II. ГРУППОВЫЕ КОДЫ

2.1. НЕКОТОРЫЕ СВЕДЕНИЯ ИЗ АЛГЕБРЫ. ГРУППЫ, КОЛЬЦА, ПОЛЯ

В данном разделе книги излагаются некоторые сведения из алгебры, необходимые для изучения блоковых кодов.

Построение наиболее известных корректирующих кодов основано на использовании некоторых алгебраических систем, например таких, как: группа (***Group***), поле (***Field***), кольцо (***Ring***) и идеал (***Ideal***).

Алгебраическая система – это множество S некоторых абстрактных элементов a, b, c, …, над которыми определены некоторые операции. Естественно допущение о том, что все абстрактные элементы a, b, c, …, множества S ***различны*** [1.7, с. 9-11].

ОПРЕДЕЛЕНИЕ 2.1. ***n-арная*** *алгебраическая операция – отображение, сопоставляющее всякому упорядоченному набору n элементов данного множества S определённый элемент этого же множества; число n фиксировано для данной операции.*

END

В частном случае ***n-арная*** *алгебраическая операция* может выполняться над одним и тем же элементом $a \in S$, который в этом случае будет иметь n вхождений в выражение, описывающее ***n-арную*** *алгебраическую операцию.*

Если $n = 1$, *то операция называется* ***унарной***, *а в случае* $n = 2$ – ***бинарной*** [2.7, с. 11 – 12].

Условимся в общем случае записывать бинарную операцию над элементами множества S a и b в виде $a \circ b$.

Конкретную бинарную операцию записывают как $a + b = c$ или как $ab = c$ и называют, соответственно, *сложением* или *умножением*, даже если она не является арифметическим сложением или арифметическим умножением обычных чисел. В частных случаях, например при изучении двоичных кодов, под операцией « + » может подразумеваться операция « ⊕ » – сложение по модулю 2.

Так, в частности, возможны записи вида:

$$S(\{a, b, \ldots\}, +), \quad S(\{a, b, \ldots\}, \cdot) \text{ или } S(\{a, b, \ldots\}, +, \cdot). \quad (2\text{-}1)$$

В зависимости от числа операций, определённых на S, а также от свойств этих операций различают такие простейшие алгебраические системы, как «группа», «кольцо» и «поле».

ГРУППЫ. ПОДГРУППЫ

ОПРЕДЕЛЕНИЕ 2.2. ***Группой*** *называется множество элементов S, на котором определена* ***одна*** *операция «∘» –* ***сложение*** *или* ***умножение****, и выполняются аксиомы G* 2.1, *G* 2.2, *G* 2.3, *G* 2.4;

или

группой *называется множество элементов S, на котором определена* ***одна*** *операция «∘» –* ***сложение*** *или* ***умножение****, и выполняются законы A*1, *A*2, *A*4, *A*5 или *M*1, *M*2, *M*4, *M*5 *соответственно* (табл. 2.1).

END

АКСИОМА *G* 2.1 (*Замкнутость*). *Для любой пары элементов* $a, b \in S$ *существует и при том единственный элемент* $a \circ b \in S$.

END

В частном случае, при равенстве двух элементов, *входящих в выражение* типа $a \circ b$, одному и тому же элементу a множества S, возможно получение соотношения типа:

$$a \circ a \in S. \quad (2\text{-}1a)$$

Таблица 2.1

Законы, которым могут удовлетворять операции типа «$a \circ b$», определённые для абстрактных элементов a, b, c, множества S	Операция и условные обозначения законов	
	Сложение (*Addition*)	Умножение (*Multiplication*)
Замкнутость: для любой пары элементов $a,\ b \in S$ существует и при том единственный элемент $a \circ b \in S$	*A*1 $a \circ b = a+b$	*M*1 $a \circ b = a \cdot b = ab$
Ассоциативность: $(a \circ b) \circ c = a \circ (b \circ c);\ \ a, b, c \in S$	*A*2 $(a+b)+c = a+(b+c)$	*M*2 $(ab)c = a(bc)$
Коммутативность: $a \circ b = b \circ a;\ \ a, b \in S$	*A*3 $a+b = b+a$	*M*3 $ab = ba$
Наличие единичного элемента: среди элементов S существует единственный элемент e, такой, что для любого $a \in S$ $e \circ a = a \circ e = a$	*A*4 $a+e = e+a = a$ $(e = 0)$	*M*4 $ae = ea = a$ $(e = 1)$
Наличие обратных элементов: для каждого элемента $a \in S$ существует единственный ***по сложению*** обратный элемент $\bar{a} \in S$ такой, что $a \circ \bar{a} = \bar{a} \circ a = e = 0$ (*A*5), или для каждого элемента $a \in S$ (за исключением элемента $a = 0$) существует единственный ***по умножению*** обратный элемент $\bar{a} \in S$ такой, что $a \circ \bar{a} = \bar{a} \circ a = e = 1$ (*M*5)	*A*5 $a + \bar{a} = \bar{a} + a = e$ $(\bar{a} = -a)$	*M*5 $a\,\bar{a} = \bar{a}a = e$ $(\bar{a} = a^{-1},\ a \neq 0)$
Дистрибутивность (распределительный закон):	*D*1. $a(b+c) = ab + ac$ *D*2. $(b+c)a = ba + ca$	

