Глава вторая

ГРУППЫ

Содержание Объяснение основополагающих для всей книги важнейших теоретико-групповых понятий: группы, подгруппы, изоморфизма, гомоморфизма, нормальной подгруппы, факторгруппы.

§ 6. Понятие группы

Определение. Непустое множество $\mathfrak{G}$ элементов произвольной природы (например, чисел, отображений, преобразований) называется *группой*, если выполняются четыре следующих условия.

1. Задан *закон композиции*, который каждой паре элементов a, b из $\mathfrak{G}$ сопоставляет третий элемент этого же множества, называемый, как правило, *произведением* элементов a и b и обозначаемый через ab или через $a \cdot b$. (Произведение может зависеть от порядка следования сомножителей: не обязательно $ab = ba$.)

2. *Закон ассоциативности*. Для любых трех элементов a, b, c из $\mathfrak{G}$ имеет место равенство

$$ab \cdot c = a \cdot bc.$$

3. В $\mathfrak{G}$ существует (левая) *единица* e, т. е. элемент e, выделяемый следующим свойством:

$$ea = a \text{ для всех } a \text{ из } \mathfrak{G}.$$

4. Для каждого элемента a из $\mathfrak{G}$ существует (по крайней мере) один (левый) *обратный элемент* a^{-1} в $\mathfrak{G}$, определяемый свойством:

$$a^{-1}a = e.$$

Группа называется *абелевой*, если, кроме того, оказывается выполненным тождество $ab = ba$ (*закон коммутативности*).

Примеры. Если элементами рассматриваемого множества являются числа, а законом композиции служит обычное умножение, то для того, чтобы получить группу, прежде всего следует исключить нуль, потому что у него нет обратного элемента; все рациональные числа, отличные от нуля, уже образуют группу (единичным элементом является число 1). Точно так же образуют группу числа —1 и 1, а также число 1 само по себе.

Аддитивные группы. В определение понятия группы обозначение операции через $a \cdot b$ не входит: операцией может служить

и сложение, например, обычное сложение целых чисел или векторов. В этом случае в аксиомах 1 — 4 следует всюду вместо «произведение $a \cdot b$» читать «сумма $a+b$». Группа $\mathfrak{G}$ называется тогда *аддитивной группой* или *модулем*. Вместо единичного элемента e здесь фигурирует *нулевой элемент* 0 со свойством

$$0+a=a \text{ для всех } a \text{ из } \mathfrak{G},$$

а вместо обратного элемента a^{-1} — элемент $-a$ со свойством

$$-a+a=0.$$

Обычно предполагают, что сложение — коммутативная операция, т. е.

$$a+b=b+a.$$

Вместо $a+(-b)$ пишут кратко $a-b$. В этих обозначениях

$$(a-b)+b=a+(-b+b)=a+0=a.$$

Примеры. Целые числа образуют модуль; четные числа тоже.

Подстановки. Под *подстановкой* множества M мы подразумеваем взаимно однозначное отображение этого множества на себя, т. е. сопоставление s каждому элементу a из M некоторого образа $s(a)$, причем каждый элемент из M является образом в точности одного элемента a. Элемент $s(a)$ обозначают также через sa. В случае бесконечных множеств M подстановки называют также *преобразованиями*, но слово «преобразование» в дальнейшем у нас будет использоваться как синоним слова «отображение».

Если множество M конечно и его элементы занумерованы числами $1, 2, \ldots, n$, то каждую подстановку можно полностью описать схемой, в которой под каждым номером k указывается номер $s(k)$ элемента, являющегося образом элемента с номером k. Например, схема

$$s=\begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 4 & 3 & 1\end{pmatrix}$$

изображает подстановку цифр 1, 2, 3, 4, в которой 1 переходит в 2, 2 переходит в 4, 3 переходит в 3 и 4 переходит в 1.

Под *произведением* st двух подстановок s и t понимается подстановка, которую мы получаем, осуществляя сначала подстановку t, а затем применяя к результату подстановку s [1]), т. е.

$$st(a)=s(t(a)).$$

Например, для $s=\begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 4 & 3 & 1\end{pmatrix}$ и $t=\begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 1 & 4 & 3\end{pmatrix}$ произведение $st=\begin{pmatrix}1 & 2 & 3 & 4\\ 4 & 2 & 1 & 3\end{pmatrix}$. Аналогично, $ts=\begin{pmatrix}1 & 2 & 3 & 4\\ 1 & 3 & 4 & 2\end{pmatrix}$.

