МИНОБРНАУКИ РОССИИ

Санкт-Петербургский государственный электротехнический
университет «ЛЭТИ» им. В. И. Ульянова (Ленина)

И. Г. ЗЕЛЬВЕНСКИЙ

ВВЕДЕНИЕ В СОВРЕМЕННУЮ АЛГЕБРУ

Санкт-Петербург
Издательство СПбГЭТУ «ЛЭТИ»
2014

УДК 512
ББК В14
З50

Зельвенский И. Г.
З50 Введение в современную алгебру: учеб. пособие. СПб.: Изд-во СПбГЭТУ «ЛЭТИ», 2014. 64 с.

ISBN 978-5-7629-1610-3

Охватывает некоторые разделы современной прикладной алгебры, мало освещенные в отечественной литературе.

Предназначено для поддержки алгебраических дисциплин на ФКТИ и РТФ, будет также полезно студентам и аспирантам других факультетов, слушателям курсов повышения квалификации.

УДК 512
ББК В14

Рецензенты: кафедра высшей математики СПбГПУ; доц. каф. высш. матем. И. М. Фролов (НИУ ИТМО).

Утверждено
редакционно-издательским советом университета
в качестве учебного пособия

ISBN 978-5-7629-1610-3

In Galois fields, full of flowers
primitive elements dance for hours
climbing sequentially through the trees
and shouting occasional parities...

Weinstein S.B. "In Galois fields"

В отличие от многих 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 шифрование, языки программирования. В учебном пособии рассмотрены базовые понятия теории групп (§ 1–9) и коммутативных колец и полей (§ 10–22), необходимые студентам ФКТИ, 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 ■, после которого может следовать подсказка. Список использованной литературы помещен в конце. Он может также служить ориентиром при углубленном изучении рассмотренных тем.

§1. ПРЯМОЕ ПРОИЗВЕДЕНИЕ МНОЖЕСТВ. ОТОБРАЖЕНИЯ

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

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 $\big(A_1 \times A_2 \neq A_2 \times A_1$ при $A_1 \neq A_2\big)$, 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:

$$A \times (B_1 \cup B_2) = (A \times B_1) \cup (A \times B_2),$$

$$A \times (B_1 \cap B_2) = (A \times B_1) \cap (A \times B_2).$$

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. ■ `Подсказка`: использовать метод математической индукции.

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 $F\colon A \to B$ 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 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 T, определяемое условием „aTb, если $ab \geqslant 0$“, рефлексивно и симметрично, но не транзитивно, так как $1T0,\ 0T(-1)$, но не $1T(-1)$.

4. 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: $A\backslash T$).

5. Пусть $\mathbb{Z}$ означает множество целых, а $\mathbb{N}$ – множество натуральных чисел. На прямом произведении $\mathbb{Z} \times \mathbb{N}$ отношение эквивалентности $\sim$ определим следующим образом: $(a, b) \sim (c, d)$ тогда и только тогда, когда $ad = bc$. Соответствующее фактормножество называют *рациональными числами* и обозначают символом $\mathbb{Q}$ (пару (a, b) можно рассматривать как дробь $\frac{a}{b}$).

6. 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).

7. Рассмотрим множество $\mathbb{Z}$ всех целых чисел, зафиксируем положительное число $n \in \mathbb{Z}$ и введем на $\mathbb{Z}$ отношение сравнения $a \equiv b \pmod{n}$, если $a-b$ делится (нацело) на n. Множество $\mathbb{Z}$ оказывается, таким образом, разбитым на классы эквивалентности $K_0, K_1, \ldots, K_{n-1}$, 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 через $\mathbb{Z}_n$.

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 C, для которого равенство $F(a) = F(c)$ равносильно отношению aTc. ■ `Подсказка`: в качестве множества C возьмите фактормножество $A\backslash T$.

Следствием из этой теоремы является следующая теорема об отображениях множеств.

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 $F(a) = F(b)$“. ■

Упражнение

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.

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

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 A называется *ассоциативной*, если $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ для любых a, b, c из A.

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

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

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

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

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

– операция $\cdot$ ассоциативна;

– в G существует нейтральный элемент e;

– 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 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 через a^{-1}.

3. Множество целых чисел образует бесконечную 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 (0, естественно, не имеет обратного элемента). Нейтральный элемент – это число 1.

5. Множество из двух чисел $\{1, -1\}$ образует абелеву группу относительно умножения.

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

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

8. *Группа кватернионов* является примером конечной некоммутативной группы, состоящей из p^3 элементов при простом p. (Можно доказать, что все группы, содержащие p или p^2 элементов, коммутативны.) Эта группа состоит из восьми элементов: 1, -1, i, $-i$, j, $-j$, k, $-k$ (здесь знак минус служит только различительным значком при задании некоторых элементов). Операция умножения в группе задается таблицей

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

Правила умножения кватернионов удобно описывать следующими соотношениями: $i^2 = j^2 = k^2 = -1$, $ij = k = -ji$, $jk = i = -kj$, $ki = j = -ik$.

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. Найдите все возможные бинарные операции на множестве $G = \{e, a, b, c\}$, задающие на G структуру группы с нейтральным элементом e. Приведите только те примеры, которые не преобразуются друг в друга перестановкой символов a, b и c.

3. Докажите, что множество Ω всех подмножеств непустого множества M является абелевой группой относительно операции *симметрической разности*

$$A \triangle B = (A \setminus B) \cup (B \setminus A).$$

4. Докажите, что если $g^2 = e$ для любого элемента группы G, то эта группа абелева (примером подобной группы является группа из предыдущего упражнения).

5. 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?

6. Докажите, что множество $S(M)$ биективных отображений множества M на себя с операцией, введенной в упражнении 5, образует группу.

Рассмотрим группу $S(M)$ из упражнения 6 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 через S_n и называют *симметрической* группой степени n. 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 $a_i = s(i)$, $s \in S_n$, $i = 1, 2, \ldots, n$. 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 через $(a_{i_1}, a_{i_2}, \ldots, a_{i_k})$).

7. Докажите, что любую подстановку множества из n элементов можно представить в виде произведения *независимых* (непересекающихся) 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 7 § 3.

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

Лемма 1. Чтобы подмножество H группы G являлось подгруппой необходимо и достаточно:

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

– чтобы вместе с каждым $a \in H$ обратный элемент a^{-1} также принадлежал H. ■

Замечание 1. 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 $a - b$). ■

Замечание 2. Если H – конечное подмножество группы G, то второе условие леммы излишне. ■

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

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 в 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 любой гомоморфизм всегда переводит 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. ■

Замечание. Если $f : G_1 \to G_2$ – гомоморфизм групп, то образ всей группы $f(G_1)$ называют также *образом гомоморфизма* f и обозначают $\operatorname{Im} f$.

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 $(\mathbf{R}^+, \cdot)$ положительных чисел (относительно умножения), то такое отображение f является взаимно однозначным (обратное отображение – логарифм) и поэтому f осуществляет изоморфизм между $(\mathbb{R}, +)$ и $(\mathbb{R}^+, \cdot)$.

7. Линейное отображение векторных пространств переводит сумму векторов в сумму и потому является гомоморфизмом аддитивных групп 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: $\mathrm{id}(x) = x$.

Определение. *Порядком* $|G|$ конечной группы G называется число элементов этой группы.

Следующая теорема показывает, что подгруппами конечных симметрических групп исчерпываются по существу все конечные группы.

Теорема (Кэли). Всякая конечная группа порядка n изоморфна некоторой подгруппе симметрической группы S_n.

Доказательство. Предположим, что группа G имеет порядок n и пусть ее элементы, записанные в определенном порядке, будут

$$g_1,\ g_2,\ \ldots,\ g_n\,.$$

Если s – произвольный элемент группы G, то все произведения $g_i s = g_{k_i}$ $(i = 1,\, 2, \ldots,\, n)$ различны между собою, т. е. упорядоченный набор

$$g_{k_1},\ g_{k_2},\ \ldots,\ g_{k_n}$$

снова содержит все элементы группы G и отличается от первоначального лишь расположением элементов. Элементу s ставится в соответствие подстановка

$$\begin{pmatrix} 1 & 2 & \ldots & n \\ k_1 & k_2 & \ldots & k_n \end{pmatrix}.$$

Таким образом, каждому элементу группы G ставится в соответствие вполне определенная подстановка n-ой степени. Двум различным элементам соответствуют различные подстановки, так как из $g_i s = g_i s'$ следовало бы $s = s'$. Найдем подстановку, соответствующую произведению st, где t снова есть некоторый элемент группы G. Если элементу t соответствует подстановка

$$\begin{pmatrix} k_1 & k_2 & \ldots & k_n \\ l_1 & l_2 & \ldots & l_n \end{pmatrix},$$

т. е. $g_{k_i} t = g_{l_i}$, то из $g_i(st) = g_{k_i} t = g_{l_i}$ следует, что элементу st соответствует подстановка

$$\begin{pmatrix} 1 & 2 & \ldots & n \\ l_1 & l_2 & \ldots & l_n \end{pmatrix},$$

являющаяся, очевидно, произведением

$$\begin{pmatrix} 1 & 2 & \dots & n \\ k_1 & k_2 & \dots & k_n \end{pmatrix} \cdot \begin{pmatrix} k_1 & k_2 & \dots & k_n \\ l_1 & l_2 & \dots & l_n \end{pmatrix}.$$

Этим доказано, что группа G изоморфно отображается на некоторую подгруппу группы S_n.

Следствие. Существует лишь конечное число неизоморфных конечных групп фиксированного порядка n.

Доказательство. Это утверждение немедленно следует из теоремы Кэли, если учесть, что конечная группа может обладать лишь конечным числом подгрупп.

Замечание. Теорема Кэли может быть перенесена и на бесконечные группы. В этом случае группа $S(G)$ всех биективных отображений группы G на себя (см. упр. 6 §3) зависит только от *мощности* группы G.

Упражнения

1. Докажите, что комплексные матрицы $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$, $\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$, $\begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}$, $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$, $\begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}$ образуют группу по умножению, изоморфную группе кватернионов (см. пример 8 §3).

2. Опишите все подгруппы симметрической группы S_3.

3. Являются ли множества подстановок $A = \{(1), (12)(34), (13)(24), (14)(23)\}$ и $B = \{(1), (123), (132), (1243)\}$ подгруппами симметрической группы S_4?

4. Найдите две подгруппы симметрической группы S_4, содержащие по 4 элемента, но не изоморфные друг другу.

§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 $\{ah : h \in H\}$. Далее мы будем использовать обозначение aH (вместо более абстрактной записи K_a из §2) 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. *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 следующая 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.

Замечание. Обратное утверждение неверно: если порядок n группы G делится на m, то G может не иметь подгруппу порядка m. Примером может служить знакопеременная группа A_4 порядка 12, не имеющая подгрупп порядка 6. Однако, если делитель m является степенью простого числа, то подгруппа такого порядка в группе G обязательно найдется (теорема Силова).

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_2a 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 все матрицы вида tE, где E – единичная матрица, а t – 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 $\operatorname{Im} f \subset G_2$.

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

$$f(x^{-1}hx) = f(x^{-1})f(h)f(x) = f(x^{-1})e_2f(x) =$$
$$= f(x^{-1})f(x) = f(x^{-1}x) = f(e_1) = e_2,$$

откуда $x^{-1}Hx \subset H$, 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 $f(x)$.

Обратим 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 следующая 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 $f(a) = f(b)$ равносильно тому, 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 $\operatorname{Im} f$ 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.

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 $f(t) = e^{2\pi it} = \cos 2\pi t + i \sin 2\pi t$ 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 $\operatorname{Im} f = U = \{z \in \mathbb{C} : |z| = 1\}$ – 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. Найдите все подгруппы группы кватернионов (пример 8 §3) и докажите, что каждая из них является нормальной.

3. Перечислите все подгруппы симметрической группы S_3. Какие из них являются нормальными подгруппами?

4. Пусть $H_1 \subset H_2$ – две подгруппы группы G. Докажите, что если индекс $(G : H_1)$ конечен, то имеет место обобщение теоремы 1:

$$(G : H_1) = (G : H_2) \cdot (H_2 : H_1).$$

5. Докажите, что $(S_n : A_n) = 2$, т. е. порядок знакопеременной группы A_n (см. пример 5 §4) равен $\frac{1}{2}\, n!$.

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

7. Пусть G – группа и H – ее единственная подгруппа, имеющая порядок n. Докажите, что H – нормальная подгруппа.

8. Докажите, что знакопеременная группа A_4 не имеет подгрупп порядка 6.

9. 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.

10. Пусть G_1 и G_2 – две конечные группы, порядки которых взаимно просты. Докажите, что существует ровно один гомоморфизм группы G_1 в группу G_2.

§6. ДЕЙСТВИЕ ГРУППЫ НА МНОЖЕСТВЕ

Пусть M – конечное множество, содержащее n элементов, а G – произвольная *группа перестановок* множества M, т. е. подгруппа симметрической группы S_n (см. §3). Для любого $m \in M$ *орбитой* элемента m называется множество

$$G(m) = \{g(m) \,:\, g \in G\}.$$

Лемма 1. Любые две орбиты $G(m_1)$ и $G(m_2)$ или совпадают, или не пересекаются.

Доказательство. Предположим, что $G(m_1) \cap G(m_2) \neq \varnothing$. Пусть $m \in G(m_1) \cap G(m_2)$. Тогда существуют такие элементы g_1 и g_2 из группы G, что $m = g_1(m_1) = g_2(m_2)$. Возьмем произвольный $s \in G(m_1)$. Элемент $s = g_3(m_1)$ для некоторого $g_3 \in G$, но $m_1 = g_1^{-1}(g_2(m_2))$, поэтому $s = g_3(g_1^{-1}(g_2(m_2))) = (g_3 \cdot g_1^{-1} \cdot g_2)(m_2)$ и $s \in G(m_2)$. Следовательно, $G(m_1) \subset G(m_2)$. Аналогично доказывается и обратное включение.

Следствие. Множество M распадается в объединение непересекающихся подмножеств – орбит группы G.

Может оказаться, что все множество M совпадает с единственной орбитой: $M = G(m)$. В этом случае группа G называется *транзитивной*. Все другие группы перестановок называются *интранзитивными*.

