ГРУППЫ, КОЛЬЦА, ПОЛЯ

Группы, кольца, поля: Методические указания по дисциплине “Геометрия и алгебра” / И. Г. Зельвенский; СПбГЭТУ.

In Galois fields, full of flowers
primitive elements dance for hours
climbing sequentially through the trees
and shouting occasional parities . . .
S. B. Weinstein “In Galois Fields”

В отличие от других математических дисциплин, алгебра (за исключением ее “классической” части – теории уравнений в полях вещественных и комплексных чисел) приобрела черты прикладной науки лишь во 2-й половине XX в. Идеи и методы современной алгебры уже нашли широкое применение в таких областях, как теория автоматов и вычислительных машин, передача сообщений и кодирование, языки программирования. В методических указаниях рассмотрены базовые понятия теории групп (§ 1–7), коммутативных колец и полей (§ 8–14), необходимые студентам ФАВТ, РТФ и других факультетов ЭТУ.

Упражнения, приведенные в конце параграфов, или иллюстрируют изложенный материал, или предлагают доказать результаты, примыкающие к основному тексту. Теоремы и леммы, доказательство которых оставлено для самостоятельной работы, отмечены знаком $\Diamond$. Список использованной литературы помещен в конце. Он может также служить ориентиром при углубленном изучении рассмотренных тем.

Содержание

§ 1. Прямое произведение множеств. Отображения

Определение. Пусть A_1, A_2, ... , A_n – одинаковые или различные, конечные или бесконечные множества. *Прямым произведением* этих множеств $A_1 \times A_2 \times \cdots \times A_n$ называется множество, состоящее из всевозможных элементов вида $(a_1, a_2, \ldots, a_n)$, где $a_1 \in A_1$, $a_2 \in A_2$, ... , $a_n \in A_n$.

Примеры.

1. Пусть $\mathbb{R}$ – множество всех вещественных (действительных) чисел. Тогда $\mathbb{R}^3 = \mathbb{R} \times \mathbb{R} \times \mathbb{R}$ есть множество, состоящее из троек чисел (a_1, a_2, a_3). Элементы этого прямого произведения можно отождествить с точками трехмерного пространства, заданными своими координатами.

2. Каждое не более чем n-значное целое неотрицательное число в десятичной системе счисления можно рассматривать как элемент прямого произведения n одинаковых множеств, состоящих из цифр $0, 1, \ldots, 9$ (при этом, если число фактически имеет менее n знаков, соответствующие разряды заполняются нулями).

3. Каждое отличное от нуля комплексное число может быть однозначно записано в показательной форме $re^{\varphi i}$, где $r > 0$ и $-\pi < \varphi \leqslant \pi$. Поэтому ненулевые комплексные числа являются элементами прямого произведения $A_1 \times A_2$, где $A_1 = (0, +\infty)$, а $A_2 = (-\pi, \pi]$.

Операция $\times$ не является ни коммутативной (так как $A_1 \times A_2 \neq A_2 \times A_1$ при $A_1 \neq A_2$), ни ассоциативной $\big(A_1 \times (A_2 \times A_3) \neq (A_1 \times A_2) \times A_3\big)$, однако с операциями объединения и пересечения множеств она связана привычными дистрибутивными (распределительными) законами:

$$A \times (B_1 \cup B_2) = (A \times B_1) \cup (A \times B_2), \quad A \times (B_1 \cap B_2) = (A \times B_1) \cap (A \times B_2).$$

Лемма. Для каждого $i = 1, 2, \ldots, n$ обозначим через m_i количество элементов конечного множества A_i. Тогда множество $A_1 \times A_2 \times \cdots \times A_n$ содержит $m_1 m_2 \ldots m_n$ элементов. $\Diamond$

На языке прямых произведений можно определить некоторые основные математические понятия: отображения, отношения, операции.

Определение. Пусть в прямом произведении двух множеств $A \times B$ задано подмножество F со следующим условием: для каждого $a \in A$ существует только одно $b \in B$ такое, что пара $(a, b) \in F$. Тогда мы говорим, что задано *отображение* F множества A в множество B $(F : A \to B)$, и обозначаем через $F(a)$ тот (единственный) элемент, принадлежащий B, для которого $(a, F(a)) \in F$.

Отображение $F : A \to B$ называется *инъективным*, если $F(a_1) \neq F(a_2)$ для любой пары различных элементов a_1 и a_2 множества A. Примером инъективного отображения является естественное вложение множества A в объединение $A \cup C$. Отображение $F : A \to B$ называется *сюръективным* (*"отображением на"*), если

для любого элемента $b \in B$ найдется элемент $a \in A$ такой, что $b = F(a)$. Пример подобного отображения дает проекция $P : A_1 \times A_2 \to A_1$, определяемая равенством $P(a_1, a_2) = a_1$. Отображение, являющееся одновременно инъективным и сюръективным, называется *биективным*. Примерами могут служить естественные биекции $A_1 \times A_2 \to A_2 \times A_1$ и $A_1 \times (A_2 \times A_3) \to A_1 \times A_2 \times A_3$. Для любого биективного отображения очевидным образом определяется обратное отображение.

Определение. Пусть F – отображение множества A в множество B, $C \subset A$ и $D \subset B$. *Образом* $F(C)$ множества C называется часть множества B, образованная элементами y, для каждого из которых найдется $x \in C$ такое, что $y = F(x)$. *Полным прообразом* $F^{-1}(D)$ множества D называется часть множества A, образованная теми элементами x, для которых $F(x) \in D$.

§ 2. Отношения эквивалентности. Фактормножества

Определение. Пусть задано подмножество T "квадрата" $A \times A$, где A – произвольное множество. Будем говорить, что элементы a и b из A находятся в *отношении* T (запись: aTb), если пара (a, b) из $A \times A$ содержится в T. Отношение T на множестве A называется *рефлексивным*, если aTa для любого $a \in A$. Отношение T *симметрично*, если из aTb следует bTa для всех a и b. И наконец, отношение T называется *транзитивным*, если всегда из aTb и bTc следует aTc. Отношение, обладающее одновременно этими тремя свойствами, называется *отношением эквивалентности*.

Примеры.

1. На множестве $\mathbb{R}$ вещественных чисел отношение $\leqslant$ является рефлексивным и транзитивным, но не симметричным.

2. Отношение T, определяемое условием "aTb, если $ab \neq 0$", симметрично и транзитивно, но не рефлексивно, поскольку $0T0$ неверно.

3. Отношение равенства является отношением эквивалентности. Также отношением эквивалентности является отношение подобия на множестве всех треугольников.

Определение. Пусть T – отношение эквивалентности на множестве A, a – некоторый элемент A. Обозначим через K_a подмножество множества A, состоящее из всех $x \in A$, для которых xTa. Подмножество K_a называется *классом эквивалентности* отношения T, а элемент a – *представителем* этого класса.

Теорема 1. Пусть T – отношение эквивалентности на множестве A. Если aTb, то классы эквивалентности K_a и K_b совпадают, в противном случае они не пересекаются.

Доказательство. Пусть x – произвольный элемент класса K_a. Это означает, что xTa. Кроме того aTb, откуда по транзитивности получаем xTb, т. е. $x \in K_b$. Следовательно, $K_a \subset K_b$. Аналогично получается, что $K_b \subset K_a$, поэтому K_a и K_b совпадают. Предположим теперь, что пересечение $K_a \cap K_b$ не пусто и $c \in K_a \cap K_b$. Тогда cTa и cTb, откуда в силу симметричности и транзитивности отношения эквивалентности aTb и, значит, $K_a = K_b$. Теорема доказана.

Следствие. Множество A с отношением эквивалентности T является объединением непересекающихся классов эквивалентности (иначе говоря, классы эквивалентности отношения T образуют *разбиение* множества A).

Для доказательства следствия достаточно заметить, что для любого $a \in A$ имеем aTa, т. е. $a \in K_a$, и поэтому каждое a принадлежит одному (и только одному) классу эквивалентности.

Определение. Множество всех различных классов эквивалентности, отвечающих отношению эквивалентности T на множестве A, называется *фактормножеством* множества A по отношению эквивалентности T (запись: $A\backslash T$).

Примеры.

4. Пусть $\mathbb{C}$ – множество комплексных чисел, а отношение T определяется условием: "aTb, если $|a| = |b|$". T – отношение эквивалентности. Классы K_a – множества комплексных чисел, имеющих одинаковый модуль (на плоскости это концентрические окружности), а фактормножество $\mathbb{C}\backslash T$ – множество всех окружностей с центром в начале координат, включая "окружность нулевого радиуса", т. е. класс, содержащий только начало координат. Ясно, что это фактормножество находится в биективном соответствии с неотрицательными вещественными числами (всеми возможными модулями комплексных чисел).

5. Рассмотрим множество $\mathbb{Z}$ всех целых чисел, зафиксируем положительное число $n \in \mathbb{Z}$ и введем на $\mathbb{Z}$ отношение сравнения $a \equiv b \pmod{n}$ (читается: a сравнимо с b по модулю n), если $a-b$ делится (нацело) на n. Множество $\mathbb{Z}$ оказывается, таким образом, разбитым на классы эквивалентности K_0, K_1, ... , K_{n-1}, причем каждый класс K_j состоит из целых чисел, дающих остаток j $(0 \leqslant j \leqslant n-1)$ при делении на n. Классы K_j называются *классами вычетов по модулю* n и образуют фактормножество, обозначаемое в дальнейшем $\mathbb{Z}_n$.

Теорема 2. Пусть F – отображение множества A в множество B. Тогда отношение T, заданное на множестве A условием "aTb означает, что $F(a) = F(b)$", является отношением эквивалентности. Обратно, если T – отношение эквивалентности на множестве A, то существует сюръективное отображение F множества A на некоторое множество B, для которого равенство $F(a) = F(b)$ равносильно отношению aTb. $\Diamond$

Теорема 3. Пусть F – отображение множества A в множество B. Тогда образ отображения F находится в биективном соответствии с фактормножеством $A\backslash T$, где T – отношение эквивалентности, определяемое условием "aTb означает, что $F(a) = F(b)$". $\Diamond$

Упражнения.

1. Докажите, что отношение T, определяемое условием "aTb, если $ab \geqslant 0$", рефлексивно и симметрично, но не транзитивно.