---

[1]) Порядок следования сомножителей — дело соглашения. У других авторов st обозначает иногда «сначала s, потом t».

Закон ассоциативности

$$(rs)\,t = r\,(st)$$

в общем случае произвольных отображений можно доказать так: применим обе части к произвольному объекту a; тогда

$$(rs)\,t\,(a) = (rs)\,(t\,(a)) = r\,(s\,(t\,(a))),$$
$$r\,(st)\,(a) = r\,(st\,(a)) = r\,(s\,(t\,(a))),$$

т. е. в обоих случаях получается одно и то же.

Тождественной или *единичной подстановкой* является такое отображение I, которое каждый объект переводит в себя самого:

$$I\,(a) = a.$$

Тождественная подстановка обладает, очевидно, характерным свойством единичного элемента группы: для каждой подстановки s имеет место равенство $Is = s$. Вместо I иногда пишут также 1.

Подстановкой, *обратной* к подстановке s, является такая подстановка, которая переводит $s\,(a)$ в a, тогда как s действует наоборот. Если ее обозначить через s^{-1}, то можно будет записать равенство

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

а также равенство

$$s^{-1}s = I.$$

Задача 1. Непустое множество $\mathfrak{G}$ преобразований некоторого множества M является группой, если: а) вместе с двумя любыми преобразованиями оно содержит их произведение и б) вместе с каждым преобразованием содержит обратное к нему.

Задача 2. Повороты плоскости вокруг фиксированной точки P образуют абелеву группу. Но если к этому добавить еще и отражения относительно всех прямых, проходящих через точку P, то получится уже неабелева группа.

Задача 3. Доказать, что элементы e, a с законом композиции

$$ee = e, \quad ea = a, \quad ae = a, \quad aa = e$$

образуют (абелеву) группу.

Замечание. Закон композиции в группе можно представить с помощью «групповой таблицы»; ею служит таблица с двумя входами, в которую заносится произведение каждых двух элементов. Например, таблица для приведенной выше группы следующая:

	e	a
e	e	a
a	a	e

Задача 4. Составить таблицу для группы подстановок трех чисел.

Из доказанного следует, что аксиомы 1—4 выполнены для совокупности подстановок произвольного множества M. Следовательно, эти подстановки образуют группу. Для конечного мно-

жества M из n элементов группу подстановок называют также *симметрической группой* и обозначают через $\mathfrak{S}_n$ [1]).

Вернемся теперь к общей теории групп.

Вместо $ab \cdot c$ или $a \cdot bc$ пишут кратко abc.

Из аксиом 3 и 4 следует, что

$$a^{-1}aa^{-1} = ea^{-1} = a^{-1};$$

таким образом, если умножить последнее равенство слева на элемент, обратный к a^{-1}, то получится

$$eaa^{-1} = e$$

или

$$aa^{-1} = e;$$

иными словами, каждый левый обратный элемент является и правым обратным. Таким же способом устанавливается, что обратным к a^{-1} служит a. Далее:

$$ae = aa^{-1}a = ea = a,$$

т. е. каждая левая единица является и правой единицей.

Отсюда следует *возможность* (двустороннего) *деления*:

5. *Уравнение $ax = b$ обладает решением в группе $\mathfrak{G}$, как и уравнение $ya = b$, где a и b — произвольные элементы из $\mathfrak{G}$.*

А именно, этими решениями служат $x = a^{-1}b$ и $y = ba^{-1}$, так как

$$a(a^{-1}b) = (aa^{-1})b = eb = b,$$
$$(ba^{-1})a = b(a^{-1}a) = be = b.$$

Столь же просто доказывается и *однозначность деления:*

6. *Из $ax = ax'$ и из $xa = x'a$ следует, что $x = x'$.*

Умножая обе части равенства $ax = ax'$ на a^{-1}, получаем $x = x'$. Точно так же доказывается вторая часть утверждения.

В частности, отсюда следует единственность единичного элемента (как решения уравнения $xa = a$) и единственность обратного элемента (как решения уравнения $xa = e$). Единичный элемент часто будет обозначаться через 1.