Упражнения

1. Группа симметрий D_n правильного n-угольника (группа всех самосовмещений правильного n-угольника в трехмерном пространстве) называется *группой диэдра*. Проверьте, что D_n – некоммутативная группа порядка $2n$. Докажите, что D_n – транзитивная группа.

Замечание. В частности $|D_3| = 6$, и поэтому $D_3 = S_3$. $|D_4| = 8$ и группа D_4 (наряду с группой кватернионов) является еще одним примером некоммутативной группы порядка 8.

При рассмотрении пространственных тел назовем прямую *осью симметрии n-го порядка*, если тело совмещается с собой при вращениях вокруг этой прямой на углы, кратные $\frac{2\pi}{n}$. Например, у тетраэдра 4 оси симметрии 3-го порядка – они проходят через вершины 1, 2, 3, 4, и центры противолежащих граней. Соответствующие вращения помимо тождественного описываются подстановками типа (2 3 4), (2 4 3) и т. п. Кроме того имеются 3 оси симметрии 2-го порядка, проходящие через середины противоположных ребер – им соответствуют подстановки типа (1 4)(2 3). Всего вместе с тождественным преобразованием получается $1+4\cdot 2+3 = 12$ подстановок, образующих *группу вращений тетраэдра*, изоморфную знакопеременной группе A_4.

2. Докажите, что группа диэдра D_4 и группа кватернионов не изоморфны.

3. Докажите, что группа вращений куба (а значит, и *двойственного* многогранника – октаэдра) изоморфна симметрической группе S_4.

Замечание. Группа вращений икосаэдра и додекаэдра изоморфна знакопеременной группе A_5. У этих многогранников 6 осей симметрии порядка 5, 10 осей порядка 3 и 15 осей порядка 2.

В связи с разбиением группой перестановок G множества M на орбиты возникают следующие два важных вопроса:

– на какое количество орбит разбивается множество M?

– какова *длина* каждой из этих орбит, т. е. из скольких элементов они состоят?

Вначале ответим на второй вопрос.

Определение. *Стабилизатором* G_m элемента $m \in M$ называется множество перестановок из G, для которых элемент m неподвижен:

$$G_m = \{g \in G : g(m) = m\}.$$

Лемма 2. Стабилизатор любого элемента является подгруппой группы G. ■

Теорема 1. Длина орбиты $G(m)$ равна индексу стабилизатора G_m в группе G, т. е.

$$|G(m)| = (G : G_m).$$

Доказательство. Пусть $G_m = \{h_0 = e, h_1, \ldots, h_{s-1}\}$, а элементы $a_0 = e, a_1, \ldots, a_{t-1} \in G$ образуют множество всех представителей левых смежных классов по подгруппе G_m. Тогда элементы группы G можно записать в виде следующей таблицы:

$$\begin{array}{ccccc} a_0h_0, & a_0h_1, & a_0h_2, & \ldots & a_0h_{s-1}, \\ a_1h_0, & a_1h_1, & a_1h_2, & \ldots & a_1h_{s-1}, \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ a_{t-1}h_0, & a_{t-1}h_1, & a_{t-1}h_2, & \ldots & a_{t-1}h_{s-1}. \end{array}$$

Эти элементы попарно различны и исчерпывают всю группу G. Для любого $j = 0, 1, \ldots, t-1$ применение s перестановок, образующих j-ю строку таблицы, к элементу m дает один и тот же элемент $a_j(m)$. Все t элементов $a_j(m)$ попарно различны. Действительно, если бы $a_j(m) = a_k(m)$ для некоторых j, k, то $m = a_j^{-1}a_k(m)$, т. е. перестановка $a_j^{-1}a_k \in G_m$. Но это возможно только, когда a_j и a_k содержатся в одном левом смежном классе группы G по подгруппе G_m, чего быть не может.

Таким образом, длина орбиты $G(m)$ равна числу строк в таблице, а это и есть индекс стабилизатора G_m.

Следствие. Длина любой орбиты относительно группы перестановок G является делителем порядка группы G.

Доказательство. Это следствие немедленно вытекает из теоремы Лагранжа (теорема 1 §5).

Вернемся теперь к вопросу о числе орбит.

Пусть $\mathrm{Fix}(g)$ – число неподвижных точек перестановки g, $N(G)$ – число орбит группы перестановок $G = \{g_0 = e, g_1, \ldots, g_{k-1}\}$, действующей на множестве $M = \{1, 2, \ldots, n\}$.

Теорема 2 (лемма Бернсайда). Для любой группы перестановок имеет место равенство

$$N(G) = \frac{1}{|G|} \sum_{g \in G} \mathrm{Fix}(g).$$

Доказательство. Построим матрицу размера $|G| \times n$, строки которой нумеруются элементами $g_j \in G$, а столбцы – элементами множества $M = \{1, 2, \ldots, n\}$. На пересечении строки g_j и столбца m поставим 1, если $g_j(m) = m$ (перестановка g_j сохраняет элемент m), и 0 – в противном случае. В каждом столбце с номером m стоит ровно $|G_m|$ единиц, где

G_m – стабилизатор m. Таким образом, число всех единиц матрицы равно $\sum\limits_{m\in M}|G_m|$. По теореме 1

$$\sum m \in M|G_m| = \sum_{m\in M}\frac{|G|}{|G(m)|} = |G|\sum_{m\in M}\frac{1}{|G(m)|}.$$

Так как для всех точек m одной орбиты длина орбиты $|G(m)|$ одинакова, то последняя сумма равна $\sum\limits_{i=1}^{N(G)} 1 = N(G)$ – числу орбит группы G на множестве M.

С другой стороны, в каждой строке матрицы число единиц совпадает с числом неподвижных элементов $\mathrm{Fix}(g_j)$ перестановки g_j, откуда $|G|\cdot N(G) = \sum\limits_{i=0}^{k-1}\mathrm{Fix}(g_j)$, что и требовалось доказать.

Следствие. Если G – транзитивная группа перестановок на множестве M, то $|G| = \sum\limits_{g\in G}\mathrm{Fix}(g)$.

Применим лемму Бернсайда к решению следующей комбинаторной задачи: сколькими способами можно раскрасить вершины тетраэдра в три цвета (например, *б* – белый, *с* – синий и *к* – красный)?

Если тетраэдр жестко закреплен (или его вершины пронумерованы), то задача решается очень легко: таких раскрасок ровно $3^4 = 81$. Будем однако считать *геометрически неотличимыми* раскраски, если они совпадут после некоторого вращения тетраэдра, и уточним поставленную задачу: сколькими геометрически различными способами можно раскрасить вершины тетраэдра в три цвета?

Пусть M – множество всех фиксированных тетраэдров, окрашенных по-разному, G – группа вращений тетраэдра. Отождествим G с группой A_4, $|G| = 12$. Число геометрически различных раскрасок совпадает с числом орбит группы G на множестве M. В силу теоремы 2 число орбит N можно вычислить через числа неподвижных точек $\mathrm{Fix}(g)$ перестановок g.

8 вращений вокруг осей симметрии 3-го порядка имеют $3\cdot 3 = 9$ неподвижных точек: (*ббб*)(*б*), (*ббб*)(*с*), (*ббб*)(*к*) и т. д. 3 вращения вокруг осей симметрии 2-го порядка также имеют 9 неподвижных точек: (*бб*)(*бб*), (*бб*)(*сс*), (*бб*)(*кк*) и т. д. Тождественная подстановка имеет, естественно, 3^4 неподвижных точек, поэтому число различных орбит (геометрически различных раскрасок) равно $\frac{1}{12}\left(3^4 + 8\cdot 9 + 3\cdot 9\right) = 15$.

Рассмотрим еще один пример: сколько различных ожерелий из 7 бусин можно составить из бусин трех цветов – белого, красного и синего?

Если переформулировать эту задачу с тем, чтобы можно было использовать лемму Бернсайда, то получим следующий вопрос: сколькими геометрически различными способами можно раскрасить вершины правильного семиугольника в три цвета?

В трехмерном пространстве группу симметрий правильного семиугольника можно отождествить с группой диэдра (см. упр. 1) D_7, порядок которой равен 14. 6 вращений вокруг центра многоугольника имеют только 3 неподвижные точки $<$*бббббббб*$>$, $<$*кккккккк*$>$ и $<$*ссссссс*$>$ (перечисляем раскраски бусин по кругу). 7 вращений вокруг осей симметрии 2-го порядка имеют 3^4 неподвижных точек, например, $<$*бсбккбс*$>$. Тождественная подстановка имеет 3^7 неподвижных точек. Таким образом, число различных ожерелий равно $\frac{1}{14}\left(3^7 + 6 \cdot 3 + 7 \cdot 3^4\right) = 198$.

4. Пусть G – группа порядка p^k (p – простое), действующая на множестве из n элементов. Докажите, что если n не делится на p, то в M найдется *неподвижная точка* (т. е. точка, длина орбиты которой равна 1).

5. Докажите, что число геометрически различных раскрасок вершин куба в 3 цвета равно 333.

6. Сколько различных ожерелий из 6 бусин можно составить из бусин трех цветов?

§7. 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 через $a^2, a^3, \ldots, a^n$ (в аддитивно записанной группе эти „степени“ приобретают вид na и называются n-кратными элемента a). Положим также $a^0 = e, a^{-n} = (a^n)^{-1}$ 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 о гомоморфизмах 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 в $\mathbb{Z}$ либо нулевая, либо имеет вид $m\mathbb{Z}$, где m – натуральное число.

Доказательство. Пусть H – какая-то ненулевая подгруппа группы $\mathbb{Z}$. Так как вместе с каждым числом, принадлежащим H, эта подгруппа 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 – неполное 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 $m\mathbf{Z}$ 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 ξ группы целых чисел в мультипликативную группу $\mathbb{C}^*$ ненулевых комплексных чисел, определенный формулой $\xi(n) = e^{\frac{2\pi i}{m}n} = \cos\frac{2\pi n}{m} + i\sin\frac{2\pi n}{m}$. Так как $\xi(n) = \big(\xi(1)\big)^n$, то $\xi(\mathbb{Z})$ является множеством степеней одного элемента $\xi(1)$. Ядро $\operatorname{Ker}\xi$ – это группа $m\mathbb{Z}$, и теорема о гомоморфизмах дает нам возможность отождествить факторгруппу $\mathbf{Z}/m\mathbb{Z}$ с образом ξ. А образ ξ – это группа всех комплексных корней степени m из 1, которую мы будем далее обозначать как U_m. Таким образом, $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z} \cong U_m$.

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 U_m порядка $m \geqslant 1$.

Доказательство. Ранее показано, 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 U_m. Следовательно, в этом случае $D \cong \mathbb{Z}/\operatorname{Ker} f = \mathbb{Z}/m\mathbb{Z} \cong U_m$, что и требовалось доказать.

Отметим, что случай $m = 1$ возможен лишь для нейтрального элемента группы G.

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 $q = \frac{n}{m}$. Для

любого такого числа m существует единственная подгруппа порядка $\frac{n}{m}$ в группе G, которая порождается элементом a^m. ■

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.

Эта теорема является прямым следствием теоремы Лагранжа (теорема 1 §5). Очевидным также представляется следующее утверждение.

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 циклов (см. упр. 7 §3).

3. Найдите все гомоморфизмы группы $\mathbb{Z}_{10}$ в группу $\mathbb{Z}_6$.

4. Найдите все автоморфизмы (см. пример 8 §4) группы $\mathbb{Z}_{10}$.

§8. ПРЯМОЕ ПРОИЗВЕДЕНИЕ ГРУПП

Определение. *(Внешним) прямым произведением* произвольных групп G_1 и G_2 называется прямое произведение множеств $G_1 \times G_2$ с бинарной операцией $(a_1, a_2)(b_1, b_2) = (a_1b_1, a_2b_2)$, 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 групп (обычно абелевых) 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 через H_1H_2, если каждый элемент $g \in G$ может быть представлен в виде $g = h_1h_2$, 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 $H_1H_2 = G$, то $G \cong H_1 \times H_2$.

Доказательство. Из равенства $H_1H_2 = G$ следует, что любой элемент $g \in G$ записывается в виде $g = h_1h_2$, где $h_1 \in H_1$, $h_2 \in H_2$. Если еще $g = k_1k_2$, $k_1 \in H_1$, $k_2 \in H_2$, то $h_1h_2 = k_1k_2$, откуда $k_1^{-1}h_1 = k_2h_2^{-1} \in H_1 \cap H_2 = \{e\}$. Следовательно, $h_1 = k_1$, $h_2 = k_2$, и мы приходим к выводу, что запись $g = h_1h_2$ однозначна. Так как H_1 – нормальная подгруппа, то $h_1h_2h_1^{-1}h_2^{-1} = h_1(h_2h_1^{-1}h_2^{-1}) = h_1h_1' \in H_1$, а так как и H_2 – нормальна, то $h_1h_2h_1^{-1}h_2^{-1} = (h_1h_2h_1^{-1})h_2^{-1} = h_2'h_2^{-1} \in H_2$, т. е. $h_1h_2h_1^{-1}h_2^{-1} \in H_1 \cap H_2 = \{e\}$ и, стало быть, $h_1h_2 = h_2h_1$.

Определим теперь отображение $\varphi : G \to H_1 \times H_2$, полагая $\varphi(g) = (h_1, h_2)$ для любого $g = h_1h_2$. 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, внешнее прямое произведение $G = H_1 \times H_2$ 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 $g = h_1h_2 \ldots h_n$, где $h_j \in H_j$.

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. Легко проверяется, что $\mathbb{C} = \mathbb{R} \oplus \boldsymbol{I}$, где $\boldsymbol{I} = \{z \in \mathbb{C} : \operatorname{Re} z = 0\}$.

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

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

Отметим,что можно определить внешнее прямое произведение бесконечного числа групп. Однако, 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 осмыслено и бесконечное произведение элементов подгрупп $h_1 h_2 \ldots h_j \ldots$, поскольку фактически перемножается лишь конечное число неединичных элементов.