2. Приведите примеры отношений на множестве вещественных чисел $\mathbb{R}$, которые удовлетворяли бы только одному из трех основных свойств отношений.

§ 3. Бинарные операции. Группы

Определение. Пусть A – произвольное множество. Отображение прямого произведения $A \times A$ в множество A называется *бинарной операцией* на множестве A.

Название "бинарная" связано с тем, что операция определена на прямом произведении двух множеств. Результат отображения $A \times A$ в A мы будем обычно (но не обязательно) записывать как умножение или сложение, т. е. будем писать: $c = a \cdot b$ или $c = a + b$, где $a, b, c \in A$.

Примеры.

1. На множестве положительных рациональных чисел бинарными операциями являются сложение, умножение и деление (но не вычитание!).

2. Пусть Ω – некоторое множество, а M – множество всевозможных его подмножеств (включая пустое множество $\varnothing$). Тогда объединение $\cup$ и пересечение $\cap$ – это бинарные операции на множестве M.

Если в каком-нибудь множестве с операцией $\cdot$ взять три произвольных элемента a, b, c, то "произведения" $(a \cdot b) \cdot c$ и $a \cdot (b \cdot c)$ могут оказаться различными (достаточно рассмотреть деление чисел или векторное произведение векторов).

Определение. Операция $\cdot$ на множестве M называется *ассоциативной*, если $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ для любых a, b, c из M.

В множестве с ассоциативной операцией скобки можно расставлять произвольно в случае любого числа сомножителей, поэтому выражение вида $(a \cdot (b \cdot c)) \cdot d$

можно записывать просто $a \cdot b \cdot c \cdot d$ или даже еще короче $abcd$, снимая знак бинарной операции.

Определение. Операция $\cdot$ на множестве M называется *коммутативной*, если $a \cdot b = b \cdot a$ для любых $a, b \in M$.

Определение. Элемент e из множества M с операцией $\cdot$ называется *нейтральным*, если $e \cdot a = a \cdot e = a$ для любого $a \in M$.

Нейтральный элемент называется также *единицей*, если операция записывается как умножение, и *нулем*, если операция записывается как сложение (заметим, что под сложением всегда понимается коммутативная бинарная операция). В примере 2 само множество Ω является нейтральным элементом относительно операции пересечения ($A \cap \Omega = \Omega \cap A = A$, так как $A \subset \Omega$). Соответственно, для операции объединения нейтральным элементом является пустое множество.

Определение. Множество G с бинарной операцией $\cdot$ называется *группой*:

1) если операция $\cdot$ ассоциативна;

2) в G существует нейтральный элемент e;

3) для любого $a \in G$ существует *обратный* элемент, т. е. такой элемент $a' \in G$, что $a' \cdot a = a \cdot a' = e$.

Если, кроме того, операция $\cdot$ коммутативна, то группа G называется *коммутативной*, или *абелевой* (в честь норвежского математика Н. Х. Абеля).

Теорема. Пусть G – группа с нейтральным элементом e. Тогда e – единственный нейтральный элемент в группе. Кроме того, любой элемент группы G обладает единственным обратным элементом.

Доказательство. Предположим, что какой-то элемент c также является нейтральным элементом группы G. Тогда $c = ce = e$. Если же a' и b – два обратных элемента для $a \in G$, то имеем $b = be = b(aa') = (ba)a' = ea' = a'$, что и требовалось доказать.

В дальнейшем в группе с операцией "умножения" обратный к a элемент будем обозначать a^{-1}.

Примеры.

3. Множество целых чисел образует абелеву группу относительно сложения, нейтральным элементом здесь является нуль. "Обратный" элемент для числа n – это противоположное число "$-n$". То же верно для множества четных чисел, для множеств рациональных, вещественных, комплексных чисел.

4. Множества положительных и всех ненулевых рациональных чисел являются абелевыми группами относительно умножения (нуль, естественно, не имеет обратного элемента). Нейтральный элемент в этих группах – это число 1.

5. Множество из четырех комплексных чисел $\{1, -1, i, -i\}$ – абелева группа относительно умножения.

6. Множество квадратных невырожденных (т. е. имеющих ненулевой определитель) матриц одного порядка с вещественными элементами образует группу относительно умножения. Эта группа коммутативной уже не является.

Упражнения.

1. Докажите, что в определении группы достаточно было предполагать наличие левого нейтрального ($e \cdot a = a$ для любого $a \in G$) и левого обратного ($a' \cdot a = e$) элементов.

2. Пусть M – произвольное множество и $E(M)$ – множество отображений M в M (преобразований множества M). В качестве бинарной операции на $E(M)$ рассмотрим суперпозицию отображений. Иными словами, если $f, g \in E(M)$, то $f \cdot g$ – такое отображение, что $(f \cdot g)(x) = f(g(x))$ для любого $x \in M$. Докажите, что эта операция ассоциативна. Какое отображение является ее нейтральным элементом?

3. Докажите, что множество $S(M)$ биективных отображений множества M на себя с операцией, введенной в упр. 2, образует группу.

Рассмотрим группу $S(M)$ из упр. 3 подробнее в случае конечного множества M. Элементы множества M, содержащего n элементов, проще всего обозначать натуральными числами $1, 2, \ldots, n$. Задать биективное отображение s на таком множестве M – это значит задать те числа, в которые переходят элементы $1, 2, \ldots, n$, т. е. задать последовательность $\{a_1, a_2, \ldots, a_n\}$, где $a_i = s(i)$, $i = 1, 2, \ldots, n$. При этом $\{a_1, a_2, \ldots, a_n\}$ – это снова числа $1, 2, \ldots, n$, причем каждое число $j \in \{1, 2, \ldots, n\}$ встречается среди $a_1, a_2, \ldots, a_n$ ровно один раз. Иначе говоря, $\{a_1, a_2, \ldots, a_n\}$ – перестановка чисел $\{1, 2, \ldots, n\}$. Группу $S(M)$, где $M = \{1, 2, \ldots, n\}$, обозначают S_n и называют *симметрической* группой n элементов. Элементы группы S_n называются *подстановками* и записываются в виде $\begin{pmatrix} 1 & 2 & \ldots & n \\ a_1 & a_2 & \ldots & a_n \end{pmatrix}$, где $a_i = s(i)$, $s \in S_n$. Количество элементов группы S_n равно числу перестановок n элементов, т. е. $n!$.

Пусть $A = \{a_{i_1}, a_{i_2}, \ldots, a_{i_k}\}$ – произвольное подмножество множества M, содержащее k элементов. *Циклом длины* k называется такая подстановка s, что $s(a_{i_1}) = a_{i_2}, \ldots, s(a_{i_{k-1}}) = a_{i_k}$, $s(a_{i_k}) = a_{i_1}$, а все остальные элементы из M эта подстановка оставляет на месте (обозначается такой цикл $(a_{i_1}, a_{i_2}, \ldots, a_{i_k})$).

Упражнение.

4. Докажите, что любую подстановку множества из n элементов можно представить в виде произведения непересекающихся (*независимых*) циклов.

§ 4. Подгруппы. Гомоморфизмы групп

Определение. *Подгруппой* группы $G = (G, \cdot)$ называется такое подмножество H группы G, которое само является группой относительно бинарной операции $\cdot$, заданной в G.

Примеры.

1. Сама группа G и ее подмножество, состоящее из одного нейтрального элемента, являются подгруппами группы G.

2. Множество целых чисел, кратных фиксированному целому числу m, является подгруппой в группе всех целых чисел относительно сложения.

3. Два числа $\{1, -1\}$ образуют подгруппу в группе ненулевых рациональных чисел относительно умножения.

4. Матрицы, определители которых равны 1, образуют подгруппу в группе из примера 6 § 3.

5. В симметрической группе S_n множество всех *четных*, т. е. представимых в виде произведения четного числа циклов длины 2, подстановок – подгруппа; она называется *знакопеременной* группой.

Лемма 1. Для того чтобы подмножество H группы G являлось подгруппой, необходимо и достаточно:

1) чтобы для любых $a, b \in H$ произведение ab принадлежало H;

2) вместе с каждым $a \in H$ обратный элемент a^{-1} также принадлежал H. $\Diamond$

Замечание. Два условия леммы можно заменить одним: чтобы для любых $a, b \in H$ произведение ab^{-1} принадлежало H (в аддитивной записи выражение ab^{-1}, естественно, заменяется на $a - b$). $\Diamond$

Лемма 2. Пересечение двух (и вообще любого количества) подгрупп группы является подгруппой той же группы. $\Diamond$

Определение. Пусть $(G_1, \cdot)$ и $(G_2, *)$ – две группы, а f – отображение множества G_1 в множество G_2. Отображение f называется *гомоморфизмом* группы G_1 в группу G_2, если для любых $a, b \in G_1$ имеет место равенство $f(a \cdot b) = f(a) * f(b)$. Если, кроме того, f – биективное отображение, то f называется *изоморфизмом* G_1 на G_2 (запись: $G_1 \cong G_2$).

Изоморфные группы с абстрактной точки зрения неразличимы. Точнее, множества элементов могут иметь совершенно различную природу, но все соотношения в обеих группах одинаковы.

Если операции в группах G_1 и G_2 записываются одинаково (например, как умножение), то условие гомоморфности выглядит так: $f(ab) = f(a)f(b)$ для любых a и b из G_1. Нейтральный элемент любым гомоморфизмом всегда переводится в нейтральный.

Лемма 3. Пусть f – гомоморфизм группы G_1 в группу G_2. Тогда образ $f(H)$ любой подгруппы H группы G_1 является подгруппой группы G_2. Кроме того, полный прообраз $f^{-1}(S)$ любой подгруппы S группы G_2 является подгруппой группы G_1. $\Diamond$

Примеры.

6. Пусть $(\mathbb{R}, +)$ – группа вещественных чисел относительно сложения, а $(\mathbb{R}^*, \cdot)$ – группа ненулевых вещественных чисел относительно умножения. Отображение $f(x) = e^x$ является гомоморфизмом, поскольку $f(x+y) = e^{x+y} = e^x \cdot e^y = f(x)f(y)$. Это отображение не биективно, так как отрицательные числа не представляются в виде e^x. Но если в качестве второй группы рассмотреть группу $(\mathbb{R}^+, \cdot)$ положительных чисел (относительно умножения), то такое отображение f является взаимно однозначным (обратное отображение – логарифм), и поэтому f – это изоморфизм группы $(\mathbb{R}, +)$ на группу $(\mathbb{R}^+, \cdot)$.