Возможность деления, указанная в утверждении 5, в качестве аксиомы может заменить аксиомы 3 и 4. Действительно, предположим, что 1, 2 и 5 выполнены и попробуем сначала доказать 3. Выберем произвольный элемент c и будем подразумевать под e решение уравнения $xc = c$. Тогда

$$ec = c.$$

---

[1]) Это название выбрано в соответствии с тем, что функции от $x_1, \ldots, x_n$, остающиеся инвариантными при действии подстановок рассматриваемой группы, являются «симметрическими функциями».

Для произвольного же a решим уравнение

$$cx = a.$$

Тогда

$$ea = ecx = cx = a,$$

откуда следует 3. Аксиома 4 является непосредственным следствием разрешимости уравнения $xa = e$.

В соответствии с этим мы можем вместо 1, 2, 3, 4 равным образом использовать 1, 2 и 5 как аксиомы группы.

Если $\mathfrak{G}$ — *конечное множество, то условие* 5 *можно вывести из условия* 6. Для этого нужно использовать не возможность деления, а (кроме аксиом 1 и 2) лишь его однозначность.

Доказательство. Пусть a — произвольный элемент. Сопоставим каждому элементу x элемент ax. Согласно условию 6 это сопоставление однозначно обратимо, т. е. оно взаимно однозначно отображает множество $\mathfrak{G}$ на некоторое подмножество произведений ax. Поскольку $\mathfrak{G}$ конечно, оно не может взаимно однозначно отображаться на собственное подмножество. Поэтому совокупность элементов ax должна совпадать с $\mathfrak{G}$, а это означает, что каждый элемент b записывается в виде $b = ax$, как утверждает первое из условий в 5. Точно так же доказывается разрешимость уравнений $b = xa$. Таким образом, 5 следует из 6.

Число элементов конечной группы называется ее *порядком*.

Дальнейшие правила оперирования. Для элемента, обратного к произведению, имеет место равенство:

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

Действительно,

$$(b^{-1}a^{-1})\,ab = b^{-1}\,(a^{-1}ab) = b^{-1}b = e.$$

Сложные произведения и суммы. Степени. Подобно тому как вместо $ab \cdot c$ мы стали кратко записывать abc, введем *сложные произведения* многих сомножителей

$$\prod_{\nu=1}^{n} a_\nu = \prod_{1}^{n} a_\nu = a_1 a_2 \ldots a_n.$$

Пусть даны $a_1, \ldots, a_N$; определим по индукции (для $n < N$):

$$\left.\begin{aligned} &\prod_{1}^{1} a_\nu = a_1, \\ &\prod_{1}^{n+1} a_\nu = \left(\prod_{1}^{n} a_\nu\right) \cdot a_{n+1}\,{}^{1)}. \end{aligned}\right\}$$

---

[1]) Символ ν, обозначающий переменный индекс, можно, конечно, заменить на любой другой, не меняя значения произведения.

В частности, $\prod_1^3 a_\nu$ — это наше прежнее $a_1a_2a_3$, а $\prod_1^4 a_\nu = a_1a_2a_3a_4 = (a_1a_2a_3)\,a_4$ и т. д.

Докажем, используя лишь один закон ассоциативности, следующее правило:

$$\prod_{\mu=1}^{m} a_\mu \cdot \prod_{\nu=1}^{n} a_{m+\nu} = \prod_{\nu=1}^{m+n} a_\nu. \tag{1}$$

Словами: *произведение двух сложных произведений является сложным произведением всех участвующих сомножителей в их прежнем порядке.* Например,

$$(ab)(cd) = abcd$$

является частным случаем равенства (1).

Формула (1) очевидна при $n=1$ (по определению символа $\prod$). Если она уже доказана для некоторого значения n, то для следующего значения $n+1$ имеем:

$$\prod_1^m a_\mu \cdot \prod_1^{n+1} a_{m+\nu} = \prod_1^m a_\mu \cdot \left(\prod_1^n a_{m+\nu} \cdot a_{m+n+1}\right) =$$

$$= \left(\prod_1^m a_\mu \cdot \prod_1^n a_{m+\nu}\right) a_{m+n+1} = \left(\prod_1^{m+n} a_\mu\right) a_{m+n+1} = \prod_1^{m+n+1} a_\nu.$$

Тем самым доказано (1).

Замечание. Вместо $\prod_1^n a_{m+\nu}$ пишут также $\prod_{m+1}^{m+n} a_\nu$. Кроме того, в отдельных случаях, если это удобно, пишут $\prod_1^0 a_\nu = e$.

