G и для всех $x, y, z \in K$ имеем $xy^{-1}z \in K$, то K — правый смежный класс группы G по некоторой её подгруппе H.

6. Доказать, что если H_1 и H_2 — подгруппы конечных индексов в группе G, то их пересечение — также подгруппа конечного индекса в G.

7. Пусть G — группа, H_1 и H_2 — её подгруппы порядков m_1 и m_2, $\text{НОД}(m_1, m_2) = 1$. Доказать, что $H_1 \cap H_2 = \{1\}$.

8. Пусть G — группа порядка $2k$, H — её подгруппа порядка k. Доказать, что квадраты всех элементов G принадлежат H.

§5. Гомоморфизмы групп.

Связи между различными алгебраическими структурами одного типа устанавливаются при помощи гомоморфизмов. Понятие гомоморфизма отличается от понятия изоморфизма тем, что оно не требует биективности. В одном случае мы уже встречались с этим понятием. А именно, гомоморфизмы векторных пространств — это не что иное, как их линейные отображения. Дадим точное определение гомоморфизма групп.

Определение 5.1. *Отображение групп $f : G \to H$ называется* ***гомоморфизмом****, если $f(xy) = f(x)f(y)$ для всех $x, y \in G$. Инъективный гомоморфизм называется* ***мономорфизмом****. Сюръективный гомоморфизм называется* ***эпиморфизмом****.*

Биективный гомоморфизм является ***изоморфизмом****. Изоморфизм группы на себя называется* ***автоморфизмом****. Гомоморфизм группы в себя называется ее* ***эндоморфизмом****.*

Пусть $f : G \to H$ — гомоморфизм. Установим некоторые общие свойства гомоморфизмов групп.

Предложение 5.2.

$$f(1) = 1, \qquad f(a^{-1}) = f(a)^{-1}$$

для любого элемента $a \in G$.

Доказательство. По определению гомоморфизма

$$f(1) = f(1 \cdot 1) = f(1)f(1).$$

Умножая обе части на $f(1)^{-1}$ слева, получаем $f(1) = 1$. Далее,

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

Значит, элемент $f(a^{-1})$ является обратным к $f(a)$. □

Предложение 5.3. *Если K — подгруппа в G, то множество*

$$f(K) = \{f(x) \mid x \in K\}$$

является подгруппой в H, называемой ***образом*** *K. В частности, образ гомоморфизма f*

$$\operatorname{Im}(f) = f(G)$$

является подгруппой группы H.

Доказательство следует из определения гомоморфизма и упражнения 5.2.

Предложение 5.4. *Множество*

$$\operatorname{Ker}(f) = \{a \in G \mid f(a) = 1\}$$

является подгруппой группы G и называется ***ядром*** *гомоморфизма f.*

Если K — подгруппа в H, то множество

$$f^{-1}(K) = \{x \in G \mid f(x) \in K\}$$

является подгруппой в G, называемой ***полным прообразом*** *K, при этом* $\operatorname{Ker}(f) \leq f^{-1}(K)$.

Доказательство. Достаточно доказать, что $f^{-1}(K) \leq G$, поскольку $\operatorname{Ker}(f) = f^{-1}(\{1\})$ — полный прообраз единичной подгруппы.

$$a, b \in f^{-1}(K) \Rightarrow f(a), f(b) \in K \Rightarrow f(ab) = f(a)f(b) \in K \Rightarrow$$
$$\Rightarrow ab \in f^{-1}(K),$$
$$a \in f^{-1}(K) \Rightarrow f(a) \in K \Rightarrow f(a^{-1}) = f(a)^{-1} \in K \Rightarrow a^{-1} \in f^{-1}(K).$$

Следовательно, $f^{-1}(K) \leq G$. Далее, поскольку $1 \in K$, то $f^{-1}(1) = \operatorname{Ker}(f) \leq f^{-1}(K)$. □

Таким образом, гомоморфизм $f : G \to H$ является мономорфизмом (т.е. инъективен) тогда и только тогда, когда $\operatorname{Ker}(f) = \{1\}$; гомоморфизм f является эпиморфизмом (т.е. сюръективен) тогда и только тогда, когда $\operatorname{Im}(f) = H$; гомоморфизм f является изоморфизмом (т.е. биективен) тогда и только тогда, когда $\operatorname{Im}(f) = H$ и $\operatorname{Ker}(f) = \{1\}$.

Предложение 5.5. *Пусть $a, b \in G$. Тогда*

$$f(a) = f(b) \Leftrightarrow a\operatorname{Ker}(f) = b\operatorname{Ker}(f) \Leftrightarrow a^{-1}b \in \operatorname{Ker}(f).$$

Доказательство. Учитывая предложение 4.3 и то, что f — гомоморфизм, получаем

$$f(a) = f(b) \Leftrightarrow f(a)^{-1}f(b) = f(a^{-1})f(b) = f(a^{-1}b) = 1 \Leftrightarrow$$
$$\Leftrightarrow a^{-1}b \in \mathrm{Ker}(f) \Leftrightarrow a\,\mathrm{Ker}(f) = b\,\mathrm{Ker}(f).$$

Предложение доказано. □

Предложение 5.6. *Пусть $f : G \to H$ — изоморфизм групп. Тогда обратное отображение $f^{-1} : H \to G$ — также изоморфизм.*

Доказательство. Ясно, что f^{-1} — биекция. Пусть $x, y \in H$ и $f^{-1}(x) = a$, $f^{-1}(y) = b$. Тогда

$$f(ab) = f(a)f(b) = xy \Rightarrow ab = f^{-1}(xy),$$

а это и означает, что f^{-1} — гомоморфизм. □

Приведем примеры гомоморфизмов групп.

1. Пусть G — произвольная абелева группа. Тогда для любого $n \in \mathbb{Z}$ отображение $f : G \to G$, $f(x) = x^n$ является эндоморфизмом группы G. (Для неабелевой группы это неверно.) В случае $G = C^*$ отображение f является эпиморфизмом, а его ядром является группа C_n корней n-й степени из 1.

2. Согласно основному свойству экспоненты, отображение exp является гомоморфизмом аддитивной группы $\mathbb{R}$ в мультипликативную группу $\mathbb{R}^*$. Его образ — это подгруппа $\mathbb{R}^{*+}$ положительных чисел, а ядро тривиально.

3. Отображение $x \mapsto \cos x + i \sin x$ является гомоморфизмом аддитивной группы $\mathbb{R}$ в группу $\mathbb{C}^*$. Его образ — подгруппа $T = \{z \in \mathbb{C} \mid |z| = 1\}$ в $\mathbb{C}^*$ (окружность радиуса 1 с центром в начале координат), а ядро — все вещественные числа вида $2k\boldsymbol{\pi}$, $k \in \mathbb{Z}$.

5. Формула умножения определителей означает, что отображение $det : \mathrm{GL}_n(K) \to K^*$, $A \mapsto \det A$, является гомоморфизмом. Его ядро — это группа $\mathrm{SL}_n(K)$ матриц с определителем 1.

6. Отображение $f : \mathbb{Z} \to \mathbb{Z}_n$, ставящее в соответствие каждому элементу $x \in \mathbb{Z}$ соответствующий класс вычетов $\overline{x}$ по модулю n, является гомоморфизмом циклических групп $\mathbb{Z}$ и $\mathbb{Z}_n$. Его ядром явля-

ется циклическая подгруппа $\langle n\rangle < \mathbb{Z}$, порожденная n. Фактически, $\langle n\rangle = \{nt \mid t \in \mathbb{Z}\}$.

7. Рассмотрим отображение $\operatorname{sgn} : S_n \to H = \{\pm 1\}$, где H — циклическая группа порядка 2, определенное по правилу

$$\operatorname{sgn}(\boldsymbol{\sigma}) = \begin{cases} 1, & \text{если } \boldsymbol{\sigma} \text{ — четная подстановка,} \\ -1, & \text{если } \boldsymbol{\sigma} \text{ — нечетная подстановка.} \end{cases}$$

Легко проверить, что sgn является гомоморфизмом из G в H. Ядром этого гомоморфизма является *знакопеременная группа* A_n степени n, состоящая из всех четных подстановок.

Предложение 5.7. *Пусть $f : G \to H$, $g : H \to K$ — гомоморфизмы. Тогда*

1) $gf : G \to K$ — гомоморфизм;

2) если f и g — изоморфизмы, то gf также изоморфизм.

Доказательство. 1) Следующее вычисление показывает, что gf — гомоморфизм:

$$gf(xy) = g(f(xy)) = g(f(x)f(y)) = g(f(x))g(f(y)) = gf(x)gf(y).$$

2) Достаточно заметить, что композиция биективных отображений — биективное отображение. □

В заключение рассмотрим автоморфизмы групп. Обозначим через $\operatorname{Aut} G$ множество всех автоморфизмов группы G.

Предложение 5.8. $\operatorname{Aut} G$ *является группой относительно операции композиции автоморфизмов.*

Доказательство немедленно следует из предложений 5.6 и 5.7.

Пусть G — произвольная группа и $g \in G$. Рассмотрим отображение

$$i_g : G \to G, \qquad i_g(x) = gxg^{-1}.$$

Предложение 5.9. *i_g является автоморфизмом группы G и называется* ***внутренним*** *автоморфизмом (или* ***сопряжением*** *при помощи g).*

Доказательство. Справедливы равенства

$$i_g(xy) = gxyg^{-1} = (gxg^{-1})(gyg^{-1}) = i_g(x)i_g(y),$$
$$i_g i_{g^{-1}} = i_{gg^{-1}} = i_1 = \mathrm{id}\,.$$

Следовательно, $i_g^{-1} = i_{g^{-1}}$ — также внутренний автоморфизм. □

Множество всех внутренних автоморфизмов обозначается $\mathrm{Inn}\ G$ и $\mathrm{Inn}\ G \leq \mathrm{Aut}\, G$. Действительно,

$$i_g i_h = i_{gh} \in \mathrm{Inn}\ G, \qquad i_g^{-1} = i_{g^{-1}} \in \mathrm{Inn}\ G.$$

Теорема 5.10 (Кэли). *Любая конечная группа G порядка n изоморфна подгруппе симметрической группы S_n.*

Доказательство. Пусть $G = \{g_1, \ldots, g_n\}$. Будем рассматривать группу S_n как группу подстановок множества G. Любой элемент $\boldsymbol{\alpha} \in S_n$ можно записать в виде таблицы

$$\boldsymbol{\alpha} = \begin{pmatrix} g_1 & \ldots & g_n \\ g_{i_1} & \ldots & g_{i_n} \end{pmatrix}.$$

Поставим в соответствие элементу $a \in G$ подстановку

$$\boldsymbol{\sigma}_a = \begin{pmatrix} g_1 & \ldots & g_n \\ ag_1 & \ldots & ag_n \end{pmatrix}.$$

$\boldsymbol{\sigma}_a$ действительно подстановка, так как элементы $ag_1, \ldots, ag_n$ второй строки попарно различны. Пусть $H = \{\boldsymbol{\sigma}_{g_1}, \ldots, \boldsymbol{\sigma}_{g_n}\} \subset S_n$. Так как для любых элементов $a, b, g \in G$

$$\boldsymbol{\sigma}_a\boldsymbol{\sigma}_{a^{-1}}(g) = \boldsymbol{\sigma}_a(a^{-1}g) = aa^{-1}g = g,$$
$$\boldsymbol{\sigma}_a\boldsymbol{\sigma}_b(g) = \boldsymbol{\sigma}_a(bg) = abg = \boldsymbol{\sigma}_{ab}(g), \tag{5.1}$$

то $(\boldsymbol{\sigma}_a)^{-1} = \boldsymbol{\sigma}_{a^{-1}} \in H$ и $\boldsymbol{\sigma}_a\boldsymbol{\sigma}_b = \boldsymbol{\sigma}_{ab} \in H$. Значит, H — подгруппа в S_n. Остается проверить, что отображение

$$f : G \to H, \qquad f(a) = \boldsymbol{\sigma}_a,$$

является изоморфизмом. То, что f — гомоморфизм, следует из (5.1). Сюръективность f очевидна. Если же $f(a) = f(b)$, то $\boldsymbol{\sigma}_a = \boldsymbol{\sigma}_b$ и

$$\boldsymbol{\sigma}_a(1) = a = \boldsymbol{\sigma}_b(1) = b,$$

что доказывает инъективность f. □

Упражнения

1. Пусть $f : G \to H$ — гомоморфизм групп, $x \in G$. Доказать, что $f^{-1}(f(x)) = x\,\mathrm{Ker}(f) = \mathrm{Ker}(f)x$.

2. Пусть $f : G \to H$, $g : H \to K$ — гомоморфизмы групп.

(1) Доказать, что если gf — мономорфизм, то и f тоже мономорфизм.

(2) Доказать, что если gf — эпиморфизм, то и g тоже эпиморфизм.

3. Пусть $f : G \to H$ — эпиморфизм группы G на группу H. Доказать, что если G — абелева, то абелева и H. Верно ли обратное утверждение?

4. Доказать, что отображение $f : G \to G$, $f(x) = x^2$ является гоморфизмом группы в себя тогда и только тогда, когда группа G абелева.

5. Пусть $f : G \to H$ — гомоморфизм групп, G — конечная группа. Доказать, что для любого элемента $g \in G$ справедливо $\mathrm{ord}(f(g)) \mid \mathrm{ord}(g)$.

6. Доказать, что группа $\mathrm{Aut}\,\mathbb{Z}$ изоморфна циклической группе второго порядка.

7. Найти $\mathrm{Aut}\,\mathbb{Z}_n$ при $n = 4, 6, 8, 9$.

§6. Нормальные подгруппы. Факторгруппы.

Пусть H — подгруппа группы G и $g \in G$. Рассмотрим множество

$$gHg^{-1} = \{ghg^{-1} \mid g \in G\}.$$

Равенства

$$(gxg^{-1})(gyg^{-1}) = gxyg^{-1} \in gHg^{-1}, \qquad (gxg^{-1})^{-1} = gx^{-1}g^{-1} \in gHg^{-1}$$

показывают, что gHg^{-1} является подгруппой в G.

Определение 6.1. *Говорят, что H — **нормальная подгруппа** в G и пишут $H \lhd G$, если $gHg^{-1} \subset H$ для любого $g \in G$.*

Если $H \lhd G$, то на самом деле $gHg^{-1} = H$ для любого $g \in G$. Достаточно убедиться в том, что $H \subset gHg^{-1}$. Но $h = g(g^{-1}hg)g^{-1} \in$

gHg^{-1} для любого $h \in H$, поскольку $g^{-1}hg \in H$ в силу нормальности H.

Рассмотрим примеры нормальных подгрупп.

1. $\mathrm{SL}_n(K) \lhd \mathrm{GL}_n(K)$. Если $g \in \mathrm{GL}_n(K)$, $h \in \mathrm{SL}_n(K)$, то

$$\det(ghg^{-1}) = \det(g)\det(h)(\det(g))^{-1} = 1,$$

следовательно, $ghg^{-1} \in \mathrm{GL}_n(K)$.

2. В абелевой группе G любая подгруппа H нормальна.

3. $\{1\} \lhd G$, $G \lhd G$ — нормальные подгруппы в любой группе G.

Предложение 6.2. *Пусть $f : G \to H$ — гомоморфизм групп. Тогда $\mathrm{Ker}(f) \lhd G$.*

Доказательство. Мы уже знаем, что $\mathrm{Ker}(f) \leq G$ (см. предложение 5.4). Пусть $g \in G$, $x \in \mathrm{Ker}(f)$. Тогда

$$f(gxg^{-1}) = f(g)f(x)f(g)^{-1} = f(g)f(g)^{-1} = 1,$$

следовательно, $gxg^{-1} \in \mathrm{Ker}(f)$ и $\mathrm{Ker}(f) \lhd G$. □

Предложение 6.3. *Пусть $f : G \to H$ — гомоморфизм групп и $K \lhd G$, $T \lhd H$. Тогда $f(K) \lhd f(G)$, $f^{-1}(T) \lhd G$.*

Доказательство. Пусть $g \in f(G)$, $x \in f(K)$. Тогда $g = f(h)$, $x = f(y)$ для некоторых элементов $h \in G$, $y \in K$ и мы получаем

$$gxg^{-1} = f(h)f(y)f(h)^{-1} = f(hyh^{-1}) \in f(K),$$

поскольку в силу нормальности K элемент $hyh^{-1} \in K$. Это доказывает, что $f(K) \lhd f(G)$.

Пусть теперь $z \in f^{-1}(T)$ и $a \in G$. Тогда

$$f(aza^{-1}) = f(a)f(z)f(a)^{-1} \in T,$$

потому что $f(z) \in T$ и $T \lhd H$. Поэтому $aza^{-1} \in f^{-1}(T)$, что и доказывает нормальность $f^{-1}(T)$. □

Предложение 6.4. *Пусть $H \leq G$. Тогда $H \lhd G$ тогда и только тогда, когда левый смежный класс xH совпадает с правым смежным классом Hx для произвольного элемента x из G.*

Доказательство. Так как для любого элемента $h \in H$ имеем $xh = (xhx^{-1})x = h_1x$, где $h_1 = xhx^{-1} \in H$ в силу нормальности H, то $xH \subset Hx$. Аналогично, $Hx \subset xH$. Значит, $xH = Hx$.

Если $xH = Hx$ для произвольного элемента x из G, то для произвольного элемента $h \in H$ имеем $xh = h_1x$ для некоторого элемента $h_1 \in H$. Следовательно, $xhx^{-1} = h_1 \in H$ и $H \lhd G$. □

Определение 6.5. *Если A, B — произвольные подмножества группы G, то их произведением называется множество*

$$AB = \{ab \mid a \in A, b \in B\}.$$

Предложение 6.6. *Пусть $H \lhd G$ и $K \leq G$. Тогда*

1. *$H \cap K$ — нормальная подгруппа в K.*

2. *Множество HK совпадает с KH и является подгруппой в G, а если $K \lhd G$, то и $HK \lhd G$.*

Доказательство. Первое утверждение следует непосредственно из определения нормальной подгруппы.

Докажем, что $HK = KH$. Множество HK (соответственно KH) является объединением смежных классов Hk (соответственно kH), $k \in K$. По предложению 6.4 $kH = Hk$, значит, KH и HK состоят из одних и тех же смежных классов. Поэтому $HK = KH$.

Докажем, что $HK \leq G$. Пусть $hk, h_1k_1 \in HK$. Тогда

$$hkh_1k_1 = h(kh_1k^{-1})kk_1 = (hh_2)(kk_1) \in HK,$$

где $h_2 = kh_1k^{-1} \in H$ в силу нормальности H, поэтому $hh_2 \in H$, $kk_1 \in K$. Кроме того,

$$(hk)^{-1} = k^{-1}h^{-1} = (k^{-1}h^{-1}k)k^{-1} \in HK,$$

поскольку снова в силу нормальности H имеем $k^{-1}h^{-1}k \in H$. Значит, HK является подгруппой в G.

Предположим теперь, что $K \lhd G$. Тогда для любых элементов $h \in H$, $k \in K$, $x \in G$ имеем

$$xhkx^{-1} = (xhx^{-1})(xkx^{-1}) \in HK$$

в силу того, что H и K являются нормальными подгруппами по условию, а поэтому $xhx^{-1} \in H$, $xkx^{-1} \in K$. Значит, $HK \lhd G$. $\square$

Замечание 6.1. Если обе подгруппы H и K не являются нормальными подгруппами в G, то не всегда HK — подгруппа в G. Например, рассмотрим симметрическую группу S_3 и в ней две циклические подгруппы $H = \langle(12)\rangle$ и $K = \langle(13)\rangle$. Тогда множество $HK = \{1, (12), (13), (132)\}$ состоит из четырех элементов и не является подгруппой в S_3, поскольку 4 не делит порядок S_3, который равен 6.

Предложение 6.7. *Пусть $H \lhd G$ и $a, b \in G$. Тогда*

$$(aH)(bH) = abH. \tag{6.1}$$

Доказательство. Из равенства $abh = (a\cdot 1)(bh)$ следует, что $abH \subset (aH)(bH)$. Пусть $z \in (aH)(bH)$. Тогда

$$z = ah_1bh_2 = ab(b^{-1}h_1b)h_2.$$

Так как H — нормальная подгруппа, то $b^{-1}h_1b \in H$; значит, $z \in abH$ и $(aH)(bH) \subset abH$. Два противоположных включения влекут, что $(aH)(bH) = abH$. $\square$

Замечание 6.2. Отметим, что если выполнено свойство (6.1) для любых элементов $a, b \in G$, то нетрудно доказать, что $H \lhd G$.

Обозначим через G/H множество левых смежных классов группы G по подгруппе H. Предложение 6.7 дает нам возможность задать на G/H алгебраическую операцию формулой (6.1).

Теорема 6.8. *Множество G/H с введенной выше операцией умножения смежных классов является группой, которая называется* ***факторгруппой*** *группы G по нормальной подгруппе H. При этом смежный класс $1H = H$ является единичным элементом в G/H, а смежный класс $a^{-1}H$ — обратным элементом к aH.*

Доказательство. Так как

$$(aHbH)cH = abHcH = (ab)cH, \qquad aH(bHcH) = aHbcH = a(bc)H$$

и умножение в группе ассоциативно, т.е. $(ab)c = a(bc)$, то

$$(ab)cH = a(bc)H.$$

Следовательно, умножение смежных классов ассоциативно. Далее,

$$aHH = HaH = aH,$$

значит, H — единица в G/H. Непосредственным умножением проверяется, что $a^{-1}H$ является обратным элементом к aH. □

Определим отображение

$$f : G \to G/H, \qquad f(g) = gH.$$

Предложение 6.9. *Отображение f является сюръективным гомоморфизмом группы G на факторгруппу G/H и называется* ***каноническим гомоморфизмом****, при этом* $\mathrm{Ker}(f) = H$.

Доказательство. Равенства

$$f(xy) = xyH = xHyH = f(x)f(y)$$

доказывают, что f — гомоморфизм. Очевидно, f сюръективен. Найдем ядро f.

$$f(x) = xH = H \Leftrightarrow x \in H.$$

Таким образом, $\mathrm{Ker}(f) = H$. □

Ранее (см. предложение 6.2) мы доказали, что ядро любого гомоморфизма является нормальной подгруппой. Предложение 6.9 утверждает обратное: любая нормальная подгруппа является ядром некоторого гомоморфизма, а именно, канонического гомоморфизма.

Изучая циклические группы, мы установили в теореме 3.10, что подгруппа циклической группы — циклическая. Рассмотрим теперь факторгруппы циклических групп.

Предложение 6.10. *Пусть $G = \langle a \rangle$ — циклическая группа и $H \leq G$. Тогда G/H — циклическая группа.*

Доказательство. Так как G абелева, то $H \lhd G$. Любой элемент из G/H имеет вид $a^nH = (aH)^n$ для некоторого $n \in \mathbb{Z}$. Значит, $G/H = \langle aH \rangle$ — циклическая группа, порожденная смежным классом aH. □

Обозначим через $L(G,H)$ совокупность подгрупп группы G, содержащих подгруппу H. В частности, $L(G,1)=L(G)$ — совокупность всех подгрупп группы G, $L(G,G)=\{G\}$.

Теорема 6.11 (О соответствии). *Пусть $f: G \to H$ — сюръективный гомоморфизм групп.*

1. *Отображение $\psi: L(G, \operatorname{Ker} f) \to L(H)$, сопоставляющее подгруппе $K \in L(G, \operatorname{Ker} f)$ подгруппу $\psi(K) = f(K) \in L(H)$, является биекцией, сохраняющей включение. В частности, $f^{-1}(f(K)) = K$.*

2. *Эта биекция сохраняет нормальность: если $K \in L(G, \operatorname{Ker} f)$, то*

$$K \lhd G \Leftrightarrow f(K) \lhd H.$$

3. *Эта биекция сохраняет индексы: если $\operatorname{Ker} f \leq K \leq G$, то $[G:K] = [H:f(K)]$.*

Доказательство. 1. Отображение ψ является сюръективным, так как по предложению 5.4 полный прообраз $K = f^{-1}(T)$ подгруппы T группы H является подгруппой в G, содержащей $\operatorname{Ker} f$, и очевидно, что $\psi(K) = f(K) = T$. Проверим инъктивность ψ.Пусть K_1, K_2 — две подгруппы в G, содержащие $\operatorname{Ker} f$, и $K_1 \neq K_2$. Предположим, что $f(K_1) = f(K_2)$. Так как $K_1 \neq K_2$, то найдется элемент x, лежащий в одной из этих групп и не лежащий в другой. Пусть, например, $x \in K_1$ и $x \notin K_2$. Тогда $f(x) \in f(K_1) = f(K_2)$, значит, $f(x) = f(y)$ для некоторого элемента $y \in f(K_2)$. Следовательно, $1 = f(x)f(y)^{-1} = f(xy^{-1})$, т.е. $xy^{-1} = z \in \operatorname{Ker} f$. Таким образом, $x = zy \in \operatorname{Ker} f \subset K_2$ — противоречие, доказывающее биективность ψ.

2. Утверждение этого пункта немедленно следует из более общего предложения 6.3.

3. Отображение из множества левых смежных классов G по K в множество левых смежных классов H по $f(K)$, заданное правилом $xK \mapsto f(x)f(K)$, очевидно, является сюръективным отображением. Это отображение инъективно, так как из $f(x)f(K) = f(y)f(K)$ следует $f(x)^{-1}f(y) = f(x^{-1}y) \in f(K)$, то есть $x^{-1}y \in K$ в силу пункта 1 нашей теоремы. Следовательно, $xK = yK$. $\square$

Упражнения

1. Пусть $C(G) = \{g \in G \mid gh = hg \text{ для всех } h \in G\}$ — **центр** группы G. Доказать, что $C(G)$ — нормальная подгруппа в G.