7. Линейное отображение векторных пространств переводит сумму векторов в сумму и потому является гомоморфизмом между аддитивными группами векторов. В частности, гомоморфным является отображение проектирования.

8. Операция сопряжения на комплексных числах биективна и переводит сумму в сумму и произведение в произведение. Поэтому сопряжение является изоморфизмом как между группами $(\mathbb{C}, +)$ и $(\mathbb{C}, +)$, так и между группами $(\mathbb{C}^*, \cdot)$ и $(\mathbb{C}^*, \cdot)$. Отметим, что изоморфное отображение любой группы на самое себя (с той же операцией) называется *автоморфизмом*. Соответственно, сопряжение на группах комплексных чисел есть автоморфизм. Простейшим автоморфизмом является тождественное отображение id: $\mathrm{id}(x) = x$.

Упражнения.

1. Докажите, что если H – конечное подмножество группы G, то условие 2 в лемме 1 можно опустить.

2. Пусть $G = (G, \cdot)$ – произвольная группа. Рассмотрим отображение f группы G в группу $S(G)$ (см. упр. 3 § 3), заданное следующим образом: $f(g)$ для каждого $g \in G$ есть *подстановка* $\tilde{g} \in S(G)$, которая действует на элементы из G по правилу $\tilde{g}(x) = g \cdot x$. Исследуйте свойства отображения f и докажите следующую теорему: каждая группа изоморфна некоторой группе подстановок на множестве своих элементов (теорема Кэли).

§ 5. Смежные классы. Нормальные подгруппы

Пусть G – мультипликативно записанная группа, H – подгруппа группы G. Рассмотрим на элементах группы G отношение $a \sim b$, означающее, что $a^{-1}b \in H$.

Легко проверить, что это отношение является отношением эквивалентности. Соответствующие классы эквивалентности называются *левыми смежными классами* группы G по подгруппе H. Условие $a^{-1}b \in H$ может быть иначе записано как $b = ah$, где $h \in H$, или $b \in aH$, если под aH понимать множество $\{ah \mid h \in H\}$. Далее мы будем использовать обозначение aH для левого смежного класса, содержащего a. Аналогично можно определить *правые смежные классы* Ha с помощью условия $ba^{-1} \in H$ при введении отношения эквивалентности. Очевидно, что в коммутативных группах понятия левых и правых смежных классов совпадают, поскольку тогда $aH = Ha$.

Легко заметить, что все классы aH (как и Ha) при любых $a \in G$ находятся в биективном соответствии друг с другом ($ah \leftrightarrow bh$, $h \in H$). В частности, если подгруппа H конечна, то все смежные классы по этой подгруппе имеют одинаковое число элементов, равное числу элементов подгруппы H.

Определение. *Порядком* $|G|$ конечной группы G называется число элементов этой группы. *Индексом* $(G : H)$ подгруппы H в группе G называется число различных левых (равно как и правых) смежных классов по подгруппе H, если это число конечно.

Если группа конечна, то конечны все ее подгруппы и их индексы. С другой стороны, бесконечная группа может иметь конечные подгруппы, а также подгруппы (бесконечные) конечного индекса. Для конечных групп из равномощности смежных классов вытекает теорема Лагранжа.

Теорема 1. Порядок конечной группы G равен произведению порядка подгруппы H на индекс этой подгруппы, т. е. $|G| = |H| \cdot (G : H)$.

Следствие. Порядок подгруппы конечной группы является делителем порядка группы.

Определение. Подгруппа H группы G называется *нормальной подгруппой*, если для любого $a \in G$ левый aH и правый Ha смежные классы совпадают.

Равенство смежных классов aH и Ha не означает, что $ah = ha$ для любого $h \in H$; важно лишь, чтобы каждое произведение ah_1, где $h_1 \in H$, было равно произведению $h_2 a$ при каком-либо $h_2 \in H$. Ясно, что в коммутативных группах все подгруппы нормальны.

Примеры.

1. Пусть G – группа квадратных невырожденных матриц одного порядка, а H – подгруппа матриц с определителем, равным 1. Для произвольной матрицы $A \in G$ как левый AH, так и правый HA смежные классы представляют собой множество всех матриц, имеющих одинаковый ненулевой определитель, откуда $AH = HA$ и подгруппа H нормальна.

2. Пусть H – подгруппа из тех элементов группы G, которые коммутируют (перестановочны) со всеми элементами группы. Такая подгруппа называется *центром* группы G (например, в группе невырожденных матриц одного порядка центр образуют *скалярные* матрицы, т. е. матрицы вида cE, где E – единичная матрица, а c – число, отличное от нуля). Очевидно, что центр любой группы является нормальной подгруппой.

Определение. Пусть f – гомоморфизм группы G_1 в группу G_2. *Ядром* гомоморфизма f (запись: $\operatorname{Ker} f$) называется полный прообраз подгруппы $\{e_2\}$, состоящей из одного нейтрального элемента e_2 группы G_2.

Лемма. Пусть f – гомоморфизм группы G_1 в группу G_2. Ядро гомоморфизма f является нормальной подгруппой; смежные классы по ядру – это полные прообразы элементов из $f(G_1) \subset G_2$.

Доказательство. В силу леммы 3 § 4 $H = \operatorname{Ker} f$ – подгруппа; убедимся, что она нормальна в G_1. Действительно, если через e_1 и e_2 обозначить соответствующие нейтральные элементы групп, то для любого $h \in H$ и любого $x \in G_1$ имеем

$$f(x^{-1}hx) = f(x^{-1})f(h)f(x) = f(x^{-1})e_2 f(x) = f(x^{-1})f(x) = f(x^{-1}x) = f(e_1) = e_2,$$

т. е. $x^{-1}Hx \subset H$, или $Hx \subset xH$. Аналогично проверяется, что $xH \subset Hx$. Следовательно, $xH = Hx$, т. е. $\operatorname{Ker} f$ – нормальная подгруппа. Ясно также, что при любом $x \in G_1$ все элементы из xH, и только они, отображаются гомоморфизмом f в элемент $f(x)$. Лемма доказана.

Заменим теперь постановку вопроса. Предположим, что задана некоторая нормальная подгруппа H группы G. Можно ли построить группу $\overline{G}$ – гомоморфный образ G, элементам которой в точности соответствовали бы смежные классы G по H? По аналогии с § 2, обозначим множество смежных классов по подгруппе H через $G\backslash H$ и определим на этом множестве умножение по правилу $aH \cdot bH = (ab)H$. Такое определение нуждается в проверке корректности: если $a_1H = aH$ и $b_1H = bH$, то должно быть $(a_1b_1)H = (ab)H$. Но из того, что $a_1H = aH$ и $b_1H = bH$, следует, что $a_1 = ah_1$ и $b_1 = bh_2$ при каких-то $h_1, h_2 \in H$. Тогда $a_1b_1 = ah_1bh_2 = abh_1'h_2$, где h_1' определяется равенством $h_1b = bh_1'$. Так как $h_1' = b^{-1}h_1b \in aHa^{-1} = H$ в силу нормальности подгруппы H, то $h_1'h_2 \in H$, и поэтому $a_1b_1 \in (ab)H$. Очевидно, что и обратно, $ab \in (a_1b_1)H$, и наше определение корректно.

Легко проверяется, что относительно введенной операции множество $G\backslash H$ является группой. Нейтральным элементом этой группы служит $eH = H$, а обратным элементом для класса aH является класс $a^{-1}H$.

Определение. *Факторгруппой* группы G по нормальной подгруппе H называется фактормножество $G\backslash H$ с определенной выше бинарной операцией. Факторгруппа обозначается G/H.

Построим отображение группы G в факторгруппу G/H по правилу $\varphi(x) = xH = Hx$. Так как $\varphi(a)\varphi(b) = aHbH = (ab)H = \varphi(ab)$, то φ – гомоморфизм, причем сюръективный, поскольку каждый смежный класс aH – это образ элемента a.

Аналогом теоремы 3 § 2 является теорема о гомоморфизмах групп.

Теорема 2. Гомоморфный образ группы изоморфен факторгруппе этой группы по ядру гомоморфизма.

Доказательство. Пусть $f : G_1 \to G_2$ – гомоморфизм групп. Согласно теореме 3 § 2 образ отображения f находится в биективном соответствии с фактормножеством $G_1\backslash T$, где T – отношение эквивалентности, определяемое условием $aTb \iff f(a) = f(b)$. Обозначим через H ядро гомоморфизма f. Равенство $f(a) = f(b)$ означает, что $f(b^{-1}a) = e$, т. е. $b^{-1}a \in H$. Таким образом, эквивалентность aTb означает, что $a \in bH$. Следовательно, фактормножество $G_1\backslash T$ – это фактормножество $G_1\backslash H$, и образ $f(G_1)$ находится в биективном соответствии с множеством смежных классов $G_1\backslash H$. Но на этом множестве определена структура группы G_1/H, так как H – нормальная подгруппа в G_1. Значит, имеется биекция $\psi : f(G_1) \to G_1/H$, определяемая равенством $\psi(f(x)) = xH$, где $x \in G_1$. Для $x_1, x_2 \in G_1$ имеем

$$\psi(f(x_1)f(x_2)) = \psi(f(x_1x_2)) = x_1x_2H = x_1H \cdot x_2H = \psi(f(x_1))\psi(f(x_2)),$$

т. е. ψ – гомоморфное отображение, а поскольку оно еще и биективно, то ψ – изоморфизм, и теорема доказана.

Примеры.

3. Пусть G – мультипликативная группа вещественных невырожденных квадратных матриц порядка n. Отображение $f(X) = \det X$, $X \in G$, является гомоморфизмом (сюръективным) группы G на мультипликативную группу ненулевых вещественных чисел $\mathbb{R}^*$. Поскольку $H = \operatorname{Ker} f$ – подгруппа матриц с единичным определителем, то имеем $G/H \cong \mathbb{R}^*$.