END

АКСИОМА *G* 2.2 (*Ассоциативность*). *Для любых трёх элементов* $a, b, c \in S$ *справедливо соотношение* $(a \circ b) \circ c = a \circ (b \circ c)$.

END

Наличие свойства ассоциативности означает, что порядок выполнения операций в *выражении* несущественен, и поэтому использование скобок, определяющих порядок выполнения операций, не обязательно.

В частном случае, *при вхождении в исходное выражение n элементов* с некоторым распределением скобок и при равенстве этих n элементов одному и тому же элементу a множества S, возможен результат

$$a \circ a \ldots a \circ a = \begin{cases} a^n, & \text{если } a \circ b = ab, \\ \\ na, & \text{если } a \circ b = a + b, \end{cases} \qquad (2\text{-}1б)$$

где n – число вхождений элемента a в левую часть соотношения (2-1б), a^n – *n-я степень* элемента a, na – *кратное* элемента a; $a, b \in S$.

АКСИОМА *G* 2.3 (*Наличие единичного элемента*). *Среди элементов S существует единичный элемент e, такой, что для любого* $a \in S$ *выполняется соотношение*

$$e \circ a = a \circ e = a. \qquad (2\text{-}1в)$$

END

Если групповая операция является *сложением* или *умножением*, то e называется *нулём* и *единицей* соответственно:

$$e + a = a + e = a, \quad e = 0, \qquad (2\text{-}1г)$$

$$ea = ae = a, \quad e = 1. \qquad (2\text{-}1д)$$

Ниже будет доказано, что существует *единственный* единичный элемент группы e, такой, что для любого $a \in S$ выполняется соотношение (2-1в).

АКСИОМА *G* 2.4 (*Наличие обратных элементов*). *Для каждого элемента* $a \in S$ (*исключая элемент* $a = 0$ *при заданной в* S *операции умножения*) *существует обратный элемент* $\bar{a} \in S$, *такой, что*

$$\bar{a} \circ a = a \circ \bar{a} = e. \qquad (2\text{-}1e)$$

END

Если групповая операция является сложением или умножением, то $\bar{a}$ определяется из соответствующих уравнений и обозначается следующим образом:

$$\bar{a} + a = 0, \quad \bar{a} = -a, \qquad (2\text{-}2)$$

$$\bar{a}\, a = 1, \quad \bar{a} = a^{-1}. \qquad (2\text{-}2а)$$

Группа называется *коммутативной* или *абелевой*, если кроме аксиом *G* 2.1 - *G* 2.4 справедлива также аксиома *G* 2.5.

АКСИОМА *G* 2.5 (*Коммутативность*). *Для любых произвольных* a *и* b *из* S *имеет место*

$$a \circ b = b \circ a. \qquad (2\text{-}2б)$$

END

Ниже будет доказано, что для каждого элемента $a \in S$ существует *единственный* обратный элемент $\bar{a} \in S$, такой, что выполняется соотношение (2-1е).

ТЕОРЕМА 2.1. *Группа обладает единственным единичным элементом, и каждому элементу группы соответствует единственный обратный элемент* (*исключая нулевой элемент при заданной операции умножения*).