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 $q = \pm\frac{a}{b}$, где a и b – натуральные числа. Раскладывая числитель и знаменатель на простые множители, получаем, что $q = \pm p_1^{k_1} p_2^{k_2} \ldots p_j^{k_j} \ldots$, где все показатели k_j, кроме конечного числа, равны нулю. Ввиду однозначности разложения натуральных чисел на простые множители, такое представление q единственно. Следовательно, $\mathbb{Q}^*$ – прямое произведение бесконечного числа подгрупп $\mathbb{Q}^* = H_1 \times H_2 \times H_3 \times H_5 \times \ldots$

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 $\mathbb{Z}_m \oplus \mathbb{Z}_n$.

3. Для всех целых n от 2 до 16 найдите количество попарно неизоморфных абелевых групп порядка n.

4. Пусть $A \oplus A \cong B \oplus B$, где A и B – конечные абелевы группы. Докажите, что $A \cong B$.

5. Докажите, что конечная абелева группа порядка n, не делящегося на квадрат целого числа, большего 1, является циклической.

§9. ХАРАКТЕРЫ КОНЕЧНЫХ АБЕЛЕВЫХ ГРУПП

Определение. *Характером* абелевой группы A называется гомоморфизм группы A в мультипликативную группу точек единичной окружности $U = \{z \in \mathbb{C}^* : |z| = 1\}$.

Все абелевы группы в этом параграфе будем записывать мультипликативно. Характеры группы можно перемножать. Именно, если χ_1 и χ_2 – характеры группы A, то положим $(\chi_1\chi_2)(a) = \chi_1(a) \cdot \chi_2(a)$ для любого элемента $a \in A$. Очевидно, что $\chi_1\chi_2$ – также гомоморфизм A в U.

Относительно введенного произведения характеры образуют группу. Ассоциативность очевидна. Нейтральным элементом служит характер χ_0, тождественно равный единице (его называют *главным* или *тривиальным* характером). Обратный элемент для характера χ – это такой характер χ^{-1}, что $(\chi^{-1}(a) = \chi(a^{-1}) = (\chi(a))^{-1}$ для всех $a \in A$. Группу характеров группы A обозначают $\widehat{A}$ и называют *двойственной (дуальной)* к группе A. В силу введенного определения $\widehat{A}$ – коммутативная группа, поскольку коммутативна сама группа A.

Заметим, что для любой конечной абелевой группы A образ произвольного характера $\chi \in \widehat{A}$ никогда не равен всей группе U, ибо последняя – бесконечна. Если m – *показатель* группы A (т. е. такое число, что $a^m = 1$ для любого a), то $(\chi(a))^m = \chi(a^m) = \chi(1) = 1$, откуда $\chi(a)$ – корень степени m из 1, т. е. одно из чисел $e^{2\pi ik/m}$, $k = 0, 1, ..., m-1$. Поскольку эти числа образуют циклическую группу порядка m, то в действительности характеры – это гомоморфизмы A в U_m.

Пусть f – произвольный гомоморфизм абелевых групп $A \to B$. Построим *двойственный гомоморфизм* $\hat{f} : \widehat{B} \to \widehat{A}$ на группах характеров. Именно, для $\psi \in \widehat{B}$ положим $\hat{f}(\psi) = \chi$ – такой характер на A, что $\chi(a) = \hat{f}(\psi)(a) = \psi(f(a))$. Легко проверить, что $\hat{f}$ – действительно гомоморфизм.

Лемма. Если $f : A \to B$ – сюръективный гомоморфизм, то двойственный гомоморфизм $\hat{f} : \widehat{B} \to \widehat{A}$ является инъективным.

Доказательство. Если $\psi \in \widehat{B}$ принадлежит ядру гомоморфизма $\hat{f}$, то имеем $\chi_0 = \hat{f}(\psi)$, то есть $1 = \chi_0(a) = \hat{f}(\psi)(a) = \psi(f(a))$ для любого $a \in A$. Тогда для любого $b \in B$ имеем $b = f(a)$ (в силу сюръективности

$f(A) = B$) и поэтому $\psi(b) = \psi(f(a)) = 1$. Значит, ψ – главный характер на B, т. е. $\operatorname{Ker} \hat{f}$ единичное.

Теорема 1. Пусть группа A раскладывается в прямое произведение абелевых групп A_1 и A_2. Тогда группа $\widehat{A}$ изоморфна прямому произведению групп $\widehat{A}_1$ и $\widehat{A}_2$.

Доказательство. Рассмотрим „проекции“ A на свои сомножители A_1 и A_2: $f_1(a_1a_2) = a_1$, $f_2(a_1a_2) = a_2$. Ясно, что f_1 и f_2 – сюръективные гомоморфизмы. Соответственно имеем инъективные двойственные гомоморфизмы $\hat{f}_1 : \widehat{A}_1 \to \widehat{A}$, $\hat{f}_2 : \widehat{A}_2 \to \widehat{A}$. Построим отображение $\theta : \widehat{A}_1 \times \widehat{A}_2 \to \widehat{A}$, полагая $\theta(\chi_1, \chi_2) = \hat{f}_1(\chi_1)\hat{f}_2(\chi_2)$, где $\chi_1 \in \widehat{A}_1$, $\chi_2 \in \widehat{A}_2$. Иначе говоря, для любого $a = a_1a_2 \in A \quad (a_1 \in A_1,\ a_2 \in A_2)$ $\theta(\chi_1, \chi_2)(a) = (\hat{f}_1(\chi_1)\hat{f}_2(\chi_2))(a) = \chi_1(f_1(a))\chi_2(f_2(a)) = \chi_1(a_1)\chi_2(a_2)$. Ясно, что $\theta(\chi_1, \chi_2)$ – характер на A. Покажем, что θ – изоморфизм. Для двух пар (χ_1', χ_2') и (χ_1'', χ_2'') из $\widehat{A}_1 \times \widehat{A}_2$ имеем

$$\theta((\chi_1', \chi_2')(\chi_1'', \chi_2''))(a_1a_2) = \theta(\chi_1'\chi_1'', \chi_2'\chi_2'')(a_1a_2) =$$

$$= (\chi_1'\chi_1'')(a_1) \cdot (\chi_2'\chi_2'')(a_2) = \chi_1'(a_1)\chi_1''(a_1)\chi_2'(a_2)\chi_2''(a_2) =$$

$$= \chi_1'(a_1)\chi_2'(a_2)\chi_1''(a_1)\chi_2''(a_2) = \theta(\chi_1', \chi_2')(a_1a_2) \cdot \theta(\chi_1'', \chi_2'')(a_1a_2),$$

т. е. $\theta((\chi_1', \chi_2')(\chi_1'', \chi_2'')) = \theta(\chi_1', \chi_2') \cdot \theta(\chi_1'', \chi_2'')$. Следовательно, θ – гомоморфизм.

Если $(\chi_1, \chi_2) \in \operatorname{Ker} \theta$, то $1 = \theta(\chi_1, \chi_2)(a_1a_2) = \chi_1(a_1)\chi_2(a_2)$ для любых $a_1 \in A_1$, $a_2 \in A_2$. Полагая $a_1 = 1$, получаем $\chi_2(a_2) = 1$ для любого a_2, откуда χ_2 – главный характер на A_2; аналогично χ_1 – главный характер на A_1. Поэтому $\operatorname{Ker} \theta$ единичное и θ инъективно. Наконец, для произвольного $\chi \in \widehat{A}$ положим $\chi_1(a_1) = \chi(a_1)$, $\chi_2(a_2) = \chi(a_2)$ для $a_1 \in A_1$, $a_2 \in A_2$. Тогда $\chi_1 \in \widehat{A}_1$, $\chi_2 \in \widehat{A}_2$ и, таким образом, $\chi(a) = \chi(a_1a_2) = \chi(a_1)\chi(a_2) = \chi_1(a_1)\chi_2(a_2) = \theta(\chi_1, \chi_2)(a_1a_2)$, т. е. $\widehat{A} = \operatorname{Im} \theta$. Теорема доказана.

Теорема 1 легко обобщается по индукции на любое число прямых сомножителей.

Теорема 2. Конечная абелева группа A изоморфна своей двойственной группе $\widehat{A}$.

Доказательство. Каждая конечная абелева группа раскладывается в прямое произведение циклических групп, поэтому докажем сначала теорему для циклической группы.

Пусть A – циклическая группа порядка n с образующей a. Рассмотрим характер $\chi_1 : A \to U$, полагая $\chi_1(a) = e^{2\pi i/n}$, откуда $\chi_1(a^k) = e^{2\pi ik/n}$. Характеры $\chi_0,\ \chi_1,\ \chi_1^2, \ldots,\ \chi_1^{n-1}$ попарно различны (поскольку различны их значения на a), причем $\chi_1^n = \chi_0$. Следовательно, эти характеры образуют циклическую группу порядка n.

Пусть теперь χ – произвольный характер из $\widehat{A}$. Так как $(\chi(a))^n = \chi(a^n) = \chi(1) = 1$, то $\chi(a)$ – корень n-й степени из 1, т. е. $\chi(a) = e^{2\pi il/n} = \chi_1^l(a)$ при некотором l. Но тогда $\chi(a^k) = (\chi(a))^k = (\chi_1^l(a))^k = \chi_1^l(a^k)$, откуда $\chi = \chi_1^l$. Таким образом, циклическая группа, порожденная характером χ_1, – это вся группа характеров циклической группы A, и $\widehat{A} \cong A$.

Перейдем теперь к общему случаю. Пусть $A = A_1 \times A_2 \times \ldots \times A_m$ – прямое произведение циклических групп $A_1,\ A_2, \ldots,\ A_m$. На основании предыдущей теоремы $\widehat{A} \cong \widehat{A}_1 \times \widehat{A}_2 \times \ldots \times \widehat{A}_m$. Но $\widehat{A}_i \cong A_i$, откуда $\widehat{A} \cong A_1 \times A_2 \times \ldots \times A_m = A$.

Следствие. Пусть A – конечная абелева группа и $\widehat{A}$ – ее группа характеров. Тогда группа, двойственная к группе $\widehat{A}$, изоморфна A.

Заметим, что изоморфизм $\widehat{A} \cong A$ строился довольно искусственно. Он зависел от выбора прямых сомножителей группы A (а они определяются неоднозначно) и от выбранного изоморфизма циклических подгрупп. В то же время, изоморфизм $A \to \widehat{\widehat{A}}$ можно построить „естественно“. Именно, любому $a \in A$ можно сопоставить характер ψ_a на группе характеров $\widehat{A}$, положив $\psi_a(\chi) = \chi(a)$ для всех $\chi \in \widehat{A}$.

Теорема 3. Пусть $f : A \to B$ – инъективный гомоморфизм конечных абелевых групп. Тогда двойственный гомоморфизм $\hat{f} : \widehat{B} \to \widehat{A}$ сюръективен.

Доказательство. Положим $B_1 = \operatorname{Im} f \subset B$ и $B_2 = B/B_1$. Обозначим через g стандартный гомоморфизм группы B на факторгруппу B_2. Так как g сюръективен, то отображение $\hat{g} : \widehat{B}_2 \to \widehat{B}$ инъективно.

Докажем, что $\operatorname{Im} \hat{g} = \operatorname{Ker} \hat{f}$. Пусть $\chi \in \operatorname{Im} \hat{g}$, т. е. $\chi = \hat{g}(\psi)$, где $\psi \in \widehat{B}_2$. Значит, $\chi(b) = \psi(g(b))$, $b \in B$. Характер $\hat{f}(\chi) \in \widehat{A}$ и определен формулой $\hat{f}(\chi)(a) = \chi(f(a)) = \psi(g(f(a))) = \psi(1) = 1$, поскольку $f(a) \in \operatorname{Im} f = B_1$, а g – единичное отображение на B_1. Следовательно, $\chi \in \operatorname{Ker} \hat{f}$, т. е. $\operatorname{Im} \hat{g} \subset \operatorname{Ker} \hat{f}$. Обратно: пусть $\chi \in \operatorname{Ker} \hat{f}$. Это означает, что для любого $a \in A$ имеет место равенство $\hat{f}(\chi)(a) = \chi(f(a)) = 1$ и $f(a) \in B_1$. Определим характер $\psi \in B_2$ формулой $\psi(b_2) = \psi(g(b)) = \chi(b)$, где

$b_2 \in B_2$, $b \in B$. Это определение корректно, поскольку если $g(b) = g(b')$, то $b' = bb_0$, где $b_0 \in \operatorname{Ker} g = \operatorname{Im} f$, т. е. $b_0 = f(a)$, и $\chi(b') = \chi(bb_0) = \chi(b)\chi(f(a)) = \chi(b)\hat{f}(\chi)(a) = \chi(b)$. Для таким образом построенного характера $\psi \in \widehat{B}_2$ имеем $\hat{g}(\psi)(b) = \psi(g(b)) = \chi(b)$ для всех $b \in B$, т. е. $\hat{g}(\psi) = \chi$. Значит, $\chi \in \operatorname{Im} \hat{g}$, и $\operatorname{Ker} \hat{f} \subset \operatorname{Im} \hat{g}$. Итак, $\operatorname{Im} \hat{g} = \operatorname{Ker} \hat{f}$. На основании теоремы о гомоморфизме групп получаем теперь, что $\operatorname{Im} \hat{f} \cong \widehat{B}/\operatorname{Ker} \hat{f} = \widehat{B}/\operatorname{Im} \hat{g}$.

Посчитаем порядки этих групп. В силу инъективности $\hat{g}$ и учитывая изоморфизм двойственных групп имеем $|\operatorname{Im} \hat{f}| = |\widehat{B}\,|/|\operatorname{Im} \hat{g}| = |\widehat{B}\,|/|\widehat{B}_2| = |B|/|B_2| = |B|/|B/B_1| = |B_1| = |\operatorname{Im} f| = |A| = |\widehat{A}\,|$. Так как $\operatorname{Im} \hat{f} \subset \widehat{A}$ и $|\operatorname{Im} \hat{f}| = |\widehat{A}\,|$, то группы $\operatorname{Im} \hat{f}$ и $\widehat{A}$ совпадают. Теорема доказана.