4. Рассмотрим аддитивную группу вещественных чисел $\mathbb{R}$. Положим $f(t) = e^{2\pi ti} = \cos 2\pi t + i \sin 2\pi t$ для $t \in \mathbb{R}$. Так как $f(t_1 + t_2) = f(t_1)f(t_2)$, то f – гомоморфизм $\mathbb{R}$ в мультипликативную группу комплексных чисел $\mathbb{C}^*$. Ясно, что $\operatorname{Ker} f = \mathbb{Z}$ – группа целых чисел, а образ отображения $f(\mathbb{R}) = \{z \in \mathbb{C} \mid |z| = 1\}$ – группа комплексных чисел, расположенных на единичной окружности. Следовательно, эта группа изоморфна факторгруппе $\mathbb{R}/\mathbb{Z}$.

Упражнения.

1. Докажите, что отношение $\sim$, введенное в начале параграфа, является отношением эквивалентности.

2. Приведите примеры конечной подгруппы и подгруппы конечного индекса в мультипликативной группе ненулевых комплексных чисел $\mathbb{C}^*$.

3. Пусть $H_1 \subset H_2$ – две подгруппы группы G. Докажите, что если индекс $(G : H_1)$ конечен, то имеет место обобщение теоремы Лагранжа: $(G : H_1) = (G : H_2) \cdot (H_2 : H_1)$.

4. Докажите, что в любой группе все подгруппы индекса 2 нормальны.

5. Проверьте, что центр (см. пример 2) любой группы образует подгруппу.

6. Пусть G – множество отображений $\mathbb{R}$ в $\mathbb{R}$ вида $x \to ax + b$, где $a \neq 0$, а H – множество сдвигов $x \to x + t$. Докажите, что G – группа, H – нормальная подгруппа, и укажите факторгруппу G/H.

§ 6. Циклические группы

Пусть G – мультипликативно записанная группа (т. е. операция в G – умножение). Для произвольного элемента $a \in G$ рассмотрим произведения вида $a \cdot a$, $a \cdot a \cdot a$ и т. д. Как и для чисел, такие произведения будем называть степенями элемента a и обозначать $a^2, a^3, \ldots, a^n$ (в аддитивно записанной группе эти "степени" приобретают вид na и называются n-кратными элемента a). Положим, естественно, $a^0 = e, a^{-n} = (a^n)^{-1}$ для натурального n. Чтобы исследовать структуру множества степеней $\{a^n\}$, воспользуемся результатами § 5.

Возьмем группу целых чисел $\mathbb{Z}$ и рассмотрим отображение $f : \mathbb{Z} \to G$, определенное формулой $f(n) = a^n$, где $n \in \mathbb{Z}$ и a – фиксированный элемент группы G. Легко проверяется, что f – гомоморфизм. По теореме 2 § 5 множество элементов $D = \{a^n | n \in \mathbb{Z}\} = f(\mathbb{Z})$ является подгруппой G и изоморфно факторгруппе $\mathbb{Z}/\operatorname{Ker} f$.

Теорема 1. Всякая подгруппа группы целых чисел $\mathbb{Z}$ либо нулевая, либо имеет вид $m\mathbb{Z} = \{mn \mid n \in \mathbb{Z}\}$, где m – натуральное число.

Доказательство. Пусть H – какая-то ненулевая подгруппа группы $\mathbb{Z}$. Так как вместе с каждым числом, принадлежащим H, H содержит и противоположное число, то в подгруппе H есть положительные числа. Обозначим через m наименьшее натуральное число, содержащееся в H, и пусть n – произвольное целое число из подгруппы H. Разделим n на m с остатком, т. е. запишем n в виде $n = mq + r$, где q – частное, а r – остаток, который удовлетворяет ограничению $0 \leqslant r \leqslant m - 1$. Но тогда $r = n - mq = n + q(-m) \in H$, так как n и $-m$ принадлежат H, а поскольку m – наименьшее натуральное число из H, то $r = 0$. Таким образом, любое число из H делится на m, т. е. $H \subset m\mathbb{Z}$. Обратное

включение $H \supset m\mathbb{Z}$ очевидно, поскольку H – группа. Тем самым, $H = m\mathbb{Z}$, и теорема доказана.

Отметим, что подгруппа $m\mathbb{Z}$ изоморфна самой группе $\mathbb{Z}$ (хотя при $m \neq 1$ и не совпадает с ней), поэтому к подгруппам в $m\mathbb{Z}$ применима та же теорема 1.

Исследуем теперь факторгруппу $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$. Считаем, что $m > 0$ (факторгруппа $\mathbb{Z}/\{0\}$ – это сама группа $\mathbb{Z}$). Рассмотрим гомоморфизм φ группы $\mathbb{Z}$ в мультипликативную группу $\mathbb{C}^*$ ненулевых комплексных чисел, определенный формулой $\varphi(n) = e^{2\pi ni/m} = \cos(2\pi n/m) + i\sin(2\pi n/m)$. Так как $\varphi(n) = \big(\varphi(1)\big)^n$, то $\varphi(\mathbb{Z})$ является множеством степеней одного элемента $\varphi(1)$. Ядро $\operatorname{Ker}\varphi$ – это группа $m\mathbb{Z}$, и теорема о гомоморфизмах дает нам возможность отождествить факторгруппу $\mathbb{Z}/m\mathbb{Z}$ с образом φ. А образ φ – это группа всех комплексных корней степени m из 1, которую мы будем далее обозначать как C_m. Таким образом, $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z} \cong C_m$.

Вернемся к рассмотрению подгруппы степеней $\{a^n\}$ произвольного элемента a группы G.

Определение. Группа, состоящая из степеней одного элемента a, называется *циклической* группой, порожденной этим элементом.

Теорема 2. Подгруппа D, порожденная элементом a группы G, изоморфна либо бесконечной циклической группе $\mathbb{Z}$, либо циклической группе C_m порядка $m \geqslant 1$.

Доказательство. Мы видели, что циклическая подгруппа D изоморфна факторгруппе $\mathbb{Z}/\operatorname{Ker} f$, где $f(n) = a^n,\ n \in \mathbb{Z}$. Если $\operatorname{Ker} f$ – нулевая подгруппа, то D изоморфна группе $\mathbb{Z}$. Если же $\operatorname{Ker} f$ – ненулевая подгруппа, то по предыдущей теореме $\operatorname{Ker} f = m\mathbb{Z}$ при каком-то натуральном m. Но $\mathbb{Z}/m\mathbb{Z}$ изоморфна группе C_m. Следовательно, в этом случае $D \cong \mathbb{Z}/\operatorname{Ker} f = \mathbb{Z}/m\mathbb{Z} \cong C_m$, что и требовалось доказать.

Следствие. Подгруппа циклической группы G, порожденной элементом a, снова циклическая. Она состоит или из единичного элемента, или из степеней элемента a^m с наименьшим возможным положительным показателем m. При этом для бесконечной циклической группы число m произвольно, а для циклической группы порядка n число m должно быть некоторым делителем n. В последнем случае подгруппа имеет порядок $q = n/m$. Для любого такого числа m существует единственная подгруппа порядка n/m в группе G, которая порождается элементом a^m. $\Diamond$

Определение. *Порядком элемента* a из группы G называется порядок конечной циклической подгруппы, порожденной этим элементом. Если же эта подгруппа изоморфна $\mathbb{Z}$, то будем говорить, что элемент a имеет бесконечный порядок.

Ясно, что в любой конечной группе порядок каждого элемента конечен. В бесконечной группе могут встретиться как элементы конечного, так и бесконечного порядка (например, в $\mathbb{C}^*$ корни различных степеней из 1 имеют конечный порядок, а все остальные числа – бесконечный).

Теорема 3. В конечной группе порядок любого элемента есть делитель порядка группы. $\Diamond$

Следствие. Любая группа простого порядка циклическая.

Упражнения.

1. Докажите, что факторгруппа циклической группы является циклической группой.

2. Докажите, что порядок подстановки в симметрической группе равен наименьшему общему кратному длин ее независимых циклов (см. упр. 4 § 3).

§ 7. Прямое произведение групп

Определение. *Прямым произведением* двух групп G_1 и G_2 называется прямое произведение множеств $G_1 \times G_2$ с бинарной операцией $(a_1, a_2)(b_1, b_2) = (a_1 b_1, a_2 b_2)$, где $a_1, b_1 \in G_1$ и $a_2, b_2 \in G_2$ (для упрощения записи все операции обозначаются одинаково). При аддитивной записи абелевых групп естественно говорить о *прямой сумме* $G_1 \oplus G_2$.

Легко проверяется, что прямое произведение групп само является группой. В этой группе содержатся подгруппы $G_1 \times \{e_2\}$, $\{e_1\} \times G_2$, изоморфные соответственно G_1 и G_2. Отображение $\psi : G_1 \times G_2 \to G_2 \times G_1$, заданное равенством $\psi((a_1, a_2)) = (a_2, a_1)$, очевидно, устанавливает изоморфизм групп $G_1 \times G_2$ и $G_2 \times G_1$. Аналогично можно убедиться, что $(G_1 \times G_2) \times G_3 \cong G_1 \times (G_2 \times G_3)$. Свойства коммутативности и ассоциативности прямого произведения дают нам возможность говорить о прямом произведении любого конечного числа групп G_1, $G_2, \ldots, G_n$ и писать просто $G_1 \times G_2 \times \cdots \times G_n$.

Определение. Группа G называется *произведением* своих подгрупп H_1 и H_2 и обозначается $H_1 H_2$, если каждый элемент $g \in G$ может быть представлен в виде $g = h_1 h_2$, где $h_1 \in H_1$, $h_2 \in H_2$.

Теорема 1. Пусть G – группа с нормальными подгруппами H_1 и H_2. Если $H_1 \cap H_2 = \{e\}$ и $H_1 H_2 = G$, то $G \cong H_1 \times H_2$.