2. Знакопеременная группа A_n — нормальная подгруппа симметрической группы S_n.

3. Пусть H_i, $i \in I$, — нормальные подгруппы в группе G. Доказать, что $H = \bigcap\limits_{i \in I} H_i \lhd G$.

4. Доказать, что если G — абелева группа и $H \lhd G$, то факторгруппа G/H — абелева.

5. Найти все нормальные подгруппы группы S_3.

6. Верно ли, что $GL_n(\mathbb{Q}) \lhd GL_n(\mathbb{R})$?

7. Доказать, что в любой группе подгруппа индекса 2 является нормальной.

8. Пусть M — подмножество группы G. Положим $C_G(M) = \{g \in G \mid gm = mg$ для любого $m \in M\}$ (*централизатор* M в G). Доказать, что если $H \lhd G$, то $C_G(H) \lhd G$.

9. Доказать, что для циклической группы G из $G/A = G/B$ следует $A = B$.

10. Группа называется *периодической*, если каждый её элемент имеет конечный порядок. Доказать, что если нормальная подгруппа H и факторгруппа G/H группы G периодические, то и сама группа G — периодическая.

11. Доказать, что в факторгруппе $\mathbb{Q}^+/\mathbb{Z}^+$ каждый элемент имеет конечный порядок. Конечна ли эта факторгруппа?

12. Пусть $H_1, H_2 \lhd G$, причём G/H_1 и G/H_2 — абелевы. Доказать, что $G/(H_1 \cap H_2)$ также абелева.

§7. Теоремы о гомоморфизмах.

Теорема 7.1 (Основная о гомоморфизмах групп). *Пусть $f : G \to H$ — гомоморфизм групп. Тогда*

$$f(G) \simeq G/\operatorname{Ker} f.$$

Доказательство. Рассмотрим отображение

$$\psi : G/\operatorname{Ker} f \to f(G), \qquad \psi(g \operatorname{Ker} f) = f(g).$$

Убедимся, что ψ корректно определено, т.е. если $g \operatorname{Ker} f = h \operatorname{Ker} f$, то $\psi(g \operatorname{Ker} f) = \psi(h \operatorname{Ker} f)$ или, что эквивалентно, $f(g) = f(h)$. По предложению 4.3 равенство смежных классов $g \operatorname{Ker} f = h \operatorname{Ker} f$ означает, что $g^{-1}h \in \operatorname{Ker} f$. Значит, $f(g^{-1}h) = f(g^{-1})f(h) = 1$, откуда $f(g) = f(h)$.

Отображение ψ является гомоморфизмом, поскольку

$$\psi(g \operatorname{Ker} f \; h \operatorname{Ker} f) = \psi(gh \operatorname{Ker} f) = f(gh) = \\ = f(g)f(h) = \psi(g \operatorname{Ker} f)\psi(h \operatorname{Ker} f).$$

Очевидно, ψ сюръективно, поскольку для любого элемента $f(g) \in f(G)$ мы имеем $f(g) = \psi(g \operatorname{Ker} f)$.

И наконец, ψ инъективно, поскольку если $\psi(g \operatorname{Ker} f) = \psi(h \operatorname{Ker} f)$, то $f(g) = f(h)$ и, следовательно, $1 = f(g)^{-1}f(h) = f(g^{-1}h)$. Значит, $g^{-1}h \in \operatorname{Ker} f$, поэтому по предложению 4.3 $g \operatorname{Ker} f = h \operatorname{Ker} f$. □

Теорема 7.2 (Вторая о гомоморфизмах). *Если H и N — нормальные подгруппы группы G, причем $N \leq H$, то H/N — нормальная подгруппа группы G/N и*

$$(G/N)/(H/N) \simeq G/H.$$

Доказательство. По теореме о соответствии 6.11 подгруппа H/N нормальна в G/N. Факторгруппа $(G/N)/(H/N)$ состоит из смежных классов $gN(H/N)$, где gN — элемент факторгруппы G/N. Рассмотрим отображение $f : G \to (G/N)/(H/N)$, определяемое равенством $f(g) = gN(H/N)$. Очевидно, f сюръективно. Далее, f является гомоморфизмом, поскольку

$$f(gt) = gtN(H/N) = gN(H/N)tN(H/N) = f(g)f(t).$$

Докажем, что $\operatorname{Ker}(f) = H$. Очевидно, $H \subset \operatorname{Ker}(f)$, поскольку если $h \in H$, то $f(h) = hN(H/N) = H/N$ — единичный элемент группы $(G/N)/(H/N)$. Докажем противоположное включение. Пусть $f(g) = gN(H/N) = H/N$. Тогда $gN \in H/N$, откуда $gN = hN$ для некоторого элемента $h \in H$. Значит, по предложению 4.3 $h^{-1}g = h_1 \in H$, следова-

тельно, $g = hh_1 \in H$. Таким образом, $\mathrm{Ker}(f) \subset H$ и мы должны иметь равенство $\mathrm{Ker}\, f = H$.

Применяя основную теорему о гомоморфизмах, получаем $G/H \simeq (G/N)/(H/N)$. □

Замечание 7.1. Отметим, что теорема 7.2 дополняет теорему 6.11. Биекция $\boldsymbol{\psi}$ из теоремы 6.11 сохраняет не только номальность подгрупп и не только индексы, но также индуцирует биекцию между множеством факторгрупп группы G по нормальным подгруппам H, содержащим N, и множеством факторгрупп группы G/N.

Теорема 7.3 (Третья о гомоморфизмах). *Пусть H — нормальная подгруппа группы G. Тогда для любой подгруппы A пересечение $A \cap H$ является нормальной подгруппой в A и*

$$A/A \cap H \simeq AH/H.$$

Доказательство. В силу предложения 6.6, $A \cap H \lhd A$, $AH \leq G$. Поскольку H — нормальная подгруппа группы G, то тем более $H \lhd AH$. Поэтому определены рассматриваемые в теореме факторгруппы AH/H и $A/A \cap H$. Любой элемент факторгруппы AH/H имеет вид $ahH = aH$ для некоторого $a \in A$. Зададим отображение $f : A \to AH/H$ формулой $f(a) = aH$.

Следующее вычисление показывает, что f — гомоморфизм.

$$f(ab) = abH = aHbH = f(a)f(b).$$

Очевидно, f является сюръективным отображением. Найдем ядро f. Так как $f(h) = hH = H$, то $H \subset \mathrm{Ker}\, f$. Далее, если $x \in \mathrm{Ker}\, f$, то $f(x) = xH = H$. Следовательно, $x \in H$, откуда получаем $H = \mathrm{Ker}\, f$. Применяя основную теорему о гомоморфизмах, получаем $AH/H \simeq A/A \cap H$. □

Упражнения

1. Пусть E — единичная подгруппа группы G. Доказать, что $G/E \simeq G$.

2. Пусть U обозначает мультипликативную группу комплексных чисел с модулем, равным 1. Доказать, что $\mathbb{R}^+/\mathbb{Z}^+ \simeq U$.

3. Для натурального n рассмотрим отображение $f : U \to U$, $x \mapsto x^n$. Доказать, что f гомоморфизм, найти ядро f и доказать, что $U/\operatorname{Ker} f \simeq U$.

4. Пусть $F = \{(x_1, \ldots, x_m, 0, \ldots, 0)\}$ — подгруппа аддитивной группы $\mathbb{R}^n$. Найти факторгруппу $\mathbb{R}^n/F$.

5. Пользуясь основной теоремой о гомоморфизмах, доказать, что:
а) $S_n/A_n \simeq \{\pm 1\}$; б) $\mathrm{GL}_n(K)/\mathrm{SL}_n(K) \simeq K^*$.

6. Пусть $M_n(R)$ — кольцо квадратных матриц n-го порядка с элементами из кольца R. Найти фактогруппу (т.е. указать, какой из известных групп она изоморфна):

1) $M_2(\mathbb{R})^+/H$, где $H = \left\{ \begin{pmatrix} a & b \\ c & -a \end{pmatrix} \mid a, b, c \in \mathbb{R} \right\}$;

2) $M_2(\mathbb{R})^+/H$, где $H = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a + b + c + d = 0 \right\}$;

3) $GL_n(\mathbb{C})/H$, где $H = \{a \mid \det a = \pm 1\}$;

4) $GL_n(\mathbb{R})/H$, где $H = \{a \mid \det a > 0\}$;

§8. Коммутант.

Определение 8.1. *Выражение*

$$[x, y] = xyx^{-1}y^{-1}$$

называется ***коммутатором*** *элементов x, y группы G.*

Коммутатор служит корректирующим множителем, необходимым для того, чтобы поменять местами x и y:

$$xy = [x, y]yx.$$

Отсюда следует простое, но полезное

Предложение 8.2. *Элементы x и y перестановочны тогда и только тогда, когда коммутатор $[x, y] = 1$.*

Определение 8.3. ***Коммутантом*** *группы G называют подгруппу $[G,G]$, порожденную множеством всех коммутаторов $[x,y]$, $x,y \in G$.*

Хотя $[x,y]^{-1} = yxy^{-1}x^{-1} = [y,x]$ — снова коммутатор, однако произведение двух коммутаторов быть им уже не обязано. Таким образом, $[G,G]$ состоит из всевозможных произведений вида

$$[x_1,y_1][x_2,y_2]\dots[x_k,y_k], \qquad x_i,y_i \in G.$$

Предложение 8.4. *Если $K \lhd G$, то $[K,K] \lhd G$. В частности, $[G,G] \lhd G$.*

Доказательство. Непосредственное вычисление показывает, что для любых элементов $x_i, y_i \in K$, $1 \le i,j \le n$, и любого $g \in G$

$$g[x_1,y_1]\dots[x_k,y_k]g^{-1} = [gx_1g^{-1}, gy_1g^{-1}]\dots[gx_kg^{-1}, gy_kg^{-1}] \in [K,K],$$

поскольку по условию $K \lhd G$ и поэтому $gx_ig^{-1}, gy_ig^{-1} \in K$ $(i = 1,\dots,k)$. □

Докажем теперь общее утверждение, вскрывающее внутренний смысл понятия коммутант.

Теорема 8.5. *Факторгруппа $G/[G,G]$ абелева. Любая подгруппа $K \le G$, содержащая коммутант $[G,G]$, нормальна в G и факторгруппа G/K абелева. Обратно, если $K \lhd G$ и факторгруппа G/K абелева, то $[G,G] \le K$ (в частности, если G — конечная группа, то максимальный порядок абелевой факторгруппы G/K равен индексу $[G:[G,G]]$).*

Доказательство. Докажем, что факторгруппа $G/[G,G]$ абелева.

$$[a[G,G], b[G,G]] = a[G,G]\cdot b[G,G]\cdot a^{-1}[G,G]\cdot b^{-1}[G,G] = \\ = aba^{-1}b^{-1}[G,G] = [a,b][G,G] = [G,G],$$

т.е. коммутатор любых двух злементов факторгруппы G/K равен единичному элементу K. По предложению 8.2 любые два элемента факторгруппы G/K перестановочны. Значит, $G/[G,G]$ — абелева группа.

Докажем, что если $[G,G] \le K$, то $K \lhd G$. Если $x \in K$, $g \in G$, то

$$gxg^{-1} = (gxg^{-1}x^{-1})x = [g,x]x \in [G,G]K = K,$$

откуда $K \lhd G$.

Докажем, что G/K — абелева. В силу второй теоремы о гомоморфизмах групп,

$$G/K \simeq (G/[G,G])/(K/[G,G]).$$

Поскольку $G/[G,G]$ — абелева группа, то в силу упражнения 4 из §6 факторгруппа $(G/[G,G])/(K/[G,G])$ также абелева. Значит, G/K — абелева.

Обратно, если $K \lhd G$ и факторгруппа G/K абелева, то

$$[a,b]K = aba^{-1}b^{-1}K = (aK)(bK)(a^{-1}K)(b^{-1}K) = [aK,bK] = K$$

для всех $a, b \in G$. Значит, $[a,b] \in K$ для всех $a, b \in G$. Следовательно, $[G,G] \leq K$, поскольку $[G,G]$ порождается коммутаторами $[a,b]$. □

Определение 8.6. *Пусть H и K — подгруппы группы G.* ***Взаимным коммутантом*** *групп H и K называется подгруппа $[H,K]$, порожденная всеми комутаторами вида $[h,k]$, $h \in H$, $k \in K$.*

Предложение 8.7. *Пусть $H \lhd G$, $K \lhd G$ и $H \cap K = \{1\}$. Тогда $[H,K] = 1$. В частности, любой элемент $h \in H$ перестановочен с любым элементом $k \in K$.*

Доказательство. Для произвольных элементов $h \in H$, $k \in K$ рассмотрим элемент $[h,k] = hkh^{-1}k^{-1}$. Так как $kh^{-1}k^{-1} \in H$ в силу нормальности H, то $[h,k] \in H$. С другой стороны, $hkh^{-1} \in K$ в силу нормальности K, поэтому $[h,k] \in K$. Следовательно, $[h,k] \in H \cap K = \{1\}$, откуда получаем $[H,K] = 1$. □

Упражнения

1. Доказать, что если H и K — нормальные подгруппы группы G, то их взаимный коммутант $[H,K]$ является нормальной подгруппой в G.

2. Найти коммутант группы

а) S_3; б) $GL_2(\mathbb{R})$; в) мультипликативной группы матриц вида $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$, где $a, b \in \mathbb{R}$, $a \neq 0$; в) S_n.

3. Пусть $f : G \to H$ — эпиморфизм групп. Доказать, что $f([G,G]) = [H,H]$. Верно ли, что $[G,G] = f^{-1}(H)$?

4. Доказать, что подгруппа индекса 2 содержит коммутант группы.

5. Пусть коммутант группы G содержится в её центре. Доказать, что для любых $a, b, c \in G$ $[ab, c] = [a, c][b, c]$.

§9. Прямое произведение групп.

Сейчас мы рассмотрим конструкцию, которая позволяет строить новые группы с помощью уже известных.

Пусть $G_1, \ldots, G_n$ — произвольные группы,

$$G = G_1 \times \cdots \times G_n = \{(g_1, \ldots, g_n) \mid g_i \in G_i, i = 1, \ldots, n\} —$$

их декартово произведение. Определим на G алгебраическую операцию формулой

$$(g_1, \ldots, g_n) \cdot (h_1, \ldots, h_n) = (g_1 h_1, \ldots, g_n h_n). \tag{9.1}$$

Теорема 9.1. *Декартово произведение $G = G_1 \times \cdots \times G_n$ с введенной выше алгебраической операцией является группой, которая называется* ***(внешним) прямым произведением*** *групп $G_1, \ldots, G_n$.*

Доказательство. Умножение в G, определяемое формулой (9.1), является ассоциативным, поскольку, фактически, сводится к умножению элементов в каждой из групп G_i. Элемент $e = (1_{G_1}, \ldots, 1_{G_n})$, где 1_{G_i} — единичный элемент группы G_i, очевидно, является нейтральным элементом относительно введенной операции. Наконец, $(g_1, \ldots, g_n)^{-1} = (g_1^{-1}, \ldots, g_n^{-1})$ — элемент, обратный к $(g_1, \ldots, g_n)$. □

При аддитивной записи групповой операции в $G_1, \ldots, G_n$ говорят о **прямой сумме** групп $G_1, \ldots, G_n$ и пишут $G_1 \oplus \cdots \oplus G_n$.

Отметим простейшие свойства прямых произведений групп.

1. Если $G_1, \ldots, G_n$ — конечные группы, то $G = G_1 \times \cdots \times G_n$ — конечная группа и

$$|G| = |G_1| \ldots |G_n|.$$

2. Если $G_1 \simeq H_1, \ldots, G_n \simeq H_n$, то $G_1 \times \cdots \times G_n \simeq H_1 \times \cdots \times H_n$.

Действительно, если $f_i : G_i \to H_i$ — изоморфизм, то отображение

$$f : G_1 \times \cdots \times G_n \to H_1 \times \cdots \times H_n, \quad f(g_1, \ldots, g_n) = (f_1(g_1), \ldots, f_n(g_n)),$$

очевидно, является требуемым изоморфизмом.

3. Для каждой группы G_i рассмотрим гомоморфизм

$$\varphi_i : G_i \to G, \qquad \varphi_i(g) = (1, \ldots, 1, g, 1, \ldots, 1)$$

(g находится на i-м месте). Ясно, что φ_i инъективен и, по основной теореме о гомоморфизмах, группа G_i изоморфна подгруппе $G_i' = \varphi_i(G_i) \leq G$. Кроме того, $G_i' \lhd G$, поскольку

$$(g_1, \ldots, g_n)(1, \ldots, 1, g, 1, \ldots, 1)(g_1, \ldots, g_n)^{-1} = \\ = (1, \ldots, 1, g_i g g_i^{-1}, 1, \ldots, 1) \in G_i'.$$

Непосредственно из определения подгрупп G_i' следует, что если $i \neq j$, то $G_i' \cap G_j' = \{1\}$. Легко проверить, что при $i \neq j$ любые элементы $x \in H_i$, $y \in H_j$ перестановочны, т.е. $xy = yx$.

Предложение 9.2. *Произвольный элемент $x \in G$ единственным образом представляется в виде произведения $y_1 \ldots y_n$, где $y_i \in G_i'$.*

Доказательство. Пусть $x = (x_1, \ldots, x_n)$. Положим

$$y_i = (1, \ldots, 1, x_i, 1, \ldots, 1) \in H_i.$$

Непосредственное вычисление показывает, что $x = y_1 \ldots y_n$. Если бы мы имели другое разложение $x = z_1 \ldots z_n$, где

$$z_i = (1, \ldots, 1, x_i', 1, \ldots, 1) \in H_i,$$

то тогда

$$x = (x_1', \ldots, x_n') = (x_1, \ldots, x_n),$$

откуда $x_i = x_i'$, $i = 1, \ldots, n$. Следовательно, $y_i = z_i$, что и доказывает единственность разложения. □

Предложение 9.2 подводит нас к следующему определению.

Определение 9.3. *Пусть $G_1, \ldots, G_n$ — нормальные подгруппы группы G. Говорят, что G является* ***внутренним прямым произведением*** *своих подгрупп $G_1, \ldots, G_n$, если каждый элемент*

$g \in G$ единственным образом представляется в виде произведения $g = g_1 \dots g_n$, где $g_i \in G_i$, $i = 1, \dots, n$.

Учитывая это определение, можно сказать, что внешнее прямое произведение групп $G_1, \dots, G_n$ является внутренним прямым произведением своих нормальных подгрупп $G_1', \dots, G_n'$, причем каждая из групп G_i' является изоморфной копией группы G_i.

Предложение 9.4. *Если G является внутренним прямым произведением своих нормальных подгрупп $G_1, \dots, G_n$, то*

1) *$G_i \cap G_j = \{1\}$ при $i \neq j$;*

2) *$xy = yx$ для любых элементов $x \in G_i$, $y \in G_j$, $i \neq j$.*

Доказательство. Пусть $z \in G_i \cap G_j$. Элемент z можно двумя способами представить в виде произведения элементов из подгрупп $G_1, \dots, G_n$:

$$z = 1 \cdot \dots \cdot 1 \cdot z \cdot 1 \cdot \dots \cdot 1 = 1 \cdot \dots \cdot 1 \cdot z \cdot 1 \cdot \dots \cdot 1$$

(в первом случае z стоит на i-ом месте, а во втором — на j-ом). Из единственности такого представления следует, что $z = 1$.

Утверждение 2) немедленно следует из предложения 8.7. □

Теорема 9.5. *Если G — внутреннее прямое произведение своих нормальных подгрупп $G_1, \dots, G_n$, то $G \simeq G_1 \times \dots \times G_n$.*

Доказательство. Рассмотрим отображение $f : G_1 \times \dots \times G_n \to G$, $f((g_1, \dots, g_n)) = g_1 \dots g_n$. Поскольку каждый элемент $g \in G$ представляется в виде произведения $g = g_1 \dots g_n$, то отображение f сюръективно. Из единственности такого представления следует инъективность f.

Пусть $x = (g_1, \dots, g_n)$, $y = (h_1, \dots, h_n)$. В силу пункта 2 предложения 9.4 элементы g_i и h_j перестановочны при $i \neq j$. Тогда следующее вычисление показывает, что f — гомоморфизм:

$$f(xy) = f((g_1h_1, \dots, g_nh_n)) = g_1h_1 \dots g_nh_n = \\ = g_1 \dots g_nh_1 \dots h_n = f(x)f(y).$$

Значит, f — искомый изоморфизм. □

Отличие внутреннего прямого произведения от внешнего состоит в том, что в первом случае G содержит сами нормальные подгруппы $G_1, \ldots, G_n$, а во втором — подгруппы $G'_1, \ldots, G'_n$, которые изоморфны группам $G_1, \ldots, G_n$.

Теорема 9.5 показывает, что если группа G есть внутреннее прямое произведение своих нормальных подгрупп $G_1, \ldots, G_n$, то изучение G полностью сводится к изучению ее подгрупп $G_1, \ldots, G_n$,

Рассмотрим более подробно случай двух множителей.

Теорема 9.6. *Группа G разлагается в прямое произведение своих подгрупп G_1 и G_2 тогда и только тогда, когда выполнены следующие условия*

1) *подгруппы G_1 и G_2 нормальны;*

2) $G_1 \cap G_2 = \{1\}$*;*

3) $G = G_1 G_2$*, т. е. каждый элемент $g \in G$ представляется в виде $g = g_1 g_2$, где $g_1 \in G_1$, $g_2 \in G_2$.*

Доказательство. Утверждение "только тогда"уже доказано выше. Пусть, обратно, выполнены условия 1)–3) предложения. Остается проверить единственность представления элемента $g \in G$ в виде $g = g_1 g_2$, где $g_1 \in G_1$, $g_2 \in G_2$. Пусть

$$g_1 g_2 = g'_1 g'_2 \qquad (g_1, g'_1 \in G_1,\ g_2, g'_2 \in G_2).$$

Тогда

$$g_1^{-1} g'_1 = g_2 {g'_2}^{-1} \in G_1 \cap G_2 = \{1\},$$

откуда

$$g_1 = g'_1, \quad g_2 = g'_2,$$

что и требуется доказать. □

Пример 1. Пусть $G = \{1, a, b, c\}$ — нециклическая группа порядка 4. Легко видеть, что квадрат любого из элементов a, b, c равен единице, а произведение любых двух из них (в любом порядке) равно третьему. Отсюда следует, что G есть прямое произведение любых двух различных циклических подгрупп второго порядка, например,

$$G = \{1, a\} \times \{1, b\}.$$

Пример 2. Возможность и единственность представления комплексного числа, отличного от нуля, в тригонометрической форме означает, что

$$\mathbb{C}^* = \mathbb{R}^* \times T,$$

где $T = \{z \in \mathbb{C} \mid |z| = 1\}$.

Пример 3. Пусть $G = GL_n^+(\mathbb{R})$ — группа матриц с положительным определителем, G_1 — подгруппа скалярных матриц λE с $\lambda > 0$ и $G_2 = SL_n(\mathbb{R})$. Тогда $G = G_1 \times G_2$. В самом деле, G_1 и G_2 — нормальные подгруппы, $G_1 \cap G_2 = \{E\}$ и $G = G_1 G_2$, так как каждая матрица $A \in G$ может быть представлена в виде

$$A = \lambda A_1 = (\lambda E) A_1,$$

где

$$\lambda = \sqrt[n]{\det A}, \qquad A_1 = \frac{1}{\lambda} A \in G_2 = SL_n(\mathbb{R}).$$

В следующей теореме описывается строение факторгрупп прямых произведений по нормальным подгруппам специального вида. Эта теорема будет использоваться в следующем параграфе при доказательстве теоремы о строении конечно порожденных абелевых групп.

Теорема 9.7. *Пусть $G = G_1 \times \cdots \times G_n$ и $H_i \leq G_i$, $i = 1, \ldots, n$.*

1. *Прямое произведение $H = H_1 \times \cdots \times H_n$ является подгруппой в G.*

2. *Если $H_i \lhd G_i$, $i = 1, \ldots, n$, то $H \lhd G$ и*

$$G/H \simeq G_1/H_1 \times \cdots \times G_n/H_n.$$

Доказательство. 1. Непосредственная проверка показывает, что $H \leq G$.

2. Пусть $x = (x_1, \ldots, x_n) \in H$, $y = (y_1, \ldots, y_n) \in G$. Тогда

$$yxy^{-1} = (y_1 x_1 y_1^{-1}, \ldots, y_n x_n y_n^{-1}) \in H$$

в силу того, что $H_i \lhd G_i$, откуда $H \lhd G$.

Рассмотрим отображение

$$f : G \to G_1/H_1 \times \cdots \times G_n/H_n, \quad f((g_1, \ldots, g_n)) = (g_1 H_1, \ldots, g_n H_n).$$

Несложное вычисление показывает, что f — гомоморфизм. Кроме того, очевидно, f сюръективно. Найдем ядро f. Имеем следующие эквивалентные утверждения:

$$g = (g_1, \ldots, g_n) \in \operatorname{Ker} f \Leftrightarrow f(g) = (g_1 H_1, \ldots, g_n H_n) = (H_1, \ldots, H_n) \Leftrightarrow$$
$$g_i \in H_i,\ i = 1, \ldots, n \Leftrightarrow g \in H.$$

Значит, $\operatorname{Ker} f = H$ и по основной теореме о гомоморфизмах $G/H \simeq G_1/H_1 \times \cdots \times G_n/H_n$. □

Замечание. Отметим, что если H — произвольная подгруппа в $G = G_1 \times \cdots \times G_n$, то не обязательно $H = H_1 \times \cdots \times H_n$ для некоторых подгрупп $H_i \leq G_i$. Например, если $G = \langle a \rangle$ — циклическая группа порядка 2 и $K = G \times G$, то циклическая подгруппа $H = \langle (a, a) \rangle < K$ имеет порядок 2 и, очевидно, не может быть прямым произведением двух групп, порядок каждой из которых больше единицы.