ДОКАЗАТЕЛЬСТВО

Предположим, что в группе имеется два единичных элемента: левый e и правый e'; при этом для произвольного $a \in S$ имеют место соотношения

$$e \circ a = a \circ e' = a. \qquad (2\text{-}2в)$$

Из (2-2в) следует, что, с одной стороны, $e \circ e' = e'$ и, с другой стороны, $e \circ e' = e$. Следовательно,

$$e = e'. \qquad (2\text{-}2г)$$

Предположим теперь, что некоторому элементу a группы соответствуют два обратных элемента: левый $\bar{a}_л$ и правый $\bar{a}_п$; при этом имеют место соотношения

$$\bar{a}_л \circ a = a \circ \bar{a}_п = e. \qquad (2\text{-}2д)$$

Из (2-2д) следует, что в рассматриваемом случае должна выполняется цепочка равенств

$$\bar{a}_п = e \circ \bar{a}_п = \bar{a}_л \circ a \circ \bar{a}_п = \bar{a}_л \circ e = \bar{a}_л.$$

Следовательно,

$$\bar{a}_п = \bar{a}_л. \qquad (2\text{-}2е)$$

ЧТД

В табл. 2.1 приведены законы, которым могут удовлетворять операции, определённые на множестве абстрактных элементов S, которые фигурируют в определении группы и устанавливаются теоремой 2.1.

Если в группе определена операция – сложение или умножение, то эта операция подчиняется законам *A*1, *A*2, *A*4, *A*5 *или M*1, *M*2, *M*4, *M*5 соответственно, а группа называется *аддитивной или мультипликативной*; если к тому же введённая операция подчиняется законам *A*3 или *M*3 (аксиома *G* 2.5), то группа называется *коммутативной* или *абелевой*.

Группа, имеющая конечное число элементов, называется *конечной*; при этом число её элементов называется *порядком группы*; в противном случае группа называется *бесконечной* (счётной или несчётной). Будем обозначать порядок группы G как $|G|$.

ПРИМЕР 2.1. Для описания группы в необходимых случаях будем использовать записи типа

$$(G, \circ) = (\{0, 1\}, \oplus), \qquad (2\text{-}3)$$

где G – множество элементов, а « $\oplus$ » – символ операции их сложения по mod 2; или

$$(G, \circ) = (\{0, 1\}, \cdot), \qquad (2\text{-}3a)$$

«·» – символ операции умножения: $ab = a \cdot b$. В тех случаях, когда операции известны, допустимым обозначением группы будет, например, такое: G.

Минимальный порядок конечной группы равен единице. Действительно, алгебраическая система $(\{e\}, \circ)$ является группой, так как при этом аксиомы G 2.1 – G 2.4 выполняются. Примеры подобных групп: $(\{0\}, \oplus)$ и $(\{1\}, \cdot)$.

END

ПРИМЕР 2.2. Дана коммутативная группа $(G, \circ)$ и уравнения относительно элемента x внутри этой группы:

$$\text{a) } a \circ x = b; \qquad \text{b) } x \circ a = b;$$

где a и b – некоторые конкретные элементы $(G, \circ)$.

Требуется решить эти уравнения относительно элемента x.

РЕШЕНИЕ. Опираясь на свойства групповой операции, найдём

$$\text{a) } \bar{a} \circ (a \circ x) = \bar{a} \circ b \Rightarrow e \circ x = \bar{a} \circ b \Rightarrow x = \bar{a} \circ b;$$

$$\text{b) } (x \circ a) \circ \bar{a} = b \circ \bar{a} \Rightarrow x \circ e = b \circ \bar{a} \Rightarrow x = b \circ \bar{a}$$

и, так как имеет место коммутативность, то

$$x = \bar{a} \circ b = b \circ \bar{a}.$$

END

ПРИМЕР 2.3

1. Множество всех целых чисел, множество всех чётных чисел, множество всех рациональных чисел, множество всех действительных чисел, множество всех комплексных чисел с операцией сложения – *бесконечные* аддитивные абелевы группы.

Множество всех натуральных чисел с операцией сложения не является аддитивной группой так как не выполняется закон *A*5.

2. Множество всех положительных действительных чисел без 0, множество всех рациональных чисел без 0, множество всех комплексных чисел без 0 с операцией умножения – *бесконечные* мультипликативные абелевы группы.

Множество всех целых положительных чисел с операцией умножения не является мультипликативной группой, так как не выполняется закон *M*5.

3. Множество всех корней n-й степени из единицы с операцией умножения – *конечная* мультипликативная абелева группа порядка n [2.9, с. 127 – 129, 401].