Доказательство. Из равенства $H_1 H_2 = G$ следует, что любой элемент $g \in G$ записывается в виде $g = h_1 h_2$, где $h_1 \in H_1$, $h_2 \in H_2$. Если еще $g = k_1 k_2$, $k_1 \in H_1$, $k_2 \in H_2$, то $h_1 h_2 = k_1 k_2$, откуда $k_1^{-1} h_1 = k_2 h_2^{-1} \in H_1 \cap H_2 = \{e\}$. Следовательно, $h_1 = k_1$, $h_2 = k_2$, и мы приходим к выводу, что запись $g = h_1 h_2$ однозначна. Так как H_1 – нормальная подгруппа, то $h_1 h_2 h_1^{-1} h_2^{-1} = h_1 (h_2 h_1^{-1} h_2^{-1}) = h_1 h_1' \in H_1$, а так как и H_2 – нормальна, то $h_1 h_2 h_1^{-1} h_2^{-1} = (h_1 h_2 h_1^{-1}) h_2^{-1} = h_2' h_2^{-1} \in H_2$, т. е. $h_1 h_2 h_1^{-1} h_2^{-1} \in H_1 \cap H_2 = \{e\}$ и, стало быть, $h_1 h_2 = h_2 h_1$.

Определим теперь отображение $\varphi : G \to H_1 \times H_2$, полагая $\varphi(g) = (h_1, h_2)$ для любого $g = h_1 h_2$. Это отображение – гомоморфизм, так как $\varphi(gg') =$

$= \varphi(h_1h_2h_1'h_2') = \varphi(h_1h_1'h_2h_2') = (h_1h_1', h_2h_2') = (h_1, h_2)(h_1', h_2') = \varphi(h_1h_2)\varphi(h_1'h_2') =$
$= \varphi(g)\varphi(g')$.

Поскольку $\varphi(h_1h_2) = (e, e)$ тогда и только тогда, когда $h_1 = h_2 = e$, то $\operatorname{Ker}\varphi = \{e\}$, т. е. φ инъективен. Сюръективность φ очевидна. Таким образом, φ удовлетворяет всем свойствам изоморфного отображения групп.

Группу G, удовлетворяющую условиям теоремы 1, принято называть *внутренним прямым произведением* своих подгрупп H_1 и H_2. Разумеется, произведение $G = H_1 \times H_2$, введенное в начале параграфа и называемое иногда *внешним* прямым произведением, является также внутренним произведением подгрупп $H_1 \times \{e\}$, $\{e\} \times H_2$, и при некотором навыке можно не делать различия между ними, употребляя сокращенное словосочетание "прямое произведение".

Следствие. Группа G является прямым произведением нормальных подгрупп $H_1, H_2, \ldots, H_n$, если каждый элемент $g \in G$ допускает однозначную запись в виде $g = h_1h_2 \ldots h_n, \;\; h_j \in H_j$.

Примеры.

1. Каждое комплексное число имеет вид $z = x+yi$, где x и y – вещественные числа. Рассмотрим в аддитивной группе комплексных чисел $\mathbb{C}$ подгруппы вещественных и чисто мнимых чисел. Ясно, что $\mathbb{C} = \mathbb{R} \oplus I$, если $I = \{z \in \mathbb{C} \mid \operatorname{Re} z = 0\}$.

2. Мультипликативная группа $\mathbb{R}^*$ есть прямое произведение подгруппы $\mathbb{R}^+$ положительных вещественных чисел и подгруппы второго порядка $\{\pm 1\}$.

3. Задание ненулевых комплексных чисел в показательной форме $z = re^{i\varphi}$ устанавливает разложение группы $\mathbb{C}^*$ в прямое произведение $\mathbb{R}^+$ и группы комплексных чисел с единичным модулем.

Отметим, что можно определить внешнее прямое произведение бесконечного числа групп. Однако для того, чтобы сохранить его связь с внутренним произведением, в качестве внешнего прямого произведения групп $G_1, G_2, \ldots, G_j, \ldots$ рассматривают только такие последовательности $g_1, g_2, \ldots, g_j, \ldots$, в которых "почти все" элементы нейтральны, т. е. $g_j = e_j$ для всех j кроме, разве лишь, конечного их числа. В этом случае осмысленно и бесконечное произведение элементов подгрупп $h_1h_2 \ldots h_j \ldots$, поскольку фактически перемножается лишь конечное число неединичных элементов.

Пример.

4. Рассмотрим мультипликативную группу ненулевых рациональных чисел $\mathbb{Q}^*$. Выделим в ней подгруппу $H_1 = \{\pm 1\}$ и бесконечное множество бесконечных циклических подгрупп $H_p = \{\, p^n \,\}$, где p – простые натуральные числа $(p = 2, 3, 5, 7, 11, \ldots)$. Каждое ненулевое рациональное число имеет вид $q = \pm a/b$, где a и b – натуральные числа. Раскладывая числитель и знаменатель на простые множители, получаем $q = \pm p_1^{k_1} p_2^{k_2} \ldots p_j^{k_j} \ldots$, где все показатели k_j, за исключением конечного числа, равны нулю. Ввиду однозначности разложения натуральных чисел на простые множители, такое представление q единственно. Следовательно, $\mathbb{Q}^* = H_1H_2H_3H_5 \ldots$ – прямое произведение бесконечного числа подгрупп.

Понятие прямого произведения (прямой суммы в аддитивной записи) позволяет исчерпывающим образом описать строение конечных абелевых групп.

Определение. Циклические группы порядка p^k, где p – простое число, называются *примарными* циклическими группами.

Приведем без доказательства основную теорему о конечных абелевых группах.

Теорема 2. Всякая конечная абелева группа является прямой суммой примарных циклических подгрупп. Любые два таких разложения имеют по одинаковому числу слагаемых каждого порядка.

Упражнения.

1. Докажите, что бесконечную циклическую группу $\mathbb{Z}$ нельзя разложить в прямую сумму своих ненулевых подгрупп.

2. Докажите, что если m и n – взаимно простые натуральные числа, то циклическая группа $\mathbb{Z}_{mn}$ изоморфна прямой сумме $\mathbb{Z}_m \oplus \mathbb{Z}_n$.

§ 8. Кольца

Определение. Множество A называется *кольцом*, если на нем определены две бинарные операции: $+$ (сложение) и $\cdot$ (умножение), – обладающие следующими свойствами:

1) $(A, +)$ является абелевой группой;

2) умножение $\cdot$ ассоциативно;

3) операции сложения и умножения связаны *дистрибутивными* законами, т. е. $(a+b)c = ac + bc,\ c(a+b) = ca + cb$ для всех $a, b, c \in A$.

Определение. Абелева группа $(A, +)$ называется *аддитивной группой кольца* A. Если операция умножения в кольце обладает нейтральным элементом (его принято обозначать обычной единицей 1), то говорят, что A – *кольцо с единицей*. Если в кольце операция умножения коммутативна, то кольцо называется *коммутативным*.

Примеры.

1. При обычных операциях кольцами являются множества:

– целых чисел $\mathbb{Z}$;

– рациональных чисел $\mathbb{Q}$;

– вещественных чисел $\mathbb{R}$;

– комплексных чисел $\mathbb{C}$;

– 0, состоящее из одного числа 0;

– $n\mathbb{Z}$, состоящее из целых чисел, кратных некоторому числу n (в этом кольце нет единицы);

– комплексных чисел вида $m + ni$, где $m, n \in \mathbb{Z}$ (*кольцо целых гауссовских чисел*);

– вещественных чисел вида $m + n\sqrt{2}$, где $m, n \in \mathbb{Z}$;

– вещественных функций с общей областью определения;

– многочленов от одного или нескольких неизвестных с коэффициентами из некоторого коммутативного кольца;

– квадратных матриц порядка n с элементами из некоторого коммутативного кольца (так как при $n > 1$ матрицы, как правило, неперестановочны, то это кольцо некоммутативно).

2. Множество $\mathbb{Z}^2$ (множество пар целых чисел) образует кольцо, если операции определены по формулам:

$$(a, b) + (c, d) = (a + c, b + d), \quad (a, b)(c, d) = (ac, bd).$$

Определение. *Обратным элементом* для данного элемента a любого кольца с единицей называется такой элемент a^{-1}, который удовлетворяет условию $aa^{-1} = a^{-1}a = 1$.

Ясно, что в кольце $\mathbb{Z}$ обратимы (т. е. обладают обратным элементом) только 1 и -1, а, например, в кольце $\mathbb{Q}$ обратимы уже все ненулевые числа.

Теорема 1. Если в кольце один из сомножителей равен нулю, то и все произведение равно нулю.

Доказательство. Действительно, $a \cdot 0 + a \cdot 0 = a \cdot (0 + 0) = a \cdot 0$, откуда немедленно следует, что $a \cdot 0 = 0$ (аналогично $0 \cdot a = 0$).

Замечание. Обратное утверждение, верное для колец вещественных или комплексных чисел, не сохраняется для любых колец. В кольце из примера 2, приведенного выше, $(a, 0)(0, b) = (0, 0)$ при любых целых a и b.

Определение. Элементы a и b кольца, для которых $ab = 0$ или $ba = 0$, и при этом $a \neq 0$, $b \neq 0$, называются *делителями нуля*.

Теорема 2. Если $ab = ac$ или $ba = ca$, то $b = c$, если только $a \neq 0$ и не является делителем нуля. $\Diamond$

Определение. Подмножество B кольца A называется *подкольцом*, если оно само является кольцом при тех же операциях сложения и умножения, которые определены в кольце A.

Теорема 3. Для того чтобы подмножество $B \neq \varnothing$ кольца A было его подкольцом, необходимо и достаточно, чтобы разность и произведение любых двух элементов из B снова принадлежали B. $\Diamond$

Упражнения.

1. Докажите, что множество обратимых элементов кольца образует группу по умножению.

2. Докажите, что делитель нуля не может иметь обратный элемент.

3. Приведите пример делителей нуля в кольце квадратных матриц второго порядка с вещественными элементами.

4. Какие кольца из примера 1 являются подкольцами других колец из того же примера?

§ 9. Поля

Определение. *Полем* называется коммутативное кольцо K, содержащее не менее двух элементов, в котором все ненулевые элементы образуют группу по умножению (*мультипликативную группу* K^* поля K).

Из определения немедленно следует, что поле всегда содержит единицу.

Примеры.

1. Из колец примера 1 § 8 полями являются только множества рациональных, вещественных и комплексных чисел.