В заключение исследуем вопрос, какие циклические группы раскладываются в прямое произведение своих подгрупп.

Определение 9.8. *Конечная группа G называется p-группой, если $|G| = p^k$, где p — простое число.*

Теорема 9.9. *Пусть n — натуральное число и $n = p_1^{k_1} \ldots p_s^{k_s}$ — его разложение на простые множители.*

1. *Если G — циклическая группа порядка n, то $G \simeq H = C_1 \times \cdots \times C_s$, где C_i — циклическая p_i-группа порядка $p_i^{k_i}$, $i = 1, \ldots, s$.*

2. *Циклическая группа $G = \langle a \rangle$ порядка p^k, где p простое число, неразложима в прямое произведение нетривиальных подгрупп.*

3. *Бесконечная циклическая группа неразложима в прямое произведение нетривиальных подгрупп.*

Доказательство. 1. Пусть a_i — образующая циклической группы C_i, $i = 1, \ldots, s$. Тогда $\operatorname{ord} a_i = p_i^{k_i}$. В группе H рассмотрим элемент $h = (a_1, \ldots, a_n)$ и найдем его порядок. Если

$$h^k = (a_1^k, \ldots, a_n^k) = (1, \ldots, 1),$$

то это эквивалентно тому, что $a_i^k = 1$ для $i = 1, \ldots, s$. Значит, k делится на каждое из чисел $\operatorname{ord} a_i = p_i^{k_i}$ и поэтому является их общим

кратным. Наименьшее такое k является наименьшим общим кратным чисел $p_1^{k_1}, \ldots, p_s^{k_s}$ и равно их произведению в силу того, что $p_1, \ldots, p_s$ — попарно различные простые числа. Значит, $k = n = \operatorname{ord} h$. Поскольку n — это порядок группы H, то $H = \langle h \rangle$ — циклическая группа порядка n. Так как все циклические группы одного и того же порядка изоморфны, то $G \simeq H$.

2. Пусть H и K — нетривиальные подгруппы в $G = \langle a \rangle$. По теореме 3.10 H и K — циклические подгруппы в G и по теореме Лагранжа их порядки делят p^k. Значит, $|H| = p^l$, $|K| = p^m$, где $0 < l, m < k$. Снова в силу теоремы 3.10 группа H порождается элементом $h = a^t$, где $t = p^k/p^l = p^{k-l}$, а группа K — элементом $k = a^r$, где $r = p^k/p^m = p^{k-m}$. Пусть для определенности $t \leq r$. Тогда $l \geq m$ и

$$k = a^r = a^{p^{k-m}} = (a^{p^{k-l}})^{p^{l-m}} = h^{p^{l-m}} \in H.$$

Значит, любые две нетривиальные подгруппы в G имеют нетривиальное пересечение и G не может быть их прямым произведением.

3. В качестве бесконечной циклической группы возьмем $\mathbb{Z}$. Пусть H и K — ненулевые подгруппы в $\mathbb{Z}$. Тогда H и K — циклические группы с образующими n и m соответственно и $0 \neq nm \in H \cap K$. Значит, любые две ненулевые подгруппы в $\mathbb{Z}$ имеют ненулевое пересечение и $\mathbb{Z}$ не может быть их прямым произведением. □

Упражнения

1. Выяснить, при каких n

$$GL_n(\mathbb{R}) = \{\lambda E \mid \lambda \in \mathbb{R}^*\} \times SL_n(\mathbb{R}).$$

2. Элементы каких порядков встречаются в группе:

а) $S_3 \times \mathbb{Z}_4$; б) $S_3 \times S_3$; в) $A_4 \times \mathbb{Z}_5$.

3. Найти все подгруппы в группе $S_3 \times \mathbb{Z}_2$.

4. Сколько элементов порядка 2 содержится в группе $\mathbb{Z}_{10} \times \mathbb{Z}_{10} \times \mathbb{Z}_{10}$?

5. Найти число подгрупп в:

а) $\mathbb{Z}_p \times \mathbb{Z}_q$, p, q — различные простые; б) $\mathbb{Z}_p \times \mathbb{Z}_p$, p — простое.

6. Доказать, что $[G \times H, G \times H] = [G, G] \times [H, H]$.

7. Доказать, что $Z(G \times H) = Z(G) \times Z(H)$, где $Z(G)$ — центр группы G.

8. Доказать, что если группа $A \times B$ циклическая, то A и B — конечные циклические.

§10. Конечно порожденные абелевы группы.

В этом параграфе описывается строение конечно порожденных абелевых групп. Все абелевы группы будут предполагаться аддитивными, т.е. групповая операция — сложение, нейтральный элемент — 0.

Определение 10.1. *Множество элементов $e_1, \ldots, e_n$ является базисом абелевой группы A, если*

1) *элементы $e_1, \ldots, e_n$ целочисленно независимы, т.е. из того, что*

$$m_1 e_1 + \cdots + m_n e_n = 0, \quad \text{где } m_1, \ldots, m_n \in \mathbb{Z},$$

следует, что $m_1 = \cdots = m_n = 0$;

2) *элементы $e_1, \ldots, e_n$ порождают группу A, т.е. каждый элемент $x \in A$ представим в виде $x = m_1 e_1 + \cdots + m_n e_n$.*

*Группа A **свободна**, если она обладает базисом. **Рангом** свободной абелевой группы A называется число элементов в базисе A.*

Предложение 10.2. *Если A — свободная абелева группа с базисом $e_1, \ldots, e_n$, то A является прямой суммой своих бесконечных циклических подгрупп $\langle e_1 \rangle, \ldots, \langle e_n \rangle$, т.е.*

$$A = \langle e_1 \rangle \oplus \cdots \oplus \langle e_n \rangle .$$

Доказательство. Из определения свободной абелевой группы следует, что элементы e_i, $i = 1, \ldots, n$, имеют бесконечный порядок, т.е. $\langle e_i \rangle$ — бесконечная циклическая группа, и что каждый элемент $x \in A$ представим единственным образом в виде

$$x = m_1 e_1 + \cdots + m_n e_n, \tag{10.1}$$

при этом $m_i e_i \in \langle e_i \rangle$, $i = 1, \ldots, n$. Значит, A является прямой суммой подгрупп $\langle e_1 \rangle, \ldots, \langle e_n \rangle$. □

Предложение 10.3. 1. *Группа* $\mathbb{Z}^n = \underbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}_{n}$ *— свободная абелева группа ранга* n.

2. *Если* A *— свободная абелева группа ранга* n, *то* $A \simeq \mathbb{Z}^n$.

Доказательство. 1. Элементарная проверка показывает, что элементы

$$e_i = (0, \ldots, 0, 1, 0, \ldots, o), \quad i = 1, \ldots, n,$$

где 1 находится на i-м месте, образуют базис $\mathbb{Z}^n$.

2. Если $e_1, \ldots, e_n$ — базис A, то зададим $f : A \to \mathbb{Z}^n$ по правилу: если $x \in A$ имеет представление (10.1), то $f(x) = (m_1, \ldots, m_n)$. Очевидно, f является биекцией. Если $y = l_1 e_1 + \cdots + l_n e_n$, то $x + y = (m_1 + l_1)e_1 + \cdots + (m_n + l_n)e_n$, откуда

$$f(x+y) = (m_1 + l_1, \ldots, m_n + l_n) = (m_1, \ldots, m_n) + (l_1, \ldots, l_n) = \\ = f(x) + f(y).$$

Значит, f — искомый изоморфизм. □

Теорема 10.4. *Пусть* A *— свободная абелева группа с базисом* $e_1, \ldots, e_n$. *Предположим, что* $c_1, \ldots, c_n$ *— элементы произвольной абелевой группы* C. *Тогда существует, и притом единственный, гомоморфизм* $f : A \to C$ *такой, что* $f(e_i) = c_i$, $1 \leq i \leq n$.

Доказательство. Вначале докажем существование гомоморфизма f. Каждый элемент $x \in A$ представим единственным образом в виде $x = m_1 e_1 + \cdots + m_n e_n$. Поэтому мы имеем корректно определенное отображение

$$f : A \to C, \qquad f(x) = m_1 c_1 + \cdots + m_n c_n.$$

Если $y = l_1 e_1 + \cdots + l_n e_n$, то $x + y = (m_1 + l_1)e_1 + \cdots + (m_n + l_n)e_n$, откуда

$$f(x+y) = (m_1 + l_1)c_1 + \cdots + (m_n + l_n)c_n = \\ = (m_1 c_1 + \cdots + m_n c_n) + (l_1 c_1 + \cdots + l_n c_n) = f(x) + f(y).$$

Значит, f — искомый гомоморфизм.

Если $g : A \to C$ — другой гомоморфизм со свойством $g(e_i) = c_i$, $1 \le i \le n$, то для любого $x = m_1 e_1 + \cdots + m_n e_n \in A$ имеем

$$g(x) = m_1 g(e_1) + \cdots + m_n g(e_n) = m_1 c_1 + \cdots + m_n c_n = f(x).$$

Значит, $f = g$. □

Следствие 10.5. *Пусть A — свободная абелева группа с базисом $e_1, \ldots, e_n$. Тогда число различных гомоморфизмов из A в циклическую группу порядка 2 равно 2^n. В частности, ранг A определен однозначно.*

Доказательство. Пусть $\mathbb{Z}_2 = \{0, 1\}$ — циклическая группа порядка 2. В силу теоремы 10.4 имеется взаимно однозначное соответствие между гомоморфизмами $f : A \to \mathbb{Z}_2$ и наборами $x_1, \ldots, x_n$, состоящими из нулей и единиц. Количество таких наборов равно 2^n, что и доказывает следствие. □

Теорема 10.6 (О согласованном базисе). *Пусть B — ненулевая подгруппа в свободной абелевой группе A ранга n. Тогда в A существует такой базис $e_1, \ldots, e_n$ и такие ненулевые целые числа $d_1, \ldots, d_k$, $k \le n$, что множество элементов $d_1 e_1, \ldots, d_k e_k$ образует базис B. В частности B свободна и ранг B не больше, чем ранг A.*

Доказательство. Воспользуемся индукцией по рангу A. Если $\operatorname{rank} A = 1$, то $A = \mathbb{Z}$ — бесконечная циклическая группа с базисом 1, а подгруппа B является циклической и порождается некоторым элементом $n = n \cdot 1 \in \mathbb{Z}$, что и утверждается в теореме.

Предположим, что теорема справедлива для всех свободных абелевых групп ранга $< n$. Выберем в A базис

$$v = \{v_1, \ldots, v_n\}. \tag{10.2}$$

Любой элемент $b \in B$ можно единственным образом записать в виде $b = m_1(b)v_1 + \cdots + m_n(b)v_n$, где $m_i(b) \in \mathbb{Z}$. Обозначим через $S(v)$ следующее множество натуральных чисел:

$$S(v) = \{|m_i(b)| \mid 1 \le i \le n,\ b \in B,\ m_i(b) \ne 0\}.$$

Пусть $d(v) = \min\limits_{a \in S(v)} a$ и пусть $d_1 = \min\limits_{v} d(v)$, где минимум ищется по всем базисам v. Поскольку любое подмножество в множестве натураль-

ных чисел имеет наименьший элемент, то этот минимум достигается для некоторого базиса v группы A и некоторого элемента $b_1 \in B$, т.е. $b_1 = d_1v_1 + m_2v_2 + \cdots + m_nv_n$.

Лемма 10.7. *$d_1|m_i$, $i = 2, \ldots, n$.*

Доказательство. Разделим m_i на d_1 с остатком:

$$m_i = d_1q_i + r_i, \qquad 0 \leq r_i < d_1.$$

Положим $e_1 = v_1 + q_2v_2 + \cdots + q_nv_n$. Ясно, что множество элементов

$$e_1, v_2, \ldots, v_n \tag{10.3}$$

образует базис A (проверьте!) и в этом базисе $b_1 = d_1e_1 + r_2v_2 + \cdots + r_nv_n$. Если хотя бы один из остатков r_i, $i = 2, \ldots, n$, больше нуля, то мы получим противоречие с минимальностью d_1. Значит, $r_i = 0$, $i = 2, \ldots, n$, и в базисе (10.3) $b_1 = d_1e_1$. □

Пусть $A_1 = \langle v_2, \ldots, v_n \rangle$ — свободная абелева группа ранга $n - 1$, $B_1 = A_1 \cap B$, $B_2 = \langle b_1 \rangle < B$.

Лемма 10.8. *Группа B является прямой суммой своих подгрупп B_1 и B_2.*

Доказательство. Докажем вначале, что $B = B_1 + B_2$. Пусть $b = l_1e_1 + l_2v_2 + \cdots + l_nv_n$ — произвольный элемент из B. Разделим l_1 на d_1 с остатком: $l_1 = m_1q + r$, $0 \leq r < d_1$. Тогда

$$b' = b - qb_1 = re_1 + l_2v_2 + \cdots + l_nv_n \in B$$

и если $r \neq 0$, то мы снова имеем противоречие с с минимальностью d_1. Значит, $r = 0$ и $b' = l_2v_2 + \cdots + l_nv_n \in B_1$. Тогда $b = b' + qb_1 \in B_1 + B_2$.

Покажем теперь, что $B_1 \cap B_2 = \{0\}$. Пусть $0 \neq x \in B_1 \cap B_2$. Так как $x \in B_1 \leq A_1$, то $x = m_2v_2 + \cdots + m_nv_n$. С другой стороны, $x \in B_2$, поэтому $x = m_1b_1 = m_1d_1e_1$, где $m_1d_1 \neq 0$. Отсюда мы получаем, что $m_2v_2 + \cdots + m_nv_n = m_1d_1e_1$ — нетривиальная целочисленная линейная зависимость между элементами базиса 10.3. Полученное противоречие и доказывает лемму. □

Теперь мы можем завершить доказательство теоремы. По предположению индукции в A_1 и B_1 существуют согласованные базисы, т.е.

найдется базис $e_2, \ldots, e_n$ группы A_1 и отличные от нуля целые числа $d_2, \ldots, d_k$ такие, что множество элементов $b_2 = d_2 e_2, \ldots, b_k = d_k e_k$ образует базис B_1. Тогда множество $b_1, b_2, \ldots, b_k$ является базисом B. $\square$

Теорема 10.9 (О строении конечно порожденных абелевых групп). *Пусть A — конечно порожденная абелева группа. Тогда A изоморфна прямому произведению свободной абелевой группы и конечного числа циклических p-групп, где p пробегает некоторое множество простых чисел.*

Доказательство. Пусть $a_1, \ldots, a_n$ — образующие группы A. По теореме 10.4 существует эпиморфизм $f : \mathbb{Z}^n \to A$. Пусть $B = \mathrm{Ker}(f)$. По основной теореме о гомоморфизмах $A \simeq \mathbb{Z}^n / B$. По теореме 10.6 о согласованных базисах в $\mathbb{Z}_n$ существует базис $e_1, \ldots, e_n$ такой, что множество элементов $d_1 e_1, \ldots, d_k e_k$ образует базис B, где $d_1, \ldots, d_k$ — натуральные числа, $1 \leq k \leq n$. Положим

$$N_i = \begin{cases} \langle d_i e_i \rangle, & \text{если } 1 \leq i \leq k, \\ \{0\}, & \text{если } k < i \leq n. \end{cases}$$

Тогда по предложению 10.2

$$\mathbb{Z}^n = \langle e_1 \rangle \oplus \cdots \oplus \langle e_n \rangle, \quad B = N_1 \oplus \cdots \oplus N_n, \quad N_i \leq \langle e_i \rangle.$$

По теореме 9.7 получаем

$$A \simeq \mathbb{Z}^n / B \simeq \langle e_1 \rangle / N_1 \oplus \cdots \oplus \langle e_n \rangle / N_n.$$

Если $1 \leq i \leq k$, то

$$\langle e_i \rangle / N_i \simeq \mathbb{Z} / d_i \mathbb{Z}$$

(отметим, что если $d_i = 1$, то $\langle e_i \rangle / N_i \simeq \mathbb{Z}/\mathbb{Z} = \{0\}$ и это прямое слагаемое можно отбросить). По теореме 9.9 циклическая группа $\mathbb{Z}/d_i\mathbb{Z}$ разлагается в прямую сумму циклических p-групп, где p пробегает множество простых делителей числа d_i. Если $k < i \leq n$, то $N_i = \{0\}$, и поэтому $\langle e_i \rangle / N_i = \langle e_i \rangle \simeq \mathbb{Z}$. Таким образом получаем

$$A \simeq (C_1 \oplus \cdots \oplus C_s) \oplus \mathbb{Z}^{n-k}, \tag{10.4}$$

где $C_1, \ldots, C_s$ — циклические p-группы и p пробегает некоторое множество простых чисел. □

Определение 10.10. *Группа G не имеет кручения, если в ней нет отличных от нейтрального элементов конечного порядка.*

Следствие 10.11. *Конечно порожденная абелева группа A без кручения свободна.*

Доказательство. Поскольку A без кручения, то в разложении 10.4 нет слагаемых $C_1, \ldots, C_s$. Значит $A \simeq \mathbb{Z}^r$ и по предложению 10.3 A свободна. □

Следствие 10.12. *Если абелева группа конечна, то она разлагается в прямую сумму циклических p-подгрупп, где p пробегает некоторое множество простых чисел.*

Доказательство. Поскольку A конечна, то в разложении 10.4 нет слагаемого $\mathbb{Z}^{n-k}$, значит $A \simeq C_1 \oplus \cdots \oplus C_s$, где $C_1, \ldots, C_s$ — циклические p-группы. □

Замечание 10.1. При разложении конечно порожденной абелевой группы в прямую сумму циклических p-подгрупп и бесконечных циклических подгрупп набор порядков этих подгрупп определен однозначно.

Упражнения

1. Какие из групп $\mathbb{Z}_6 \oplus \mathbb{Z}_{36}$, $\mathbb{Z}_{12} \oplus \mathbb{Z}_{18}$ и $\mathbb{Z}_9 \oplus \mathbb{Z}_{24}$ изоморфны?

2. Каков максимальный порядок элемента в группе $\mathbb{Z}_{42} \oplus \mathbb{Z}_{78} \oplus \mathbb{Z}_{36}$?

3. Сколько подгрупп шестого порядка у нециклической абелевой группы порядка 18?

4. Пусть $G = \langle a, b, c \rangle$ — свободная абелева группа ранга 3, H — подгруппа, порожденная элементами $5a+11b+7c$ и $2a+5b+4c$. Найти в G и H согласованные базисы. Найти разложение в прямую сумму циклических слагаемых (бесконечных и примарных) факторгруппы G/H.

5. Среди всех абелевых групп порядка 72 найти группу с максимальным числом элементов порядка 18.

6. Найти все (с точностью до изоморфизма) абелевы группы порядка 300, которые не изоморфны прямому произведению группы порядка 6 и группы порядка 50.

7. Указать все абелевы группы порядка 32, в которых есть единственная подгруппа порядка 8.

8. Найти все абелевы группы порядка 64, в которых все подгруппы индекса 2 изоморфны.

9. Разложить в прямую сумму примарных и бесконечных циклических подгрупп абелеву группу $G = \langle a, b, c \mid A \begin{pmatrix} a \\ b \\ c \end{pmatrix} = 0 \rangle$, где A — матрица:

а) $A = \begin{pmatrix} 6 & 3 & 6 \\ 6 & 4 & -2 \\ 4 & 3 & -6 \end{pmatrix}$; б) $A = \begin{pmatrix} 9 & 7 & 8 \\ 3 & 3 & -6 \\ 6 & 6 & -1 \end{pmatrix}$; в) $A = \begin{pmatrix} 5 & 7 & -1 \\ 2 & -2 & 2 \\ 7 & 5 & 1 \end{pmatrix}$.

10. Пусть $G = \langle a \mid 9a = 0 \rangle \oplus \langle b \mid 27b = 0 \rangle$. Найти разложение факторгруппы $G/(3a + 9b)$ в прямую сумму примарных циклических слагаемых.

11. Изоморфны ли факторгруппы $G/(2b)$ и $G/(a+2b)$ группы $G = \langle a \mid 2a = 0 \rangle \oplus \langle b \mid 4b = 0 \rangle$?

12. Пусть $m = \exp(G)$ — экспонента группы G (т.е. наименьшее число k такое, что $x^k = 1$ для всех элементов $x \in G$). Доказать, что если G — конечная абелева, то:

1) для любого $g \in G$ $\operatorname{ord}(g) | m$;

2) m — наибольший из порядков элементов G;

3) m равно наименьшему общему кратному порядков элементов группы G.

13. Пусть G — конечная абелева группа. Доказать, что равносильны два утверждения:

1) G — циклическая;

2) $\exp(G) = |G|$.

14. Доказать, что конечно порожденная абелева группа конечной экспоненты конечна.

Глава 2
ОСНОВЫ ТЕОРИИ КОЛЕЦ И ПОЛЕЙ

§11. Понятия кольца, поля, подкольца, подполя, примеры.

В отличие от групп кольца и поля — это алгебраические структуры с двумя операциями, называемыми обычно сложением и умножением. Их аксиомы подсказаны свойствами операций над вещественными числами.

Определение 11.1. ***Кольцом*** *называется непустое множество K с операциями сложения и умножения, обладающими следующими свойствами:*

1) *относительно сложения K есть абелева группа (называемая аддитивной группой кольца K);*

2) $a(b+c) = ab + ac$ *и* $(a+b)c = ac + bc$ *для любых* $a, b, c \in K$ *(дистрибутивность умножения относительно сложения).*

Выведем некоторые следствия аксиом кольца, не входящие в число следствий аксиом аддитивной абелевой группы.

1) $a0 = 0a = 0$ для любого $a \in K$.

В самом деле, пусть $a0 = b$. Тогда $b + b = a0 + b0 = a(0+0) = a0 = b$, откуда $b = b - b = 0$. Аналогично доказывается, что $0a = 0$.

2) $a(-b) = (-a)b = -ab$ для любых $a, b \in K$.

В самом деле, $ab + a(-b) = a(b + (-b)) = a0 = 0$ и, аналогично, $ab + (-a)b = 0$.

3) $a(b-c) = ab - ac$ и $(a-b)c = ac - bc$ для любых $a, b, c \in K$.

В самом деле, $a(b-c) + ac = a(b-c+c) = ab$ и, аналогично, $(a-b)c = ac - bc$.

Определение 11.2. *Кольцо K называется* ***коммутативным****, если умножение в нем коммутативно, т.е. $ab = ba$ для любых $a, b \in K$. Кольцо K называется* ***ассоциативным****, если умножение в нем ассоциативно, т.е. $(ab)c = a(bc)$ для любых $a, b, c \in K$. Кольцо K*

называется ***кольцом с единицей****, если в K существует нейтральный элемент относительно умножения, обозначаемый обычно через* 1*, т.е.* $1a = a1 = a$ *для любого* $a \in K$*.*

Так же, как в случае мультипликативной группы, доказывается, что в кольце не может быть двух различных единиц (но может не быть ни одной).

Замечание 11.1. Если $1 = 0$, то для любого $a \in K$ имеем $a = a1 = a0 = 0$, т.е. кольцо состоит из одного нуля. Таким образом, если кольцо содержит более одного элемента, то $1 \neq 0$.

Пример 1. Числовые множества $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ являются коммутативными ассоциативными кольцами с единицей относительно обычных операций сложения и умножения.

Пример 2. Множество $2\mathbb{Z}$ четных чисел является коммутативным ассоциативным кольцом без единицы.

Пример 3. Множество всех функций, определенных на заданном подмножестве числовой прямой, является коммутативным ассоциативным кольцом с единицей относительно обычных операций сложения и умножения функций.

Пример 4. Множество векторов пространства $\mathbb{R}^3$ с операциями сложения и векторного умножения является некоммутативным и неассоциативным кольцом. Однако в нем выполняются следующие тождества, которые в некотором смысле заменяют коммутативность и ассоциативность:

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

Пример 5. Множество квадратных матриц $M_n(K)$ над полем K является некоммутативным ассоциативным кольцом с единицей.

Пример 6. Множество классов вычетов $\mathbb{Z}_n$ по модулю n является коммутативным ассоциативным кольцом с единицей.

Пример 7. Множество многочленов $K[x_1, \ldots, x_n]$, где K — коммутативное ассоциативное кольцо с единицей, является коммутативным ассоциативным кольцом с единицей.

Определение 11.3. *Элемент a^{-1} кольца с единицей называется* ***обратным*** *к элементу a, если $aa^{-1} = a^{-1}a = 1$ (В коммутативном кольце достаточно требовать, чтобы $aa^{-1} = 1$).*

Так же, как в случае группы, доказывается, что в ассоциативном кольце с единицей никакой элемент не может иметь двух различных обратных элементов (но может не иметь ни одного). Элемент, имеющий обратный, называется обратимым.

Определение 11.4. ***Полем*** *называется коммутативное ассоциативное кольцо с единицей, содержащее не менее двух элементов, в котором всякий ненулевой элемент обратим.*

Примерами полей служат поле рациональных чисел $\mathbb{Q}$, поле вещественных чисел $\mathbb{R}$, поле комплексных чисел $\mathbb{C}$. Мы знаем также, что если p — простое число, то кольцо классов вычетов $\mathbb{Z}_p$ является полем. Кольцо $\mathbb{Z}$ не является полем: в нем обратимы только ± 1.