END

ПРИМЕР 2.4. Доказать, что в группе $(G, \circ)$ выполняется соотношение

$$(a \circ b)^{-1} = b^{-1} \circ a^{-1}. \qquad (2\text{-}4)$$

РЕШЕНИЕ. Таким образом, требуется доказать, что $b^{-1} \circ a^{-1}$ *является обратным элементом для* $a \circ b$. Для этого докажем, что $b^{-1} \circ a^{-1}$ одновременно является левым и правым обратным элементом для $a \circ b$:

$$(b^{-1} \circ a^{-1}) \circ (a \circ b) = b^{-1} \circ (a^{-1} \circ a) \circ b = b^{-1} \circ 1 \circ b = 1$$

и докажем аналогично, что:

$$(a \circ b) \circ (b^{-1} \circ a^{-1}) = 1.$$

END

Предположим, что дана группа G. Пусть H – некоторое подмножество элементов группы G. Зададимся вопросом, может ли H являться группой относительно операции, определённой в G ?

ОПРЕДЕЛЕНИЕ 2.3. *Некоторое подмножество элементов H группы G называется* ***подгруппой*** *H этой группы, если по отношению к операции, определённой в G, оно само является группой.*

END

ПРИМЕР 2.5. Пусть задана группа с операцией $\oplus$:

$$G = (\{00, 01, 10, 11\}, \oplus). \qquad (2\text{-}5)$$

Требуется перечислить все подгруппы этой группы.

Заданная аддитивная группа имеет подгруппы:

$H_1 = (\{00, 01, 10, 11\}, \oplus)$, $H_2 = (\{00, 01\}, \oplus)$,
$H_3 = (\{00, 10\}, \oplus)$, $H_4 = (\{00, 11\}, \oplus)$,
$H_5 = (\{00\}, \oplus)$.

END

ПРИМЕР 2.6. Пусть задана мультипликативная группа:

$$G = (\{1\}, \cdot). \qquad (2\text{-}5а)$$

Требуется перечислить все подгруппы этой группы.

Заданная мультипликативная группа имеет лишь одну подгруппу:

$$H = (\{1\}, \cdot) = G. \qquad (2\text{-}5б)$$

END

Для того, чтобы установить, является ли подмножество H всех элементов G подгруппой группы G, необходимо проверить наличие в H свойств операции:

1) ***замкнутости*** и 2) ***наличия обратных элементов***.

Действительно, если подмножество H замкнуто относительно заданной в G операции, то из наличия обратных элементов в нём вытекает, что оно содержит и единичный элемент. Ассоциативный же закон в H заведомо выполняется, так как он справедлив для всех элементов G. Поэтому H *является* группой, а следовательно, и подгруппой группы G.

ПРИМЕР 2.7. Примером конечной мультипликативной *некоммутативной* группы G является множество всевозможных *подстановок* (или перестановок), определённых на множестве абстрактных элементов S [2.9, с. 31].

1. Рассмотрим частный случай преобразования множества $S = \{1, 2, 3\}$ *на себя* – подстановку. Принято описывать конкретную подстановку с помощью таблицы, две строки которой образованы элементами S; а каждый столбец состоит из верхнего преобразуемого элемента S и получаемого из него вследствие выполнения подстановки нижнего элемента:

$$\begin{pmatrix}123\\321\end{pmatrix} \quad \text{или} \quad \begin{pmatrix}321\\123\end{pmatrix},$$

где обе таблицы определяют одну и ту же подстановку: 1→3, 2→2, 3→1; подобные подстановки являются тождественными, и в дальнейшем нами различаться не будут. Число всевозможных различных подстановок в данном случае равно 3! = 6; вот эти подстановки:

$$a = \begin{pmatrix}123\\123\end{pmatrix}, \qquad b = \begin{pmatrix}123\\132\end{pmatrix}, \qquad c = \begin{pmatrix}123\\213\end{pmatrix},$$

$$d = \begin{pmatrix}123\\231\end{pmatrix}, \qquad e = \begin{pmatrix}123\\312\end{pmatrix}, \qquad f = \begin{pmatrix}123\\321\end{pmatrix}. \qquad (2\text{-}5в)$$

Очевидно, что при последовательном выполнении любой пары из этих шести подстановок равносильно выполнению некоторой одной из этих же шести подстановок и, следовательно, можно говорить о бинарной операции с её свойством *замкнутости*, определённой на множестве $G = \{a, b, c, d, e, f\}$.

Ведённую бинарную операцию, т.е. последовательное выполнение двух конкретных подстановок, естественно назвать операцией умножения с *единственной единицей* $a = 1$, см. (2-5в) и приведенную ниже таблицу умножения – табл. 2.2. Например:

$$be = \begin{pmatrix}123\\132\end{pmatrix}\begin{pmatrix}123\\312\end{pmatrix} = \begin{pmatrix}123\\321\end{pmatrix} = f, \qquad (2\text{-}5г)$$

$$eb = \begin{pmatrix}123\\312\end{pmatrix}\begin{pmatrix}123\\132\end{pmatrix} = \begin{pmatrix}123\\213\end{pmatrix} = c \neq f = be. \qquad (2\text{-}5д)$$

Таблица умножения «·» для бинарной операции «$b \circ d$» обычно создаётся следующим образом: на пересечении строки b и столбца d пишется результат выполнения указанной бинарной операции $b \circ d$; подобным образом создана таблица умножения (см. табл. 2.2) для рассматриваемого примера.