2. При обычных операциях полями являются множества:

– комплексных чисел вида $a + bi$, где $a, b \in \mathbb{Q}$ (*поле гауссовских чисел*);

– вещественных чисел вида $a + b\sqrt{2}$, где $a, b \in \mathbb{Q}$;

– вещественных чисел вида $a + b\sqrt[3]{2} + c\sqrt[3]{4}$, где $a, b, c \in \mathbb{Q}$;

– всех алгебраических дробей (дробно-рациональных функций) от одного или нескольких неизвестных с коэффициентами из некоторого коммутативного кольца без делителей нуля;

– из двух элементов, которые мы обозначим 0 и 1, при следующем определении операций:

$$0 + 0 = 1 + 1 = 0,\ 0 + 1 = 1 + 0 = 1,\ 0 \cdot 0 = 0 \cdot 1 = 1 \cdot 0 = 0,\ 1 \cdot 1 = 1.$$

Теорема 1. Поле не имеет делителей нуля.

Доказательство. Пусть $ab = 0$ и $a \neq 0$. Тогда $0 = a^{-1}ab = 1 \cdot b$, откуда следует, что $b = 0$ (сравните с упр. 2 § 8).

Кольцо целых чисел является примером кольца без делителей нуля, не являющегося полем. Однако для конечных коммутативных колец верна и обратная теорема.

Теорема 2. Всякое конечное коммутативное кольцо без делителей нуля, содержащее более одного элемента, является полем. ◊ (Используйте биективность отображения $x \to ax$ при $a \neq 0$.)

Произведение ab^{-1} в поле записывается также в виде *дроби* (*частного*) $\frac{a}{b}$ (или a/b в линейной записи). Легко проверить, что в любом поле $(ab)^{-1} = a^{-1}b^{-1}$ и $(a^n)^{-1} = (a^{-1})^n$ при всех натуральных n. Естественно принять $a^{-n} = (a^{-1})^n$ и $a^0 = 1$. Таким образом, определены целые степени любого отличного от 0 элемента a. Правила оперирования с дробями и степенями обычные.

Упражнение. Постройте поле из трех элементов.

§ 10. Идеалы и кольца классов вычетов

Начиная с этого параграфа мы будем рассматривать только коммутативные кольца, не всегда указывая это явно.

Определение. Подкольцо H коммутативного кольца A называется *идеалом*, если произведение $ha = ah$ лежит в H при любых $a \in A$ и $h \in H$.

Примеры.

1. В любом кольце A все кольцо A и подмножество $\mathcal{O}=\{0\}$ являются идеалами.

2. Множество $n\mathbb{Z}$ – идеал кольца $\mathbb{Z}$.

3. В кольце функций, определенных на $[a, b]$, идеалом является множество всех функций f таких, что $f(c) = 0$ для некоторого $c \in [a, b]$.

4. Множество всех нильпотентных элементов кольца является идеалом (элемент b кольца называется *нильпотентным*, если существует такое натуральное число n, что $b^n = 0$).

Теорема 1. В кольце A множество $\{xa \,|\, x \in A\}$ всех кратных любого фиксированного элемента $a \in A$ является идеалом в A. $\Diamond$

Определение. Идеал кольца A, состоящий из кратных элемента a, называется *главным идеалом, порожденным элементом* a, и обозначается (a).

Нулевой идеал $\mathcal{O}=(0)$ всегда является главным. Если кольцо A имеет единицу 1, то *единичный идеал* (1) является, как легко видеть, всем кольцом A.

Теорема 2. Любое поле не содержит идеалов, отличных от нулевого и единичного.

Доказательство. Пусть H – ненулевой идеал поля K. Возьмем $h \in H$, $h \neq 0$. Так как K – поле, то существует $h^{-1} \in K$, а тогда $1 = hh^{-1} \in H$, откуда следует, что $K \subset H$, и, значит, $H = K$.

Замечание. Ясно, что в любом кольце, отличном от поля, любой необратимый элемент $a \neq 0$ порождает идеал (a), не совпадающий ни с (0), ни с (1).

Теорема 3. Все идеалы в кольце целых чисел $\mathbb{Z}$ главные. $\Diamond$

В следующем параграфе мы докажем обобщение теоремы 3. Таким образом, подкольца $n\mathbb{Z}$ $(n = 0, 1, 2, 3 \dots)$ исчерпывают все идеалы кольца $\mathbb{Z}$.

Дальнейшие определения и теоремы о кольцах классов вычетов мы будем приводить для главных идеалов, хотя почти без изменений они переносятся и на произвольные идеалы.

Определение. Пусть $H = (h)$ – главный идеал коммутативного кольца A. Два элемента a и b кольца A называются *сравнимыми по модулю* h (или *по идеалу* H), если их разность $a - b$ принадлежит идеалу H. При этом пишут $a \equiv b \pmod{h}$.

Ясно, что отношение $\equiv$ является отношением эквивалентности, а так как аддитивная группа $(H, +)$ – подгруппа коммутативной группы $(A, +)$, то любой класс эквивалентности с представителем a по этому отношению совпадает с классом смежности $a + H$ по подгруппе H.

Определение. Класс смежности $a + H$ называется *классом вычетов по модулю* h.

Теорема 4. Пусть $H = (h)$ – идеал кольца A. Множество классов вычетов по модулю h образует кольцо $A/H = A/(h)$ с операциями

$$(a + H) + (b + H) = (a + b) + H, \quad (a + H)(b + H) = ab + H.$$

Доказательство. Убедимся только в корректности определения умножения. После этого то, что A/H – коммутативное кольцо, проверяется тривиально. Действительно, при всех $a, b \in A$, $h_1, h_2 \in H$ произведение $(a + h_1)(b + h_2) = ab + {} + (ah_2 + h_1b + h_1h_2) \in ab + H$, так как H – идеал и потому содержит $ah_2 + h_1b + h_1h_2$.

Следствие. В любом коммутативном кольце, если $a_1 \equiv a_2$ и $b_1 \equiv b_2 \pmod{h}$, то $a_1 \pm b_1 \equiv a_2 \pm b_2$ и $a_1b_1 \equiv a_2b_2 \pmod{h}$.

Определение. Кольцо A/H называется *кольцом классов вычетов* кольца A *по модулю* h.

Примерами колец классов вычетов могут служить кольца классов вычетов кольца целых чисел $\mathbb{Z}_n = \mathbb{Z}/(n)$, где $n = 2, 3, 4, \ldots$

Определение. Пусть A – кольцо с единицей, отличное от $\mathcal{O}$. Целое положительное число m называется *характеристикой* кольца A, если

$$m \cdot 1 = \underbrace{1 + 1 + \cdots + 1}_{m \text{ раз}} = 0$$

и никакое положительное число, меньшее m, этим свойством не обладает. Если указанное свойство не имеет места ни для какого положительного числа, то говорят, что кольцо имеет *характеристику* 0.

Характеристика кольца $\mathbb{Z}$, полей $\mathbb{R}$ и $\mathbb{C}$ равна 0, кольцо $\mathbb{Z}_n$ имеет характеристику n.

Следующая лемма является прямым следствием последнего определения.

Лемма. Если характеристика кольца A равна m, то для всякого $a \in A$

$$ma = \underbrace{a + a + \cdots + a}_{m \text{ раз}} = 0.$$

Теорема 5. Характеристика любого кольца A без делителей нуля (в частности, поля) или равна 0, или является простым числом.

Доказательство. Пусть составное натуральное число m – характеристика кольца A ($m \neq 1$, так как полагаем A отличным от $\mathcal{O}$), тогда $m = kl$, $k > 1$, $l > 1$. Следовательно, $0 = m \cdot 1 = (kl) \cdot 1 = (k \cdot 1) \cdot (l \cdot 1)$. Так как A не содержит делителей нуля, то или $k \cdot 1 = 0$, или $l \cdot 1 = 0$, что противоречит определению характеристики кольца и, тем самым, доказывает теорему.

Определение. Идеал H кольца A называется *простым*, если из $ab \in H$ следует, что либо $a \in H$, либо $b \in H$.

Единичный идеал $(1)=A$ всегда прост. В кольце целых чисел идеал (p) прост при p простом.

Теорема 6. Идеал H кольца A является простым тогда и только тогда, когда кольцо классов вычетов A/H не содержит делителей нуля.

Доказательство. Кольцо классов вычетов A/H не имеет делителей нуля в том и только том случае, если из $(a+H)(b+H) = H$ следует, что либо $a+H = H$, либо $b+H = H$. Но это условие равносильно утверждению, что из $ab \in H$ следует или $a \in H$, или $b \in H$. Оно справедливо, согласно определению, в точности для простых идеалов.

Следствие. Кольцо классов вычетов кольца целых чисел по модулю n является полем тогда и только тогда, когда n – простое число. $\Diamond$

Определение. Подмножество L поля K называется *подполем* поля K, если оно само является полем при тех же операциях сложения и умножения, которые заданы в поле K.

Так, $\mathbb{Q}$ является подполем поля $\mathbb{R}$, а последнее – подполем поля $\mathbb{C}$.

Упражнения.

1. Докажите, что пересечение любого множества идеалов кольца A является идеалом.

2. Понятия гомоморфизма, изоморфизма и т. п. (см. § 4) очевидным образом распространяются на кольца. Докажите, что в случае гомоморфизма колец ядро гомоморфизма всегда является идеалом.

3. Убедитесь, что в кольце многочленов с целыми коэффициентами множество многочленов с четным свободным членом образует идеал. Докажите, что этот идеал не является главным.

4. Покажите, что из сравнения $ca_1 \equiv ca_2 \pmod{h}$ не следует сравнение $a_1 \equiv a_2 \pmod{h}$.

5. Сформулируйте и докажите для подполей теорему, аналогичную теореме 3, § 8.

6. Докажите, что любое поле содержит подполе изоморфное или полю рациональных чисел, или полю вычетов кольца целых чисел по простому модулю.

7. Докажите, что $(a+b)^p = a^p + b^p$ в любом поле характеристики p.

§ 11. Евклидовы кольца

Определение. *Евклидовым кольцом* называется кольцо D без делителей нуля, в котором каждому ненулевому элементу a сопоставляется целое неотрицательное число $v(a)$, называемое *нормой*, со следующими свойствами:

1) $v(ab) \geqslant v(a)$ для всех $a \neq 0$, $b \neq 0$ из D;

2) для любых $a, b \in D$, $b \neq 0$, существует элемент $q \in D$ такой, что $a = bq+r$, где $r = 0$ или $v(r) < v(b)$.