Рассмотрим произвольную конечную абелеву группу A. Для каждой ее подгруппы A_1 определим подгруппу $A_1^* \subset \widehat{A}$ как совокупность тех характеров $\chi \in \widehat{A}$, которые действуют тривиально на A_1 (т. е. $\chi(a_1) = 1$ для всех $a_1 \in A_1$). Легко видеть, что если $A_1 \subset A_2$, то $A_1^* \supset A_2^*$; кроме того, как следует из теоремы, $A_1^* \cong \widehat{A/A_1}$. Аналогично для любой подгруппы $B \subset \widehat{A}$ можно определить подгруппу $B^* \subset A$ как совокупность тех $a \in A$, на которые действуют тривиально все характеры $\chi \in B$. Если $B_1 \subset B_2$, то так же имеем $B_1^* \supset B_2^*$. При этом $B \cong \widehat{A/B^*}$, т. е. каждая подгруппа группы характеров реализуется как группа характеров факторгруппы.

В частности, при $B = \widehat{A}$ имеем изоморфизм $\widehat{A} \cong \widehat{A/A^*}$, откуда следует, что A^* – единичная подгруппа. Это значит, что если $\chi(a) = 1$ для всех $\chi \in \widehat{A}$, то $a = 1$.

Теорема 4. Пусть χ_1, $\chi_2 \in \widehat{A}$. Тогда

$$\sum_{a \in A} \chi_1(a)\chi_2(a)^{-1} = \begin{cases} 0, & \text{если } \chi_1 \neq \chi_2; \\ |A|, & \text{если } \chi_1 = \chi_2. \end{cases}$$

Доказательство. Рассмотрим сначала сумму $S = \sum\limits_{a \in A} \chi(a)$, когда χ – не главный характер, т. е. существует фиксированный $a_1 \in A$, для которого $\chi(a_1) \neq 1$. Тогда $\sum\limits_{a \in A} \chi(aa_1) = \sum\limits_{a \in A} \chi(a) = S$, поскольку элементы aa_1 пробегают всю группу A, когда a пробегает всю группу A. С другой стороны, $S = \sum\limits_{a \in A} \chi(aa_1) = \sum\limits_{a \in A} \chi(a)\chi(a_1) = \chi(a_1)S$. Так как $\chi(a_1) \neq 1$, то равенство

$\chi(a_1)S = S$ возможно лишь при $S = 0$. Если же χ – главный характер, то $\chi(a) = 1$ для всех $a \in A$, и $\sum\limits_{a\in A} \chi(a)$ равна порядку группы A.

Применим теперь приведенные рассуждения к характеру $\chi_1\chi_2^{-1}$. Получаем

$$\sum_{a\in A} \left(\chi_1\chi_2^{-1}\right)(a) = \begin{cases} 0, & \text{если } \chi_1 \neq \chi_2; \\ |A|, & \text{если } \chi_1 = \chi_2. \end{cases}$$

Осталось заметить, что $\left(\chi_1\chi_2^{-1}\right)(a) = \chi_1(a)\chi_2(a)^{-1}$.

Следствие. Если $\chi \neq \chi_0$, то $\sum\limits_{a\in A} \chi(a) = 0$.

Теорема 5. Пусть a_1, $a_2 \in A$. Тогда

$$\sum_{\chi\in\widehat{A}} \chi(a_1)\chi(a_2)^{-1} = \begin{cases} 0, & \text{если } a_1 \neq a_2; \\ |A|, & \text{если } a_1 = a_2. \end{cases}$$

Доказательство теоремы 5 аналогично доказательству предыдущей теоремы.

Соотношения теорем 4 и 5 называются *соотношениями ортогональности.*

Упражнения

1. Определите группу характеров бесконечной циклической группы.

2. Пусть A – конечная абелева группа, B – ее собственная (т. е. $B \neq A$) подгруппа и $a \in A$, $a \notin B$. Докажите, что существует такой характер χ группы A, что $\chi(b) = 1$ для всех $b \in B$, но при этом $\chi(a) \neq 1$.

§10. КОЛЬЦА

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

– $(A, +)$ является абелевой группой;

– умножение $\cdot$ ассоциативно;

– операции сложения и умножения связаны *дистрибутивными* законами

$$(a + b)c = ac + bc, \quad c(a + b) = ca + cb$$

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:

– множество целых чисел $\mathbb{Z}$;

– множество рациональных чисел $\mathbb{Q}$;

– множество вещественных чисел $\mathbb{R}$;

– множество комплексных чисел $\mathbb{C}$;

– множество $\mathbb{O}$, состоящее из одного числа 0;

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

– множество $\mathbb{Z}[i]$ комплексных чисел вида $m+ni$, где $m, n \in \mathbb{Z}$ (*кольцо целых гауссовых чисел*);

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

– множество многочленов с одним или несколькими неизвестными и коэффициентами из некоторого коммутативного кольца;

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

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

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

3. Пусть даны произвольное множество M и произвольное множество A. Рассмотрим множество A^M всевозможных функций на M со значениями в A, т. е. всевозможных отображений f множества M в кольцо A. Это множество отображений превращается в *полное кольцо функций*, если сумма и произведение функций будут определены, как обычно, равенствами

$$(f + g)(x) = f(x) + g(x),\ (fg)(x) = f(x) \cdot g(x) \quad x \in M.$$

Построенное кольцо будет кольцом с единицей или коммутативным, если только кольцом с единицей или соответственно коммутативным является исходное кольцо A. Если M – множество точек числовой прямой, а $A = \mathbb{R}$, то полученное кольцо будет обычным кольцом всех вещественных функций вещественного переменного.

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

4. В кольце целых чисел обратным элементом обладают только 1 и -1.

5. В кольце многочленов с вещественными коэффициентами обратимы только ненулевые вещественные числа (т. е. многочлены нулевой степени).

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. Другой иллюстрацией может служить произведение матриц

$$\begin{pmatrix} 0 & m \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & n \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

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. ■

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. Чтобы (непустое) подмножество B кольца A было его подкольцом, необходимо и достаточно, чтобы разность и произведение любых двух элементов из B снова принадлежали B. ■

Упражнения

1. Докажите, что если кольцо содержит единицу, то она единственна.

2. Докажите, что множество обратимых элементов кольца образует группу.

3. Докажите, что множество комплексных чисел вида $m + ni\sqrt{3}$, где $m, n \in \mathbb{Z}$ является кольцом с единицей и найдите группу обратимых элементов этого кольца.

4. Докажите, что любое полное кольцо функций на множестве M, содержащем не менее двух элементов, со значениями в кольце $A \neq \mathbb{O}$ обладает делителями нуля.

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

6. Индукцией по n докажите для произвольного коммутативного кольца *теорему о биноме*:

$$(a + b)^n = a^n + \frac{n!}{(n-1)!1!}a^{n-1}b + \frac{n!}{(n-2)!2!}a^{n-2}b^2 + \ldots + b^n.$$

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

8. Найдите группу обратимых элементов кольца целочисленных квадратных матриц порядка n.

§11. ПОЛЯ

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

Из определения немедленно следует, что поле всегда содержит единицу.

Примеры

1. Из колец примера 1 §10 полями

являются только множества рациональных, вещественных и комплексных чисел.

2. При обычных операциях полями являются:

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

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

– множество всех алгебраических дробей с одним или несколькими неизвестными и коэффициентами из некоторого коммутативного кольца без делителей нуля;

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

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

Произведение ab^{-1} в поле записывается обычно в виде *отношения* или *частного* $\frac{a}{b}$. Легко проверить, что в любом поле $(ab)^{-1} = a^{-1}b^{-1}$ и $(a^n)^{-1} = (a^{-1})^n$ при всех натуральных n. Можно положить $a^{-n} = (a^{-1})^n$ и $a^0 = 1$. Таким образом, определены целые степени любого отличного от 0 элемента a. Правила оперирования со степенями, а также с дробями вида $\frac{a}{b}$ обычные.

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. 5 §10).

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. ■ `Подсказка`: используйте биективность отображения $x \to ax$ при $a \neq 0$.

Что касается произвольного коммутативного кольца A без делителей нуля, то оно всегда может быть вложено в поле. Действительно, рассмотрим множество пар $(a, b),\ b \neq 0,$ элементов A. Введем на этом множестве

отношение $\sim$ условием:

$$(a, b) \sim (c, d) \Leftrightarrow ad = bc.$$

Отношение $\sim$ является отношением эквивалентности, ему соответствует разбиение множества пар на классы. Класс эквивалентности, в котором лежит пара (a, b), обозначается формальной „дробью“ $\frac{a}{b}$. Из определения отношения $\sim$ следует, в частности, что

$$\frac{0}{b} = \frac{0}{d}; \quad \frac{ac}{bc} = \frac{a}{b}; \quad \frac{a}{a} = \frac{c}{c}.$$

На множестве классов эквивалентности определим сложение и умножение:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}; \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

Эти операции определены *корректно*, т. е. результат не зависит от выбора представителей. По отношению к сложению символы $\frac{a}{b}$ образуют абелеву группу с нулем $\frac{0}{b}$; по отношению к умножению все ненулевые дроби образуют абелеву группу с единицей $\frac{a}{a}$ и с обратным для $\frac{a}{b}$ элементом $\frac{b}{a}$. Умножение со сложением связано дистрибутивностью. Таким образом, построено поле, которое называется *полем частных* для кольца A.

Кольцо A могло не содержать единицу – в поле частных она появляется. И наконец, кольцо A *вкладывается* в свое поле частных посредством отождествления $\frac{ab}{b} = a$.

Очевидно, что поле частных для кольца целых чисел есть поле $\mathbb{Q}$ рациональных чисел (сравните с примером 5 §2).

Упражнения

1. Проверьте, что отношение $\sim$, описанное выше, является отношением эквивалентности.

2. Проверьте, что бинарные операции на множестве классов эквивалентности, введенные для построения поля частных, определены корректно.

3. Докажите, что кольцо $\mathbb{Z}[i]$ целых гауссовых чисел не содержит делителей нуля и что полем частных для него является поле $\mathbb{Q}(i)$.

§12. ИДЕАЛЫ И КОЛЬЦА КЛАССОВ ВЫЧЕТОВ

Начиная с этого параграфа 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. Множество $n\mathbb{Z}$ – идеал кольца $\mathbb{Z}$.

2. В кольце вещественных функций идеалом является множество всех таких функций f, что $f(0) = 0$.

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

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

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

Нулевой идеал $\mathbb{O}$ 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. ■

Таким образом, подкольца $(n) = n\mathbb{Z}$ $(n = 0, 1, 2, 3, \dots)$ 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.

Пусть $H = (h)$ – главный идеал коммутативного кольца A.

Определение. 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 со смежным классом $a + H$ по подгруппе H.

Определение. Смежный класс $a + H$ называется *классом вычетов по модулю* h (или *по идеалу* 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 $a_1 \equiv a_2 \pmod h$ и $b_1 \equiv b_2 \pmod h$, то $a_1 \pm b_1 \equiv a_2 \pm b_2 \pmod h$ и $a_1b_1 \equiv a_2b_2 \pmod h$.

Определение. Кольцо A/H называется *кольцом классов вычетов по модулю* h (или *по идеалу* 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 $\mathbb{O}$. Целое положительное число m называется *характеристикой* кольца A, если $m \cdot 1 = \underbrace{1 + 1 + \cdots + 1}_{m} = 0$ 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.

Кольцо $\mathbb{Z}$, поле $\mathbb{C}$ имеют характеристику 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 $a \in A$

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

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 $\mathbb{O}$): $m = kl$, $k > 1$, $l > 1$. 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 утверждение теоремы.

Определение. Идеал H кольца A называется простым, если из того, что $ab \in H$, 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 в 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.

Доказательство немедленно вытекает из теоремы 2 § 11.

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. Пусть I_1, I_2, $I_3\ldots$ – такие идеалы кольца A, что $I_1\subset I_2\subset I_3\subset\ldots$ Покажите, что объединение $\bigcup\limits_{n=1}^{\infty} I_n$ тоже является идеалом кольца A.

3. Пусть J – идеал коммутативного кольца A. Докажите, что множество $\{x\in A : x^n\in J \text{ при некотором } n\in\mathbb{N}\}$ также будет идеалом (этот идеал называется *радикалом* идеала J).

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

5. Найдите все гомоморфизмы кольца целых чисел $\mathbb{Z}$ в кольцо $\mathbb{Z}_{10}$.

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

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

8. Сформулируйте и докажите для подполей теорему, аналогичную теореме 3 § 10.

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

§13. 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:

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

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

Примеры

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

2. Кольцо $\mathbb{Z}[i]$ целых гауссовых чисел является евклидовым кольцом с нормой $v(m + ni) = m^2 + n^2$.

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 $\{sa + tb : s, t \in D\}$. 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 $d = sa + tb$, $a = gd$, $b = hd$.

Примером подобного представления наибольшего общего делителя (НОД) в кольце $\mathbb{Z}$ может служить равенство $3 = \text{НОД}(54, 15) = 2 \cdot 54 + {} + (-7) \cdot 15$, в кольце $\mathbb{Z}_2[x]$ – $x^2 + x = \text{НОД}(x^4 + x, x^3 + x^2) = 1 \cdot (x^4 + x) + {} + (x + 1) \cdot (x^3 + x^2)$.

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 обратим.

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

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

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. ■

`Подсказка`: использовать результат леммы 2 и индукцию по $v(a)$.

Лемма 4. Если произведение ab делится на простой элемент p, то один из сомножителей должен делиться на p (говоря 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.

Упражнения

1. Докажите теорему 3.

2. Докажите, что в кольце целых чисел бесконечно много простых чисел.

§14. КОЛЬЦА МНОГОЧЛЕНОВ

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

$$a_0 + a_1 x + \cdots + a_m x^m = \sum_{k=0}^{m} a_k x^k, \ a_k \in A \qquad (*)$$

($a_0 x^0$ 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 – кольцо с единицей и *старший коэффициент* $a_k = 1$, то многочлен $f(x)$ называется *нормированным*. Если же $a_k = 0$ для всех k, то $\deg 0$ по определению равна $-\infty$.