С помощью табл. 2.2 можно непосредственно убедиться в том, что в рассматриваемом случае имеет место свойство *ассоциативности*; например:

$$(cd)e = c(de) = c.$$

Очевидно, что каждый элемент G имеет *единственный обратный элемент* (см. табл. 2.2 и табл. 2.3).

Таблица 2.2

·	a	b	c	d	e	f
a	a	b	c	d	e	f
b	b	a	d	c	f	e
c	c	e	a	f	b	d
d	d	f	b	e	a	c
e	e	c	f	a	d	b
f	f	d	e	b	c	a

Таким образом, мы показали, что множество $G = \{a, b, c, d, e, f\}$ с определённой на нём бинарной операцией умножения является *мультипликативной некоммутативной группой.*

Таблица 2.3

$a^{-1} = a$	$b^{-1} = b$	$c^{-1} = c$	$d^{-1} = e$	$e^{-1} = d$	$f^{-1} = f$

Рассматриваемая мультипликативная группа G имеет, например, следующие подгруппы:

$$H_1 = \{a\}, \qquad H_2 = \{a, b\}, \qquad H_3 = \{a, c\}, \qquad H_4 = \{a, f\},$$

$$H_5 = \{a, d, e\}, \qquad H_6 = \{a, b, c, d, e, f\}.$$

Подстановка может быть описана также в матричной форме [2.10].

2. Если множество S состоит из n элементов, то в случае описанного в п. 1 преобразования типа подстановки, осуществляющего однозначное отображение *S на себя*, мы будем иметь *конечную мультипликативную симметрическую группу подстановок* (*перестановок*) G порядка $n!$ при $n > 2$ *некоммутативную* [2.9, с. 397; 2.10, с. 349].

Другим примером конечной мультипликативной некоммутативной группы является множество всех невырожденных квадратных матриц порядка $n \geq 2$ с действительными элементами [2.9, с.397].

END

РАЗЛОЖЕНИЕ ГРУППЫ ПО ПОДГРУППЕ

Ориентируясь на наши потребности при дальнейшем изложении материала, в ущерб общности, ограничимся рассмотрением лишь ***коммутативных групп***.

Пусть $g_1 = e$, g_2, …, $g_{(mk)}$ – элементы коммутативной группы G с заданной групповой операцией «$\circ$», а $h_1 = g_1 = e$, h_2, …, h_k – элементы некоторой её подгруппы H.

Построим табл. 2.4, называемую «разложением группы G по подгруппе H» по правилу:

первая строка образуется путём выписывания слева направо элементов подгруппы H, причём начинаться должна строка с единичного элемента подгруппы: $h_1 = e$, h_2, …, h_k; все элементы первой строки *являются различными*, так как подгруппа H состоит из *различных элементов*;

первым элементом *второй строки*, считая слева направо, может быть любой элемент группы G, не вошедший в первую строку, а все остальные элементы этой строки получаются в результате применения заданной групповой операции «$\circ$» к её первому элементу и к элементам подгруппы H, расположенным по вертикали выше в первой строке таблицы;

первым элементом *третьей строки*, считая слева направо, может быть любой элемент группы G, не вошедший в первую и вторую строки, а все остальные элементы этой строки получаются в результате применения заданной групповой операции «$\circ$» к её первому элементу и к соответствующим элементам подгруппы H, расположенным по вертикали выше в первой строке таблицы;

поступая аналогичным образом и далее,

……

будем создавать следующие строки таблицы до тех пор, пока не будут исчерпаны все элементы G, не вошедшие в таблицу, и создание таблицы не будет завершено.

Совокупность элементов *каждой строки* этой таблицы в случае коммутативной группы называется *смежным классом*, а элемент, стоящий на первом месте в каждой строке таблицы, считая слева направо, называется *образующим элементом* или *лидером* соответствующего смежного класса.