Если a, b — произвольные элементы поля K и $b \neq 0$, то в K определен элемент ab^{-1}. Для этого элемента часто используют запись

$$ab^{-1} \stackrel{\text{def}}{=} \frac{a}{b}$$

Любое поле обладает следующим важным свойством:

$$ab = 0 \Rightarrow a = 0 \text{ или } b = 0.$$

В самом деле, если $a \neq 0$, то, умножая обе части равенства $ab = 0$ на a^{-1}, получаем $b = 0$. Существуют и другие кольца, обладающие этим свойством, например, кольцо $\mathbb{Z}$. Они называются кольцами без делителей нуля. В кольце без делителей нуля возможно сокращение:

$$ac = bc \text{ (или } ca = cb) \text{ и } c \neq 0 \ \Rightarrow a = b.$$

В самом деле, равенство $ac = bc$ может быть переписано в виде $(a - b)c = 0$, откуда при $c \neq 0$ получаем $a - b = 0$, т. е. $a = b$.

Определение 11.5. *Ненулевые элементы a, b кольца K называются* ***делителями нуля****, если $ab = 0$.*

Приведем пример коммутативного ассоциативного кольца с делителями нуля.

Пример 8. В кольце функций на подмножестве X числовой прямой (см. пример 3) есть делители нуля, если только X содержит более одной точки. В самом деле, разобьем X на два непустых непересекающихся подмножества X_1, X_2 и положим при $i = 1, 2$

$$f_i(x) = \begin{cases} 1 & \text{если } x \in X_i, \\ 0 & \text{если } x \notin X_i. \end{cases}$$

Тогда $f_1 f_2 = 0$, но $f_1 \neq 0$, $f_2 \neq 0$.

Кольца $\mathbb{Z}_n$, где n не простое, и $M_n(K)$ также имеют делители нуля.

Отсутствие делителей нуля в поле означает, что произведение любых двух ненулевых элементов также является ненулевым элементом.

Пусть K — ассоциативное кольцо с единицей. Обозначим через K^* множество обратимых элементов кольца K.

Предложение 11.6. *Множество K^* является группой. Она называется* ***мультипликативной группой кольца*** *K.*

Доказательство. Достаточно проверить, что операция умножения определена на K^*. Пусть $a, b \in K^*$. Тогда $(ab)^{-1} = b^{-1}a^{-1}$, откуда $ab \in K^*$. □

В поле K все ненулевые элементы обратимы. Они образуют абелеву группу относительно умножения, которая называется **мультипликативной группой поля** K и обозначается через K^*.

Пример 9. $M_n(K)^* = \mathrm{GL}_n(K)$, $\mathbb{Z}^* = \{\pm 1\}$.

Пример 10. Если P — поле и $P[x]$ — кольцо многочленов от одной переменной, то $P[x]^* = P^*$.

Определение 11.7. *Подмножество L кольца K называется* ***подкольцом****, если*

1) *L является подгруппой аддитивной группы кольца K;*

2) *L замкнуто относительно умножения, т.е. для любых $a, b \in L$ элемент $ab \in L$.*

Очевидно, что всякое подкольцо L кольца K само является кольцом относительно операций кольца K. При этом оно наследует такие свойства, как коммутативность и ассоциативность.

Пример 1. При любом $n \in \mathbb{Z}$ множество $n\mathbb{Z}$ является подкольцом кольца $\mathbb{Z}$.

Пример 2. Множество $\left\{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\right\}$, где d фиксированное целое число, является подкольцом в $\mathbb{C}$.

Определение 11.8. *Подмножество L поля K называется* ***подполем****, если*

1) *L является подкольцом кольца K;*

2) $a \in L$, $a \neq 0 \;\Rightarrow\; a^{-1} \in L$;

3) $1 \in L$.

Очевидно, что всякое подполе L поля K является полем относительно операций поля K.

Пример 3. Поле $\mathbb{Q}$ является подполем поля $\mathbb{R}$, поле $\mathbb{R}$ является подполем поля $\mathbb{C}$.

Пример 4. Множество $\left\{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\right\}$, где d фиксированное целое число, является подполем в $\mathbb{C}$.

Упражнения

1. Пусть X — какое-либо множество и 2^X — множество всех его подмножеств. Доказать, что 2^X — кольцо относительно операций симметрической разности $M \triangle N = (M \setminus N) \cup (N \setminus M)$ и пересечения, взятых в качестве сложения и умножения соответственно. Доказать, что это кольцо коммутативно и ассоциативно.

2. Какие из следующих числовых множеств образуют кольцо, а какие — поле относительно обычных операций сложения и умножения:

1) множество $n\mathbb{Z}$, $n > 1$;

2) множество рациональных чисел, в несократимой записи которых знаменатели делят фиксированное число $n \in \mathbb{N}$;

3) множество рациональных чисел, в несократимой записи которых знаменатели не делятся на фиксированное простое число p;

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

5) множество вещественных чисел вида $x + y\sqrt{2}$, где $x, y \in \mathbb{Q}$;

6) множество вещественных чисел вида $x + y\sqrt[3]{2}$, где $x, y \in \mathbb{Q}$;

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

8) множество комплексных чисел вида $x + yi$, где а) $x, y \in \mathbb{Z}$, б) $x, y \in \mathbb{Q}$;

9) множество всевозможных сумм вида $a_1 z_1 + \cdots a_n z_n$, где $a_i \in \mathbb{Q}$, z_i — комплексный корень степени n из 1, $1 \leq i \leq n$.

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

1) множество вещественных симметрических (кососимметрических) матриц порядка n;

2) множество вещественных ортогональных матриц порядка n;

3) множество верхних (нижних) треугольных матриц порядка $n \geq 2$;

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

5) множество матриц вида $\begin{pmatrix} x & y \\ Dy & x \end{pmatrix}$, где D — фиксированное целое число, $x, y \in \mathbb{Z}$;

6) множество комплексных матриц вида $\begin{pmatrix} z & w \\ -\overline{w} & \overline{z} \end{pmatrix}$.

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

1) $C[a, b]$;

2) множество функций, имеющих вторую производную на интервале (a, b);

3) множество функций вещественного переменного, обращающихся в 0 на некотором подмножестве $D \subset \mathbb{R}$;

4) множество тригонометрических многочленов

$$a_0 + \sum_{k=1} n(a_k \cos kx + b_k \sin kx)$$

с вещественными коэффициентами, где n — произвольное натуральное число.

5. Во множестве многочленов от переменной t с обычным сложением рассматривается операция умножения, заданная правилом

$$(f \circ g)(t) = f(g(t)).$$

Является ли это множество кольцом?

6. Найти все обратимые элементы и все делители нуля в кольцах: 1) верхних треугольных матриц над полем; 2) $M_2(\mathbb{R})$; 3) $\mathbb{Z}$; 4) $\mathbb{Z}[i]$.

7. Пусть $K = \left\{a + b\sqrt{3} \mid a, b \in \mathbb{Z}\right\}$. Доказать, что группа обратимых элементов K^* бесконечна.

8. Докажите, что матрицы

$$O = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \quad E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad S = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \quad T = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

с элементами из $\mathbb{Z}_2$ образуют поле относительно обычных операций сложения и умножения матриц.

9. Доказать, что все конечные подмножества множества X образуют подкольцо кольца 2^X из упражнения 1 к § 11.

10. Найдите все подкольца колец $\mathbb{Z}_{10}$, $\mathbb{Z}_{20}$ и $\mathbb{Z}_7$.

11. Докажите, что пересечение подколец кольца K является подкольцом кольца K.

12. Докажите, что пересечение подполей поля P является подполем поля P.

13. Может ли в кольце, не являющемся полем, содержаться некоторое подполе?

14. Найдите в $\mathbb{R}$ наименьшее подкольцо с единицей и наименьшее подполе, содержащие число: 1) $\sqrt{2}$; 2) $\sqrt[3]{2}$.

§12. Гомоморфизм, изоморфизм, ядро гомоморфизма.

Определение 12.1. *Отображение f кольца A в кольцо B называется* ***гомоморфизмом****, если оно сохраняет операции, т. е. если*

$$f(x+y) = f(x) + f(y), \qquad f(xy) = f(x)f(y)$$

для любых $x, y \in A$. Если гомоморфизм f является биекцией, то он называется ***изоморфизмом****.*

Изоморфизм кольца на себя называется **автоморфизмом**.

Отметим следующие свойства гомоморфизмов и изоморфизмов.

1. Тождественное отображение $\mathrm{id} : A \to A$ является изоморфизмом.

2. Если $f : A \to B$ — изоморфизм, то $f^{-1} : B \to A$ — также изоморфизм.

3. Если $f : A \to B$, $g : B \to C$ — гомоморфизмы, то $g \circ f : A \to C$ — также гомоморфизм. Если f и g — изоморфизмы, то $g \circ f$ также изоморфизм.

4. Если $f : A \to B$ — гомоморфизм, то f является гомоморфизмом аддитивных групп A и B, а значит $f(0) = 0$, $f(-a) = -f(a)$ для любого $a \in A$.

Предложение 12.2. *Пусть $f : A \to B$ — гомоморфизм колец и $K \subset A$, $K_1 \subset B$ — подкольца. Тогда $f(K) = \{f(x) \mid x \in K\}$ — подкольцо в B, а $f^{-1}(K_1) = \{x \in A \mid f(x) \in K_1\}$ — подкольцо в A.*

Доказательство. В самом деле, K является подгруппой аддитивной группы кольца A, значит, $f(K)$ — подгруппа аддитивной группы кольца B. Если $y_1, y_2 \in f(K)$, то существуют $x_1, x_2 \in K$ такие, что $f(x_1) = y_1$, $f(x_2) = y_2$. Тогда

$$y_1 y_2 = f(x_1) f(x_2) = f(x_1 x_2) \Rightarrow y_1 y_2 \in f(K).$$

Значит, $f(K)$ — подкольцо в B.

Во втором случае K_1 является подгруппой аддитивной группы кольца B, значит, по предложению 5.4 $f^{-1}(K_1)$ — подгруппа аддитивной группы кольца A. Если $x_1, x_2 \in f^{-1}(K_1)$, то $f(x_1), f(x_2) \in K_1$ и

$$f(x_1 x_2) = f(x_1) f(x_2) \in K_1 \Rightarrow x_1 x_2 \in f^{-1}(K_1).$$

Значит, $f^{-1}(K_1)$ — подкольцо в A. □

7. Если $f : A \to B$ — гомоморфизм и A — кольцо с единицей 1_A, то $f(1_A)$ — единица кольца $f(A)$.

Действительно,

$$f(1_A) f(a) = f(1_A a) = f(a) = f(a 1_A) = f(a) f(1_A).$$

Отметим, что не всегда $f(1)$ будет являться единицей кольца B.

Пример 1. Отображение $f : \mathbb{C} \to \mathbb{C}$, $f(z) = \overline{z}$, является изоморфизмом.

Пример 2. Пусть $K = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \mid a, b \in \mathbb{R} \right\}$. Нетрудно проверить, что K — кольцо относительно обычных операций сложения и умножения матриц. Рассмотрим отображение

$$f : \mathbb{C} \to K, \qquad f(a + bi) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}.$$

Тогда f — изоморфизм.

Определение 12.3. *Если $f : A \to B$ — гомоморфизм, то множество*

$$\operatorname{Ker} f = \{a \in A \mid f(a) = 0\}$$

называется ***ядром*** *гомоморфизма f.*

Предложение 12.4. $\operatorname{Ker} f$ *является подкольцом в A.*

Доказательство. Так как $f : A \to B$ — гомоморфизм аддитивных групп колец A и B, то $\operatorname{Ker} f$ является подгруппой аддитивной группы кольца A. Если $a, b \in \operatorname{Ker} f$, то

$$f(ab) = f(a)f(b) = 0 \cdot 0 = 0 \Rightarrow ab \in \operatorname{Ker} f.$$

Значит, $\operatorname{Ker} f$ является подкольцом в A. □

Упражнения

1. Доказать, что образ коммутативного кольца при гомоморфизме является коммутативным кольцом.

2. Пусть K — поле, $c \in K$. Доказать, что отображение $\varphi : K[x] \to K$, $f(x) \mapsto f(c)$, является гомоморфизмом. Найти ядро φ.

3. Пусть K — поле, $f \in K[x]$. Доказать, что отображение $\varphi : K[x] \to K[x]$, $g(x) \mapsto g(f(x))$, является гомоморфизмом.

4. Найти все гомоморфизмы колец:

1) $\mathbb{Z} \to 2\mathbb{Z}$; 2) $2\mathbb{Z} \to 2\mathbb{Z}$; 3) $2\mathbb{Z} \to 3\mathbb{Z}$; 4) кольца $\mathbb{Z}$ в поле $\mathbb{Q}$; 5) $\mathbb{Z}_4 \to \mathbb{Z}_6$; 6) $\mathbb{Z}_6 \to \mathbb{Z}_4$.

§13. Идеалы и факторкольца.

Определение 13.1. *Подкольцо I кольца K называется* ***левым идеалом****, если для любого $a \in K$ множество $aI = \{ax \mid x \in I\}$ содержится в I.*

Подкольцо I кольца K называется ***правым идеалом****, если для любого $a \in K$ множество $Ia = \{xa \mid x \in I\}$ содержится в I.*

Подкольцо I кольца K называется ***(двусторонним) идеалом****, если I одновременно является левым и правым идеалом.*

Если K — коммутативное кольцо, то понятия левого, правого и двустороннего идеалов совпадают.

Предложение 13.2. *Если $f : A \to B$ — гомоморфизм колец, то* $\operatorname{Ker} f$ *— идеал в A.*

Доказательство. Для любых элементов $a \in A$, $x \in I = \operatorname{Ker} f$ имеем

$$f(ax) = f(a)f(x) = f(a)0 = 0, \qquad f(xa) = f(x)f(a) = 0f(a) = 0,$$

откуда $ax, xa \in I$. Значит, I — двусторонний идеал. □

Пример 1. $\{0\}$ и K являются идеалами в любом кольце K. Их называют **тривиальными идеалами.**

Пример 2. $n\mathbb{Z} = \{nt \mid t \in \mathbb{Z}\}$ является идеалом в $\mathbb{Z}$.

Предложение 13.3. *Пусть K — коммутативное ассоциативное кольцо с 1. Для любых элементов $a_1, \ldots, a_n \in K$ множество*

$$I = \{a_1x_1 + \cdots + a_nx_n \mid x_1, \ldots, x_n \in K\}$$

является идеалом в K. Его называют ***идеалом, порожденным элементами*** *$a_1, \ldots, a_n$ и обозначают $(a_1, \ldots, a_n)$.*

Доказательство. Если $a = a_1x_1 + \cdots + a_nx_n$ и $b = a_1y_1 + \cdots + a_ny_n$ — произвольные элементы из I, $z \in K$, то

$$a + b = a_1(x_1 + y_1) + \cdots + a_n(x_n + y_n) \in I$$
$$-(a_1x_1 + \cdots + a_nx_n) = a_1(-x_1) + \cdots + a_n(-x_n) \in I$$
$$(a_1x_1 + \cdots + a_nx_n)z = a_1x_1z + \cdots + a_nx_nz \in I,$$

откуда получаем, что I — идеал. $\square$

Определение 13.4. *Идеал, порожденный одним элементом $a \in K$, называют* ***главным идеалом****, порожденным элементом a, и обозначают (a) (либо aK).*

Теорема 13.5 (Критерий поля). *Пусть K — коммутативное ассоциативное кольцо с 1 и $1 \neq 0$. Если K не содержит нетривиальных идеалов, то K является полем.*

Доказательство. Нам достаточно доказать, что любой ненулевой элемент $a \in K$ имеет обратный a^{-1}. Рассмотрим главный идеал (a). Так как $(a) \neq \{0\}$, то по условию теоремы $(a) = K$. Значит, $1 \in (a)$, т.е. существует элемент $b \in K$ такой, что $1 = ab$. Следовательно, a обратим. $\square$

Предложение 13.6. *Пусть I — идеал в K, где K — ассоциативное кольцо с 1. Если I содержит обратимый элемент a, то $I = K$.*

Доказательство. Из условия следует, что $1 = aa^{-1} \in I$. Тогда для любого $z \in K$ имеем $1z = z \in I$, откуда $I = K$. $\square$

Следствие 13.7. *Поле K содержит только тривиальные идеалы.*

Доказательство. Если I — ненулевой идеал в K, то I содержит ненулевой элемент, который обратим по определению поля. По предложению 13.6 $I = K$. $\square$

Пусть K — кольцо, I — идеал в K. Так как I — подгруппа аддитивной группы K, то определена факторгруппа K/I. Элементы этой факторгруппы имеют вид $a + I$, $a \in K$, и называются **смежными классами** K по I. Определим умножение смежных классов формулой

$$(a + I)(b + I) = ab + I. \tag{13.1}$$

Докажем, что таким образом определенное умножение не зависит от выбора представителей в смежных классах.

Предложение 13.8. *Если $a + I = a_1 + I$ и $b + I = b_1 + I$, то $ab + I = a_1b_1 + I$.*

Доказательство. Из равенства смежных классов $a+I=a_1+I$ и $b+I=b_1+I$ следует по предложению 4.3, что $a_1-a, b_1-b \in I$. Тогда

$$a_1b_1-ab=a_1b_1-a_1b+a_1b-ab=a_1(b_1-b)+(a_1-a)b\in I,$$

откуда снова по предложению 4.3 $ab+I=a_1b_1+I$. □

Замечание. Когда мы рассматривали умножение смежных классов в факторгруппе G/N, то мы имели не только формально определенное равенство $gN\cdot hN=ghN$, но, фактически, множество, состоящее из попарных произведений элементов двух смежных классов gN и hN группы G дает в точности смежный класс ghN. Иначе обстоит дело в кольцах. Если мы рассмотрим множество $M=\{xy \mid x\in a+I, y\in b+I\}$, то в общем случае M не совпадает со смежным классом $ab+I$, а лишь содержится в нем. Например, поэлементное произведение двух смежных классов $2+4\mathbb{Z}$ и $2+4\mathbb{Z}$ дает множество $M=\{4+8t \mid t\in\mathbb{Z}\}$ и ясно, что $M\subsetneqq 4+4\mathbb{Z}=4\mathbb{Z}$.

Теорема 13.9. *Пусть K — кольцо, I — идеал в K. Множество K/I является кольцом, которое называют* ***факторкольцом*** *кольца K по идеалу I.*

Доказательство. Достаточно проверить дистрибутивность умножения относительно сложения. Для любых $a+I, b+I, c+I\in K/I$ имеем

$$\begin{aligned}(a+I)(b+I+c+I)=(a+I)(b+c+I)=a(b+c)+I=ab+ac+I=\\ =(ab+I)+(ac+I)=(a+I)(b+I)+(a+I)(c+I),\end{aligned}$$

$$\begin{aligned}(b+I+c+I)(a+I)=(b+c+I)(a+I)=(b+c)a+I=ba+ca+I=\\ =(ba+I)+(ca+I)=(b+I)(a+I)+(c+I)(a+I).\end{aligned}$$

Теорема доказана. □

Предложение 13.10. *Пусть K — кольцо, I — идеал в K. Отображение*

$$f: K\to K/I,\qquad f(x)=x+I,$$

является сюръективным гомоморфизмом колец и $\operatorname{Ker} f=I$. *Этот гомоморфизм называется* ***каноническим****.*

Доказательство. Для любых $a, b \in K$ имеем

$$f(ab) = ab + I = (a + I)(b + I) = f(a)f(b).$$

Сюръективность f очевидна. Кроме того,

$$a \in \operatorname{Ker} f \Leftrightarrow f(a) = a + I = I \Leftrightarrow a \in I,$$

откуда $\operatorname{Ker} f = I$. □

Теорема 13.11 (Основная о гомоморфизмах колец). *Пусть $f : A \to B$ — гомоморфизм колец, $I = \operatorname{Ker} f$. Тогда $f(A) \simeq A/I$.*

Доказательство. Так как f — гомоморфизм аддитивных групп A и B, то по основной теореме о гомоморфизмах групп $f(A)$ и A/I изоморфны как абелевы группы. Соответствующий изоморфизм $\psi : A/I \to f(A)$ задается формулой $\psi(a + I) = f(a)$. Остается доказать, что ψ сохраняет умножение. Для любых $a + I, b + I \in A/I$ имеем

$$\psi((a + I)(b + I)) = \psi(ab + I) = f(ab) = f(a)f(b) = \psi(a + I)\psi(b + I)),$$

что и завершает доказательство теоремы. □

Предложение 13.12. *Пусть $f : A \to B$ — гомоморфизм колец, I — идеал в A, J — идеал в B. Тогда $f(I)$ — идеал в $f(A)$, $f^{-1}(J)$ — идеал в A.*

Доказательство. По предложению 12.2, $f(I)$ и $f^{-1}(J)$ — подкольца в $f(A)$ и A соответственно. Если $x \in f(A)$, $y \in f(I)$ то $x = f(a)$, $y = f(b)$ для некоторых элементов $a \in A$, $b \in I$. Тогда $xy = f(a)f(b) = f(ab) \in f(I)$, поскольку $ab \in I$. Значит, $f(I)$ — идеал в $f(A)$.

Далее, если $x \in f^{-1}(J)$, $a \in A$, то $f(ax) = f(a)f(x) \in J$, поскольку $f(x) \in J$, а J — идеал. Значит, $ax \in f^{-1}(J)$ и $f^{-1}(J)$ — идеал в A. □

Упражнения

1. Доказать, что пересечение идеалов (левых, правых, двусторонних) кольца K является идеалом (соответственно левым, правым, двусторонним).

2. Будут ли следующие множества идеалами указанных ниже колец:

а) $\mathbb{Z}$ в кольце $\mathbb{Z}[x]$; б) $n\mathbb{Z}[x]$ в кольце $\mathbb{Z}[x]$; в) $\mathbb{Z}[x]$ в кольце $\mathbb{Q}[x]$; г) множество I многочленов, не содержащих членов вида ax^k для всех $k < n$, где $n > 1$, в кольце $\mathbb{Z}[x]$; д) множество I многочленов с четными свободными членами в кольце $\mathbb{Z}[x]$; е) множество I многочленов с четными старшими коэффициентами в кольце $\mathbb{Z}[x]$;

3. Пусть I и J — множества матриц вида

$$\begin{pmatrix} 0 & g & h \\ 0 & 0 & 2k \\ 0 & 0 & 0 \end{pmatrix}, \qquad \begin{pmatrix} 0 & l & 2m \\ 0 & 0 & 2n \\ 0 & 0 & 0 \end{pmatrix}$$

с целыми коэффициентами $g, h, k, \ldots$ Доказать, что I является идеалом в кольце R верхних треугольных матриц над $\mathbb{Z}$, J является идеалом кольца I, но J не является идеалом кольца R.

4. Образуют ли идеал необратимые элементы колец:

1) $\mathbb{Z}$; 2) $\mathbb{C}[x]$; 3) $\mathbb{Z}_n$.

5. Доказать, что кольцо целых чисел не содержит минимальных идеалов.

6. Доказать, что множество I_S непрерывных функций, обращающихся в 0 на фиксированном подмножестве $S \subset [a, b]$, является идеалом в кольце функций, непрерывных на $[a, b]$.

7. *Суммой идеалов* $I_1, I_2, \ldots, I_k$ коммутативного кольца R называется множество

$$I_1 + I_2 + \cdots + I_k = \{x_1 + \cdots + x_k \mid x_s \in I_s,\ s = 1, \ldots, k\}.$$

Доказать, что сумма идеалов является идеалом.

8. *Произведением идеалов* I_1, I_2 коммутативного кольца R называется множество

$$I_1 I_2 = \left\{ \sum j = 1s x_j y_j \mid x_j \in I_1, y_j \in I_2, j = 1, \ldots, s \right\}.$$

Доказать, что произведение идеалов является идеалом.

9. Доказать, что если I_1, I_2 — идеалы коммутативного кольца R и $I_1 \cap I_2 = \{0\}$, то $I_1 I_2 = \{0\}$.

10. Доказать, что

а) $F[x]/(x-a) \simeq F$ (F — поле);

б) $\mathbb{R}[x]/(x^2+1) \simeq \mathbb{C}$;

в) $\mathbb{R}[x]/(x^2+x+1) \simeq \mathbb{C}$.

11. Пусть $K = \left\{ \begin{pmatrix} a & b \\ a & b \end{pmatrix} \mid a, b \in \mathbb{R} \right\}$. Доказать, что отображение $f : K \to \mathbb{R}$, $A \mapsto \operatorname{tr} A$, — гомоморфизм. Найдите его ядро и факторкольцо $K/\ker f$.

§14. Кольца главных идеалов.

В этом параграфе будем предполагать, что A — коммутативное ассоциативное кольцо с единицей.

Определение 14.1. *Кольцо A без делителей нуля называется кольцом главных идеалов, если любой идеал в A является главным.*

Теорема 14.2. $\mathbb{Z}$ *— кольцо главных идеалов.*

Доказательство. Пусть $I \subset \mathbb{Z}$ — идеал, m — наименьшее натуральное число в I и $a \in I$. Разделим a на m с остатком.

$$a = mq + r, \qquad 0 \le r < m.$$

Так как $a, m \in I$, то $a - mq = r \in I$, откуда $r = 0$ и $a = mq$. Значит, $I = \{mq \mid q \in \mathbb{Z}\} = \langle m \rangle$. □

Теорема 14.3. *Пусть K — поле. Тогда кольцо многочленов $K[x]$ — кольцо главных идеалов.*

Доказательство. Пусть $I \subset K[x]$ — идеал, $f(x) \neq 0$ — многочлен наименьшей степени в I и $g(x) \in I$. Разделим $g(x)$ на $f(x)$ с остатком.

$$g(x) = f(x)q(x) + r(x), \qquad \deg r(x) < \deg f(x).$$

Так как $f(x), g(x) \in I$, то $g(x) - f(x)q(x) = r(x) \in I$, откуда $r(x) = 0$ и $g(x) = f(x)q(x)$. Значит, $I = \{f(x)q(x) \mid q(x) \in K[x]\} = \langle f(x) \rangle$. □

Замечание 14.1. Доказательства этих двух теорем очень похожи. Фактически, все следует из того, что и в $\mathbb{Z}$, и в $K[x]$ существует

алгоритм деления с остатком. Кольца, в которых возможно производить деление элементов с остатком, называют евклидовыми. Евклидовы кольца являются кольцами главных идеалов.