Естественным образом определяются сумма и произведение двух многочленов. Легко проверяются неравенства

$$\deg(f+g) \leqslant \max\{\deg f, \deg g\}, \quad \deg(fg) \leqslant \deg f + \deg g.$$

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. ■

Замечание 1. Аналогично кольцу $A[x]$ определяется кольцо многочленов $A[x_1, \ldots, x_n]$ от переменных $x_1, \ldots, x_n$.

Замечание 2. Над кольцом A можно также определить (формальные) *степенные ряды*

$$a_0 + a_1 x + \ldots + a_n x^n + \ldots = \sum_{n=0}^{\infty} a_n x^n, \ a_n \in A,$$

от переменной x. Определение операций с многочленов на степенные ряды переносится непосредственным образом:

$$\sum_{n=0}^{\infty} a_n x^n + \sum_{n=0}^{\infty} b_n x^n = \sum_{n=0}^{\infty} (a_n + b_n) x^n,$$

$$\sum_{n=0}^{\infty} a_n x^n \cdot \sum_{m=0}^{\infty} b_m x^m = \sum_{k=0}^{\infty} c_k x^k, \text{ где } c_k = \sum_{n+m=k} a_n b_m.$$

Выражения вида

$$a_n x^n + a_{n+1} x^{n+1} + \ldots + a_k x^k + \ldots = \sum_{k=n}^{\infty} a_k x^k, \ a_k \in A,$$

где n – любое целое (возможно, отрицательное) число, называются (формальными) *рядами Лорана*. Сложение и умножение рядов Лорана происходит аналогично сложению и умножению степенных рядов.

Теорема 2. Если D – кольцо без делителей нуля, то в $D[x]$ имеет место равенство

$$\deg(fg) = \deg f + \deg g. \ ■$$

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.

Следствие 3. Если K – поле, то кольцо $K[x]$ вкладывается в свое поле частных – *поле рациональных дробей* от переменной x с коэффициентами в K. Обозначается это поле символом $K(x)$. Аналогично определяется поле $K(x_1, \ldots, x_n)$ рациональных дробей от нескольких переменных $x_1, \ldots, x_n$.

Теорема 3. Для любого поля K кольцо многочленов $K[x]$ является евклидовым кольцом с нормой $v(f) = \deg f$. ■ `Подсказка`: 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*.

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

Последняя теорема – частный случай теоремы 3 § 13.

Приводимость или неприводимость данного многочлена существенно зависит от поля K. Многочлен $x^2 + 1$ неприводим над $\mathbb{R}$, но приводим над полем $\mathbb{C}$: $x^2 + 1 = (x - i)(x + i)$. 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 кроме линейных квадратные многочлены с отрицательным дискриминантом. Можно доказать, что над полем $\mathbb{Q}$ существуют неприводимые многочлены любой степени.

Теорема 5. Неприводимых нормированных многочленов над произвольным полем K бесконечно много.

Доказательство. Если K – бесконечное поле, то неприводимыми будут уже все линейные многочлены $x - a$, $a \in K$. Если же поле K конечно, то можно использовать рассуждение от противного. Пусть $g_1(x)$, $g_2(x), \ldots, g_n(x)$ – все неприводимые нормированные многочлены над K. Многочлен $f(x) = g_1(x)\,g_2(x)\ldots g_n(x) + 1$ имеет хотя бы один нормированный неприводимый делитель $g(x)$, поскольку степень $f(x)$ положительна (не меньше n). Если бы $g(x)$ совпал с каким-то многочленом

$g_j(x)$, то он был бы делителем разности $f(x) - g_1(x)g_2(x)\dots g_n(x)$, т. е. делил бы 1, что невозможно.

Следствие. Над любым конечным полем существуют неприводимые многочлены сколь угодно высокой степени. ■

Замечание 3. Доказательство теоремы 5 – это идея Евклида для обоснования бесконечности множества простых чисел (упр. 2 § 13).

Упражнения

1. Проверьте, что множество $A[[x]]$ всех степенных рядов с указанными сложением и умножением (см. замечание 2) образует кольцо.

2. Проверьте, что множество $A\langle x\rangle$ всех рядов Лорана с указанными сложением и умножением (см. замечание 2) образует кольцо. Докажите, что если K – поле, то кольцо рядов Лорана $K\langle x\rangle$ является полем.

3. Докажите, что многочлен $x^4 + 4$ приводим над $\mathbb{Q}$ и найдите его разложение на неприводимые сомножители над полями $\mathbb{Q}$, $\mathbb{R}$ и $\mathbb{C}$.

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

5. Пусть B – коммутативное кольцо с единицей, A – подкольцо кольца B и $b \in B$. Для любого многочлена $f(x) = \sum\limits_{j=1}^{n} a_j x^j \in A[x]$ положим

$$f(b) = \sum_{j=1}^{n} a_j b^j \in B.$$

Докажите, что

а) отображение $\varphi_b : A[x] \to B$, определенное равенством $\varphi_b(f(x)) = f(b)$, является гомоморфизмом колец;

б) если элемент b – корень некоторого многочлена $g(x) = \sum\limits_{j=1}^{m} c_j x^j$ из кольца $A[x]$, то образ гомоморфизма φ_b совпадает с множеством

$$A[b] = \left\{ \sum_{j=1}^{m} c_j b^j : c_0,\, c_1, \dots,\, c_n \in A \right\}.$$

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

7. 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 НОД этих многочленов и его линейное представление в соответствии с теоремой 2 § 13.

8. Найдите НОД многочленов $x^4 + 1$ и $x^3 + x + 1$ над полями $\mathbb{Z}_3$ и $\mathbb{Z}_5$.

9. Пусть K – поле и f – многочлен над K степени 2 или 3. Докажите, что f неприводим тогда и только тогда, когда он не имеет корней в поле K.

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

11. Разложите многочлены на неприводимые множители:

а) $x^9 + x^8 + x^7 + x + 1$ и $x^{15} + 1$ в $\mathbb{Z}_2[x]$;

б) $x^7 + x^5 + x^4 + x^3 + x^2 + x + 1$ в $\mathbb{Z}_3[x]$;

в) $x^3 + 2x^2 + 4x + 1$ в $\mathbb{Z}_5[x]$.

§15. 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 § 12). На самом деле верна более сильная теорема.

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 § 12 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 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 обычным образом, 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

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

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

и так далее.

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. 8 § 12). Если n – размерность этого пространства (степень расширения), то число элементов расширения равно p^n.

Определение. Конечные поля, содержащие p^n элементов, называются *полями Галуа* и обозначаются $\mathbb{GF}(p^n)$.

Можно доказать, что над полем вычетов $\mathbb{Z}_p = \mathbb{GF}(p)$ 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.

Замечание. В теории конечных полей выводится формула для числа $N_q(n)$ нормированных неприводимых многочленов степени n в кольце $\mathbb{GF}(q)[x]$:

$$N_q(n) = \tfrac{1}{n} \sum_{d|n} \mu\left(\tfrac{n}{d}\right) q^d = \tfrac{1}{n} \sum_{d|n} \mu(d)\, q^{\frac{n}{d}},$$

где суммирование производится по всем (положительным) делителям n. Арифметическая функция μ, использованная в формуле – это функция Мёбиуса, определяемая на множестве натуральных чисел равенствами:

$$\mu(m) = \begin{cases} 1, \text{ если } n = 1, \\ (-1)^k, \text{ если } n - \text{произведение } k \text{ различных простых чисел}, \\ 0, \text{ если } n \text{ делится на квадрат некоторого простого числа}. \end{cases}$$

Функция Мёбиуса (как и другая функция натурального аргумента – функция Эйлера $\varphi(m)$ – см. упр. 4 § 16) *мультипликативна*, т. е. для любых взаимно простых m_1 и m_2

$$\mu(m_1 \cdot m_2) = \mu(m_1) \cdot \mu(m_2).$$

Пусть, например, $q = 2$. Тогда $N_2(2) = \frac{1}{2}(2^2 - 2) = 1$, $N_2(3) = \frac{1}{3}(2^3 - 2) = 2$, $N_2(4) = \frac{1}{4}(2^4 - 2^2) = 3$, $N_2(5) = \frac{1}{5}(2^5 - 2) = 6$, $N_2(6) = \frac{1}{6}(2^6 - 2^3 - 2^2 + 2) = 9$.

Заметим, что из приведенной формулы для $N_q(n)$ можно получить доказательство существования хотя бы одного неприводимого многочлена любой степени n в любом кольце $\mathbb{GF}(q)[x]$. А именно, учитывая, что $\mu(1) = 1$ и $\mu(m) \geqslant -1$ для всех натуральных m, получаем

$$N_q(n) \geqslant \frac{1}{n}(q^n - q^{n-1} - q^{n-2} - \ldots - q) = \frac{1}{n}\left(q^n - \frac{q^n - q}{q-1}\right) > 0.$$

Примеры

1. Многочлен $x^2 + x + 1$ неприводим над полем $\mathbb{Z}_2 = \mathbb{GF}(2)$, так как ни 0, ни 1 не являются его корнями. Построим $\mathbb{GF}(4) = \mathbb{Z}_2[x]/(x^2 + x + 1)$. Пусть j означает корень многочлена x^2+x+1 в поле $\mathbb{GF}(4)$. Тогда нетрудно составить таблицы сложения и умножения в $\mathbb{GF}(4)$, 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. $\mathbb{GF}(8) = \mathbb{Z}_2[x]/(x^3+x+1)$, так как x^3+x+1 неприводим над полем

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

$\mathbb{GF}(2)$. Общий элемент поля $\mathbb{GF}(8)$ можно записать в виде $a_0 + a_1x + a_2x^2$, или просто в виде двоичного вектора (a_0, a_1, a_2), как сделано в приведенной таблице умножения ($0 = (0, 0, 0)$ в таблице опущен).

Упражнения

1. Постройте таблицы умножения для полей $\mathbb{GF}(16) = \mathbb{Z}_2[x]/(x^4+x+1)$ и $\mathbb{GF}(9) = \mathbb{Z}_3[x]/(x^2 + 1)$.

2. Проверьте, что $N_2(20) = 52377$.

§16. МУЛЬТИПЛИКАТИВНАЯ ГРУППА КОНЕЧНОГО ПОЛЯ

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

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

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

Следствие 1. Любой элемент поля $\mathbb{GF}(q)$ 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 $\mathbb{GF}(q)$ многочлен $x^q - x$ раскладывается на линейные множители

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

Следствие 3. При $K = \mathbb{GF}(p)$ многочлен $g(x)$ из теоремы 1 §15 делит многочлен $x^{q-1} - 1$ $(q = p^n$, где $n = \deg g(x))$.

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

Доказательство. Пусть $s = p_1^{r_1} \ldots p_m^{r_m}$ – разложение порядка $s = q-1$ группы $\mathbb{GF}(q)^*$ 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 $\mathbb{GF}(q)$. Так как $s/p_i < s$, то в $\mathbb{GF}(q)^*$ 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 $b = b_1 b_2 \ldots b_m$ 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, $\mathbb{GF}(q)^*$ – циклическая группа с образующим элементом b.

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

Примеры

1. Над полем $\mathbb{GF}(2)$ многочлен $x^4 + x + 1$ (так же, как и $x^4 + x^3 + 1$) является примитивным: любой его корень α имеет 15 разных степеней – $\alpha^0 = 1, \alpha, \alpha^2, \dots, \alpha^{14}$ (иначе говоря, α порождает всю мультипликативную группу $\mathbb{GF}^*(16)$), а неприводимый многочлен $x^4 + x^3 + x^2 + x + 1$ не примитивен, так как любой корень этого уравнения очевидно удовлетворяет уравнению $\alpha^5 = 1$.

Если элементы мультипликативной группы поля $\mathbb{GF}(q)$ представлены в виде степеней фиксированного примитивного элемента $\alpha \in \mathbb{GF}(q)$, то операция умножения в этом поле становится очень простой, а сложение облегчается введением так называемого *логарифма Якоби* $L(n)$, определяемого равенством

$$1 + \alpha^n = \alpha^{L(n)}.$$

В таком случае сумма элементов α^m и α^n равна

$$\alpha^m + \alpha^n = \alpha^m(1 + \alpha^{n-m}) = \alpha^{m+L(n-m)}.$$

При таком представлении элементов конечного поля (в виде 0 и степеней примитивного элемента α) для удобства вычислений можно ввести еще один формальный символ $-\infty$, такой, что $\alpha^{-\infty} = 0$.

2. Рассмотрим поле $\mathbb{GF}(8) = \mathbb{Z}_2[x]/(x^3 + x + 1)$, примитивный элемент $\alpha = (0, 1, 0)$. Вычисляем последовательно степени α: $\alpha^3 = 1 + \alpha$, $\alpha^4 = \alpha + \alpha^2$, $\alpha^5 = \alpha^2 + \alpha^3 = 1 + \alpha + \alpha^2$, $\alpha^6 = \alpha + \alpha^2 + \alpha^3 = 1 + \alpha^2$.

Таким образом, $1+\alpha = \alpha^3$, $1+\alpha^2 = \alpha^6$, $1+\alpha^3 = \alpha$, $1+\alpha^4 = 1+\alpha+\alpha^2 = = \alpha^5$, $1+\alpha^5 = \alpha^4$, $1+\alpha^6 = \alpha^2$. Получаем следующую таблицу логарифмов:

n	$-\infty$	0	1	2	3	4	5	6
$L(n)$	0	$-\infty$	3	6	1	5	4	2

3. Рассмотрим поле $\mathbb{GF}(9) = \mathbb{Z}_3[x]/(x^2+x+2)$, примитивный элемент $\alpha = (0,1,0)$. Вычисляем степени α (см. начало параграфа): $\alpha^2 = 1+2\alpha$, $\alpha^3 = 2+2\alpha$, $\alpha^4 = 2$, $\alpha^5 = 2\alpha$, $\alpha^6 = 2+\alpha$, $\alpha^7 = 1+\alpha$.

Следовательно, $1+1 = 2 = \alpha^4$, $1+\alpha = \alpha^7$, $1+\alpha^2 = 2+2\alpha = \alpha^3$, $1+\alpha^3 = 2\alpha = \alpha^5$, $1+\alpha^4 = 0$, $1+\alpha^5 = 1+2\alpha = \alpha^2$, $1+\alpha^6 = \alpha$, $1+\alpha^7 = 2+\alpha = \alpha^6$. Получаем таблицу логарифмов:

n	$-\infty$	0	1	2	3	4	5	6	7
$L(n)$	0	4	7	3	5	$-\infty$	2	1	6

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

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

Упражнения

1. Докажите, что мультипликативная группа бесконечного поля не может быть циклической группой.