Пример.

Кольцо целых чисел $\mathbb{Z}$ является евклидовым кольцом с нормой $v(n) = |n|$.

Теорема 1. В евклидовом кольце все идеалы главные.

Доказательство. Пусть H – ненулевой идеал евклидова кольца D. Выберем в H отличный от нуля элемент a с наименьшей нормой $v(a)$. Тогда любой $b \in H$ можно представить в виде $b = aq + r$, откуда $r = b - aq \in H$. Но не может быть, чтобы $v(r) < v(a)$, следовательно, $r = 0$ и $H = (a)$.

Следствие. Любое евклидово кольцо содержит единицу.

Доказательство. Применим теорему к единичному идеалу, которым является все кольцо D. Тогда $D = (a)$, откуда, в частности, следует, что $a = ae$ при некотором $e \in D$. Но тогда для любого $b \in D$ получаем, что $b = qa = qae = be$, и доказательство завершено.

Определение. Пусть D – любое кольцо без делителей нуля. Говорят, что a *делит* b (b *делится на* a), если существует $c \in D$ такой, что $ac = b$ (запись: $a|b$).

Ясно, что $a|b \iff b \in (a) \iff (b) \subset (a)$.

Теорема 2. В евклидовом кольце D любые два элемента a и b имеют наибольший общий делитель d, который представляется в виде $d = sa + tb$, где $s, t \in D$.

Доказательство. Рассмотрим множество $\{sa + tb \mid s, t \in D\}$. Легко проверить, что это множество – идеал. По теореме 1 этот идеал главный, т. е. $\{sa + tb\} = (d)$. Следовательно, существуют такие s, t, g и h в кольце D, что $c = sa + tb$, $a = gc$, $b = hc$.

Примером подобного представления наибольшего общего делителя (НОД) в кольце целых чисел может служить равенство $\text{НОД}(54, 15) = 3 = 2 \cdot 54 + (-7) \cdot 15$.

Лемма 1. В любом евклидовом кольце $a|b$ и $b|a$ тогда и только тогда, когда $a = bu$ для некоторого обратимого (т. е. имеющего в этом же кольце обратный) элемента u.

Доказательство. Если $b = aw$ и $a = bu$, то $b = buw$, откуда $uw = 1$. Обратное утверждение леммы очевидно, так как в этом случае из разложения $a = bu$ вытекает, что $b = au^{-1}$.

Определение. Необратимый элемент p евклидова кольца называется *простым*, если он допускает лишь тривиальное разложение на множители, т. е. из равенства $p = ab$ следует, что или a, или b обратимы.

В кольце $\mathbb{Z}$ простыми элементами являются числа $\pm 2, \pm 3, \pm 5, \pm 7, \pm 11, \ldots$

Теорема 3. Все элементы евклидова кольца однозначно с точностью до обратимых элементов и порядка следования сомножителей разлагаются в произведение простых элементов. $\Diamond$

Для того чтобы доказать теорему 3, последовательно доказываются следующие три леммы.

Лемма 2. Если в евклидовом кольце b делит a, но a не делит b, то $v(b) < v(a)$.

Доказательство. Разделим b на a: $b = aq + r$, $v(r) < v(a)$. Так как $a = bc$ для некоторого c, то $r = b - aq = b(1 - cq)$, что влечет за собой неравенство $v(b) \leqslant v(r) < v(a)$.

Лемма 3. В евклидовом кольце любой ненулевой необратимый элемент a можно разложить в произведение простых сомножителей. $\Diamond$ (Воспользуйтесь индукцией по $v(a)$.)

Лемма 4. Если произведение ab делится на простой элемент p, то один из сомножителей должен делиться на p (другими словами, идеал (p) прост).

Доказательство. Предположим, что p не делит a. Тогда $c = \text{НОД}(p, a)$ не делится на p, откуда c обратим. С другой стороны, $c = sa + tp$ и, значит, $b = c^{-1}cb = c^{-1}(sa + tp)b = c^{-1}sab + c^{-1}tpb$. Каждое слагаемое делится на p, следовательно, и b делится на p.

Упражнение.

Докажите, что кольцо $\mathbb{Z}(i)$ целых гауссовских чисел является евклидовым кольцом с нормой $v(m + ni) = m^2 + n^2$.

§ 12. Кольца многочленов

Определение. *Многочленом* (или *полиномом*) от *неизвестной* x над кольцом A называется выражение вида

$$a_0 + a_1x + \cdots + a_mx^m = \sum_{k=0}^{m} a_kx^k,\ a_k \in A \qquad (*)$$

(a_0x^0 полагаем равным $a_0 \in A$).

Элементы a_k называются *коэффициентами* многочлена $(*)$; все они или их часть могут быть нулевыми.

Многочлен часто символически обозначается $f(x)$; при этом он не рассматривается как отображение (функция) из A в A.

Определение. Наибольшее k такое, что $a_k \neq 0$, называется *степенью* многочлена $(*)$ и обозначается $\deg f$. Если $a_k = 0$ для всех k, то $\deg 0$, по определению, равна $-\infty$.

Естественным образом определяются сумма и произведение двух многочленов. Легко проверяются неравенства $\deg(f + g) \leqslant \max\{\deg f, \deg g\}$, $\deg(fg) \leqslant \leqslant \deg f + \deg g$.

Множество всех многочленов от x с коэффициентами из кольца A будем обозначать символом $A[x]$.

Теорема 1. Операции сложения и умножения определяют на множестве $A[x]$ структуру кольца. Многочлены нулевой степени вместе с нулем образуют подкольцо констант, изоморфное кольцу A. $\Diamond$

Теорема 2. Если D – кольцо без делителей нуля, то в $D[x]$ имеет место равенство $\deg(fg) = \deg f + \deg g$. $\Diamond$

Следствие 1. Если D – кольцо без делителей нуля, то $D[x]$ также не имеет делителей нуля.

Следствие 2. Если K – поле, то в кольце $K[x]$ обратимы ненулевые константы, и только они.

Теорема 3. Для любого поля K кольцо многочленов $K[x]$ является евклидовым кольцом с нормой $v(f) = \deg f$. $\Diamond$ (Для доказательства необходимо описать алгоритм деления в кольце $K[x]$.)

Простые элементы в кольце многочленов имеют специальное название.

Определение. Многочлен $g(x)$ из кольца $K[x]$ называется *приводимым* (над полем K), если $g(x) = g_1(x)g_2(x)$ для подходящих непостоянных многочленов $g_1, g_2 \in K[x]$; в противном случае многочлен $g(x)$ называется *неприводимым*.

Замечание. Приводимость или неприводимость данного многочлена существенно зависят от поля K. Многочлен $x^2 + 1$ неприводим над $\mathbb{R}$, но приводим над $\mathbb{C}$. Многочлен $x^2 - 2$ неприводим над $\mathbb{Q}$ и над $\mathbb{Z}_3$, но приводим над $\mathbb{Z}_7$ (в этом случае $x^2 - 2 = (x+3)(x+4)$). Ясно, что линейные многочлены неприводимы над любым полем. Над полем $\mathbb{C}$ неприводимы только они (основная теорема алгебры). Над полем $\mathbb{R}$ неприводимы еще и квадратные многочлены с отрицательным дискриминантом. Над полем $\mathbb{Q}$ существуют неприводимые многочлены любой степени.

Теорема 4. Любой непостоянный многочлен из $K[x]$ можно представить в виде произведения константы и неприводимых многочленов с единичными старшими коэффициентами. Это разложение единственно с точностью до порядка множителей.

Последняя теорема – частный случай теоремы 3 § 11.

Упражнения.

1. Приведите пример разных многочленов из $\mathbb{Z}_5[x]$, которые были бы тождественными, если их рассматривать как отображения.

2. Многочлены $x^8 + x^6 + x^5 + x^3 + x^2 + 1$ и $x^6 + x^4 + x + 1$ принадлежат кольцу $\mathbb{Z}_2[x]$. Найдите их наибольший общий делитель и его представление в соответствии с теоремой 2 § 11.

3. Найдите все неприводимые многочлены степеней 2, 3 и 4 над полем $\mathbb{Z}_2$, степеней 2 и 3 над полем $\mathbb{Z}_3$.

4. Пусть A – произвольное (коммутативное) кольцо и $f(x) \in A[x]$. Докажите, что $x - a$ делит $f(x)$ в том и только том случае, если $f(a) = 0$ в A.

§ 13. Расширения полей

Если $g(x)$ – неприводимый многочлен над полем K, то кольцо классов вычетов кольца $K[x]$ по модулю $g(x)$ является кольцом без делителей нуля (теорема 6 § 10). На самом деле верно более сильное утверждение.

Теорема 1. Кольцо классов вычетов $L = K[x]/(g(x))$ по модулю неприводимого многочлена есть поле.

Доказательство. Возьмем любой представитель $f(x)$ произвольного класса вычетов, не совпадающего с $(g(x))$. Так как $g(x)$ неприводим, то многочлены $f(x)$ и $g(x)$ взаимно просты. По теореме 2 § 11 в кольце $K[x]$ найдутся такие многочлены $s(x)$ и $t(x)$, что $s(x)f(x) + t(x)g(x) = 1$. Следовательно, $s(x)f(x) \equiv 1 \pmod{g(x)}$, так что $s(x)$ принадлежит классу, обратному к классу, содержащему $f(x)$. Таким образом, все классы, кроме нулевого, обратимы.

Ясно, что поле K является подполем поля L (точнее, мономорфно вкладывается в L). В этом случае поле L называется *расширением* поля K.

Элементы поля $L = K[x]/(g(x))$ можно представить в виде многочленов, степени которых меньше, чем $\deg g(x)$ (представителей соответствующих классов вычетов). Сложение таких многочленов осуществляется как обычно, а после умножения надо переходить к остатку от деления на $g(x)$. На практике используют замены степеней x^m (если $m \geqslant \deg g(x)$) линейными комбинациями меньших степеней x^k. Действительно, пусть $g(x) = x^n + b_{n-1}x^{n-1} + \cdots + b_1x + b_0$. Тогда

$$x^n \equiv \sum_{k=0}^{n-1}(-b_kx^k) \qquad (\mathrm{mod}\ g(x)),$$

$$x^{n+1} \equiv x\sum_{k=0}^{n-1}(-b_kx^k) \equiv \sum_{k=0}^{n-2}(-b_kx^{k+1}) - b_{n-1}\sum_{k=0}^{n-1}(-b_kx^k) \qquad (\mathrm{mod}\ g(x))$$

и т. д.