Не все кольца являются кольцами главных идеалов.

Пример 1. Пусть K — поле. Тогда кольцо многочленов от двух переменных $K[x,y]$ не является кольцом главных идеалов.

Действительно, рассмотрим множество

$$I = \{xf(x,y) + yg(x,y) \mid f(x,y), g(x,y) \in K[x,y]\}\,.$$

Нетрудно проверить, что I — нетривиальный идеал в $K[x,y]$. Допустим, что I — главный идеал. Тогда $I = (h(x,y))$ для некоторого многочлена $h(x,y) \in K[x,y]$. Поскольку $x, y \in I$, то мы должны иметь

$$x = h(x,y)f_1(x,y), \qquad y = h(x,y)f_2(x,y) \tag{14.1}$$

для некоторых многочленов $f_1(x,y), f_2(x,y) \in K[x,y]$. Сравнивая степени левых и правых частей в (14.1), получаем, что либо $\deg h(x,y) = 0$, либо $\deg h(x,y) = 1$.

В первом случае $h(x,y)$ — ненулевая константа, а поэтому обратимый элемент кольца $K[x,y]$. Тогда по предложению 13.6 $I = K[x,y]$ — противоречие, поскольку элементы из K^* не принадлежат I.

Во втором случае мы получаем $\deg f_1(x,y) = \deg f_2(x,y) = 0$, т.е. $f_1(x,y) = a$ и $f_2(x,y) = b$ — ненулевые константы. Тогда из (14.1) получаем

$$h(x,y) = a^{-1}x = b^{-1}y\ -$$

противоречие.

Упражнения

1. Пусть I — множество всех многочленов с четными свободными членами в кольце $\mathbb{Z}[x]$. Доказать, что: 1) I является идеалом, но не является главным идеалом в $\mathbb{Z}[x]$; 2) $\mathbb{Z}[x]/I \simeq \mathbb{Z}_2$.

2. Найти идеал, порожденный множеством M, если:

а) $M = \{4, 9\}$ в кольце $\mathbb{Z}$; $M = \{6, 15\}$ в кольце $\mathbb{Z}$; в) $M = \left\{x^6 - 1, x^4 - 1\right\}$ в кольце $\mathbb{R}[x]$; г) $M = \{x, x+1\}$ в кольце $\mathbb{R}[x]$.

3. В кольце $\mathbb{Z}$ найдите порождающий элемент идеалов: а) $(4)+(7)$; б) $(6) \cap (8)$; в) $(6,9)+(25,35)$; г) $(9,15,18) \cap (12,21,33)$.

4. Пусть F — поле и $f, g \in F[x]$. Доказать, что $(f) \subset (g)$ тогда и только тогда, когда g делит (f).

§15. Максимальные идеалы.

В этом параграфе будем рассматривать коммутативные ассоциативные кольца с единицей.

Определение 15.1. *Идеал $I \subset A$ называется максимальным, если I не содержится ни в одном большем идеале $J \neq A$.*

Теорема 15.2. *Идеал I максимален тогда и только тогда, когда A/I — поле.*

Доказательство. Пусть I максимален. Докажем, что в факторкольце A/I нет нетривиальных идеалов. Действительно, пусть T — нетривиальный идеал в A/I. Рассмотрим канонический гомоморфизм $f : A \to A/I$. Тогда по предложению 13.12 $J = f^{-1}(T)$ — идеал в A, содержащий I. Следовательно, $J = A$ и $f(J) = T = A/I$ — противоречие. Теперь по теореме 13.5 получаем, что A/I — поле.

Обратно, предположим, что A/I — поле, а идеал I — не максимальный. Тогда существует идеал $J \supset I$, $J \neq A$. По предложению 13.12 образ $T = f(J)$ идеала J является идеалом в A/I, при этом $T \neq \{0\}$ и $T \neq A/I$ — противоречие, поскольку A/I — поле, а поле не содержит нетривиальных идеалов. □

Теорема 15.3. 1. *Идеал $(n) \subset \mathbb{Z}$ максимален $\Leftrightarrow$ n — простое число.*

2. *Идеал $(f(x)) \subset K[x]$, где K — поле, максимален $\Leftrightarrow$ $f(x)$ — неприводимый многочлен.*

Доказательство. Докажем пункт 2 теоремы, пункт 1 доказывается совершенно аналогично.

Пусть $(f(x))$ — максимальный идеал в $K[x]$. Предположим, что $f(x) = g(x)h(x)$, где $\deg g(x) > 0$ и $\deg h(x) > 0$. Тогда $(g(x))$ — нетривиальный идеал, содержащий $(f(x))$ и не совпадающий с ним — противоречие.

Пусть теперь $f(x)$ — неприводимый многочлен и предположим, что идеал $(f(x))$ не максимален. Тогда найдется нетривиальный идеал $(g(x)) \subsetneqq (f(x))$. Так как $f(x) \in (g(x))$, то $f(x) = g(x)h(x)$, где $h(x)$ — не константа (иначе бы идеалы $(f(x))$ и $(g(x))$ совпадали). Получили противоречие с неприводимостью $f(x)$. □

Следствие 15.4. 1. $\mathbb{Z}/n\mathbb{Z}$ — *поле* $\Leftrightarrow$ n — *простое число.*

2. $K[x]/\langle f(x)\rangle$ — *поле* $\Leftrightarrow$ $f(x)$ — *неприводимый многочлен.*

Упражнения

1. Для каких a факторкольцо $\mathbb{Z}_7[x]/(x^2 - a)$ является полем?

2. Является ли факторкольцо K/I полем, если:

а) $K = \mathbb{Z}_2[x]$, $I = (x^3 + x + 1)$; б) $K = \mathbb{Z}_3[x]$, $I = (x^2 + x + 2)$; в) $K = \mathbb{Z}_5[x]$, $I = (x^3 + x^2 + 3)$.

3. Доказать, что факторкольцо $K[x]/(x^4 + x^3 + x + 1)$ не может быть полем, каким бы ни было коммутативное кольцо K с единицей.

§16. Прямая сумма колец.

Используя понятие прямой суммы абелевых групп, определим прямую сумму колец.

Определение 16.1. *Говорят, что кольцо A разлагается в прямую сумму своих подколец $A_1, \ldots, A_k$, если*

1) *аддитивная группа кольца A является прямой суммой аддитивных групп колец $A_1, \ldots, A_k$;*

2) $A_iA_j = \{0\}$.

В этом случае пишут $A = A_1 \dot{+} \cdots \dot{+} A_k$.

Если кольцо A разлагается в прямую сумму своих подколец $A_1, \ldots, A_k$, то $A_1, \ldots, A_k$ — идеалы. Действительно, произвольный элемент $a \in A$ можно представить в виде суммы $a = a_1 + \cdots a_k$, где $a_i \in A_i$,

$i = 1, \ldots, k$. Тогда для произвольного элемента $b \in A_i$ имеем

$$ab = (a_1 + \cdots a_k)b = a_1 b + \cdots a_k b = a_i b \in A_i.$$

Следовательно, A_i — идеал.

Условие 2 обеспечивает следующее "покомпонентное" правило умножения:

$$(x_1 + \cdots + x_k)(y_1 + \cdots + y_k) = x_1 y_1 + \cdots + x_k y_k. \tag{16.1}$$

Пусть теперь $A_1, \ldots, A_k$ — какие-то кольца.

Определение 16.2. *Прямой суммой колец $A_1, \ldots, A_k$ называется их прямая сумма $A_1 \oplus \cdots \oplus A_k$ как аддитивных групп с покомпонентной операцией умножения:*

$$(x_1, \ldots, x_k)(y_1, \ldots, y_k) = (x_1 y_1, \ldots, x_k y_k). \tag{16.2}$$

Очевидно, что определенная таким образом операция умножения в $A_1 \oplus \cdots \oplus A_k$ дистрибутивна по отношению к сложению, так что $A_1 \oplus \cdots \oplus A_k$ действительно является кольцом. Если все кольца $A_1, \ldots, A_k$ коммутативны, ассоциативны или обладают единицей, то и их прямая сумма обладает соответствующим свойством.

Прямая сумма колец в смысле определения 16.1 называется внутренней, а в смысле определения 16.2 — внешней. Между этими двумя понятиями имеется такая же связь, как и в случае групп или векторных пространств.

Для каждого кольца A_i рассмотрим гомоморфизм

$$\varphi_i : A_i \to A = A_1 \oplus \cdots \oplus A_k, \qquad \varphi_i(x) = (1, \ldots, 1, x, 1, \ldots, 1)$$

(x находится на i-м месте). Ясно, что φ_i инъективен и, по основной теореме о гомоморфизмах колец, кольцо A_i изоморфно подкольцу $A'_i = \varphi_i(A_i) \leq A$. Кроме того, нетрудно проверить, что A'_i является идеалом в A. Непосредственно из определения идеалов A'_i следует, что если $i \neq j$, то $A'_i A'_j = \{0\}$. Следовательно, A является внутренней прямой суммой своих подколец $A'_1, \ldots, A'_k$. Справедливо и обратное утверждение.

Теорема 16.3. *Если A — внутренняя прямая сумма своих под-*

колец $A_1, \ldots, A_k$, *то* $A \simeq A_1 \oplus \cdots \oplus A_k$.

Доказательство. Из определения внутренней прямой суммы колец следует, что аддитивная группа кольца A является внутренней прямой суммой аддитивных подгрупп $A_1, \ldots, A_k$. По теореме 9.5 A и $A_1 \oplus \cdots \oplus A_k$ изоморфны как аддитивные группы, причем изоморфизм задается формулой $f((x_1, \ldots, x_k)) = x_1 + \cdots + x_k$. В силу формул (16.1) и (16.2) f сохраняет умножение, следовательно, является изоморфизмом колец A и $A_1 \oplus \cdots \oplus A_k$. □

Теорема 16.4. *Пусть* $A_1, \ldots, A_k$ — *ассоциативные кольца с* 1. *Тогда для мультипликативных групп справедливо равенство*

$$(A_1 \oplus \cdots \oplus A_k)^* = A_1^* \times \cdots \times A_k^*.$$

Доказательство. Элемент $(x_1, \ldots, x_k) \in (A_1 \oplus \cdots \oplus A_k)^*$ тогда и только тогда, когда существует $(y_1, \ldots, y_k) \in A_1 \oplus \cdots \oplus A_k$ такой, что

$$(x_1, \ldots, x_k)(y_1, \ldots, y_k) = (x_1 y_1, \ldots, x_k y_k) = (1, \ldots, 1).$$

Это равносильно тому, что $x_i y_i = 1$, $i = 1, \ldots, n$, т.е. $x_i \in A_i^*$, $i = 1, \ldots, n$. В свою очередь, это эквивалентно тому, что $(x_1, \ldots, x_k) \in A_1^* \times \cdots \times A_k^*$. □

Упражнения

1. Пусть $R = I_1 \dot{+} I_2$ — разложение коммутативного кольца R с единицей e в прямую сумму ненулевых идеалов I_1, I_2. Доказать, что если $e = e_1 + e_2$, где $e_1 \in I_1$, $e_2 \in I_2$, то e_1, e_2 — единицы колец I_1, I_2 соответственно, но не единицы кольца R.

2. Пусть K — поле. Доказать, что если многочлены $f, g \in K[x]$ взаимно просты, то

$$K[x]/(fg) \simeq K[x]/(f) \oplus K[x]/(g).$$

3. Доказать, что если $R = I_1 \dot{+} I_2$, то $R/I_1 \simeq I_2$, $R/I_2 \simeq I_1$.

4. Разложите кольца $\mathbb{R}[x]/(x^2 + x)$, $\mathbb{C}[x]/(x^2 + 1)$ в прямую сумму собственных идеалов.

§17. Строение кольца $\mathbb{Z}/n\mathbb{Z}$.

Теорема 17.1. *Пусть $n = mk$, где m, k — взаимно простые натуральные числа. Тогда*

$$\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/k\mathbb{Z}.$$

Доказательство. Рассмотрим отображение

$$\psi : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/k\mathbb{Z}, \qquad \psi(a + n\mathbb{Z}) = (a + m\mathbb{Z}, a + k\mathbb{Z}).$$

Несложное вычисление показывает, что ψ является гомоморфизмом колец. Проверим, что ψ инъективно.

$$\psi(a+n\mathbb{Z}) = (0+m\mathbb{Z}, 0+k\mathbb{Z}) \Leftrightarrow m|a,\ k|a \Leftrightarrow n = mk|a \Leftrightarrow a+n\mathbb{Z} = n\mathbb{Z}.$$

Поскольку $|\mathbb{Z}/n\mathbb{Z}| = n$ и $|\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/k\mathbb{Z}| = mk = n$, то мы получаем, что ψ должно быть сюръективным отображением, а значит является изоморфизмом. □

Следствие 17.2. *Пусть n — натуральное число и $n = p_1^{s_1} \cdots p_k^{s_k}$ — его разложение на простые множители. Тогда*

$$\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/p_1^{s_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_k^{s_k}\mathbb{Z}.$$

Доказательство. Очевидная индукция по k. □

Теорема 17.3. *Элемент $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ обратим $\Leftrightarrow (a, n) = 1$.*

Доказательство. Пусть $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^*$. Тогда $\overline{ax} = \overline{1}$ для некоторого элемента $\overline{x} \in \mathbb{Z}/n\mathbb{Z}$. Это означает, что $ax+n\mathbb{Z} = 1+n\mathbb{Z}$, т.е. $ax = 1+nt$. Следовательно, $ax + n(-t) = 1$, откуда $(a, n) = 1$.

Обратно, пусть $(a, n) = 1$. Тогда существуют $x, t \in \mathbb{Z}$ такие, что $ax + nt = 1$, откуда $\overline{ax} = \overline{1}$ и $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^*$. □

Напомним понятие функции Эйлера. Если n — натуральное число, то через $\varphi(n)$ обозначают количество натуральных чисел, не превосходящих n и взаимно простых с n. Полученная функция φ, определенная на множестве натуральных чисел, называется **функцией Эйлера**.

Следствие 17.4. $|(\mathbb{Z}/n\mathbb{Z})^*| = \varphi(n)$.

Теорема 17.5 (Мультипликативность функции Эйлера). 1) $\varphi(mk) = \varphi(m)\varphi(k)$ *для взаимно простых натуральных чисел* m *и* k.

2) *если* $n = p_1^{s_1} \cdots p_k^{s_k}$ *— каноническое разложение натурального* n *на простые множители, то*

$$\varphi(n) = \prod_{i=1}^{k}(p_i^{s_i} - p_i^{s_i-1}) = n\prod_{i=1}^{k}(1 - \frac{1}{p_i}).$$

Доказательство. 1) По теореме 17.1

$$\mathbb{Z}/mk\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/k\mathbb{Z},$$

а по теореме 16.4

$$(\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/k\mathbb{Z})^* = (\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/k\mathbb{Z})^*.$$

Учитывая теорему 17.3, получаем

$$\varphi(mk) = |(\mathbb{Z}/mk\mathbb{Z})^*| = |(\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/k\mathbb{Z})^*| = \\ = |(\mathbb{Z}/m\mathbb{Z})^*||(\mathbb{Z}/k\mathbb{Z})^*| = \varphi(m)\varphi(k),$$

что и доказывает пункт 1) теоремы.

2) Очевидная индукция по k показывает, что если $n = p_1^{s_1} \cdots p_k^{s_k}$, то

$$\varphi(n) = \prod_{i=1}^{k}\varphi(p_i^{s_i}).$$

Поэтому достаточно уметь вычислять $\varphi(p^t)$, где p — простое число. По определению функции Эйлера $\varphi(p^t)$ — это количество целых чисел в промежутке от 1 до p^t, взаимно простых с p^t, т.е. не делящихся на p. Заметим, что количество целых чисел из этого промежутка, делящихся на p, равно p^{t-1}, поскольку это числа вида pa, где $1 \leq a \leq p^{t-1}$. Следовательно,

$$\varphi(p^t) = p^t - p^{t-1},$$

откуда мы получаем

$$\varphi(n) = \prod_{i=1}^{k}(p_i^{s_i} - p_i^{s_i-1}).$$

Вынося в разности $p_i^{s_i} - p_i^{s_i-1}$ множитель $p_i^{s_i}$ за скобки и учитывая, что

$p_1^{s_1} \cdots p_k^{s_k} = n$, получаем второе утверждение теоремы. $\square$

Следствие 17.6. 1) *Если a и $n > 1$ — взаимно простые натуральные числа, то $a^{\varphi(n)} \equiv 1 \pmod{n}$, т.е. остаток от деления $a^{\varphi(n)}$ на n равен 1 (теорема Эйлера).*

2) *Для простого числа p и произвольного a число $a^p - a$ делится на p (теорема Ферма).*

Доказательство. 1) Так как $(a, n) = 1$, то $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^*$. Поскольку $|(\mathbb{Z}/n\mathbb{Z})^*| = \varphi(n)$, то по следствию 4.10 из теоремы Лагранжа получаем $\overline{a}^{\varphi(n)} = \overline{1}$ в $\mathbb{Z}/n\mathbb{Z}$. Следовательно, $a^{\varphi(n)} \equiv 1 \pmod{n}$.

2) Если p делит a, то, очевидно, $a^p - a$ делится на p. Если p не делит a, то a и p взаимно просты. Так как $\varphi(p) = p - 1$, то по теореме Эйлера $a^{p-1} - 1$ делится на p. Значит, $a^p - a$ также делится на p. $\square$

Упражнения

1. Доказать, что любая подгруппа аддитивной группы кольца $\mathbb{Z}_n$ является идеалом кольца $\mathbb{Z}_n$ и что $\mathbb{Z}_n$ — кольцо главных идеалов.

2. Найти все идеалы колец $\mathbb{Z}_8$, $\mathbb{Z}_{15}$. Какие из них максимальны?

3. Разложите в прямую сумму собственных идеалов кольца:

а) $\mathbb{Z}_{10}$; б) $\mathbb{Z}_{12}$; в) $\mathbb{Z}_{36}$.

4. Пользуясь теоремой Эйлера, найти остаток при делении:

1) 208^{208} на 23; 2) 10^{2008} на 22.

§18. Кольцо многочленов от нескольких переменных.

Кольца, которые рассматриваются в этом параграфе, предполагаются коммутативными, ассоциативными и с единицей. Пусть дано кольцо R и независимые переменные $x_1, \ldots, x_n$. **Одночленом** относительно этих переменных называется выражение $ax_1^{k_1} \cdots x_n^{k_n}$, где коэффициент $a \in R$, а $k_1, \ldots, k_n$ — целые неотрицательные числа. Показатели $k_1, \ldots, k_n$ называются **степенями одночлена относительно соответствующих переменных**, а $k_1 + \cdots + k_n$ называется **полной**

степенью или просто **степенью одночлена**. Если какая-то из степеней k_i равна нулю, то выражение x_i^0 в одночлене не пишут. Например, вместо $x_1^2 x_2^0 x_3^4$ пишут просто $x_1^2 x_3^4$.

Два одночлена $ax_1^{k_1} \cdots x_n^{k_n}$ и $bx_1^{k_1} \cdots x_n^{k_n}$ называют **подобными**. Для подобных одночленов определено сложение

$$ax_1^{k_1} \cdots x_n^{k_n} + bx_1^{k_1} \cdots x_n^{k_n} = (a+b)x_1^{k_1} \cdots x_n^{k_n}$$

("приведение подобных членов"). Для произвольных одночленов $ax_1^{k_1} \cdots x_n^{k_n}$ и $bx_1^{m_1} \cdots x_n^{m_n}$ определено умножение:

$$(ax_1^{k_1} \cdots x_n^{k_n})(bx_1^{m_1} \cdots x_n^{m_n}) = (ab)x_1^{k_1+m_1} \cdots x_n^{k_n+m_n}.$$

Многочленом (или **полиномом**) называется формальная сумма одночленов, причем порядок слагаемых безразличен. Таким образом любой многочлен можно записать в виде

$$f(x_1, \ldots, x_n) = \sum_{i_1,\ldots,i_n} a_{i_1,\ldots,i_n} x_1^{k_1} \cdots x_n^{k_n},$$

причем в сумме присутствует лишь конечное число одночленов с ненулевым коэффициентом $a_{i_1,\ldots,i_n}$. Элементы $a_{i_1,\ldots,i_n} \in R$ называют **коэффициентами многочлена** $f(x_1, \ldots, x_n)$. Многочлен, в котором все коэффициенты равны нулю, называется **нулевым**. Максимальная из степеней одночленов, составляющих многочлен, называется его **полной степенью** или просто степенью и обозначается $\deg f$. Условимся считать, что нулевой многочлен имеет степень $-\infty$. Многочлен, все одночлены которого имеют одинаковую степень s, называется **однородным многочленом** или **формой** степени s. Максимальная из степеней одночленов относительно переменной x_i называется **степенью многочлена относительно этой переменной** и обозначается $\deg_{x_i} f$. Два многочлена считаются равными, если их разность — нулевой многочлен, т.е. они являются суммой одинаковых одночленов. Для многочленов естественным образом определяются действия сложения и умножения. Именно, **сумма двух многочленов** — это сумма всех одночленов, составляющих слагаемые; **произведение** — это сумма произведений всех одночленов первого сомножителя на все одночлены второго.

Множество всех многочленов от переменных $x_1, \ldots, x_n$ над кольцом R обозначают $R[x_1, \ldots, x_n]$. Непосредственным вычислением нетрудно доказать следующее

Предложение 18.1. *Кольцо многочленов $R[x_1, \ldots, x_n]$ является ассоциативным и коммутативным кольцом с единицей.*

Элемент a кольца R можно естественным образом отождествить с многочленом $ax_1^0 \cdots x_n^0$ и при таком отождествлении R является подкольцом в $R[x_1, \ldots, x_n]$.

Любой многочлен $f(x_1, \ldots, x_n) \in R[x_1, \ldots, x_n]$ можно записать в виде

$$f(x_1, \ldots, x_n) = f_0(x_1, \ldots, x_{n-1}) + f_1(x_1, \ldots, x_{n-1})x_n + \\ + \cdots + f_s(x_1, \ldots, x_{n-1})x_n^s,$$

где $f_i(x_1, \ldots, x_{n-1}) \in R[x_1, \ldots, x_{n-1}]$, $i = 0, \ldots, s$. Другими словами,

$$R[x_1, \ldots, x_n] = R[x_1, \ldots, x_{n-1}][x_n]. \tag{18.1}$$

Теорема 18.2. *Если R — кольцо без делителей нуля, то и кольцо многочленов $R[x_1, \ldots, x_n]$ является кольцом без делителей нуля.*

Доказательство. Применяем метод математической индукции по числу переменных. База индукции имеется — для многочленов от одной переменной теорема была доказана ранее. Предположим теперь, что кольцо многочленов от $n-1$ переменной не имеет делителей нуля. Тогда и кольцо многочленов от n переменных не имеет делителей нуля, поскольку в силу (18.1) оно является кольцом многочленов от одной переменной над кольцом многочленов от $n-1$ переменной $R[x_1, \ldots, x_{n-1}]$, которое не имеет делителей нуля по индуктивному предположению. □

Следствие 18.3. *Если R — кольцо без делителей нуля, то степень произведения двух многочленов из $R[x_1, \ldots, x_n]$ равна сумме степеней сомножителей.*

Доказательство. Пусть $f, g \in R[x_1, \ldots, x_n]$. Без ограничения общности можно считать, что f и g — ненулевые многочлены (в противном

случае утверждение теоремы тривиально). Собирая в f вместе одночлены одинаковой степени, запишем f в виде

$$f = f_0 + f_1 + \cdots + f_r,$$

где f_i — форма степени i и $f_r \neq 0$. Тогда степень f равна r. Аналогично, g запишем в виде

$$g = g_0 + g_1 + \cdots + g_s,$$

где $g_s \neq 0$. Тогда степень g равна s и

$$fg = \sum_{i,j} f_i g_j.$$

Все одночлены наибольшей степени, входящие в fg, содержатся в $f_r g_s$ и имеют полную степень $r+s$. По теореме 18.2 $f_r g_s \neq 0$. Значит, степень fg равна $r + s$. □

Предположим, что S — кольцо, содержащее R, при этом единицы в R и S совпадают. Пусть дан многочлен

$$f(x_1, \ldots, x_n) = \sum_{i_1,\ldots,i_n} a_{i_1,\ldots,i_n} x_1^{k_1} \cdots x_n^{k_n} \in R[x_1, \ldots, x_n].$$

и даны элементы $b_1, \ldots, b_n \in S$.