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

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

4. Докажите, что число примитивных элементов поля $\mathbb{GF}(q)$ 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.

5. Пусть $q = p^n$. Докажите, что при $p = 2$ все элементы поля $\mathbb{GF}(q)$ являются квадратами, а при $p > 2$ квадраты группы $\mathbb{GF}^*(q)$ образуют в ней подгруппу индекса 2.

6. Постройте таблицы логарифмов Якоби для полей $\mathbb{GF}(16)$ и $\mathbb{GF}(17)$.

7. Выведите из теоремы 3 следствие о существовании в поле $\mathbb{GF}(2^n)$ такого примитивного элемента β, *след* которого $\mathrm{Tr}(\beta) = \sum\limits_{k=0}^{n-1} \beta^{2^k} = 1$.

§17. ХАРАКТЕРЫ КОНЕЧНЫХ ПОЛЕЙ И СУММЫ ГАУССА

Определение. Пусть $\mathbb{GF}(q)$ – конечное поле, $q = p^n$. Характеры его мультипликативной группы $\mathbb{GF}^*(q)$ и аддитивной группы $(\mathbb{GF}(q), +)$ называются соответственно мультипликативными и аддитивными характерами поля $\mathbb{GF}(q)$.

Соответствующие группы характеров поля $\mathbb{GF}(q)$ обозначим через $\widehat{\mathbb{GF}^*(q)}$ и $\widehat{\mathbb{GF}(q)}$. Условимся обозначать мультипликативные и аддитивные характеры поля $\mathbb{GF}(q)$ соответственно буквами χ и ψ с индексами.

Так как группа $\mathbb{GF}^*(q)$ – циклическая порядка $q-1$, то по теореме 2 § 9 группа $\widehat{\mathbb{GF}^*(q)}$ – циклическая порядка $q-1$. Следовательно все мультипликативные характеры поля $\mathbb{GF}(q)$ имеют своими порядками делители числа $q-1$ (причем для каждого делителя d числа $q-1$ существует $\varphi(d)$ характеров порядка d – см. упражнение 4 § 16). Группа $(\mathbb{GF}(q),+)$ является прямой суммой n групп $\mathbb{Z}_p$ и, значит, все нетривиальные аддитивные характеры поля $\mathbb{GF}(q)$ имеют порядок p.

Установим связи между мультипликативными и аддитивными характерами поля $\mathbb{GF}(q)$. Для этого понадобятся так называемые суммы Гаусса.

Определение. *Суммой Гаусса* для мультипликативного характера χ и аддитивного характера ψ поля $\mathbb{GF}(q)$ называется комплексное число

$$G(\chi,\psi)=\sum_{c\in\mathbb{GF}^*(q)}\chi(c)\psi(c).$$

Модуль суммы $G(\chi,\psi)$, очевидно, не превышает $q-1$, но, как правило, гораздо меньше, что вытекает из следующей теоремы. Через χ_0 и ψ_0 будем обозначать нейтральные элементы соответствующих групп характеров (главные характеры).

Теорема 1. Пусть χ – некоторый мультипликативный, а ψ – аддитивный характеры поля $\mathbb{GF}(q)$. Тогда сумма Гаусса $G(\chi,\psi)$ удовлетворяет следующим соотношениям:

$$\text{а) } G(\chi,\psi)=\begin{cases} q-1, & \text{если } \chi=\chi_0,\ \psi=\psi_0,\\ -1, & \text{если } \chi=\chi_0,\ \psi\neq\psi_0,\\ 0, & \text{если } \chi\neq\chi_0,\ \psi=\psi_0,\end{cases}$$

$$\text{б) } |G(\chi,\psi)|=\sqrt{q},\ \text{если } \chi\neq\chi_0,\ \psi\neq\psi_0.$$

Доказательство. $G(\chi_0,\psi_0)=\sum\limits_{c\in\mathbb{GF}^*(q)}1=q-1$. Если $\chi\neq\chi_0$, то $G(\chi,\psi_0)=\sum\limits_{c\in\mathbb{GF}^*(q)}\chi(c)=0$ в силу следствия из теоремы 4 § 9. Если же $\psi\neq\psi_0$, то в силу того же следствия $G(\chi_0,\psi)=\sum\limits_{c\in\mathbb{GF}^*(q)}\psi(c)=$
$=\sum\limits_{c\in\mathbb{GF}(q)}\psi(c)-\psi(0)=0-1=-1$.

Предположим теперь, что $\chi\neq\chi_0$ и $\psi\neq\psi_0$. В этом случае

$$|G(\chi,\psi)|^2 = \overline{G(\chi,\psi)}G(\chi,\psi) =$$
$$= \sum_{c_1\in\mathbb{GF}^*(q)}\sum_{c_2\in\mathbb{GF}^*(q)} \overline{\chi(c_1)}\,\overline{\psi(c_1)}\chi(c_2)\psi(c_2) =$$
$$= \sum_{c_1\in\mathbb{GF}^*(q)}\sum_{c_2\in\mathbb{GF}^*(q)} \chi(c_1^{-1}c_2)\psi(c_2-c_1)$$

(учитываем, что $\overline{\chi(c)} = \chi(c)^{-1}$ для всех c, поскольку $\chi(c) \in U$ – группе комплексных чисел с модулем 1). Во внутренней сумме перейдем к новой переменной $d = c_1^{-1}c_2$; тогда

$$|G(\chi,\psi)|^2 = \sum_{c_1\in\mathbb{GF}^*(q)}\sum_{d\in\mathbb{GF}^*(q)} \chi(d)\psi(c_1d-c_1) =$$
$$= \sum_{d\in\mathbb{GF}^*(q)} \chi(d)\left(\sum_{c_1\in\mathbb{GF}(q)} \psi(c_1(d-1)) - \psi(0)\right) =$$
$$= \sum_{d\in\mathbb{GF}^*(q)} \chi(d) \sum_{c_1\in\mathbb{GF}(q)} \psi(c_1(d-1))$$

(в последнем равенстве опять использовали следствие из теоремы 4 § 9). Внутренняя сумма равна q, если $d = 1$, и равна 0 в остальных случаях. Поэтому $|G(\chi,\psi)|^2 = \chi(1)\,q = q$, что и требовалось.

Используя соотношения ортогональности (теоремы 4 и 5 § 9), несложно выяснить взаимосвязь между мультипликативными и аддитивными характерами поля $\mathbb{GF}(q)$.

Теорема 2. Пусть χ и ψ соответственно мультипликативный и аддитивный характеры поля $\mathbb{GF}(q)$. Тогда для любого $c \in \mathbb{GF}^*(q)$ выполняются соотношения:

$$\chi(c) = \tfrac{1}{q}\sum_{\psi\in\widehat{\mathbb{GF}(q)}} G(\chi,\overline{\psi})\psi(c); \quad \psi(c) = \tfrac{1}{q-1}\sum_{\chi\in\widehat{\mathbb{GF}^*(q)}} G(\overline{\chi},\psi)\chi(c). \quad \blacksquare$$

Эти тождества можно рассматривать как разложения Фурье, в которых коэффициентами Фурье являются суммы Гаусса.

§18. КОДИРОВАНИЕ И ДЕКОДИРОВАНИЕ

Предположим, что задано *дискретное сообщение*, представляющее собой строку символов некоторого конечного алфавита A. При передаче сообщения по каналу связи оно может исказиться под воздействием помех и очередной переданный символ с ненулевой вероятностью p будет принят неправильно. Эффективным методом увеличения надежности передачи информации является использование *кодирования*. Последовательность символов, подлежащая передаче, кодируется более длинной последовательностью тех же символов по определенной схеме. Приемник, анализируя дополнительную информацию, содержащуюся в дополнительных символах, восстанавливает первоначально переданное сообщение.

Далее будем использовать самую простую и достаточно реалистичную модель канала связи, которая называется *двоичным симметричным каналом* (ДСК). Алфавит A образован двумя символами 0 и 1 – отождествим его с полем Галуа $\mathbb{I} = \mathbb{GF}(2)$, каждый символ принимается правильно с вероятностью $q = 1 - p > 1/2$ и ошибочно с вероятностью $p < 1/2$. Кроме того предполагается, что ошибки при передаче последовательных символов происходят *независимо*. В курсе теории вероятностей выводится следующая формула Бернулли.

Теорема. Пусть по ДСК передается сообщение из 0 и 1 длины n. Вероятность того, что оно будет принято с ровно m ошибками, равна

$$C_n^m p^m q^{n-m} = \frac{n!}{m!(n-m)!} p^m (1-p)^{n-m}.$$

Определение. *Двоичным линейным* $[n, k]$*-кодом* V называется подпространство размерности k арифметического векторного (линейного) пространства $\mathbb{I}^n$, рассматриваемое вместе с парой линейных отображений $\mathcal{C} : \mathbb{I}^k \to \mathbb{I}^n$ (*схема кодирования*) и $\mathcal{D} : \mathbb{I}^n \to \mathbb{I}^k$ (*схема декодирования*), $V = \operatorname{Im} \mathcal{C}$. Отображения $\mathcal{C}$ и $\mathcal{D}$ выбираются таким образом, чтобы суперпозиция отображений $\mathcal{D} \circ \mathcal{E} \circ \mathcal{C}$, где $\mathcal{E} : \mathbb{I}^n \to \mathbb{I}^n$ – „функция ошибок“, с вероятностью, близкой к 1, была тождественной. Элементы кода, т. е. образа оператора $\mathcal{C}$, называются *кодовыми словами*, число n – их *длиной*, а отношение $R = k/n$, являющееся одной из характеристик эффективности кода, называется его *скоростью*. (Ясно, что суперпозиция $\mathcal{D} \circ \mathcal{C}$ должна быть тождественной, чтобы сообщение было принято правильно при отсутствии помех.)

Примеры

1. $[n, k = n - 1]$-код с „проверкой на четность“ позволяет *обнаруживать* (но не исправлять) одиночную ошибку. Схема кодирования определяется так:

$$\mathcal{C}(u_1, u_2, \ldots, u_k) = \left(u_1, u_2, \ldots, u_k, \sum_{i=1}^{k} u_i \right)$$

(напоминаем, что все операции выполняются в поле $\mathbb{I} = \mathbb{GF}(2)$).

Соответствующая схема декодирования такова:

$$\mathcal{D}(x_1, x_2, \ldots, x_{n-1}, x_n) = (x_1, x_2, \ldots, x_{n-1}).$$

Если $\sum_{i=1}^{n} x_i = 1$, то приемник укажет, что произошла ошибка передачи, точнее, что при передаче сообщения произошло нечетное число ошибок. Конечно, если $\sum_{i=1}^{n} x_i = 0$, то нет гарантии безошибочности, могло произойти четное число ошибок. Однако нетрудно подсчитать, скажем, при $n = 3$, что

вероятность пропуска ошибки, равная доле неисправленных ошибочных сообщений, составляет $\dfrac{3p^2q}{1-q^3} = \dfrac{p}{1+p^2/(3q)}$, а эта величина меньше p.

2. $[3k, k]$-код „с повторением“. Каждый блок символов сообщения длиной k повторяется трижды. Принятая строка $(b_1, b_2, \ldots, b_{3k})$ разбивается на блоки длиной k и принятый символ c_i полагается равным 0 или 1 в зависимости от того, какой из этих элементов преобладает в тройке $\{b_i, b_{i+k}, b_{i+2k}\}$. Ясно,что такой код обеспечивает исправление одиночной ошибки в каждой позиции, но имеет низкую скорость передачи $R = 1/3$. Код из предыдущего примера имел очень высокую скорость $R = (n-1)/n$, но обладал весьма слабой помехоустойчивостью.

Алгебраическая теория кодирования и решает задачу построения кодов с приемлемыми скоростями передачи и достаточной помехоустойчивостью.

Замечание 1. Большая часть наших результатов останется верной, если допустить, что алфавит A образован элементами любого поля Галуа. Другой класс образуют *арифметические* коды, применяемые в вычислительной технике, – они используют в качестве алфавита кóльца классов вычетов $\mathbb{Z}_n$, где $n = 2^m$ или $n = 2^m - 1$.

Замечание 2. Будем полагать далее, что длина кодовых слов превышает размерность кода как подпространства ($n > k$), случай $n = k$ может использоваться в шифровании.

Упражнения

1. Покажите, что при $p > 1/2$ инвертирование принятых символов преобразует канал связи в ДСК, а при $p = 1/2$ связь невозможна.

2. Предположим, что вероятность ошибки при передаче одного символа $p = 0,01$. Чему станет равной вероятность ошибки на один символ при использовании кода из примера 2? А какой результат будет достигнут при пятикратном повторении?

3. Постройте матрицы операторов кодирования и декодирования (в канонических базисах) кодов, описанных в примерах 1 и 2.

§19. ЛИНЕЙНЫЕ КОДЫ

Матрица G (размера $k \times n$) оператора кодирования $\mathcal{C}$ линейного кода называется *порождающей матрицей* этого кода:

$$\mathcal{C}(u_1, u_2, \ldots, u_k) = (u_1, u_2, \ldots, u_k)G = (x_1, x_2, \ldots, x_n).$$

Поскольку отображение $\mathcal{C}$ должно быть инъективным, строки матрицы G образуют базис кода $V = \operatorname{Im}\mathcal{C} \subset \mathbb{I}^n$.