Из описанного способа построения табл. 2.4 следует, что если g – произвольный элемент G, а h – произвольный элемент H, то *левый смежный класс* $gH = \{g \circ h \mid h \in H\}$ *группы* G *по подгруппе* H и *правый смежный класс* $Hg = \{h \circ g \mid h \in H\}$ *группы* G *по подгруппе* H в случае коммутативной группы G совпадают:

$$gH = Hg = \{g \circ h \mid h \in H\}. \qquad (2\text{-}5e)$$

Построение табл. 2.4 с помощью изложенного алгоритма возможно лишь в том случае, если число её строк m и число её столбцов k таковы, что произведение mk в действительности равно порядку группы G, а k в действительности равно порядку группы H; возможность выполнения этих условий вытекает из доказываемых ниже теорем 2.2 и 2.3.

Таблица 2.4

$h_1 = g_1 =$ $=g_1 \circ h_1 = e$	$h_2 =$ $=g_1 \circ h_2$	$h_3 =$ $=g_1 \circ h_3$	$\ldots =$ $=\ldots$	$h_k =$ $=g_1 \circ h_k$
$g_2 \circ h_1$	$g_2 \circ h_2$	$g_2 \circ h_3$	$\cdots$	$g_2 \circ h_k$
$g_3 \circ h_1$	$g_3 \circ h_2$	$g_3 \circ h_3$	$\cdots$	$g_3 \circ h_k$
$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$
$g_m \circ h_1$	$g_m \circ h_2$	$g_m \circ h_3$	$\cdots$	$g_m \circ h_k$

ТЕОРЕМА 2.2. *Выполнение соотношения*

$$(g \circ \bar{g}') \in H \qquad (2\text{-}6)$$

является необходимым и достаточным условием того, чтобы элементы g и g' группы G принадлежали одному и тому же смежному классу разложения G по H.

ДОКАЗАТЕЛЬСТВО

НЕОБХОДИМОСТЬ. Предположим, что g и g' принадлежат одному и тому же смежному классу с лидером g_i:

$$g = g_i \circ h_j, \quad (2\text{-}6а) \qquad g' = g_i \circ h_k, \quad (2\text{-}6б)$$

где h_j и h_k – некоторые элементы H.

Из (2-6а) и (2-6б) с учётом (2-4) следует, что

$$g \circ \bar{g}' = (g_i \circ h_j)(\bar{g}_i \circ \bar{h}_k) = h_j \circ \bar{h}_k \in H, \qquad (2\text{-}6в)$$

т.е. выполняется (2-6).

ДОСТАТОЧНОСТЬ. Пусть для некоторых двух элементов g и g' группы G выполняется (2-6). Докажем, что в этом случае элементы g и g' принадлежат одному смежному классу разложения группы G по подгруппе H.

Допустим, что имеет место (2-6а). Тогда с учётом (2-6) имеем:

$$g \circ \bar{g}' = g_i \circ h_j \circ \bar{g}' = h_j \circ (g_i \circ \bar{g}') \in H,$$

откуда следует

$$(g_i \circ \bar{g}') = h_k \in H, \qquad (2\text{-}6г)$$

где h_k – некоторый элемент H. Из (2-6г) имеем

$$(g_i \circ \bar{g}') \circ g' = g_i(\bar{g}' \circ g') = g_i = h_k \circ g',$$

откуда следует:

$$g' = (g_i \circ \bar{h}_k), \qquad (2\text{-}6д)$$

т.е. доказано, что g и g' принадлежат одному и тому же смежному классу разложения группы G по подгруппе H, лидером которого является элемент g_i.

ЧТД

ТЕОРЕМА 2.3. *Каждый элемент группы G принадлежит одному и только одному смежному классу разложения группы G по подгруппе H.*

ДОКАЗАТЕЛЬСТВО. Из самого метода построения таблицы, являющейся разложением группы G по подгруппе H, следует, что каждый элемент G содержится в таблице, *по крайней мере, один раз*.

Покажем, что каждый элемент G содержится в таблице *только один раз*. Для этого докажем,

что никакие два элемента никакой одной и той же строки не могут быть одинаковыми, и

что никакие два элемента, принадлежащие двум любым различным строкам, также не могут быть одинаковыми.

Как уже говорилось, все элементы первой строки таблицы различны. Предположим, что два элемента некоторой

строки с первым элементом g_i, $i > 1$, равны: $g_i \circ h_j = g_i \circ h_k$ $(j \neq k)$, но тогда $h_j = h_k$, что невозможно, так как первая строка состоит только из *различных элементов*.

Предположим теперь, что два одинаковых элемента, находятся в разных строках:

$$(g_i \circ h_j) = (g_k \circ h_l), \qquad (2\text{-}6е)$$

где $i > k$.