Произведение n одинаковых сомножителей называется *степенью:*

$$a^n = \prod_1^n a \quad (\text{в частности, } a^1 = a,\ a^2 = aa \text{ и т. д.})$$

Из доказанной теоремы следует, что

$$a^n \cdot a^m = a^{n+m}. \tag{2}$$

Далее:

$$(a^m)^n = a^{mn}. \tag{3}$$

Доказательство (с помощью индукции) оставляется читателю.

Для доказательства появлявшихся до сих пор правил (1), (2) и (3) требовался лишь закон ассоциативности; поэтому они будут выполнены всякий раз, когда в рассматриваемой области определены произведения и справедлив закон ассоциативности (например, в области натуральных чисел), даже если эта область не является группой.

Если умножение, кроме того, и коммутативно (случай абелевой группы), то можно доказать большее: значение сложного произведения не зависит от порядка следования сомножителей. Точнее: *если* φ — *взаимно однозначное отображение отрезка* $(1, n)$ *натурального ряда на себя, то*

$$\prod_{\nu=1}^{n} a_{\varphi(\nu)} = \prod_{1}^{n} a_\nu.$$

Доказательство. Для $n=1$ утверждение очевидно. Поэтому будем предполагать его справедливым и для $n-1$. Пусть число k отображается на n: $\varphi(k)=n$. Тогда

$$\prod_{1}^{n} a_{\varphi(\nu)} = \prod_{1}^{k-1} a_{\varphi(\nu)} \cdot a_{\varphi(k)} \cdot \prod_{1}^{n-k} a_{\varphi(k+\nu)} = \left(\prod_{1}^{k-1} a_{\varphi(\nu)} \cdot \prod_{1}^{n-k} a_{\varphi(k+\nu)}\right) \cdot a_n \text{ [1]}.$$

Заключенное в скобки произведение содержит лишь сомножители $a_1, \ldots, a_{n-1}$ в произвольном порядке. По предположению индукции это выражение равно $\prod_{1}^{n-1} a_\nu$. Поэтому

$$\prod_{1}^{n} a_{\varphi(\nu)} = \prod_{1}^{n-1} a_\nu \cdot a_n = \prod_{1}^{n} a_\nu.$$

Из доказанного правила следует, что в абелевых группах законна запись вида

$$\prod_{1 \leqslant i < k \leqslant n} a_{ik}$$

или

$$\prod_{i<k} a_{ik} \quad (i=1, \ldots, n;\ k=1, \ldots, n),$$

означающая, что множество пар индексов i, k, подчиненных условию $1 \leqslant i < k \leqslant n$, перенумеровано каким-нибудь (безразлично, каким) способом, а затем образовано произведение.

В произвольной группе обычным способом определяются нулевая и отрицательная степени любого элемента a:

$$a^0 = 1,$$
$$a^{-n} = (a^{-1})^n,$$

и без труда показывается, что правила (2), (3) выполняются для любых целочисленных показателей.

В аддитивной группе вместо $\prod_{1}^{n} a_\nu$ пишут $\sum_{1}^{n} a_\nu$, а вместо

---

[1]) В случае $k=1$ опускается первый сомножитель, а в случае $k=n$ — второй; доказательству это не мешает.

a^n — соответственно na. Все доказанное для произведений переносится теперь и на суммы.

Правило (3), записанное аддитивно, имеет вид закона ассоциативности

$$n \cdot ma = nm \cdot a,$$

в то время как (2) имеет вид закона дистрибутивности:

$$ma + na = (m + n)\, a.$$

К этим двум законам присоединяется еще один закон дистрибутивности:

$$m\,(a + b) = ma + mb$$

(в мультипликативной записи: $(ab)^m = a^m b^m$), который, однако, имеет место лишь в абелевых группах. Это легко доказать с помощью индукции.

Задача 5. Доказать, что в абелевой группе

$$\prod_{\nu=1}^{n} \prod_{\mu=1}^{m} a_{\mu\nu} = \prod_{\mu=1}^{m} \prod_{\nu=1}^{n} a_{\mu\nu}.$$

Задача 6. При тех же условиях

$$\prod_{\nu=1}^{n} \prod_{\mu=1}^{\nu} a_{\mu\nu} = \prod_{\mu=1}^{n} \prod_{\nu=\mu}^{n} a_{\mu\nu}.$$

Задача 7. Порядок симметрической группы $\mathfrak{S}_n$ равен $n! = \prod_{1}^{n} \nu$. (Индукция по n.)