Заметим еще, что любое расширение L поля K можно рассматривать как векторное пространство над K. Если L образовано, как в теореме 1, то базис этого векторного пространства состоит из многочленов (точнее, классов, которым принадлежат эти многочлены) $1, x, x^2, \ldots, x^{n-1}$, где $n = \deg g(x)$. Размерность этого пространства называют *степенью расширения* L над K и обозначают $n = [L : K]$. Например, если представить поле комплексных чисел $\mathbb{C}$ в виде $\mathbb{R}[x]/(x^2 + 1)$, то $[\mathbb{C} : \mathbb{R}] = 2$.

Теорема 2. Любое конечное поле характеристики p состоит из p^n элементов для некоторого n.

Доказательство. Любое конечное поле характеристики p является конечномерным векторным пространством над своим подполем $\mathbb{Z}_p$, порожденным единицей (см. упр. 5 § 10). Если n – размерность этого пространства (степень расширения), то число элементов расширения равно p^n.

Определение. Конечные поля, содержащие p^n элементов, называются *полями Галуа* (по имени французского математика Э. Галуа) и обозначаются $\mathrm{GF}(p^n)$.

Можно доказать, что над полем вычетов $\mathbb{Z}_p = \mathrm{GF}(p)$ существуют неприводимые многочлены любой степени, поэтому кольца классов вычетов $\mathbb{Z}_p/(g(x))$ по модулю неприводимых многочленов образуют конечные поля любой степени над $\mathbb{Z}_p$. Многочлены одинаковой степени приводят к одним и тем же (точнее, изоморфным) полям; никаких других полей из конечного числа элементов не существует.

Примеры.

1. Многочлен $x^2 + x + 1$ неприводим над полем $\mathbb{Z}_2 = \mathrm{GF}(2)$, так как ни 0, ни 1 не являются его корнями. Построим $\mathrm{GF}(4) = \mathbb{Z}_2[x]/(x^2 + x + 1)$. Пусть j означает корень многочлена $x^2 + x + 1$ в поле $\mathrm{GF}(4)$. Тогда нетрудно вычислить таблицы сложения и умножения в $\mathrm{GF}(4)$, заменяя всюду j^2 на $j + 1 = -j - 1$.

Таблица сложения

$+$	0	1	j	$j+1$
0	0	1	j	$j+1$
1	1	0	$j+1$	j
j	j	$j+1$	0	1
$j+1$	$j+1$	j	1	0

Таблица умножения

$\times$	0	1	j	$j+1$
0	0	0	0	0
1	0	1	j	$j+1$
j	0	j	$j+1$	1
$j+1$	0	$j+1$	1	j

2. $\mathrm{GF}(8) = \mathbb{Z}_2[x]/(x^3+x^2+1)$, так как x^3+x^2+1 неприводим над полем $\mathrm{GF}(2)$. Общий элемент поля $\mathrm{GF}(8)$ можно записать в виде $a_2x^2 + a_1x + a_0$ или просто в

$\times$	001	010	011	100	101	110	111
001	001	010	011	100	101	110	111
010	010	100	110	101	111	001	011
011	011	110	101	001	010	111	100
100	100	101	001	111	011	010	110
101	101	111	010	011	110	100	001
110	110	001	111	010	100	011	101
111	111	011	100	110	001	101	010

виде двоичного вектора (a_2, a_1, a_0), как сделано в приведенной таблице умножения ($0 = (0, 0, 0)$ в таблице опущен).

§ 14. Мультипликативная группа конечного поля

Легко убедиться, что в поле $\mathrm{GF}(4)$ все ненулевые элементы являются степенями одного элемента (j, $j^2 = j + 1$, $j^3 = j^0 = 1$), а в поле $\mathrm{GF}(8)$ аналогичную роль играет $(0, 1, 0)$ – корень многочлена $x^3 + x^2 + 1$. Еще один пример. Многочлен $x^2 + x + 2$ неприводим над полем $\mathrm{GF}(3)$. Пусть $b = (0, 1, 0)$ – корень этого многочлена. Тогда $b^2 = -(b + 2) = 2b + 1$, $b^3 = 2b + 2$, $b^4 = 2$, $b^5 = 2b$, $b^6 = b + 2$, $b^7 = b + 1$, $b^8 = b^0 = 1$.

Теорема 1. Пусть $q = p^n$ – степень простого числа. Любой ненулевой элемент поля $\mathrm{GF}(q)$ удовлетворяет уравнению $x^{q-1} = 1$.

Доказательство. Пусть a_1, a_2, ... , a_{q-1} – все ненулевые элементы поля $\mathrm{GF}(q)$. Возьмем любой элемент $c \in \mathrm{GF}(q)$, отличный от нуля. Тогда ca_1, ca_2, ... , ca_{q-1} – снова все ненулевые элементы поля. Следовательно, $a_1 a_2 \dots a_{q-1} = ca_1 \cdot ca_2 \cdot \ldots \cdot ca_{q-1}$, откуда $c^{q-1} = 1$, что и требовалось доказать.

Следствие 1. Любой элемент поля $\mathrm{GF}(q)$ удовлетворяет уравнению $x^q = x$ (для $q = p$ это так называемая малая теорема Ферма: $a^p \equiv a \pmod p$ для всех целых a).

Следствие 2. В поле $\mathrm{GF}(q)$ многочлен $x^q - x$ раскладывается на линейные множители

$$x^q - x = \prod_{a_i \in \mathrm{GF}(q)} (x - a_i).$$

Следствие 3. При $K = \mathrm{GF}(p)$ многочлен $g(x)$ из теоремы 1 § 13 делит многочлен $x^{q-1} - 1$ ($q = p^n$, где $n = \deg g(x)$).

Теорема 2. Мультипликативная группа конечного поля $\mathrm{GF}(q)$ является циклической группой порядка $q - 1$.

Доказательство. Пусть $s = p_1^{r_1} \dots p_m^{r_m}$ – разложение порядка $s = q - 1$ группы $\mathrm{GF}(q)^*$ на простые сомножители (предполагаем $q \geqslant 3$). Для каждого i, $1 \leqslant i \leqslant m$, многочлен $x^{s/p_i} - 1$ имеет не более s/p_i корней в поле $\mathrm{GF}(q)$. Так как $s/p_i < s$, то в $\mathrm{GF}(q)^*$ имеются элементы, не являющиеся корнями этого многочлена. Пусть a_i – такой элемент; положим $b_i = a_i^{s/p_i^{r_i}}$. Тогда $b_i^{p_i^{r_i}} = 1$, откуда следует, что порядок элемента b_i делит число $p_i^{r_i}$. Но $b_i^{p_i^{r_i-1}} = a_i^{s/p_i} \neq 1$, так что порядок элемента b_i равен $p_i^{r_i}$. Убедимся теперь, что элемент $b = b_1 b_2 \dots b_m$ имеет порядок s (сравните с упр. 2 § 7). Если предположить, что порядок элемента b является собственным делителем числа s, то он делит, по крайней мере, одно из m целых чисел s/p_i, скажем, s/p_1. Тогда $1 = b^{s/p_1} = b_1^{s/p_1} b_2^{s/p_2} \dots b_m^{s/p_m}$. Так как s/p_1 делится на $p_i^{r_i}$ при всех i таких, что $2 \leqslant i \leqslant m$, то $b_i^{s/p_1} = 1$. Поэтому $b_1^{s/p_1} = 1$, откуда следует, что порядок элемента b_1 должен делить число s/p_1, а это невозможно, поскольку он равен $p_1^{r_1}$. Итак, $\mathrm{GF}(q)^*$ – циклическая группа с образующим элементом b.

Определение. Элемент b конечного поля K, порождающий мультипликативную группу K^* этого поля, называется *примитивным*. Неприводимый многочлен, корнем которого является примитивный элемент, называется *примитивным многочленом*.

Пример. Над полем $\mathrm{GF}(2)$ многочлен $x^4 + x^3 + 1$ является примитивным (любой его корень имеет 15 разных степеней: $b^0 = 1$, b, b^2, ... , b^{14}), а неприводимый многочлен $x^4 + x^3 + x^2 + x + 1$ не примитивен, так как любой корень a этого уравнения очевидно удовлетворяет уравнению $a^5 = 1$.

В заключение приведем без доказательства теорему, связывающую аддитивную и мультипликативную структуры конечного поля.

Теорема 3. В каждом конечном поле $\mathrm{GF}(p^n)$, рассматриваемом как векторное пространство над $\mathrm{GF}(p)$, существует базис из элементов b, b^p, $\ldots$, $b^{p^{n-1}}$, где b – некоторый примитивный элемент поля $\mathrm{GF}(p^n)$.

Упражнения.

1. Используя следствие 2 из теоремы 1, докажите следующую теорему Вильсона: для каждого простого числа p число $(p-1)!+1$ делится на p.

2. Докажите примитивность следующих многочленов над полем $\mathrm{GF}(2)$: x^4+x+1, x^5+x^2+1, x^6+x+1, x^7+x^3+1.

3. Докажите, что число примитивных элементов поля $\mathrm{GF}(q)$ равно $\varphi(q-1)$, где $\varphi(m)$ – это функция Эйлера натурального аргумента m, т. е. количество натуральных чисел, не превосходящих m и взаимно простых с ним.

4. Выведите из теоремы 3 следствие о существовании в поле $\mathrm{GF}(2^n)$ такого примитивного элемента b, для которого $\sum\limits_{k=0}^{n-1} b^{2^k} = 1$.

Литература

Биркгоф Г., Барти Т. Современная прикладная алгебра. М.: Мир, 1976.

Кострикин А. И. Введение в алгебру. М.: Наука, 1977.

Лидл Р., Нидеррайтер Г. Конечные поля. В 2 т. М.: Мир, 1988.

Родосский К. А. Алгоритм Евклида. М.: Наука, 1988.

Холл М. Теория групп. М.: Иностр. лит., 1962.