Из (2-6е) следует, что

$$g_i = g_k \circ (h_l \circ \bar{h}_j); \qquad (2\text{-}6ё)$$

так как $(h_l \circ \bar{h}_j) \in H$, то из (2-6ё) следует, что g_i принадлежит k-му смежному классу, что противоречит правилу построения таблицы, согласно которому очередной лидер смежного класса должен выбираться из элементов G, не вошедших в предыдущие строки.

ЧТД

Число различных смежных классов в разложении группы G по подгруппе H называется «*индексом H в G*»; очевидно (см. табл. 2.4), что имеет место соотношение:

$$(\text{порядок } G) = (\text{порядок } H)(\text{индекс } H \text{ в } G). \qquad (2\text{-}6ж)$$

Справедлива следующая теорема Лагранжа.

ТЕОРЕМА 2.4. *Во всякой конечной группе порядок любой подгруппы является делителем порядка самой группы* [2.9, с. 404].

END

В случае коммутативной группы G, её подгруппа H называется *нормальной* или *нормальным делителем* [2.2, с.37; 2.3, с. 62; 2.9, с. 404].

ФАКТОР-ГРУППА

Пусть $\{g_i\}$ – смежный класс, содержащий g_i. В качестве представителя этого смежного класса $\{g_i\}$ может быть выбран его любой элемент. Операция над смежными классами – сложение или умножение – определяется правилом:

$$\{g_i\} \circ \{g_k\} = \{g_i \circ g_k\} = \{g_s\}, \qquad (2\text{-}6з)$$

которое означает, что выполнение операция «$\circ$» над любым элементом класса $\{g_i\}$ и над любым элементом класса $\{g_k\}$ даёт некоторый элемент класса $\{g_s\}$.

Легко убедиться, что смежные классы при введённой описанным образом бинарной операции над ними образуют группу. Эта группа называется фактор-группой и обозначается через G/H.

Так как операция над смежными классами была определена через бинарную операцию над элементами этих классов, то это обстоятельство упрощает изучение ряда её свойств.

1. Так как рассматриваемая операция определена для всех пар смежных классов, то она обладает свойством замкнутости.

2. Операция над смежными классами обладают свойствами ассоциативности и коммутативности, так как этими свойствами обладает операция над элементами группы G.

3. Единичным элементом фактор-группы является смежный класс $\{e\}$, образованный подгруппой H, так как

$$\{e\} \circ \{g_i\} = \{e \circ g_i\} = \{g_i\}. \qquad (2\text{-}6и)$$

4. Обратным элементом для смежного класса $\{g_i\}$ является смежный класс $\{\bar{g}_i\}$, так как

$$\{g_i\}\circ\{\bar{g}_i\} = \{g_i\circ\bar{g}_i\} = \{e\}. \qquad (2\text{-}6й)$$

ЦИКЛИЧЕСКАЯ ГРУППА

Рассмотрим дополнительно некоторые свойства мультипликативных групп конечного порядка.

Пусть g – некоторый элемент мультипликативной группы конечного порядка G. Очевидно, что из-за наличия свойства замкнутости групповой операции все степени g (g^1, g^2, …, g^i, …) также являются элементами G. Так как порядок G конечен, то должно иметь место равенство различных степеней g:

$$g^i = g^j, \quad j > i, \qquad (2\text{-}6к)$$

откуда следует $g^{j-i} = 1$ и, следовательно, некоторые *положительные* степени g равны 1. Определим наименьшее целое положительное число ξ, для которого выполняется соотношение: $g^\xi = 1$. Число ξ называется *периодом* или *порядком элемента* g.

Совокупность элементов $1, g, g^2, \ldots, g^{\xi-1}$ образует подгруппу группы G.

Легко убедиться, что с учётом определения периода ξ выполняются *достаточные условия* того, что эта совокупность элементов является подгруппой группы G: *наличие замкнутость* и *наличие обратных элементов*:

1) действительно, замкнутость для данной совокупности элементов имеет место, так как произведение любых двух элементов этой совокупности есть *некоторая степень элемента* g из совокупности целых чисел $\{0, 1, \ldots, \xi\text{-}1\}$;

2) обратным элементом для элемента g^i, $i \in \{0, 1, \ldots, \xi\text{-}1\}$, является элемент $g^{\xi-i}$.

ОПРЕДЕЛЕНИЕ 2.4. *Мультипликативная группа, образованная всеми степенями одного из её элементов, называется* ***циклической*** *группой.*

END

Приведём два свойства циклических групп.