§ 7. Подгруппы

Чтобы непустое подмножество $\mathfrak{g}$ группы $\mathfrak{G}$ само было группой с тем же законом композиции, что и в $\mathfrak{G}$, необходимо и достаточно, чтобы выполнялись аксиомы 1, 2, 3, 4. Аксиома 1 утверждает, что если a и b лежат в $\mathfrak{g}$, то и их произведение ab также лежит в $\mathfrak{g}$. Аксиома 2 выполняется в $\mathfrak{g}$, если она выполняется в $\mathfrak{G}$. Аксиомы 3 и 4 означают, что в $\mathfrak{g}$ лежит единичный элемент и что вместе с каждым элементом a в множестве $\mathfrak{g}$ лежит обратный к нему элемент a^{-1}. В данном случае требование о единичном элементе излишне, потому что если a — любой элемент из $\mathfrak{g}$, то a^{-1} лежит в $\mathfrak{g}$, и, следовательно, произведение $aa^{-1} = e$ также лежит в $\mathfrak{g}$. Тем самым доказано:

для того чтобы непустое подмножество $\mathfrak{g}$ данной группы $\mathfrak{G}$ было подгруппой, необходимо и достаточно выполнение следующих условий:

1) *множество $\mathfrak{g}$ содержит вместе с любыми двумя своими элементами и их произведение;*

2) *множество* $\mathfrak{g}$ *содержит вместе с каждым своим элементом* a *обратный к нему элемент* a^{-1}.

Если, в частности, множество $\mathfrak{g}$ *конечно*, то второе из этих требований даже излишне, потому что в этом случае требования 3 и 4 могут быть заменены на требование 6, а оно, будучи выполненным в $\mathfrak{G}$, обязательно выполняется и в $\mathfrak{g}$.

Вообще, условия 1) и 2) можно объединить в одно: множество $\mathfrak{g}$ должно вместе с любыми двумя своими элементами a и b содержать произведение ab^{-1}. Тогда $\mathfrak{g}$ содержит вместе с a и единицу $aa^{-1}=e$, и обратный элемент $ea^{-1}=a^{-1}$, а потому вместе с a, b и элемент b^{-1}, и произведение $a(b^{-1})^{-1}=ab$.

Если (в абелевой группе) групповые соотношения записаны аддитивно, то подгруппа характеризуется тем, что вместе с любыми двумя своими элементами a, b она содержит $a+b$, а вместе с a и элемент $-a$. Оба эти требования можно объединить в одно: вместе с a и b в подгруппе должен лежать элемент $a-b$.

Примеры подгрупп.

Каждая группа имеет в качестве подгруппы *единичную группу* $\mathfrak{E}$, состоящую из одного-единственного единичного элемента.

Важнейшей подгруппой симметрической группы $\mathfrak{S}_n$ всех подстановок n объектов является *знакопеременная группа* $\mathfrak{A}_n$, состоящая из тех подстановок, которые, будучи применены к переменным $x_1, \ldots, x_n$, переводят функцию

$$\Delta=\prod_{i<k}(x_i-x_k) \tag{1}$$

в себя. Такие подстановки называются *четными*, а остальные — *нечетными*. Последние меняют знак у функции Δ. Каждая *транспозиция* (т. е. подстановка, меняющая местами две цифры) является нечетной подстановкой. Произведение двух четных или двух нечетных подстановок — четная подстановка; произведение четной и нечетной подстановки — нечетная подстановка. Из первого свойства следует, что $\mathfrak{A}_n$ — группа. Так как фиксированная транспозиция при умножении переводит четные подстановки в нечетные и наоборот, количество четных и нечетных подстановок одинаково и равно $n!/2$ (ср. § 6, задача 7).