Определение 18.4. *Значением многочлена $f(x_1, \ldots, x_n)$ в точке $(b_1, \ldots, b_n)$ (или при $x_1 = b_1, \ldots, x_n = b_n$) называется*

$$f(b_1, \ldots, b_n) = \sum_{i_1,\ldots,i_n} a_{i_1,\ldots,i_n} b_1^{k_1} \cdots b_n^{k_n} \in S.$$

Ясно, что если

$$h(x_1, \ldots, x_n) = f_1(x_1, \ldots, x_n) + f_2(x_1, \ldots, x_n),$$
$$g(x_1, \ldots, x_n) = f_1(x_1, \ldots, x_n) f_2(x_1, \ldots, x_n),$$

то

$$h(b_1, \ldots, b_n) = f_1(b_1, \ldots, b_n) + f_2(b_1, \ldots, b_n), \tag{18.2}$$
$$g(b_1, \ldots, b_n) = f_1(b_1, \ldots, b_n) f_2(b_1, \ldots, b_n). \tag{18.3}$$

Предложение 18.5. *Пусть S — кольцо, содержащее R, при этом единицы в кольцах R и S совпадают. Для любых элементов*

$b_1, \ldots, b_n \in S$ существует единственный гомоморфизм

$$\psi : R[x_1, \ldots, x_n] \to S,$$

для которого

$$\psi(x_1) = b_1, \ldots, \psi(x_n) = b_n, \quad \psi(1_R) = 1_S.$$

Доказательство. Определим отображение

$$\psi : R[x_1, \ldots, x_n] \to S, \quad f(x_1, \ldots, x_n) \mapsto f(b_1, \ldots, b_n).$$

В силу (18.2) и (18.3) ψ является гомоморфизмом. Докажем единственность ψ. Если $\psi_1 : R[x_1, \ldots, x_n] \to S$ — другой гомоморфизм, удовлетворяющий условиям теоремы, и $f = \sum_{i_1,\ldots,i_n} a_{i_1,\ldots,i_n} x_1^{k_1} \cdots x_n^{k_n}$, то

$$\psi_1(f) = \psi_1\Big(\sum_{i_1,\ldots,i_n} a_{i_1,\ldots,i_n} x_1^{k_1} \cdots x_n^{k_n}\Big) = \sum_{i_1,\ldots,i_n} a_{i_1,\ldots,i_n} \psi_1(x_1)^{k_1} \cdots \psi_1(x_n)^{k_n} =$$

$$= \sum_{i_1,\ldots,i_n} a_{i_1,\ldots,i_n} b_1^{k_1} \cdots b_n^{k_n} = f(b_1, \ldots, b_n) = \psi(f).$$

Значит, $\psi_1 = \psi$. □

Пусть R — кольцо без делителей нуля, содержащее бесконечно много элементов. Мы знаем, что в кольце многочленов $R[x]$ от одной переменной каждый многочлен $f(x)$ однозначно определяется своими значениями в $d = \deg f + 1$ различных точках $b_1, \ldots, b_d$. Другими словами, если $g(b_i) = f(b_i)$, $i = 1, \ldots, d$, для некоторого многочлена $g(x)$ и $\deg g \leq \deg f$, то $g = f$. В частности, никакие два неравных многочлена от одной переменной не могут принимать одинаковые значения в бесконечном количестве различных точек.

Ситуация коренным образом меняется, когда мы рассматриваем многочлены от нескольких переменных. Например, многочлены x_1 и x_1x_2 из кольца $R[x_1, x_2]$ принимают значение 0 во всех точках $(0, b)$, где $b \in R$, однако они не равны. Тем не менее справедлива следующая теорема.

Теорема 18.6 (О тождестве). *Если многочлены $f_1(x_1, \ldots, x_n)$ и $f_2(x_1, \ldots, x_n)$ принимают одинаковые значения во всех точках $(b_1, \ldots, b_n)$, где $b_1, \ldots, b_n \in R$, то они равны.*

Доказательство. Для доказательства достаточно доказать следующее утверждение: Если все значения многочлена $h(x_1, \ldots, x_n) \in R[x_1, \ldots, x_n]$ во всех указанных в теореме точках равны нулю, то h — нулевой многочлен. Действительно, достаточно перейти от многочленов f_1 и f_2 к их разности $h = f_1 - f_2$.

Предположим, что h — ненулевой многочлен. Покажем, что найдутся значения $b_1, \ldots, b_n$ для переменных $x_1, \ldots, x_n$, при которых h принимает значение, отличное от нуля.

Применим метод математической индукции по числу переменных n. При $n = 1$ утверждение следует из того, что ненулевой многочлен от одной переменной имеет корней не больше, чем его степень. Действительно, по условию R — бесконечное кольцо, и если бы все элементы из R являлись корнями h, то ненулевой многочлен h имел бы бесконечно много корней — противоречие.

Пусть теперь $n > 1$ и $h(x_1, \ldots, x_n)$ — ненулевой многочлен. Запишем $h(x_1, \ldots, x_n)$ как многочлен от x_n с коэффициентами из кольца $R[x_1, \ldots, x_{n-1}]$:

$$h(x_1, \ldots, x_n) = a_0(x_1, \ldots, x_{n-1}) + a_1(x_1, \ldots, x_{n-1})x_n + \ldots + \\ + a_s(x_1, \ldots, x_{n-1})x_n^s.$$

Можно считать, что $a_s(x_1, \ldots, x_{n-1})$ — ненулевой многочлен. В силу индуктивного предположения найдется набор значений $b_1, \ldots, b_{n-1}$ из R такой, что $a_s(b_1, \ldots, b_{n-1}) \neq 0$. Тогда

$$h(b_1, \ldots, b_{n-1}, x_n) = a_0(b_1, \ldots, b_{n-1}) + a_1(b_1, \ldots, b_{n-1})x_n + \\ + a_s(b_1, \ldots, b_{n-1})x_n^s = c_0 + c_1x_n + \cdots + c_sx_n^s,$$

где $c_i = a_i(b_1, \ldots, b_{n-1})$ и $c_s \neq 0$. Поскольку теорема справедлива при $n = 1$, то найдется такое $b_n \in R$, что

$$h(b_1, \ldots, b_{n-1}, b_n) = c_0 + c_1b_n + \cdots + c_sb_n^s \neq 0,$$

что и требовалось доказать. □

Мы можем немного ослабить требования теоремы 18.6. Оказывается, достаточно сравнивать значения многочленов не во всех точках из R^n, а только в точках из некоторого подмножества из R^n.

Следствие 18.7 (о несущественности алгебраических неравенств). *Пусть R — бесконечное кольцо без делителей нуля и пусть f_1 и f_2 — два многочлена из $R[x_1, \ldots, x_n]$, принимающие одинаковые значения во всех точках $(b_1, \ldots, b_n)$, где выполнены неравенства*

$$h_1(b_1, \ldots, b_n) \neq 0, \ldots, h_k(b_1, \ldots, b_n) \neq 0,$$

где $h_1, \ldots, h_k$ — отличные от нуля многочлены из $R[x_1, \ldots, x_n]$. Тогда многочлены f_1 и f_2 равны.

Доказательство. Рассмотрим многочлен $(f_1 - f_2)h_1 \cdots h_k$. Он равен нулю при всех наборах переменных, так как там, где $h_1 \neq 0, \ldots, h_k \neq 0$, обращается в нуль первый множитель. В силу теоремы о тождестве 18.6 $(f_1 - f_2)h_1 \cdots h_k = 0$. Но $R[x_1, \ldots, x_n]$ не имеет делителей нуля и $h_1 \neq 0, \ldots, h_k \neq 0$. Следовательно, $f_1 - f_2 = 0$, т. е. $f_1 = f_2$, что и требовалось доказать. □

Установленная теорема оказывается полезной в довольно часто встречающейся ситуации, когда равенство значений двух многочленов удается установить в предположении о необращении в нуль одного или нескольких многочленов. В силу доказанной теоремы после установления такого равенства поставленные ограничения автоматически снимаются.

Замечание. Теорема о тождестве 18.6 перестает быть верной, если отбросить требование конечности кольца R. Например, в кольце многочленов $\mathbb{Z}_p[x_1, x_2]$ рассмотрим многочлены $f(x_1, x_2) = x_1^p - x_1$ и $g(x_1, x_2) = x_2^p - x_2$. По теореме Ферма $a^p - a = 0$ для любого $a \in \mathbb{Z}_p$. Следовательно, $f(a, b) = g(a, b) = 0$ для любой точки (a, b), где $a, b \in \mathbb{Z}_p$, но при этом $f \neq g$.

Для многочленов от одного неизвестного мы имеем два естественных способа расположения членов — по возрастающим и по убывающим степеням неизвестного. В случае многочленов от нескольких неизвестных такие способы уже отсутствуют: если дан многочлен

$$f(x_1, x_2, x_3) = x_1x_2^2x_3^2 + x_1^4x_3 + x_2^3x_3^2 + x_1^2x_2x_3^2,$$

то его можно записать и в виде

$$f(x_1, x_2, x_3) = x_1^4 x_3 + x_1^2 x_2 x_3^2 + x_1 x_2^2 x_3^2 + x_2^3 x_3^2,$$

и нет оснований одну из этих записей предпочесть другой. Существует, однако, способ вполне определенного расположения одночленов в многочлене от нескольких неизвестных. Этот способ, впрочем, зависит от выбора нумерации неизвестных. Этот способ называют **лексикографическим** и он подсказан обычным приемом расположения слов в словарях. Пусть даны два одночлена

$$a x_1^{k_1} \cdots x_n^{k_n} \tag{18.4}$$

$$b x_1^{m_1} \cdots x_n^{m_n}, \tag{18.5}$$

где $a \neq 0$, $b \neq 0$ и $(k_1, \ldots, k_n) \neq (m_1, \ldots, m_n)$.

Определение 18.8. *Говорят, что одночлен (18.4)* ***выше*** *одночлена (18.5), если первая отличная от нуля среди разностей $k_1 - m_1$, $k_2 - m_2$, ..., $k_n - m_n$ положительна. В этом случае записываем $a x_1^{k_1} \cdots x_n^{k_n} \succ b x_1^{m_1} \cdots x_n^{m_n}$. Получаемое таким образом упорядочение на множестве одночленов называют* ***лексикографическим****.*

Предложение 18.9. *Пусть R — кольцо без делителей нуля. Отношение лексикографического упорядочения одночленов обладает следующими свойствами:*

1) *если $A \succ B$ и $B \succ C$, то $A \succ C$;*
2) *если $A \succ B$, то $AC \succ BC$ для любого одночлена C;*
3) *если $A_1 \succ B_1$ и $A_2 \succ B_2$, то $A_1 A_2 \succ B_1 B_2$.*

Первое из этих свойств, собственно, и дает основание называть отношение $\succ$ упорядочением.

Доказательство. 1) Пусть первая переменная, которая не входит во все одночлены A, B, C с одним и тем же показателем, входит в них с показателями k, l, m соответственно. Тогда по условию

$$k \geq l \geq m,$$

причем хотя бы в одном из двух случаев имеет место строгое неравенство. Следовательно, $k > m$, а это и означает, что $A \succ C$.

2) При умножении на C к показателям, с которыми каждая из переменных входит в A и B, добавляется одно и то же число, и знак неравенства (или равенства) между этими показателями не меняется, а только эти неравенства и имеют значение при лексикографическом сравнении одночленов.

3) Пользуясь предыдущим свойством, получаем

$$A_1A_2 \succ B_1A_2 \succ B_1B_2.$$

Предложение доказано. □

Очевидно, что из любых двух различных одночленов многочлена $f(x_1, \ldots, x_n)$ один будет выше другого. Записывая раньше тот из двух одночленов, входящих в f, который выше, мы получим лексикографическую запись f. Например, многочлен

$$f(x_1, x_2, x_3, x_4) = x_1^4 + 3x_1^2x_2^3x_3 - x_1^2x_2^2x_4^2 + 5x_1x_3x_4^2 + 2x_2 + x_3^2x_4 - 4$$

записан лексикографически. Обратите внимание на то, что одночлен $3x_1^2x_2^3x_3$ лексикографически ниже одночлена x_1^4, хотя его степень больше.

Определение 18.10. ***Высшим одночленом*** *ненулевого многочлена $f(x_1, \ldots, x_n)$ называется такой одночлен, который выше всех других одночленов, входящих в f.*

Предложение 18.11. *Пусть R — кольцо без делителей нуля. Высший одночлен произведения многочленов $h_1, \ldots, h_k \in R[x_1, \ldots, x_n]$ равен произведению их высших одночленов.*

Доказательство. Достаточно доказать это утверждение для двух многочленов, а затем использовать очевидную индукцию по числу многочленов k. Пусть h_1, h_2 — ненулевые многочлены, A, B — их высшие одночлены и A_1, B_1 — какие-то их произвольные одночлены. Если $A \neq A_1$ или $B \neq B_1$, то в силу предложения 18.9

$$AB \succ A_1B_1.$$

Это означает, что после приведения подобных слагаемых в произведении f_1f_2 произведение AB сохранится в качестве ненулевого одночлена (ведь ему не с чем сокращаться), который старше всех остальных. □

Замечание. Кроме лексикографического существуют и другие мономиальные упорядочения одночленов из $R[x_1, \ldots, x_n]$, обладающие всеми свойствами из предложения 18.9. Каждое из этих упорядочений имеет свою область применения.

§19. Симметрические многочлены.

В этом параграфе будем предполагать, что R — ассоциативное коммутативное кольцо без делителей нуля.

Определение 19.1. *Многочлен $f \in R[x_1, \ldots, x_n]$ называется* ***симметрическим****, если он не изменяется ни при каких перестановках переменных.*

Так как любая перестановка может быть осуществлена путем последовательных перестановок двух элементов, то многочлен является симметрическим, если он не изменяется при перестановке любых двух переменных.

Пример 1. Степенные суммы

$$s_k = x_1^k + \cdots + x_n^k, \qquad (k = 1, 2, \ldots),$$

очевидно, являются симметрическими многочленами.

Пример 2. Следующие симметрические многочлены называются **элементарными симметрическими многочленами**:

$$\begin{aligned}
\sigma_1 &= x_1 + x_2 + \cdots + x_n, \\
\sigma_2 &= x_1x_2 + x_1x_3 + \cdots + x_{n-1}x_n, \\
&\cdots \qquad \cdots \\
\sigma_k &= \sum_{i_1<i_2<\ldots<i_k} x_{i_1}x_{i_2}\cdots x_{i_k}, \\
&\cdots \qquad \cdots \\
\sigma_n &= x_1x_2\cdots x_n.
\end{aligned}$$

Напомним, что эти многочлены встречались ранее в курсе алгебры в связи с теоремой Виета.

Пример 3. Многочлен

$$(x_1 + x_2 - x_3 - x_4)(x_1 - x_2 + x_3 - x_4)(x_1 - x_2 - x_3 + x_4)$$

является симметрическим.

Очевидно, что сумма, разность и произведение симметрических многочленов являются симметрическими многочленами. Иными словами, симметрические многочлены образуют подкольцо в кольце всех многочленов от n переменных.

Следовательно, если $F \in R[y_1, \ldots, y_m]$ — произвольный многочлен от m переменных $y_1, \ldots, y_m$ и $f_1, \ldots, f_m \in R[x_1, \ldots, x_n]$ — какие-то симметрические многочлены от $x_1, \ldots, x_n$, то значение $F(f_1, \ldots, f_m)$ многочлена F при $y_1 = f_1, \ldots, y_m = f_m$ является симметрическим многочленом от $x_1, \ldots, x_n$. Естественно поставить вопрос, нельзя ли найти такие симметрические многочлены $f_1, \ldots, f_m$, чтобы всякий симметрический многочлен можно было выразить через них указанным способом. Оказывается, что в качестве таких многочленов можно взять элементарные симметрические многочлены $\boldsymbol{\sigma}_1, \ldots, \boldsymbol{\sigma}_n$.

Теорема 19.2 (Основная о симметрических многочленах). *Пусть $f \in R[x_1, \ldots, x_n]$ — симметрический многочлен. Тогда найдется такой многочлен $F \in R[y_1, \ldots, y_n]$, что*

$$f(x_1, \ldots, x_n) = F(\boldsymbol{\sigma}_1, \ldots, \boldsymbol{\sigma}_n).$$

При этом многочлен F определен однозначно. Другими словами, всякий симметрический многочлен единственным образом представляется в виде многочлена от элементарных симметрических многочленов.

Для доказательства теоремы нам необходимы две леммы.

Лемма 19.3. *Пусть $u = ax_1^{k_1}x_2^{k_2}\cdots x_n^{k_n}$ — высший одночлен симметрического многочлена f. Тогда*

$$k_1 \geq k_2 \geq \ldots \geq k_n. \tag{19.1}$$

Доказательство. Предположим, что $k_i < k_{i+1}$ для некоторого i. Наряду с одночленом u многочлен f должен содержать одночлен

$$u' = ax_1^{k_1}\cdots x_i^{k_{i+1}}x_{i+1}^{k_i}\cdots x_n^{k_n},$$

получающийся из u перестановкой x_i и x_{i+1}. Легко видеть, что $u' \succ u$. Это противоречит тому, что u — старший одночлен многочлена f. $\square$

Лемма 19.4. *Для любого одночлена $u = ax_1^{k_1}x_2^{k_2}\cdots x_n^{k_n}$, показатели которого удовлетворяют неравенствам* (19.1)*, существуют такие неотрицательные целые числа $l_1, \ldots, l_n$, что высший одночлен многочлена $a\boldsymbol{\sigma}_1^{l_1}\boldsymbol{\sigma}_2^{l_2}\cdots\boldsymbol{\sigma}_n^{l_n}$ совпадает с u. Числа $l_1, \ldots, l_n$ определены этим условием однозначно.*

Доказательство. Легко видеть, что высший одночлен многочлена $\boldsymbol{\sigma}_k$ равен $x_1x_2\cdots x_k$. В силу предложения 18.11 высший одночлен многочлена $a\boldsymbol{\sigma}_1^{l_1}\boldsymbol{\sigma}_2^{l_2}\cdots\boldsymbol{\sigma}_n^{l_n}$ равен

$$ax_1^{l_1}(x_1x_2)^{l_2}\cdots(x_1x_2\cdots x_n)^{l_n} = ax_1^{l_1+l_2+\cdots+l_n}x_2^{l_2+l_3+\cdots+l_n}\cdots x_n^{l_n}.$$

Приравнивая его одночлену u, получаем систему линейных уравнений

$$\begin{cases} l_1 + l_2 + \cdots + l_n = k_1, \\ \qquad l_2 + \cdots + l_n = k_2, \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ \qquad\qquad\qquad l_n = k_n. \end{cases}$$

Эта система, очевидно, имеет единственное решение

$$l_i = k_i - k_{i+1} \qquad (i = 1, 2, \ldots, n-1), \qquad l_n = k_n. \tag{19.2}$$

Из условия леммы следует, что определенные таким образом числа $l_1, \ldots, l_n$ неотрицательны. □

Доказательство теоремы 19.2. Если $f = 0$, то можно взять $F = 0$. В противном случае пусть $u_1 = ax_1^{k_1}x_2^{k_2}\cdots x_n^{k_n}$ — высший одночлен многочлена f. По лемме 19.3 выполняются неравенства $k_1 \geq k_2 \geq \ldots \geq k_n$. По лемме 19.4 существуют такие неотрицательные целые числа $l_1, \ldots, l_n$, что высший одночлен многочлена $a\boldsymbol{\sigma}_1^{l_1}\boldsymbol{\sigma}_2^{l_2}\cdots\boldsymbol{\sigma}_n^{l_n}$ совпадает с u_1. Обозначим $F_1 = ay_1^{l_1}y_2^{l_2}\cdots y_n^{l_n} \in K[y_1, \ldots, y_n]$ и рассмотрим симметрический многочлен

$$f_1 = f - F_1(\boldsymbol{\sigma}_1, \boldsymbol{\sigma}_2, \ldots, \boldsymbol{\sigma}_n).$$

Если $f_1 = 0$, то можно взять $F = F_1$. В противном случае пусть u_2 — высший одночлен многочлена f_1. Ясно, что $u_1 \succ u_2$. Снова по лемме 19.4 существует такой одночлен $F_2 \in K[y_1, \ldots, y_n]$, что что высший одночлен многочлена $F_2(\boldsymbol{\sigma}_1, \boldsymbol{\sigma}_2, \ldots, \boldsymbol{\sigma}_n)$ равен u_2. Рассмотрим симмет-

рический многочлен

$$f_2 = f_1 - F_2(\sigma_1, \sigma_2, \ldots, \sigma_n).$$

Если $f_2 = 0$, то можно взять $F = F_1 + F_2$. В противном случае, продолжая процесс, получаем последовательность симметрических многочленов $f, f_1, f_2, \ldots$, высшие одночлены которых удовлетворяют неравенствам

$$u_1 \succ u_2 \succ \ldots$$

По лемме 19.4 показатель при любой переменной в любом из одночленов u_m не превосходит показателя при x_1 в этом одночлене, а он, в свою очередь, не превосходит k_1. Поэтому для наборов показателей одночленов u_m имеется лишь конечное число возможностей, так что описанный выше процесс должен оборваться. Это означает, что $f_M = 0$ для некоторого M. В качестве F можно тогда взять $F_1 + F_2 \cdots + F_M$.

Докажем теперь, что многочлен F определен однозначно. Предположим, что F и G — такие многочлены из $K[y_1, \ldots, y_n]$, что

$$F(\sigma_1, \sigma_2, \ldots, \sigma_n) = G(\sigma_1, \sigma_2, \ldots, \sigma_n).$$

Рассмотрим их разность $H = F - G$. Тогда

$$H(\sigma_1, \sigma_2, \ldots, \sigma_n) = 0.$$

Нам нужно доказать, что H — нулевой многочлен. Предположим, что это не так, и пусть $H_1, H_2, \ldots, H_s$ — все ненулевые одночлены многочлена H. Обозначим через w_i $(i = 1, 2, \ldots, s)$ высший одночлен многочлена

$$H_i(\sigma_1, \sigma_2, \ldots, \sigma_n) \in K[x_1, x_2, \ldots, x_n].$$

В силу леммы 19.4 среди одночленов $w_1, w_2, \ldots, w_s$ нет пропорциональных. Выберем из них наивысший. Пусть это будет w_1. По построению одночлен w_1 выше всех остальных одночленов многочлена $H_1(\sigma_1, \sigma_2, \ldots, \sigma_n)$ и всех одночленов многочленов $H_i(\sigma_1, \sigma_2, \ldots, \sigma_n)$ $(i = 2, \ldots, s)$. Поэтому после приведения подобных одночленов в сумме

$$H_1(\sigma_1, \sigma_2, \ldots, \sigma_n) + \cdots + H_s(\sigma_1, \sigma_2, \ldots, \sigma_n) = H(\sigma_1, \sigma_2, \ldots, \sigma_n)$$

одночлен w_1 сохранится (ему не с чем сокращаться), так что эта сумма

не будет равна нулю, что противоречит нашему предположению. □

Следующее утверждение позволяет по-новому осмыслить полученный в предыдущей теореме результат.

Предложение 19.5. *Подкольцо S симметрических многочленов кольца $R[x_1, \ldots, x_n]$ изоморфно кольцу всех многочленов $R[x_1, \ldots, x_n]$.*

Доказательство. Рассмотрим кольцо многочленов $R[y_1, \ldots, y_n]$, которое изоморфно $R[x_1, \ldots, x_n]$, и отображение

$$\psi : R[y_1, \ldots, y_n] \to R[x_1, \ldots, x_n], \quad \psi(f) = f(\sigma_1, \ldots, \sigma_n),$$

т.е. в качестве $\psi(f)$ мы берем значение f при $y_1 = \sigma_1, \ldots, y_n = \sigma_n$. В силу предложения 18.5 ψ — гомоморфизм. Очевидно, $\operatorname{Im}\psi \subseteq S$. По основной теореме о симметрических многочленах 19.2 любой симметрический многочлен $h \in S$ можно представить в виде $h = f(\sigma_1, \ldots, \sigma_n)$ для некоторого многочлена $f \in R[y_1, \ldots, y_n]$. Это означает, что $h = \psi(f)$, т.е. $\operatorname{Im}\psi = S$. Кроме того, отображение ψ инъективно в силу единственности такого представления. Значит, ψ — изоморфизм колец $R[y_1, \ldots, y_n]$ и S. □

Следуя доказательству этой теоремы, можно в принципе найти выражение любого конкретного симметрического многочлена через σ_1, σ_2, …, σ_n. На практике для однородных симметрических многочленов удобнее применять другой способ, который мы поясним на следующем примере.

Пример. Выразим через $\sigma_1, \sigma_2, \sigma_3, \sigma_4$ многочлен

$$f = (x_1x_2 + x_3x_4)(x_1x_3 + x_2x_4)(x_1x_4 + x_2x_3).$$

В обозначениях доказательства теоремы 19.2 имеем $u_1 = x_1^3x_2x_3x_4$. Не производя вычислений, можно найти с точностью до коэффициентов множество возможных кандидатов на роль одночленов $u_2, u_3, u_4, \ldots$. Во-первых, их показатели должны удовлетворять неравенствам леммы 19.3. Во-вторых, поскольку f — однородный многочлен степени 6, сумма их показателей должна равняться 6. В-третьих, они должны быть младше u_1. Выпишем в таблицу все наборы показателей одночленов, удовлетворяющих этим условиям, в порядке лексикографического

убывания, начиная с набора показателей одночлена u_1, а справа выпишем соответствующие произведения элементарных симметрических многочленов, найденные по формулам (19.2):

3	1	1	1	$\sigma_1^2\sigma_4$
2	2	2	0	σ_3^2
2	2	1	0	$\sigma_2\sigma_4$

Итак, мы можем утверждать, что

$$f = \sigma_1^2\sigma_4 + a\sigma_3^2 + b\sigma_2\sigma_4.$$

Для того чтобы найти коэффициенты a и b, будем придавать в этом равенстве переменным x_1, x_2, x_3, x_4 какие-нибудь выбранные значения. Представим вычисления в виде таблицы, в правом столбце которой будем выписывать получаемые уравнения:

x_1	x_2	x_3	x_4	σ_1	σ_2	σ_3	σ_4	f	
1	1	1	0	3	3	1	0	1	$a = 1$
1	1	-1	-1	0	-2	0	1	8	$-2b = 8$

Таким образом, $a = 1$ и $b = -4$, так что

$$f = \sigma_1^2\sigma_4 + \sigma_3^2 - 4\sigma_2\sigma_4.$$

В случае неоднородного симметрического многочлена этот способ можно применить к каждой его однородной компоненте и полученные выражения сложить.