1. Период ξ любого элемента g циклической группы G является делителем порядка этой группы.

Действительно, если ξ – период некоторого элемента g циклической группы G, то в G, согласно определению периода ξ элемента g группы G, существует подгруппа H порядка ξ и, следовательно, согласно (2-6ж) ξ является делителем порядка группы G.

2. Любая подгруппа циклической группы сама является циклической группой.

Это свойство является следствием определения понятия «подгруппы».

КОЛЬЦА

ОПРЕДЕЛЕНИЕ 2.5. ***Кольцом*** *называется множество элементов S, на котором определены две основные операции:*

сложение*, обозначаемое как $a + b$, и*

умножение*, обозначаемое как ab, даже если эти операции не являются обычными операциями сложения и умножения чисел,*

и выполняются аксиомы R 2.1 – R 2.4.

END

АКСИОМА R 2.1 *Множество S относительно операции сложения является аддитивной абелевой группой.*

END

АКСИОМА R 2.2 (*Замкнутость*). *Для любых двух элементов $a, b \in S$ определено произведение ab, причём $ab \in S$.*

END

АКСИОМА *R* 2.3 (*Ассоциативность*). *Для любых трёх элементов* $a, b, c \in S$ *справедливо соотношение*: $a(bc) = (ab)c$.

END

АКСИОМА *R* 2.4 (*Дистрибутивность*). *Для любых трёх элементов* $a, b, c \in S$ *справедливы соотношения*:

$$a(b + c) = ab + ac, \qquad (2\text{-}7)$$

$$(a + b)c = ac + bc. \qquad (2\text{-}8)$$

END

Если в кольце операция «·» является коммутативной, то это кольцо называется *коммутативным*.

Если в кольце существует единичный элемент *e* относительно операции «·», то кольцо называется *кольцом с мультипликативной единицей или с единицей по умножению*.

ТЕОРЕМА 2.5. *Для любых двух элементов a и b любого кольца справедливы соотношения*:

$$a0 = 0a = 0, \qquad (2\text{-}9)$$

$$a(-b) = (-a)b = -ab. \qquad (2\text{-}10)$$

ДОКАЗАТЕЛЬСТВО. Согласно аксиоме *R* 2.4 для любого элемента *a* любого кольца выполняется равенство $a(0 + 0) = a0 + a0$. Так как $0 + 0 = 0$, то $a0 = a0 + a0$. Согласно аксиоме *R* 2.1 элемент $a0$ должен иметь обратный элемент относительно операции сложения. Прибавляя этот обратный элемент к правой и левой частям последнего равенства, получим $0 = a0$. Аналогично докажем справедливость соотношения $0 = 0a$. Таким образом, справедливость соотношения (2-9) доказана.

Докажем соотношение (2-10). Очевидно, что $0 = a0 = a(b + (-b)) = ab + a(-b)$ и, следовательно, $a(-b) = -ab$. Аналогично доказывается справедливость соотношения $(-a)b = -ab$. Следовательно, справедливость соотношения (2-10) доказана.

Таким образом, кольцо имеет две операции – сложение и умножение, удовлетворяющие законам *A*1, *A*2, *A*3, *A*4, *A*5; *M*1, *M*2; *D*1, *D*2 соответственно, если к тому же операция умножения удовлетворяет закону *M*3, то кольцо называется *коммутативным* (см. табл. 2.1).

Кольцо, имеющее конечное число элементов, называется *конечным*; при этом число его элементов называется *порядком кольца*; в противном случае кольцо называется *бесконечным* (счётным или несчётным). Будем обозначать порядок кольца *R* как $|R|$.

Множество, состоящее из одного элемента 0, с операциями, определяемыми правилами $0 + 0 = 0$; $(0)(0) = 0$, является кольцом.

ПРИМЕР 2.8

1. Множество всех действительных чисел, множество всех рациональных чисел, множество всех целых чисел с операциями сложения и умножения являются (числовыми) кольцами.

2. Множество всех положительных вещественных чисел с операциями сложения и умножения не является кольцом, так как отсутствует свойство *A*5.

END

ПОЛЯ

ОПРЕДЕЛЕНИЕ 2.6. ***Полем*** *называется множество элементов S, на котором определены две основные операции – сложение и умножение, и эти операции обладают всеми свойствами, приведенными в табл.* 2.1, *кроме наличия обратного элемента для* 0 *в M*5.

END

ПРИМЕР 2.9

1. Множество всех рациональных чисел, множество всех действительных чисел, множество всех комплексных чи-