Существует и другой способ описания кодов при помощи матриц. Пусть даны векторы $\boldsymbol{u} = (u_1, u_2, \ldots, u_n)$, $\boldsymbol{v} = (v_1, v_2, \ldots, v_n) \in \mathbb{I}^n$. Тогда

их *скалярное произведение* определим равенством $\boldsymbol{u} \cdot \boldsymbol{v} = u_1 v_1 + u_2 v_2 + \ldots$ $\ldots + u_n v_n$. Если $\boldsymbol{u} \cdot \boldsymbol{v} = 0$, то векторы $\boldsymbol{u}$ и $\boldsymbol{v}$ называются *ортогональными*. *Ортогональное дополнение* $V^\perp$ подпространства V определяется как

$$V^\perp = \{\boldsymbol{u} \in \mathbb{I}^n \ : \ \boldsymbol{u} \cdot \boldsymbol{v} = 0 \ \ \forall\, \boldsymbol{v} \in V\}.$$

Легко видеть, что ортогональное дополнение $V^\perp$ само является линейным $[n, n-k]$-кодом, он называется *двойственным* к коду V. Пусть H – порождающая матрица двойственного кода $V^\perp$. Вектор $\boldsymbol{x}$ принадлежит V тогда и только тогда, когда он ортогонален каждой строке матрицы H, т. е. когда

$$H\boldsymbol{x}^T = \mathbf{0}.$$

Матрица H размера $(n-k)\times n$ называется *проверочной матрицей* кода V, с матрицей G она очевидно связана равенством $HG^T = O$, где O обозначает нулевую матрицу размера $(n-k) \times k$.

Примеры

1. Проверочная и порождающая матрицы (размерами $1 \times (k+1)$ и $k \times (k+1)$ соответственно) кода с проверкой на четность имеют вид:

$$H = \begin{pmatrix} 1 & 1 & \ldots & 1 \end{pmatrix}, \quad G = \begin{pmatrix} 1 & 0 & \ldots & 0 & 1 \\ 0 & 1 & \ldots & 0 & 1 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & 1 & 1 \end{pmatrix}.$$

2. У кода с троекратным повторением проверочная и порождающая матрицы размерами $2k \times 3k$ и $k \times 3k$ следующие:

$$H = \begin{pmatrix} 1 & 0 & \ldots & 0 & 1 & 0 & \ldots & 0 \\ 0 & 1 & \ldots & 0 & 0 & 1 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & 1 & 0 & 0 & \ldots & 0 \\ 1 & 0 & \ldots & 0 & 0 & 0 & \ldots & 0 \\ 0 & 1 & \ldots & 0 & 0 & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & 1 & 0 & 0 & \ldots & 1 \end{pmatrix}, \ G = \begin{pmatrix} 1 & 0 & \ldots & 0 & 1 & 0 & \ldots & 0 & 1 & 0 & \ldots & 0 \\ 0 & 1 & \ldots & 0 & 0 & 1 & \ldots & 0 & 0 & 1 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & 1 & 0 & 0 & \ldots & 1 & 0 & 0 & \ldots & 1 \end{pmatrix}.$$

Замечание. В отличие от векторов в евклидовых пространствах (над полем $\mathbb{R}$) ненулевой вектор над конечным полем может быть ортогонален сам себе. Например, вектор (1 1 1 1) принадлежит как $[4, 3]$-коду V с проверкой на четность, так и двойственному коду $V^\perp$.

Предположим, что был принят вектор $\boldsymbol{y} = (y_1, y_2, \ldots, y_n)$. Декодирование начинается с вычисления вектора $\boldsymbol{s} = (s_1, s_2, \ldots, s_{n-k})^T = H\boldsymbol{y}^T$, который называется *синдромом* $\boldsymbol{y}$. Синдром вектора $\boldsymbol{y}$ равен нулю, если и

только если $\boldsymbol{y} = \boldsymbol{x}$ – кодовое слово. Поэтому, если никаких ошибок не произошло, синдром вектора $\boldsymbol{y}$ равен нулю (но не обратное). В общем случае, если $\boldsymbol{y} = \boldsymbol{x} + \boldsymbol{e}$, где $\boldsymbol{x} \in V$, а $\boldsymbol{e}$ – так называемый *вектор ошибок*, то

$$\boldsymbol{s} = H\boldsymbol{y}^T = H\boldsymbol{e}^T.$$

Теорема. Для двоичного кода синдром равен сумме тех столбцов проверочной матрицы H, где произошли ошибки. ■

Таким образом, чтобы построить код исправляющий одну ошибку, необходимо выбрать столбцы матрицы H ненулевыми – в противном случае ошибка в этой позиции не будет влиять на синдром, а значит, будет необнаруживаемой – и различными, – поскольку если два столбца H равны, то ошибки в соответствующих двух позициях будут неразличимы.

Если матрица H имеет $r = n - k$ строк (у кода r проверочных символов), то существует $2^r - 1$ допустимых столбцов, представляющих собой двоичные записи чисел от 1 до $2^r - 1$. Соответствующий $[2^r - 1, 2^r - 1 - r]$-код ($r \geqslant 2$) называется *кодом Хэмминга.*

§20. КОДЫ БЧХ

Коды Хэмминга исправляют одиночные ошибки. Существуют обобщения этих кодов на случай нескольких ошибок, которые называются кодами Боуза–Чоудхури–Хоквингема (или, кратко, кодами БЧХ). Чтобы построить коды БЧХ, необходимо использовать поля Галуа. Рассмотрим далее построение проверочной матрицы для исправления двух ошибок.

Двоичный код Хэмминга длины $n = 2^r - 1$, должен иметь r проверочных символов, чтобы исправлять одну ошибку. Естественно предположить, что для исправления двух ошибок необходимо $2r$ проверочных символов. Попытаемся построить проверочную матрицу H кода, исправляющего две ошибки, добавляя еще r строк к проверочной матрице H' кода Хэмминга.

В качестве примера возьмем $r = 4;\ n = 15$. Матрица H' имеет своими столбцами все возможные ненулевые 4-мерные векторы:

$$H' = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

Для краткости используем условную запись матрицы H':

$$H' = \begin{pmatrix} 1 & 2 & 3 & \dots & 14 & 15 \end{pmatrix},$$

где числом i обозначен соответствующий 4-мерный двоичный вектор. Добавим к H' еще 4 строки:

$$H = \begin{pmatrix} 1 & 2 & 3 & \dots & 14 & 15 \\ f(1) & f(2) & f(3) & \dots & f(14) & f(15) \end{pmatrix}.$$

В матрице H значением некоторого оператора $f(i)$ также является 4-мерный вектор из нулей и единиц. Таким образом, i-й столбец $H_i = \binom{i}{f(i)}$ матрицы H представляет собой 8-мерный вектор-столбец. Если произошли две ошибки в позициях i и j, то по теореме из предыдущего параграфа синдром равен

$$\boldsymbol{s} = H_i + H_j = \binom{i+j}{f(i)+f(j)} = \binom{z_1}{z_2}.$$

Необходимо выбрать оператор f так, чтобы декодер по синдрому $\boldsymbol{s}$ мог найти i и j, т. е. чтобы можно было решить систему уравнений

$$\begin{cases} i + j = z_1, \\ f(i) + f(j) = z_2 \end{cases}$$

относительно 4-мерных векторов i и j при заданных векторах z_1 и z_2. Для того, чтобы решить эту систему необходимо уметь выполнять все арифметические операции с векторами. Поэтому будем рассматривать их как элементы поля $\mathbb{GF}(2^4) = \mathbb{GF}(16)$, а оператор f зададим равенством $f(i) = i^3$. Тогда система уравнений приобретает вид

$$\begin{cases} i + j = z_1 \neq 0, \\ i^3 + j^3 = z_2 \end{cases}$$

и может быть однозначно решена.

Действительно, $i^2 + ij + j^2 = \frac{z_2}{z_1}$, а поскольку $i^2 + j^2 = (i+j)^2$, то $ij = \frac{z_2}{z_1} + z_1^2$. Таким образом, z_1 и z_2 являются корнями квадратного уравнения

$$x^2 + z_1 x + \left(\frac{z_2}{z_1} + z_1^2\right) = 0.$$

Заметим, что если ошибок нет, то $z_1 = z_2 = 0$, а если произошла одна ошибка в позиции i, то $z_2 = i^3 = z_1^3$.

Получаем следующую схему декодирования.

1. Если $z_1 = z_2 = 0$, то решают, что ошибок не было.

2. Если $z_1 \neq 0,\ z_2 = z_1^3$, то исправляют одиночную ошибку в позиции $i = z_1$.

3. Если $z_1 \neq 0,\ z_2 \neq z_1^3$, то находят корни квадратного многочлена $g(x) = x^2 + z_1 x + \left(z_2/z_1 + z_1^2\right)$. Если он имеет два разных корня i и j, исправляют ошибки в соответствующих позициях.

4. Если же многочлен $g(x)$ не имеет корней или если $z_1 = 0,\ z_2 \neq 0$, то заключают, что произошло не менее трех ошибок.

Замечание. При решении квадратных уравнений над полем $\mathbb{GF}(2^m)$ нельзя использовать обычную формулу, так как в полях характеристики 2 невозможно деление на 2. Одним из возможных методов поиска корней может быть прямой перебор.

Как правило, столбцы матрицы H переставляют так, чтобы она приняла вид:

$$H = \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 & \alpha^8 & \alpha^9 & \alpha^{10} & \alpha^{11} & \alpha^{12} & \alpha^{13} & \alpha^{14} \\ 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} \end{pmatrix},$$

где α – примитивный элемент поля $\mathbb{GF}(2^4)$ (корень многочлена x^4+x+1). В данном случае повторения во второй строке объясняются тем, что элемент α^3 не является примитивным: $(\alpha^3)^5 = 1$.

В двоичной форме матрица H выглядит следующим образом:

$$H = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Примеры

1. Предположим, что произошли ошибки на позициях 3 и 12, т. е. в столбцах $\begin{pmatrix} \alpha^2 \\ \alpha^6 \end{pmatrix}$ и $\begin{pmatrix} \alpha^{11} \\ \alpha^3 \end{pmatrix}$.

Тогда $z_1 = (0\,1\,0\,1)^T = \alpha^9$, $z_2 = (0\,0\,1\,0)^T = \alpha^2$ и $z_2/z_1+z_1^2 = \alpha^8+\alpha^3 = $ $= (1\,0\,1\,1)^T = \alpha^{13}$.

Таким образом, квадратное уравнение для определения позиций с ошибками имеет вид:

$$x^2 + \alpha^9 x + \alpha^{13} = (x + \alpha^2)(x + \alpha^{11}) = 0.$$

Корни уравнения и указывают на расположение двух ошибок.

2. Если ошибки произошли на позициях 1, 2 и 4, то синдром, как легко убедиться, равен $(1\,1\,0\,1\,1\,1\,0\,0)^T$. Тогда $z_1 = \alpha^7$, $z_2 = \alpha^4$ и получившееся уравнение $x^2 + \alpha^7 x + \alpha^5 = 0$ не имеет корней в поле $\mathbb{GF}(2^4)$. Декодер решает, что произошло не менее трех ошибок.

Ясно, что рассмотрение произвольных полей Галуа $\mathbb{GF}(2^r)$ позволяет построить семейство линейных $[2^r - 1, 2^r - 1 - 2r]$-кодов, исправляющих

двойные ошибки. В алгебраической теории кодирования строятся, в частности, *примитивные* (использующие примитивные элементы конечного поля) коды БЧХ длины 2^r-1, исправляющие любое заданное число ошибок.

Упражнения

1. Покажите, что определение оператора f равенствами $f(i)=i$ или $f(i)=i^2$ не решает поставленную задачу.

2. Докажите, что квадратное уравнение $x^2+x+\beta=0$, где $\beta\in\mathbb{GF}(2^m)$, имеет два корня в $\mathbb{GF}(2^m)$, если след $\mathrm{Tr}(\beta)=\sum\limits_{k=0}^{m-1}\beta^{2^k}=0$, и не имеет корней (многочлен $x^2+x+\beta$ неприводим) в $\mathbb{GF}(2^m)$, если $\mathrm{Tr}(\beta)=1$.

3. В каких позициях были ошибки, если при использовании $[15,7]$-кода БЧХ синдром $\boldsymbol{s}=(1\,0\,0\,1\,0\,1\,1\,0)^T$? А если $\boldsymbol{s}=(0\,1\,0\,1\,1\,1\,1\,1)^T$?

4. При использовании $[15,7]$-кода БЧХ принятый вектор (длины 15) имеет вид $(1\,1\,0\,0\,\ldots\,0\,0)$. Какое слово передавалось?

§21. КОДЫ ГОППЫ И КРИПТОГРАФИЯ

Примитивные коды БЧХ фактически являются частным случаем так называемых *кодов Гоппы* длины $n=2^r$, проверочная матрица которых строится следующим образом. Выберем неприводимый многочлен $g(x)$ степени t над полем Галуа $\mathbb{GF}(2^r)$. Обозначим через α_1, α_2, $\ldots$, α_n все элементы этого поля. Проверочная матрица H кода Гоппы имеет вид

$$H=\begin{pmatrix} g^{-1}(\alpha_1) & g^{-1}(\alpha_2) & \ldots & g^{-1}(\alpha_n)\\ \alpha_1 g^{-1}(\alpha_1) & \alpha_2 g^{-1}(\alpha_2) & \ldots & \alpha_n g^{-1}(\alpha_n)\\ \ldots & \ldots & \ldots & \ldots\\ \alpha_1^{t-1} g^{-1}(\alpha_1) & \alpha_2^{t-1} g^{-1}(\alpha_2) & \ldots & \alpha_n^{t-1} g^{-1}(\alpha_n)\end{pmatrix}$$

(где каждый элемент должен быть заменен на соответствующий столбец из r элементов над $\mathbb{GF}(2)$).

Можно доказать, что множество двоичных векторов, аннулируемых матрицей H, образует $[n=2^r, k\geqslant 2^r-tr]$-код, исправляющий t ошибок (значение k может быть больше граничного, так как строки матрицы H могут оказаться линейно зависимыми).

Замечание. Коды БЧХ, исправляющие t ошибок, можно получить из кодов Гоппы, если удалить 0 из набора $\{\alpha_j\}$ элементов поля $\mathbb{GF}(2^r)$ и отказаться от неприводимости многочлена $g(x)$ (в результате чего станет на один информационный символ меньше).