Упражнения

1. Следующие многочлены выразить в виде многочленов от элементарных симметрических многочленов:

а) $x_1^2x_2 + x_1x_2^2 + x_1^2x_3 + x_1x_3^2 + x_2^2x_3 + x_2x_3^2$;

б) $x_1^4 + x_2^4 + x_3^4 - 2x_1^2x_2^2 - 2x_1^2x_3^2 - 2x_2^2x_3^2$;

в) $(x_1x_2 + x_3)(x_1x_3 + x_2)(x_2x_3 + x_1)$;

г) $(x_1 + x_2)(x_1 + x_3)(x_1 + x_4)(x_2 + x_3)(x_2 + x_4)(x_3 + x_4)$.

2. Найти значение симметрического многочлена F от корней многочлена $f(x)$:

а) $F = x_1^3(x_2+x_3)+x_2^3(x_1+x_3)+x_3^3(x_1+x_2)$, $f(x) = x^3-x^2-4x+1$;

б) $F = (x_1-x_2)^2(x_1-x_3)^2(x_2-x_3)^2$, $f(x) = x^3+a_1x^2+a_2x+a_3$.

3. Решить над полем комплексных чисел систему уравнений

$$\begin{cases} x_1^2+x_2^2+x_3^2 = 6 \\ x_1^3+x_2^3+x_3^3-x_1x_2x_3 = -4 \\ x_1x_2+x_1x_3+x_2x_3 = -3 \end{cases}$$

4. Доказать, что значение от корней степени n из 1 всякого симметрического многочлена от n переменных с целыми коэффициентами является целым числом.

5. Вычислить сумму пятых степеней корней многочлена $x^6-4x^5+3x^3-4x^2+x+1$.

6. Найти многочлен третьей степени, корнями которого являются:

а) кубы корней многочлена x^3-x-1;

б) четвертые степени корней многочлена $2x^3-x^2+2$.

§20. Поле частных кольца без делителей нуля.

Пусть A — коммутативное ассоциативное кольцо без делителей нуля с единицей. Таким же образом, как кольцо целых чисел расширяется до поля рациональных чисел, кольцо A можно расширить до поля.

На множестве пар $(a,b) \in A^2$, $b \neq 0$, определим отношение эквивалентности по правилу

$$(a,b) \sim (a_1,b_1) \Leftrightarrow ab_1 = a_1b.$$

Рефлексивность и симметричность этого отношения очевидны; докажем его транзитивность. Если $(a,b) \sim (a_1,b_1)$ и $(a_1,b_1) \sim (a_2,b_2)$, то

$$(ab_1)b_2 = (a_1b)b_2 = (a_1b_2)b = (a_2b_1)b.$$

Поскольку $b_1 \neq 0$ и A — кольцо без делителей нуля, то мы можем обе части равенства сократить на b_1 и получим

$$ab_2 = a_2b,$$

т.е. $(a,b) \sim (a_2,b_2)$.

Класс эквивалентности, содержащий пару (a,b), условимся запи-

сывать как "дробь" $\dfrac{a}{b}$ (пока это просто символ, не подразумевающий фактического деления). Множество всех дробей обозначим через $Q(A)$.

Определим теперь сложение и умножение дробей по правилам

$$\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd}, \qquad \frac{a}{b}\,\frac{c}{d}=\frac{ac}{bd}.$$

Лемма 20.1. *Введенные операции над дробями корректно определены, т.е. не зависят от выбора представителей в классах эквивалентности.*

Доказательство. Пусть $\frac{a}{b}=\frac{a_1}{b_1}$, $\frac{c}{d}=\frac{c_1}{d_1}$. Тогда $ab_1=a_1b$, $cd_1=c_1d$. Имеем

$$\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd}, \quad \frac{a_1}{b_1}+\frac{c_1}{d_1}=\frac{a_1d_1+b_1c_1}{b_1d_1}.$$

Проверим, что справа стоят равные дроби:

$$(ad+bc)b_1d_1-(a_1d_1+b_1c_1)bd=(ab_1-a_1b)dd_1+(cd_1-c_1d)bb_1=0,$$

что и требовалось. Аналогичное вычисление показывает корректность умножения. □

Теорема 20.2. *$Q(A)$ относительно введенных операций является полем. Это поле называют* ***полем частных*** *кольца A*

Доказательство. Заметим, что $\frac{a}{b}=\frac{ac}{bc}$ для любого $0\neq c\in A$. Поэтому любое конечное множество дробей можно привести к общему знаменателю, а сложение дробей с одинаковыми знаменателями сводится к сложению их числителей. Поэтому сложение дробей коммутативно и ассоциативно. Дробь $\frac{0}{1}$ служит нулем для операции сложения дробей, а дробь $-\frac{a}{b}$ противоположна дроби $\frac{a}{b}$. Таким образом, дроби образуют абелеву группу относительно сложения.

Коммутативность и ассоциативность умножения очевидны. Следующая цепочка равенств доказывает дистрибутивность умножения дробей относительно сложения:

$$\left(\frac{a_1}{b}+\frac{a_2}{b}\right)\frac{c}{d}=\frac{(a_1+a_2)c}{bd}=\frac{a_1c+a_2c}{bd}=\frac{a_1}{b}\frac{c}{d}+\frac{a_2}{b}\frac{c}{d}.$$

Дробь $\frac{1}{1}$ служит единицей для операции умножения дробей, а при $a\neq 0$ дробь $\frac{b}{a}$ обратна дроби $\frac{a}{b}$. □

Сложение и умножение дробей вида $\frac{a}{1}$ сводятся к соответствующим операциям над их числителями. Кроме того, $\frac{a}{1} = \frac{b}{1}$ только при $a = b$. Следовательно, дроби такого вида образуют подкольцо, изоморфное A. Условившись отождествлять дробь вида $\frac{a}{1}$ с элементом a кольца A, мы можем считать, что кольцо A содержится в поле $Q(A)$. Далее, поскольку

$$\frac{a}{b}\frac{b}{1} = \frac{a}{1},$$

то дробь $\frac{a}{b}$ равна отношению элементов a и b кольца A в поле $Q(A)$. Таким образом, обозначение $\frac{a}{b}$ можно теперь понимать содержательным образом как деление элементов a и b в поле $Q(A)$.

Следствие 20.3. *Пусть A — коммутативное ассоциативное кольцо с 1. Кольцо A содержится в некотором поле K тогда и только тогда, когда A — кольцо без делителей нуля.*

Доказательство. Если A — кольцо без делителей нуля, то по теореме 20.2 существует поле частных $Q(A)$ и $A \subset Q(A)$. Наоборот, если A содержится в некотором поле K, то поскольку в K нет делителей нуля, кольцо A является кольцом без делителей нуля. □

Пример 1. Поле частных кольца $\mathbb{Z}$ целых чисел есть поле $\mathbb{Q}$ рациональных чисел.

Пример 2. Поле частных кольца $K[x]$ многочленов над полем K называется полем рациональных функций над полем K и обозначается через $K(x)$.

Пример 3. Поле частных кольца $K[x_1, \ldots, x_n]$ многочленов от n переменных над полем K называется полем рациональных функций от n переменных над полем K и обозначается через $K(x_1, \ldots, x_n)$.

§21. Характеристика поля.

Пусть P — поле.

Определение 21.1. *Если для любого натурального числа n элемент $n \cdot 1 = \underbrace{1 + \cdots + 1}_{n}$ поля P отличен от нуля, то говорят, что*

поле P имеет ***характеристику*** *нуль; если же для некоторого натурального n элемент $n \cdot 1$ равен нулю, то наименьшее такое натуральное n называется* ***характеристикой*** *поля P и P называется полем положительной характеристики. Характеристика поля P обозначается* $\operatorname{char} P$.

Примерами полей конечной характеристики служат все конечные поля; существуют, впрочем, и бесконечные поля, имеющие конечную характеристику. Поле $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, состоящее из p элементов, очевидно, имеет характеристику p. Поля $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ имеют характеристику нуль.

Непосредственно из определения следует, что для любого расширения $E \supset F$ справедливо $\operatorname{char} E = \operatorname{char} F$.

Теорема 21.2. *Если поле P имеет характеристику p, то число p простое.*

Доказательство. Действительно, из равенства $p = st$, где $s < p$, $t < p$, вытекало бы равенство

$$(s \cdot 1)(t \cdot 1) = (st \cdot 1) = (p \cdot 1) = 0.$$

Так как в поле не может быть делителей нуля, то или $s \cdot 1 = 0$ или $t \cdot 1 = 0$, что, однако, противоречит определению характеристики поля. □

Предложение 21.3. *Если характеристика поля P равна p, то для любого элемента $a \in P$ и любого n, делящегося на p, имеет место равенство $n \cdot a = 0$. Если же* $\operatorname{char} P = 0$, $0 \neq a \in P$ *и* $0 \neq n \in \mathbb{Z}$, *то $na \neq 0$.*

Доказательство. Пусть $\operatorname{char} P = p$ и $n = pn_1$. Тогда

$$n \cdot a = n_1 p \cdot (1a) = n_1(p \cdot 1)a = n_1 0a = 0.$$

Если $\operatorname{char} P = 0$, то из равенства $na = (n \cdot 1)a = 0$ следовало бы $n \cdot 1 = 0$. Так как характеристика поля равна нулю, то $n = 0$ — противоречие. □

Предложение 21.4. *Если поле P имеет характеристику p, то для любых элементов $x, y \in P$ и любого натурального n*

$$(x+y)^{p^n} = x^{p^n} + y^{p^n}.$$

Доказательство. Воспользуемся индукцией по n. При $n = 1$ нам нужно доказать, что

$$(x+y)^p = x^p + y^p.$$

По формуле бинома Ньютона

$$(x+y)^p = x^p + \sum_{i=1}^{p-1} C_p^i x^i y^{p-i} + y^p.$$

Так как $C_p^i = \frac{p!}{i!(p-i)!}$, то $p | C_p^i$ и по предложению 21.3 $C_p^i x^i y^{p-i} = 0$. Значит, $(x+y)^p = x^p + y^p$.

Предположим теперь, что предложение верно при $n = k-1$ и докажем его при $n = k$.

$$(x+y)^{p^k} = ((x+y)^{p^{k-1}})^p = (x^{p^{k-1}} + y^{p^{k-1}})^p = x^{p^k} + y^{p^k}.$$

Предложение доказано. □

По индукции предложение 21.4 нетрудно перенести на случай произвольного числа слагаемых:

$$(x_1 + \cdots + x_k)^{p^n} = x_1^{p^n} + \cdots + x_k^{p^n}.$$

Упражнения

1. Доказать, что любое конечное поле имеет положительную характеристику.

2. Существует ли бесконечное поле положительной характеристики?

3. Пусть F — поле и $f \in F[x]$. Доказать, что если характеристика поля F равна нулю, то $f' = 0$ тогда и только тогда, когда f — постоянный многочлен; если же характеристика поля F равна $p > 0$, то $f' = 0$ тогда и только тогда, когда $f(x) = g(x^p)$ для некоторого многочлена $g \in F[x]$.

4. Доказать, что в поле $\mathbb{Z}_p$ выполняются равенства:

а) $\sum_{k=1}^{p-1} k^{-1} = 0 \quad (p > 2)$; б) $\sum_{k=1}^{(p-1)/2} k^{-2} = 0 \quad (p > 3)$.

§22. Степень расширения.

Если поле L содержит поле K, то говорят, что L является расширением поля K. В этом случае L можно рассматривать как векторное пространство над полем K. Действительно, по определению поля L является абелевой группой относительно сложения. Далее, поскольку $K \subset L$, то определено умножение элементов поля K на элементы поля L, которые мы можем рассматривать как "векторы". Фактически, это умножение является умножением элементов поля L. При этом из определения поля вытекают следующие свойства:

$$a(x+y) = ax + ay, \quad (a+b)x = ax + bx, \quad 1x = x, \quad (ab)x = a(bx),$$

для любых элементов $a, b \in K$, $x, y \in L$. Это и означает, что L является векторным пространством над полем K.

Определение 22.1. *Размерность L над K называется* ***степенью расширения*** *L над K и обозначается $[L : K]$. Степень расширения может быть равна бесконечности.*

Если $[L : K] < \infty$, то говорят, что L — конечное расширение поля K, или что L конечно над K.

Теорема 22.2. *Пусть E, F, K — поля и $E \supset F \supset K$. Если $\{x_i\}_{i\in I}$ — базис E над F и $\{y_j\}_{j\in J}$ — базис F над K, то $\{x_i y_j\}_{i\in I, j\in J}$ — базис E над K.*

Доказательство. Вначале докажем, что любой элемент $x \in E$ можно выразить через $x_i y_j$, $i \in I$, $j \in J$, с коэффициентами из поля K. Так как $\{x_i\}_{i\in I}$ — базис E над F, то существуют элементы $\alpha_i \in F$, среди которых лишь конечное число отлично от нуля, такие, что

$$x = \sum_{i\in I} \alpha_i x_i. \tag{22.1}$$

Так как $\{y_j\}_{j\in J}$ — базис F над K, то для каждого ненулевого α_i существуют элементы $\beta_{ij} \in K$, среди которых лишь конечное число отлично от нуля, такие, что

$$\alpha_i = \sum_{j\in J} \beta_{ij} y_j. \tag{22.2}$$

Подставляя (22.2) в (22.1), получаем

$$x = \sum_{i\in I} \alpha_i x_i = \sum_{i\in I} \left(\sum_{j\in J} \beta_{ij} y_j \right) x_i = \sum_{i\in I, j\in J} \beta_{ij} x_i y_j,$$

что и требовалось.

Докажем теперь, что элементы $x_i y_j$, $i \in I$, $j \in J$, линейно независимы над K. Предположим, что существуют элементы $\beta_{ij} \in K$, $i \in I$, $j \in J$, среди которых не все равны нулю и лишь конечное число отлично от нуля, такие, что

$$\sum_{i\in I, j\in J} \beta_{ij} x_i y_j = 0.$$

Тогда

$$\sum_{i\in I} \left(\sum_{j\in J} \beta_{ij} y_j \right) x_i = 0.$$

Поскольку $\alpha_i = \sum_{j\in J} \beta_{ij} y_j \in F$, а элементы $\{x_i\}_{i\in I}$ линейно независимы над F, то

$$\sum_{j\in J} \beta_{ij} y_j = 0, \quad i \in I.$$

Так как $\{y_j\}_{j\in J}$ — базис F над K, то $\beta_{ij} = 0$ для всех $i,\ j$ — противоречие. □

Следствие 22.3 (Мультипликативность степени). *Пусть E, F, K — поля и $E \supset F \supset K$. Расширение E над K конечно тогда и только тогда, когда E конечно над F и F конечно над K. В случае их конечности справедливо соотношение*

$$[E : K] = [E : F][F : K] \tag{22.3}$$

Доказательство. Если E конечно над F и F конечно над K, то из теоремы 22.2 немедленно следует, что E конечно над K.

Если E конечно над K, то и F конечно над K, поскольку является подпространством в E. Далее, если $e_1, \ldots, e_n$ — базис E над K, то тем более элементы $e_1, \ldots, e_n$ порождают E над F (хотя и не обязаны являться базисом E над F). Значит, E конечно над F.

Формула (22.3) непосредственно следует из теоремы 22.2. □

Упражнения

1. Доказать, что если L — расширение поля K и степень $[L : K]$ — простое число, то единственными полями F, удовлетворяющими условию $K \subseteq F \subseteq L$ являются $F = K$ и $F = L$.

§23. Простые подполя.

Пусть P — поле, $K_i \subset P$, $i \in I$, — подполя.

Упражнение 23.1. Доказать, что $K = \cap_{i \in I} K_i$ — подполе в P.

Определение 23.2. *Поле, не обладающее никаким собственным подполем, называется* ***простым****.*

Предложение 23.3. *$\mathbb{Q}$ и $\mathbb{Z}_p$ — простые поля.*

Доказательство. Если $K \subset \mathbb{Q}$ — подполе, то $1 \in K$. Следовательно, $1 + \cdots + 1 = n \in K$ для любого $n \in \mathbb{Z}$, т.е. $\mathbb{Z} \subset K$. Для любых $n, m \in \mathbb{Z}$, $m \neq 0$, дробь $n/m \in K$, поскольку K — поле. Значит, $K = \mathbb{Q}$.

Если $K \subset \mathbb{Z}_p$ — подполе, то $1 \in K$. Следовательно, $n \in K$ для любого $n \in \{0, 1, \ldots, p-1\}$, т.е. $\mathbb{Z}_p \subset K$. Значит, $K = \mathbb{Z}_p$. □

Теорема 23.4. *В любом поле P содержится ровно одно простое подполе P_0. Если* $\operatorname{char} P = 0$*, то P_0 изоморфно $\mathbb{Q}$. Если* $\operatorname{char} P = p$*, то P_0 изоморфно $\mathbb{Z}_p$.*

Доказательство. Допустив существование двух различных простых подполей $P_0, P_1 \subset P$, мы получим, что их пересечение будет полем, отличным от P_0 и P_1. Это, однако, невозможно ввиду их простоты. Значит, простое подполе $P_0 \subset P$ единственно.

Рассмотрим отображение $f : \mathbb{Z} \to P$, определенное правилом $f(n) = n \cdot 1$. Отображение f является гомоморфизмом, а его ядро $\operatorname{Ker} f$ является идеалом в $\mathbb{Z}$. Так как $\mathbb{Z}$ — кольцо главных идеалов, то $\operatorname{Ker} f = m\mathbb{Z}$.

Если $\operatorname{char} P = 0$, то $m = 0$ и f является мономорфизмом. Дроби

$$\frac{s \cdot 1}{t \cdot 1} = (s \cdot 1)(t \cdot 1)^{-1},$$

имеющие смысл в P (поскольку P — поле), образуют поле P_0, изоморфное $\mathbb{Q}$. В силу предложения 23.3 P_0 будет простым подполем в P.

Если $\operatorname{char} P = p$, то $m = p$ и мы имеем по основной теореме о гомоморфизмах для колец, что

$$f(\mathbb{Z}) \simeq \mathbb{Z}/p\mathbb{Z} = \mathbb{Z}_p.$$

В силу предложения 23.3 $P_0 = f(\mathbb{Z})$ — простое подполе в P, изоморфное $\mathbb{Z}_p$. □

Упражнения

1. Доказать, что в поле из p^2 элементов, где p — простое число, имеется единственное собственное подполе.

2. Пусть K — поле из n элементов. Какое простое подполе содержит K и чему равна характеристика K, если: а) $n = 16$; б) $n = 25$; в) $n = 81$.

3. Какое простое подполе содержит следующее поле: а) $\mathbb{R}(x)$; б) $\mathbb{Z}_5(x)$.

§24. Алгебраические расширения полей.

Пусть $E \supset F$ — расширение полей.

Определение 24.1. *Элемент $a \in E$ называется* ***алгебраическим*** *над F, если существует ненулевой многочлен $f(x) \in F[x]$ такой, что $f(a) = 0$. Если такого многочлена не существует, т.е. для любого $f(x) \in F[x]$ имеем $f(a) \neq 0$, то элемент a называется* ***трансцендентным*** *над F.*

Определение 24.2. *Пусть $E \supset F$ — расширение полей и $a \in E$ — алгебраический элемент над F.* ***Минимальным многочленом*** *элемента a называется ненулевой многочлен $f(x) \in F[x]$ наименьшей степени и со старшим коэффициентом 1 такой, что $f(a) = 0$. Степень многочлена $f(x)$ называется* ***степенью*** *элемента a.*

Лемма 24.3. *Минимальный многочлен $f(x)$ элемента $a \in E$ неприводим.*

Доказательство. Допустим, что $f(x) = g(x)h(x)$, где $\deg g(x) < \deg f(x)$, $\deg h(x) < \deg f(x)$. Тогда

$$f(a) = g(a)h(a) = 0$$

и либо $g(a) = 0$, либо $h(a) = 0$ — противоречие с минимальностью $f(x)$. □

Предложение 24.4. *Если $f(x)$ — минимальный многочлен элемента a над полем F и $g(a) = 0$ для некоторого многочлена $g(x) \in F[x]$, то $g(x)$ делится на $f(x)$.*

Доказательство. Разделим $g(x)$ на $f(x)$ с остатком:

$$g(x) = f(x)q(x) + r(x), \qquad \deg r(x) < \deg f(x).$$

Подставив $x = a$, получим $0 = r(a)$, откуда $r(x) = 0$ (иначе мы имели бы противоречие с минимальностью $f(x)$). □

Определение 24.5. *Расширение полей $E \supset F$ называется* ***алгебраическим****, если все элементы из E являются алгебраическими над F.*

Теорема 24.6. *Любое конечное расширение E поля F является алгебраическим над F.*

Доказательство. Пусть $0 \neq a \in E$ и $[E : F] = n$. Тогда элементы $1, a, a^2, \ldots, a^n$ линейно зависимы над F. Значит, существуют элементы $b_0, b_1, \ldots, b_n \in F$, не все равные нулю и такие, что

$$b_0 + b_1 a + \cdots + b_n a^n = 0.$$

Пусть $f(x) = b_0 + b_1 x + \cdots + b_n x^n \in F[x]$. Тогда $f(x) \neq 0$ и $f(a) = 0$. Значит a алгебраичен над F. $\square$

Упражнения

1. Найти минимальные многочлены для элементов:

а) $\sqrt{2}$ над $\mathbb{Q}$; б) $\sqrt[3]{5}$ над $\mathbb{Q}$; в) $2 - 3i$ над $\mathbb{R}$; г) $2 - 3i$ над $\mathbb{C}$ е) $\sqrt{2} + \sqrt{3}$ над $\mathbb{Q}$.

2. Пусть K — расширение поля L, $a \in K$ — трансцендентный над L элемент и $f \in L[x]$. Доказать, что элемент $f(a) \in K$ является трансцендентным над L.

3. Доказать, что следующие числа являются алгебраическими над $\mathbb{Q}$:

а) $\sqrt[3]{1 - \sqrt{2}}$; б) $1 - i\sqrt{3}$; в) $\sqrt[5]{-2 + i\sqrt{2}}$.

§25. Простые расширения полей.

Пусть $E \supset F$ — расширение полей и $a \in E$.

Определение 25.1. *Обозначим через $F(a)$ наименьшее подполе в E, содержащее F и a. Переход от поля F к полю $F(a)$ называется* ***присоединением*** *к F элемента a. Поля вида $F(a)$ называются* ***простыми расширениями*** *поля F.*

Абстрактно, $F(a)$ может быть описано как пересечение всех подполей поля E, содержащих F и a. Следующее предложение дает более конкретное описание $F(a)$.

Предложение 25.2. $F(a) = \left\{ \dfrac{f(a)}{g(a)} \;\middle|\; f, g \in F[x],\ g(a) \neq 0 \right\}$.

Доказательство. Обозначим $K = \left\{ \frac{f(a)}{g(a)} \mid f, g \in F[x],\ g(a) \neq 0 \right\}$.

Следующие равенства показывают, что K — подполе в E.

$$\frac{f(a)}{g(a)} + \frac{f_1(a)}{g_1(a)} = \frac{f(a)g_1(a) + f_1(a)g(a)}{g(a)g_1(a)} \in K,$$

$$\frac{f(a)}{g(a)} \, \frac{f_1(a)}{g_1(a)} = \frac{f(a)f_1(a)}{g(a)g_1(a)} \in K,$$

$$\left(\frac{f(a)}{g(a)}\right)^{-1} = \frac{g(a)}{f(a)} \in K, \text{ если } f(a) \neq 0.$$

Очевидно, $a \in K$, $F \subset K$. Значит, $F(a) \subset K$.

С другой стороны, $a \in F(a)$ по определению. Тогда $f(a) \in F(a)$ для любого многочлена $f(x) \in F[x]$. Поскольку $F(a)$ — поле, то и все дроби $\frac{f(a)}{g(a)}$, где $f, g \in F[x]$, $g(a) \neq 0$, принадлежат $F(a)$. Значит, $K \subset F(a)$. Таким образом, $K = F(a)$. □

Опишем вначале простые расширения поля F в случае, когда a является алгебраическим элементом над F (простые алгебраические расширения).

Теорема 25.3. *Пусть $E \supset F$ — расширение полей и $a \in E$ — алгебраический элемент степени n над F. Тогда*

$$F(a) = \left\{ b_0 + b_1 a + b_2 a^2 + \cdots + b_{n-1} a^{n-1} \mid b_0, b_1, \ldots, b_{n-1} \in F \right\}.$$

Степень $[F(a) : F]$ равна степени минимального многочлена элемента a над F.