Пример

Рассмотрим $\mathbb{GF}(2^3) = \{0,\ 1,\ \alpha,\ \alpha^2,\ \ldots,\ \alpha^6\}$, где α – примитивный элемент поля (см. пример 2 §16), и выберем $g(x) = x^2 + x + 1$. Непосредственной проверкой легко можно убедиться, что многочлен $g(x)$ неприводим в $\mathbb{GF}(2^3)$ (все корни этого многочлена лежат в полях $\mathbb{GF}(2^2)$, $\mathbb{GF}(2^4)$, $\mathbb{GF}(2^6)$ и т. д.). Получаем $[8, 8 - 2 \cdot 3 = 2]$-код Гоппы, исправляющий 2 ошибки, с проверочной матрицей

$$H = \begin{pmatrix} g^{-1}(0) & g^{-1}(1) & g^{-1}(\alpha) & \ldots & g^{-1}(\alpha^6) \\ 0 \cdot g^{-1}(0) & 1 \cdot g^{-1}(1) & \alpha g^{-1}(\alpha) & \ldots & \alpha^6 g^{-1}(\alpha^6) \end{pmatrix}.$$

С помощью логарифмов Якоби находим:

$$H = \begin{pmatrix} 1 & 1 & \alpha^2 & \alpha^4 & \alpha^2 & \alpha & \alpha & \alpha^4 \\ 0 & 1 & \alpha^3 & \alpha^6 & \alpha^5 & \alpha^5 & \alpha^6 & \alpha^3 \end{pmatrix}.$$

Степени примитивного элемента α запишем в виде двоичных векторов (см. пример 2 § 15): $\alpha = (010),\ \alpha^2 = (001),\ \alpha^3 = (110),\ \alpha^4 = (011),\ \alpha^5 = (111),\ \alpha^6 = (101)$. Проверочная матрица принимает окончательный вид:

$$H = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}.$$

Решив однородную систему линейных уравнений с двоичной матрицей H, находим все кодовые слова данного кода:

$$\begin{cases} (0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0), \\ (1\ \ 1\ \ 0\ \ 0\ \ 1\ \ 0\ \ 1\ \ 1), \\ (1\ \ 1\ \ 1\ \ 1\ \ 0\ \ 1\ \ 0\ \ 0), \\ (0\ \ 0\ \ 1\ \ 1\ \ 1\ \ 1\ \ 1\ \ 1). \end{cases}$$

Если к кодовым словам добавить проверку на четность, то, как легко видеть, расширенный $[9, 2]$-код сможет кроме исправления двойных ошибок обнаруживать тройные.

Можно построить *криптосистему с открытым ключом*, основанную на произвольном коде Гоппы. Для этого по проверочной матрице H находим порождающую матрицу G размера $k \times n$ (см. § 19), после чего случайным образом выбираем две матрицы (тоже с элементами из $\mathbb{GF}(2)$):

невырожденную матрицу S размера $k \times k$ и матрицу перестановки P размера $n \times n$. Далее вычисляем матрицу $G' = SGP$, которую сообщаем всем желающим. Матрицы G, S и P хранятся в тайне.

Отправитель шифрует сообщение $\boldsymbol{x} \in \mathbb{I}^k$ в виде вектора

$$\boldsymbol{y} = \boldsymbol{x}G' + \boldsymbol{z},$$

где $\boldsymbol{z} \in \mathbb{I}^n$ – случайный вектор с t единицами.

Для дешифровки необходимо вычислить

$$\boldsymbol{y}P^{-1} = \boldsymbol{x}SG + \boldsymbol{z}P^{-1}$$

и использовать стандартную схему декодирования кода Гоппы. По полученному вектору $\boldsymbol{x}S$ немедленно находится сообщение $\boldsymbol{x}$.

Отправитель маскирует кодовое слово $\boldsymbol{x}G'$, изменяя t случайно выбранных символов. Так как код Гоппа может исправить t ошибок, законный получатель избавляется от этого искажения. „Злоумышленник“, не знающий матриц G, S или P, вынужден попытаться раскрыть код, задаваемый порождающей матрицей G'. Это линейный код, очень похожий на случайный, раскрыть такой код очень трудно. Пусть, например, $n = 2^{10} = 1024$ и $t = 50$. Многочлен $g(x)$ можно выбрать примерно 10^{149} способами, для матриц S и P выбор еще шире. Размерность кода не меньше $k = 1024 - 10 \cdot 50 = 524$. Таким образом, подслушивающий сталкивается с проблемой декодирования кода длиной 1024, исправляющего 50 ошибок и кажущегося случайным. Даже большое количество времени для поиска алгоритма расшифрования не помогает. Полагая, что обращение матрицы k-го порядка требует k^3 операций, *временна́я сложность* предварительного криптоанализа может быть грубо оценена как

$$\frac{k^3 C_n^k}{C_{n-t}^k}.$$

При $n = 1024$, $k = 524$ и $t = 50$ это дает величину $2^{80,71}$.

Упражнение

Пусть α – примитивный элемент поля $\mathbb{GF}(2^4) = \mathbb{Z}_2[x]/(x^4 + x + 1)$, являющийся корнем многочлена x^4+x+1. Многочлен $g(x) = x^2+x+\alpha^3$ неприводим над полем $\mathbb{GF}(2^4)$, так как след $\mathrm{Tr}(\alpha^3) = \alpha^3 + \alpha^6 + \alpha^12 + \alpha^9 = 1$ (см. упр. 2 §20). Следовательно, с помощью $g(x)$ можно построить $[16, 8]$-код Гоппы, исправляющий двойные ошибки. Найдите проверочную матрицу этого кода.

§22. ТАБЛИЦЫ

В табл. 1 приводятся все неприводимые многочлены степени n над полем $\mathbb{GF}(2)$ для всех $n \leqslant 6$. Символ $*$, расположенный перед многочленом, указывает на то, что этот многочлен примитивный.

Таблица 2 содержит по одному примитивному многочлену степени n над полем $\mathbb{GF}(2)$ для всех $n \leqslant 70$.

Таблица 3 представляет собой таблицу логарифмов Якоби $L(n)$ (см. §16) для полей $\mathbb{GF}(2^k) = \mathbb{Z}_2[x]/(g(x))$, где $2 \leqslant k \leqslant 6$. Примитивный элемент β, относительно которого строится логарифм Якоби, является корнем многочлена $g(x)$.

Таблица 1

$n = 1$	$*$	x
	$*$	$x + 1$
$n = 2$	$*$	$x^2 + x + 1$
$n = 3$	$*$	$x^3 + x + 1$
	$*$	$x^3 + x^2 + 1$
$n = 4$	$*$	$x^4 + x + 1$
	$*$	$x^4 + x^3 + 1$
		$x^4 + x^3 + x^2 + x + 1$
$n = 5$	$*$	$x^5 + x^2 + 1$
	$*$	$x^5 + x^3 + 1$
	$*$	$x^5 + x^3 + x^2 + x + 1$
	$*$	$x^5 + x^4 + x^2 + x + 1$
	$*$	$x^5 + x^4 + x^3 + x + 1$
	$*$	$x^5 + x^4 + x^3 + x^2 + 1$
$n = 6$	$*$	$x^6 + x + 1$
		$x^6 + x^3 + 1$
		$x^6 + x^4 + x^2 + x + 1$
	$*$	$x^6 + x^4 + x^3 + x + 1$
	$*$	$x^6 + x^5 + 1$
	$*$	$x^6 + x^5 + x^2 + x + 1$
	$*$	$x^6 + x^5 + x^3 + x^2 + 1$
	$*$	$x^6 + x^5 + x^4 + x + 1$
		$x^6 + x^5 + x^4 + x^2 + 1$

Таблица 2

$x+1$	$x^{36}+x^6+x^5+x^4+x^2+x+1$
x^2+x+1	$x^{37}+x^5+x^4+x^3+x^2+x+1$
x^3+x+1	$x^{38}+x^6+x^5+x+1$
x^4+x+1	$x^{39}+x^4+1$
x^5+x^2+1	$x^{40}+x^5+x^4+x^3+1$
x^6+x+1	$x^{41}+x^3+1$
x^7+x+1	$x^{42}+x^5+x^4+x^3+x^2+x+1$
$x^8+x^4+x^3+x^2+1$	$x^{43}+x^6+x^4+x^3+1$
x^9+x^4+x+1	$x^{44}+x^6+x^5+x^2+1$
$x^{10}+x^3+1$	$x^{45}+x^4+x^3+x+1$
$x^{11}+x^2+x+1$	$x^{46}+x^8+x^5+x^3+x^2+x+1$
$x^{12}+x^6+x^4+x+1$	$x^{47}+x^5+1$
$x^{13}+x^4+x^3+x+1$	$x^{48}+x^7+x^5+x^4+x^2+x+1$
$x^{14}+x^5+x^3+x+1$	$x^{49}+x^6+x^5+x^4+1$
$x^{15}+x+1$	$x^{50}+x^4+x^3+x^2+1$
$x^{16}+x^5+x^3+x^2+1$	$x^{51}+x^6+x^3+x+1$
$x^{17}+x^3+1$	$x^{52}+x^3+1$
$x^{18}+x^5+x^2+x+1$	$x^{53}+x^6+x^2+x+1$
$x^{19}+x^5+x^2+x+1$	$x^{54}+x^6+x^5+x^4+x^3+x^2+1$
$x^{20}+x^3+1$	$x^{55}+x^6+x^2+x+1$
$x^{21}+x^2+1$	$x^{56}+x^7+x^4+x^2+1$
$x^{22}+x+1$	$x^{57}+x^5+x^3+x^2+1$
$x^{23}+x^5+1$	$x^{58}+x^6+x^5+x+1$
$x^{24}+x^4+x^3+x+1$	$x^{59}+x^6+x^5+x^4+x^3+x+1$
$x^{25}+x^3+1$	$x^{60}+x+1$
$x^{26}+x^6+x^2+x+1$	$x^{61}+x^5+x^2+x+1$
$x^{27}+x^5+x^2+x+1$	$x^{62}+x^6+x^5+x^3+1$
$x^{28}+x^3+1$	$x^{63}+x+1$
$x^{29}+x^2+1$	$x^{64}+x^4+x^3+x+1$
$x^{30}+x^6+x^4+x+1$	$x^{65}+x^4+x^3+x+1$
$x^{31}+x^3+1$	$x^{66}+x^8+x^6+x^5+x^3+x^2+1$
$x^{32}+x^7+x^5+x^3+x^2+x+1$	$x^{67}+x^5+x^2+x+1$
$x^{33}+x^6+x^4+x+1$	$x^{68}+x^7+x^5+x+1$
$x^{34}+x^7+x^6+x^5+x^2+x+1$	$x^{69}+x^6+x^5+x^2+1$
$x^{35}+x^2+1$	$x^{70}+x^5+x^3+x+1$

Таблица 3

$\mathbb{GF}(4) = \mathbb{Z}_2[x]/(x^2 + x + 1)$

n	$-\infty$	0	1	2
$L(n)$	0	$-\infty$	2	1

$\mathbb{GF}(8) = \mathbb{Z}_2[x]/(x^3 + x^2 + 1)$

n	$-\infty$	0	1	2	3	4	5	6
$L(n)$	0	$-\infty$	5	3	2	6	1	4

$\mathbb{GF}(16) = \mathbb{Z}_2[x]/(x^4 + x + 1)$

n	$-\infty$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$L(n)$	0	$-\infty$	4	8	14	1	10	13	9	2	7	5	12	11	6	3

$\mathbb{GF}(32) = \mathbb{Z}_2[x]/(x^5 + x^4 + x + 1)$

n	$-\infty$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$L(n)$	0	$-\infty$	19	7	11	14	29	22	2	28	15	27	3	13	12	4

15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
9	25	21	30	1	23	17	6	20	26	16	24	10	8	5	18

$\mathbb{GF}(64) = \mathbb{Z}_2[x]/(x^6 + x^5 + x^3 + x^2 + 1)$

n	$-\infty$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$L(n)$	0	$-\infty$	8	16	53	32	38	43	62	1	45	13	51	23	10	61

15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
44	2	41	27	34	26	42	39	12	46	30	20	18	59	48	25

31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46
35	4	58	19	31	54	57	5	22	52	17	21	6	15	9	24

47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62
49	29	47	60	11	40	3	36	56	55	37	33	28	50	14	7

СПИСОК РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ

Александров П. С. Введение в теорию групп. М.: Наука, 1980.

Берлекэмп Э. Алгебраическая теория кодирования. М.: Мир, 1971.

Биркгоф Г., Барти Т. Современная прикладная алгебра. СПб.: Лань, 2006.

Калужнин Л. А., Сущанский В. И. Преобразования и перестановки. М.: Наука, 1985.

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

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

Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А. Теория кодов, исправляющих ошибки. М.: Связь, 1979.

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

Саломаа А. Криптография с открытым ключом. М.: Мир, 1995.

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

Содержание

§ 1. Прямое произведение множеств. Отображения 3
§ 2. Отношения эквивалентности. Фактормножества 5
§ 3. Бинарные операции. Группы 7
§ 4. Подгруппы. Гомоморфизмы групп 10
§ 5. Смежные классы. Нормальные подгруппы 13
§ 6. Действие группы на множестве 17
§ 7. Циклические группы 21
§ 8. Прямое произведение групп 23
§ 9. Характеры конечных абелевых групп 26
§ 10. Кольца 30
§ 11. Поля 33
§ 12. Идеалы и кольца классов вычетов 34
§ 13. Евклидовы кольца 37
§ 14. Кольца многочленов 39
§ 15. Расширения полей 43
§ 16. Мультипликативная группа конечного поля 46
§ 17. Характеры конечных полей и суммы Гаусса 48
§ 18. Кодирование и декодирование 50
§ 19. Линейные коды 52
§ 20. Коды БЧХ 54
§ 21. Коды Гоппы и криптография 57
§ 22. Таблицы 60
Список рекомендуемой литературы 63

Зельвенский Игорь Григорьевич

Введение в современную алгебру

Учебное пособие

Редактор О. Р. Крумина

Подписано в печать 26.12.14. Формат 60 × 84 1/16.
Бумага офсетная. Печать цифровая. Печ. л. 4,0.
Гарнитура «Computer Modern Roman». Тираж 90 экз. Заказ .

Издательство СПбГЭТУ «ЛЭТИ»
197376, С.-Петербург, ул. Проф. Попова, 5