Доказательство. Пусть $p(x)$ — минимальный многочлен элемента a над F. Рассмотрим гомоморфизм

$$\psi : F[x] \to E, \qquad h(x) \mapsto h(a).$$

Ядро ψ является идеалом в $F[x]$, а по теореме 14.3 $F[x]$ — кольцо главных идеалов. Поскольку по определению минимального многочлена $p(x)$ — многочлен наименьшей степени, содержащийся в $\ker \psi$, то $\ker \psi = (p(x))$. По основной теореме о гомоморфизмах колец, $\psi(F[x]) \simeq F[x]/(p(x))$. Так как $p(x)$ неприводим, то $(p(x))$ — максимальный идеал по теореме 15.3. Следовательно, по теореме 15.2 $F[x]/(p(x))$ — поле. Очевидно, что $a \in \psi(F[x])$, $F \subset \psi(F[x])$ и

$\psi(F[x]) \subset F(a)$ в силу предложения 25.2. Так как $F(a)$ — наименьшее подполе, содержащее F и a, то

$$\psi(F[x]) = \{f(a) \mid f \in F[x]\} = F(a).$$

Если $f(a) \in F(a)$, то разделив $f(x)$ на $p(x)$ с остатком, получим

$$f(x) = p(x)q(x) + r(x),$$

где $r(x) \in F[x]$ и $\deg r(x) < \deg p(x) = n$. Тогда

$$\psi(f(x)) = f(a) = p(a)q(a) + r(a) = r(a),$$

т.е. любой элемент из $F(a)$ имеет вид $b_0 + b_1 a + b_2 a^2 + \cdots + b_{n-1}a^{n-1}$, где $b_0, b_1, \ldots, b_{n-1} \in F$, что и требовалось.

Итак, мы доказали, что элементы $1, a, a^2, \ldots, a^{n-1}$ порождают $F(a)$ как векторное пространство над F. Докажем, что эти элементы линейно независимы над F. Пусть

$$b_0 + b_1 a + b_2 a^2 + \cdots + b_{n-1}a^{n-1} = 0,$$

где $b_0, b_1, \ldots, b_{n-1} \in F$ и не все из них равны нулю. Тогда $s(a) = 0$, где $0 \neq s(x) = b_0 + b_1 x + b_2 x^2 + \cdots + b_{n-1}x^{n-1} \in F[x]$ и $\deg s(x) < \deg p(x)$ — противоречие с минимальностью $p(x)$. □

Теорема 25.4. *Пусть $E \supset F$ — расширение полей и $a, b \in E$ — алгебраические элементы над F. Тогда для любой дроби $\frac{f(x,y)}{g(x,y)} \in F(x,y)$ такой, что $g(a,b) \neq 0$ элемент $\frac{f(a,b)}{g(a,b)} \in E$ алгебраичен над F. В частности, $a \pm b$, ab, $\frac{a}{b}$ — алгебраические элементы над F.*

Доказательство. Рассмотрим расширения полей $F \subset F(a) \subset F(a)(b)$. Так как b алгебраичен над F, то b алгебраичен над $F(a)$. По теореме 25.3 $F(a)(b)$ конечно над $F(a)$ и $F(a)$ конечно над F. Согласно следствию 22.3 $F(a)(b)$ конечно над F. По теореме 24.6 $F(a)(b)$ алгебраично над F. Следовательно, $\frac{f(a,b)}{g(a,b)} \in F(a)(b)$ — алгебраический элемент над F. □

Рассмотрим теперь случай простого трансцендентного расширения поля K.

Теорема 25.5. *Пусть $E \supset F$ — расширение полей и $a \in E$ —*

трансцендентный элемент над F. Тогда $F(a) \simeq F(x)$, где $F(x)$ — поле рациональных функций от одной переменной над F.

Доказательство. Рассмотрим отображение

$$\psi : F(x) \to F(a), \qquad \frac{f(x)}{g(x)} \mapsto \frac{f(a)}{g(a)}.$$

Проверим корректность определения ψ. Так как a — трансцендентный элемент над F и $g(x) \neq 0$, то $g(a) \neq 0$ и можно вычислить элемент $\frac{f(a)}{g(a)} \in F(a)$.

Если $\frac{f(x)}{g(x)} = \frac{f_1(x)}{g_1(x)}$, то $f(x)g_1(x) = f_1(x)g(x)$. Тогда $f(a)g_1(a) = f_1(a)g(a)$. В силу трансцендентности a имеем $g(a) \neq 0$, $g_1(a) \neq 0$, следовательно $\frac{f(a)}{g(a)} = \frac{f_1(a)}{g_1(a)}$.

Легко проверить, что ψ является гомоморфизмом. Очевидно, ψ — биекция. □

Упражнения

1. Пусть L/K — алгебраическое расширение. Доказать, что расширение $L(x)/K(x)$ также алгебраическое и $[L(x) : K(x)] = [L : K]$.

2. Пусть L/K и K/F — алгебраические расширения. Доказать, что расширение L/F также алгебраическое.

3. Какой вид имеют элементы простых расширений:

а) $\mathbb{Q}(\pi)$; б) $\mathbb{Q}(e^2)$; в) $\mathbb{Q}(\sqrt[3]{2})$; г) $\mathbb{Q}(e^{\frac{2\pi i}{3}})$; д) $\mathbb{Q}(e^{\frac{2\pi i}{5}})$; е) $\mathbb{R}(1 + \sqrt{2}i)$.

4. Докажите, что:

а) $\mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2} - \sqrt{3})$;

б) $\mathbb{Q}(\sqrt{p}\,, \sqrt{q}) = \mathbb{Q}(\sqrt{p}+\sqrt{q})$, где p, q — различные простые числа.

5. Докажите, что поля $\mathbb{Q}(\sqrt{p})$ и $\mathbb{Q}(\sqrt{q})$, где p, q — различные простые числа, неизоморфны.

6. Найдите все автоморфизмы полей $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt[3]{2})$.

7. Доказать, что расширение L/K является конечным тогда и только тогда, когда L может быть получено из K присоединением конечного числа алгебраических над K элементов.

§26. Алгебраически замкнутые поля.

Определение 26.1. *Поле K называется* ***алгебраически замкнутым****, если любой отличный от константы многочлен из $K[x]$ обладает в K хоть одним корнем.*

"Основная теорема алгебры"утверждает, что поле $\mathbb{C}$ алгебраически замкнуто. Следующая теорема показывает, что существуют и другие алгебраически замкнутые поля.

Теорема 26.2 (Штейница). *Для каждого поля K существует алгебраически замкнутое алгебраическое расширение $\overline{K}$. С точностью до изоморфизма, тождественного на поле K, поле $\overline{K}$ определено однозначно.*

Доказательство теоремы Штейница выходит за рамки нашего курса, его можно найти в [9, гл. VII, §2].

Поле $\overline{K}$ называется **алгебраическим замыканием** поля K.

Предложение 26.3. *Если $E \supset F$ — алгебраическое расширение полей, то алгебраическое замыкание $\overline{E}$ поля E является также алгебраическим замыканием поля F.*

Доказательство. Достаточно доказать, что любой элемент $a \in \overline{E}$ алгебраичен над F. Элемент a алгебраичен над E. Пусть $f(x) = b_0 + b_1x + \cdots + b_nx^n \in E[x]$ — минимальный многочлен a. Рассмотрим поле $F_1 = F(b_0, b_1, \ldots, b_n)$, которое получается последовательным присоединением к F элементов $b_0, b_1, \ldots, b_n$. На каждом шаге мы имеем простое алебраическое расширение, которое является конечным расширением по теореме 25.3. В силу мультипликативности степени $[F_1 : F] < \infty$. Поскольку элемент a алгебраичен над F_1 (коэффициенты минимального многочлена $f(x)$ принадлежат F_1), то $F_1(a)$ — конечное расширение F_1. В силу мультипликативности степени $F_1(a)$ — конечное расширение F. Следовательно, $F_1(a)$ — алгебраическое расширение F и элемент a алгебраичен над F. □

§27. Конечные поля.

Ранее мы уже встретились с важным классом конечных полей, т. е. полей, состоящих из конечного числа элементов. А именно, было установлено, что для каждого простого числа p кольцо $\mathbb{Z}_p$ является конечным полем, состоящим из p элементов.

Поле $\mathbb{Z}_p$ играет важную роль в общей теории полей, так как, согласно теореме 23.4, каждое поле характеристики p должно содержать изоморфное $\mathbb{Z}_p$ подполе и потому может рассматриваться как расширение поля $\mathbb{Z}_p$. Это замечание играет основную роль в классификации конечных полей, поскольку характеристика каждого конечного поля является простым числом.

Установим прежде всего одно простое предложение о числе элементов конечного поля.

Предложение 27.1. *Пусть F — конечное поле, содержащее подполе K из q элементов. Тогда F состоит из q^m элементов, где $m = [F : K]$.*

Доказательство. Поле F можно рассматривать как векторное пространство над полем K. В силу конечности F это пространство конечномерно. Если $[F : K] = m$, то F имеет базис над полем K, состоящий из m элементов, скажем, $b_1, \ldots, b_m$. Таким образом, каждый элемент поля F может быть однозначно представлен в виде линейной комбинации $a_1b_1 + a_mb_m$, где $a_1, \ldots, a_m \in K$. Так как каждый коэффициент a_i может принимать q значений, то поле F состоит в точности из q^m элементов. □

Теорема 27.2. *Пусть F — конечное поле. Тогда оно состоит из p^n элементов, где простое число p является характеристикой поля F, а натуральное число n является степенью поля F над его простым подполем $\mathbb{Z}_p$.*

Доказательство. Так как поле F конечно, то его характеристика — некоторое простое число p. Поэтому простое подполе K поля F

изоморфно Z_p и, значит, содержит p элементов. Остальное вытекает из предложения 27.1. □

Чтобы установить, что для каждого простого p и каждого натурального n существует конечное поле из p^n элементов, мы используем подход, подсказываемый следующей леммой.

Лемма 27.3. *Если F — конечное поле из q элементов, то каждый элемент $a \in F$ удовлетворяет равенству $a^q = a$. Другими словами, все элементы поля F являются корнями многочлена $x^q - x \in \mathbb{F}_p[x]$.*

Доказательство. Для $a = 0$ равенство $a^q = a$ выполняется тривиально. Что же касается ненулевых элементов поля F, то они образуют мультипликативную группу F^* порядка $q - 1$, так что для каждого ненулевого элемента $a \in F$ по следствию из теоремы Лагранжа выполняется равенство $a^{q-1} = 1$, умножение которого на a приводит к требуемому результату. □

Теперь мы в состоянии доказать главную характеризационную теорему для конечных полей.

Теорема 27.4 (О существовании и единственности конечных полей). *Для каждого простого числа p и каждого натурального числа n с точностью до изоморфизма существует единственное конечное поле из p^n элементов.*

Доказательство. Существование. Для $q = p^n$ рассмотрим многочлен $x^q - x \in \mathbb{F}_p[x]$, и пусть $\overline{\mathbb{F}_p}$ — алгебраическое замыкание поля $\mathbb{F}_p$. Многочлен $x^q - x$ не имеет кратных корней в поле $\overline{\mathbb{F}_p}$, так как его производная является постоянным многочленом:

$$(x^q - x)' = qx^{q-1} - 1 = -1 \neq 0,$$

и в силу этого не может иметь общих корней с $x^q - x$. Поэтому многочлен $x^q - x$ имеет q различных корней в поле $\overline{\mathbb{F}_p}$. Пусть

$$F = \left\{ a \in \overline{\mathbb{F}_p} \mid a^q - a = 0 \right\}.$$

Докажем, что F является подполем поля $\overline{\mathbb{F}_p}$. Если $a, b \in F$, то,

используя предложение 21.4, получаем

$$(a+b)^q = a^q + b^q = a + b, \qquad (ab)^q = a^q b^q = ab,$$
$$(a^{-1})^q = (a^q)^{-1} = a^{-1} \text{ при } a \neq 0,$$

откуда $a+b,\ ab,\ a^{-1} \in F$. Далее, если $p = 2$, то $-1 = 1$ и $(-a)^q = a^q = a = -a$. Если же $p > 2$, то $(-a)^q = -a^q = -a$. В обоих случаях получаем, что $-a \in F$.

Итак, F — конечное поле из q элементов.

Единственность. Пусть F_1, F_2 — конечные поля из $q = p^n$ элементов. Тогда $\operatorname{char} F_1 = \operatorname{char} F_2 = p$ и потому $\mathbb{F}_p$ — простое подполе в F_1 и F_2. Пусть $\overline{F_1}$ и $\overline{F_2}$ — алгебраические замыкания полей F_1 и F_2. По предложению 26.3 $\overline{F_1}$ и $\overline{F_2}$ — алгебраические замыкания поля $\mathbb{F}_p$, а поэтому изоморфны. Пусть $\alpha : \overline{F_1} \to \overline{F_2}$ — изоморфизм.

Выше мы доказали, что поле F_1 совпадает с множеством корней многочлена $x^q - x$ в поле $\overline{F_1}$, а поле F_2 совпадает с множеством корней многочлена $x^q - x$ в поле $\overline{F_2}$. Если $a \in F_1$, то $a^q - a = 0$. Применяя к обеим частям этого равенства изоморфизм α, получим $\alpha(a)^q - \alpha(a) = 0$, откуда $\alpha(a) \in F_2$. Значит, $\alpha(F_1) \subset F_2$. Так как порядки F_1 и F_2 совпадают и α инъективно, то $\alpha(F_1) = F_2$. Таким образом, ограничение α на F_1 является изоморфизмом полей F_1 и F_2. □

Доказанная в теореме 27.4 единственность позволяет говорить о вполне определенном конечном поле данного порядка q. Будем обозначать его через $\mathbb{F}_q$, где под q понимается степень некоторого простого числа p, которое и является характеристикой этого поля.

Теорема 27.5 (Критерий подполя конечного поля). *Пусть $\mathbb{F}_q$ — конечное поле из $q = p^n$ элементов (p — простое число). Тогда каждое подполе L поля $\mathbb{F}_q$ имеет порядок p^m, где m является делителем числа n. Обратно, если m — делитель числа n, то существует ровно одно подполе L поля $\mathbb{F}_q$, состоящее из p^m элементов. При этом степень $[\mathbb{F}_q : L] = \frac{n}{m}$.*

Доказательство. Ясно, что любое подполе L поля $\mathbb{F}_q$ должно иметь порядок p^m, где m — натуральное число, не превосходящее n.

Из предложения 27.1 следует, что число $q = p^n$ должно быть степенью числа p^m, так что m обязательно делит число n.

Пусть $\overline{\mathbb{F}_p}$ — алгебраическое замыкание поля $\mathbb{F}_p$. Тогда поле $\mathbb{F}_q$ совпадает с множеством корней многочлена $x^q - x$ в поле $\overline{\mathbb{F}_p}$. Если m — делитель числа n, т.е. $n = md$, то

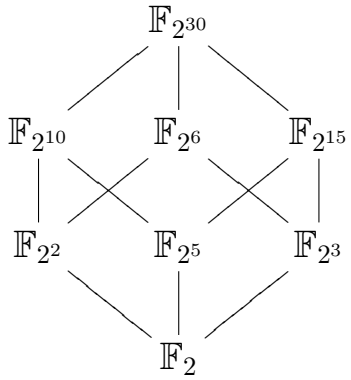
$$p^n - 1 = p^{md} - 1 = (p^m - 1)((p^m)^{d-1} + (p^m)^{d-2} + \cdots + 1),$$

откуда $p^m - 1$ делит число $p^n - 1$. Следовательно, многочлен $x^{p^m-1} - 1$ делит многочлен $x^{p^n-1} - 1 = x^{q-1} - 1$ в $\mathbb{F}_p[x]$. Значит, $x^{p^m} - x$ делит многочлен $x^q - x$ в $\mathbb{F}_p[x]$. Таким образом, каждый корень многочлена $x^{p^m} - x$ является корнем многочлена $x^q - x$ и, значит, принадлежит полю $\mathbb{F}_q$. Поэтому $\mathbb{F}_q$ должно содержать все корни многочлена $x^{p^m} - x$, а множество этих корней образует поле $\mathbb{F}_{p^m}$ порядка p^m.

Если бы поле $\mathbb{F}_q$ содержало два различных подполя порядка p^m, то эти подполя содержали бы в совокупности больше чем p^m корней многочлена $x^{p^m} - x$ в поле F_q, а это невозможно.

Далее, так как $\mathbb{F}_q \supset L$, то по предложению 27.1 $q = p^n = (p^m)^d$, где $d = [\mathbb{F}_q : L]$. Следовательно, $d = \frac{n}{m}$. □

Пример. Подполя конечного поля $\mathbb{F}_{2^{30}}$ можно найти, составив список всех положительных делителей числа 30. Отношения включения между этими подполями указаны в следующей диаграмме.



Согласно теореме 27.5, эти отношения включения равносильны отношениям делимости соответствующих делителей числа 30.

Теорема 27.6. *Любое конечное поле $\mathbb{F}_{p^n}$ имеет в точности одно расширение $L \supset \mathbb{F}_{p^n}$ степени $[L : \mathbb{F}_{p^n}] = m$ для каждого $m \geq 1$.*

Доказательство. Докажем, что расширение L существует. Пусть $L = \mathbb{F}_{p^{nm}}$. По теореме 27.5 поле L содержит единственное подполе $\mathbb{F}_{p^n}$ и степень $[\mathbb{F}_{p^{nm}} : \mathbb{F}_{p^n}] = m$. Если L_1 — другое расширение со свойством $[L_1 : \mathbb{F}_{p^n}] = m$, то число элементов в L_1 по предложению 27.1 равно $(p^n)^m = p^{nm}$. В силу единственности поля из p^{nm} элементов, поля L и L_1 изоморфны. □

Замечание. Теорему 27.6 нельзя перенести на поля нулевой характеристики. Например, если p и q — различные простые числа, то поля $\mathbb{Q}(\sqrt{p})$ и $\mathbb{Q}(\sqrt{q})$ не изоморфны (см. упражнение 5 из § 26) и имеют степень два над $\mathbb{Q}$. Таким образом, $\mathbb{Q}$ имеет бесконечно много неизоморфных расширений степени 2.

Следующий результат устанавливает одно важное свойство мультипликативной группы конечного поля.

Теорема 27.7 (О конечной мультипликативной подгруппе в поле). *Пусть K — произвольное поле, G — конечная подгруппа в K^*. Тогда G — циклическая группа. В частности, группа $\mathbb{F}_q^*$ — циклическая.*

Доказательство. Пусть n — порядок группы G и $n = p_1^{m_1} \cdots p_s^{m_s}$ — каноническое разложение n на простые множители. По основной теореме о строении конечных абелевых групп G является прямым произведением p_i-примарных циклических групп. Объединяя в один множитель примарные циклические группы, соответствующие одному простому p, получим, что

$$G = H_1 \times \cdots \times H_s,$$

где $H_i = C_{p_i^{a_1}} \times \cdots \times C_{p_i^{a_{r_i}}}$ — прямое произведение циклических p_i-групп $C_{p_i^{a_m}}$ порядка $p_i^{a_m}$. Покажем, что все $r_i = 1$, $i = 1, \ldots, s$. Предположим противное, пусть некоторое $r_i > 1$. Тогда без ограничения общности можно считать, что $p_i^{a_1} \geq p_i^{a_2} > 1$. Для любого элемента $a \in C_{p_i^{a_1}}$ по следствию из теоремы Лагранжа $a^{p_i^{a_1}} = 1$. Аналогично, для любого элемента $b \in C_{p_i^{a_2}}$ имеем $b^{p_i^{a_2}} = 1$, откуда

$$b^{p_i^{a_1}} = (b^{p_i^{a_2}})^{p_i^{a_1 - a_2}} = 1^{p_i^{a_1 - a_2}} = 1.$$

Значит все элементы групп $C_{p_i^{a_1}}$ и $C_{p_i^{a_2}}$ являются корнями многочлена $x^{p^{a_1}} - 1$. Но поскольку группа H_i — прямое произведение групп $C_{p_i^{a_m}}$, то $C_{p_i^{a_1}} \cap C_{p_i^{a_2}} = \{1\}$. Следовательно, суммарное количество элементов в этих двух группах равно

$$p_1^{a_1} + p_1^{a_2} - 1 > p_1^{a_1} = deg(x^{p^{a_1}} - 1).$$

Значит, многочлен $x^{p^{a_1}} - 1$ имеет в поле K корней больше, чем его степень, — противоречие.

Итак, $G = H_1 \times \cdots \times H_s$, где H_i — циклическая группа порядка $p_i^{m_i}$, $i = 1, \ldots, s$. По пункту 1 теоремы 9.9 циклическая группа $\mathbb{Z}_n$ изоморфна прямому произведению $H_1 \times \cdots \times H_s = G$. Значит, $G \simeq \mathbb{Z}_n$ и G — циклическая группа. □

Определение 27.8. *Образующий элемент циклической группы $\mathbb{F}_q^*$ называется примитивным элементом поля $\mathbb{F}_q$.*

Из теоремы 27.7 следует, что поле $\mathbb{F}_q$ содержит $\varphi(q-1)$ примитивных элементов, где φ — функция Эйлера. Наличием в любом конечном поле примитивных элементов можно воспользоваться, например, для доказательства того факта, что каждое конечное поле является простым алгебраическим расширением своего простого подполя.

Теорема 27.9. *Пусть $\mathbb{F}_q$ — конечное поле и $\mathbb{F}_r$ — его конечное расширение. Тогда $\mathbb{F}_r = \mathbb{F}_q(a)$, где a — любой примитивный элемент поля $\mathbb{F}_r$.*

Доказательство. Поле $\mathbb{F}_q(a)$ содержит 0 и все степени элемента a, а значит, все элементы поля $\mathbb{F}_r$. Следовательно, $\mathbb{F}_q(a) = \mathbb{F}_r$. □

Следствие 27.10. *Для каждого конечного поля $\mathbb{F}_q$ и каждого натурального числа n в кольце $\mathbb{F}_q[x]$ существует неприводимый многочлен степени n.*

Доказательство. Пусть $\mathbb{F}_r$ — расширение поля $\mathbb{F}_q$ порядка q^n, так что $[\mathbb{F}_r : \mathbb{F}_q] = n$. Согласно теореме 27.9, существует такой элемент $a \in \mathbb{F}_r$, что $\mathbb{F}_r = \mathbb{F}_q(a)$. Но тогда минимальный многочлен элемента a над $\mathbb{F}_q$ является неприводимым многочленом степени n в кольце $\mathbb{F}_q[x]$. □

Упражнения

1. Доказать неприводимость над $\mathbb{F}_2$ многочлена $f(x) = x^3+x+1 \in \mathbb{F}_2[x]$ и построить таблицы сложения и умножения для поля $\mathbb{F}_2(a)$, где a — корень многочлена f. Сколько элементов содержит поле $\mathbb{F}_2(a)$?

2. Доказать, что для каждого конечного поля, за исключением $\mathbb{F}_2$, сумма всех его элементов равна нулю.

3. Пусть a, b — элементы поля $\mathbb{F}_{2^n}$, где n — нечетно. Доказать, что из равенства $a^2 + ab + b^2 = 0$ вытекает $a = b = 0$.

4. Доказать, что отображение $f : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$, $f(x) = x^p$, является автоморфизмом поля $\mathbb{F}_{p^n}$.

5. Пусть F — поле. Доказать, что если его мультипликативная группа F^* циклическая, то F — конечное поле.

6. Найти все примитивные элементы полей $\mathbb{F}_7$, $\mathbb{F}_{17}$.

7. Доказать, что любой элемент поля $\mathbb{F}_{p^n}$ имеет в этом поле ровно один корень степени p.

8. Доказать, что для $f \in \mathbb{F}_q[x]$ верно равенство $(f(x))^q = f(x^q)$.

9. Доказать, что любой квадратный многочлен из $\mathbb{F}_q[x]$ разлагается над полем $\mathbb{F}_{q^2}$ на линейные множители.

10. Пусть $\mathbb{F}_q$ — конечное поле характеристики p. Доказать, что многочлен $f \in \mathbb{F}_q[x]$ обладает свойством $f'(x) = 0$ тогда и только тогда, когда f является p-й степенью некоторого многочлена из $\mathbb{F}_q[x]$.

11. Пусть F — некоторое поле и отображение $h : F \to F$ определяется условием $h(a) = a^{-1}$, если $a \neq 0$, и $h(0) = 0$. Доказать, что h является автоморфизмом поля F тогда и только тогда, когда F состоит не более чем из четырех элементов.

Литература

1. *Атья, М.* Введение в коммутативную алгебру. /М. Атья, И. Макдональд/ М. : Мир, 1972.

2. *Богопольский, О.В.* Введение в теорию групп. /О.В. Богопольский/ М.-Ижевск : Институт компьютерных исследований, 2002.

3. *Ван дер Варден, Б.Л.* Алгебра. /Б.Л. Ван дер Варден/ М. : Наука, 1979.

4. *Винберг, Э.Б.* Курс алгебры. /Э.Б. Винберг/ М. : Факториал Пресс, 2001.

5. *Зарисский, О.* Коммутативная алгебра. /О. Зарисский, П. Самюэль/ М. : Изд-во иностранной литературы, 1963. Т.1.

6. *Каргаполов, М.И.* Основы теории групп. /М.И. Каргаполов, Ю.И. Мерзляков/ М. : Наука, 1972.

7. *Кострикин, А.И.* Введение в алгебру. Ч.1. Основы алгебры. /А.И. Кострикин/ М. : Физико-математическая литература, 2000.

8. *Кострикин, А.И.* Введение в алгебру. Ч.3. Основные структуры. /А.И. Кострикин/ М. : Физико-математическая литература, 2001.

9. *Курош, А.Г.* Курс высшей алгебры. /А.Г. Курош/ М. : Наука, 1968.

10. *Ленг, С.* Алгебра. /С. Ленг/ М. : Мир, 1968.

11. *Лидл, Р.* Конечные поля. /Р. Лидл, Г. Нидеррайтер/ М. : Мир, 1988.

12. *Милованов, М. В.* Алгебра и аналитическая геометрия. /М.В. Милованов, Р.И. Тышкевич, А.С. Феденко/ Минск : Амалфея, 2001. Т.1.

13. *Фаддеев, Д.К.* Лекции по алгебре. /Д.К. Фаддеев/ М. : Наука, 1984.

Предметный указатель

Содержание