Для более удобного описания подгрупп симметрической группы $\mathfrak{S}_n$ используют известное *представление подстановок циклами:*

Символом $(p\ q\ r\ s)$ обозначается циклическая подстановка, переводящая p в q, q в r, r в s и s в p и оставляющая все остальные объекты неподвижными. Легко показать, что любая подстановка представляется однозначно (с точностью до порядка следования) в виде произведения циклических подстановок или «циклов»:

$$(i\ k\ l\ldots)(p\ q\ldots)\ldots,$$

где любые два цикла не имеют ни одного общего элемента. Сомножители

в этом произведении перестановочны Цикл из одного элемента, скажем (1), представляет тождественную подстановку. Конечно, имеет место равенство

$$(1\,2\,5\,4) = (2\,5\,4\,1) \text{ и т. п}$$

С помощью таких символов мы можем следующим образом представить $3! = 6$ подстановок группы $\mathfrak{S}_3$:

$$(1),\ (1\,2),\ (1\,3),\ (2\,3),\ (1\,2\,3),\ (1\,3\,2).$$

Все подгруппы в данном случае легко определяются. Вот они (кроме самой группы $\mathfrak{S}_3$):

$\mathfrak{A}_3$: (1), (1 2 3), (1 3 2);
$\mathfrak{S}_1'$: (1), (2 3); $\mathfrak{S}_2'$: (1), (1 3); $\mathfrak{S}_3'$: (1), (1 2);
$\mathfrak{G}$: (1).

Пусть a, b, ... — произвольные элементы некоторой группы $\mathfrak{G}$; тогда, кроме группы $\mathfrak{G}$, в ней могут быть такие подгруппы, которые содержат элементы a, b, ... Пересечение всех этих подгрупп снова является некоторой группой $\mathfrak{A}$. Говорят, что a, b, ... *порождают* группу $\mathfrak{A}$. Она обязательно содержит произведения типа $a^{-1}a^{-1}bab^{-1}$ (составленные из конечного числа сомножителей с повторениями или без). Такие произведения образуют группу, которая содержит элементы a, b, ... и, следовательно, включает в себя группу $\mathfrak{A}$. Поэтому она совпадает с $\mathfrak{A}$. Мы доказали следующее:

Группа, порожденная элементами a, b, ..., состоит из всевозможных конечных произведений этих элементов и элементов, обратных к ним.

В частности, отдельный элемент a порождает группу всех своих степеней $a^{\pm n}$ (включая $a^0 = e$). Так как

$$a^n a^m = a^{n+m} = a^m a^n,$$

эта группа абелева.

Группа, состоящая из степеней одного элемента, называется *циклической*.

Существуют две возможности. Либо все степени a^h различны; тогда циклическая группа

$$\ldots,\ a^{-2},\ a^{-1},\ a^0,\ a^1,\ a^2,\ \ldots$$

бесконечна. Либо они повторяются и оказывается, что

$$a^h = a^k,\ h > k.$$

Тогда

$$a^{h-k} = e \quad (h - k > 0).$$

Пусть в этом случае n — наименьший положительный показатель, при котором $a^n = e$. Тогда степени a^0, a^1, a^2, ..., a^{n-1} различны, потому что иначе

$$a^h = a^k \quad (0 \leqslant k < h < n),$$

а отсюда следовало бы, что

$$a^{h-k}=e \qquad (0<h-k<n),$$

что противоречит выбору числа n.

Если произвольное целое число m представить в виде

$$m=qn+r \qquad (0\leqslant r<n)$$

то окажется, что

$$a^m=a^{qn+r}=a^{qn}\cdot a^r=(a^n)^q\,a^r=ea^r=a^r.$$

Таким образом, все степени элемента a уже встречаются в серии $a^0, a^1, \ldots, a^{n-1}$. Поэтому циклическая группа содержит в точности n элементов, а именно — элементы

$$a^0,\ a^1,\ \ldots,\ a^{n-1}.$$

Число n — порядок циклической группы, порожденной элементом a, — называется *порядком элемента* a. Если все степени элемента a различны, то a называется *элементом бесконечного порядка*.

Примеры. Целые числа

$$\ldots,\ -2,\ -1,\ 0,\ 1,\ 2,\ldots$$

со сложением в качестве композиции образуют бесконечную циклическую группу. Описанные выше группы $\mathfrak{S}_i'$ $(i=1,\ 2,\ 3)$ и $\mathfrak{A}_3$ являются циклическими группами порядков 2, 3.

Задача 1. Существуют циклические группы подстановок любого порядка.

Задача 2. Доказать индукцией по n, что $n-1$ транспозиций (1 2), (1 3), ... (1 n) при $n>1$ порождают симметрическую группу $\mathfrak{S}_n$.

Задача 3. Точно так же $n-2$ тройных циклов (1 2 3), (1 2 4), ... (1 2 n) при $n>2$ порождают знакопеременную группу $\mathfrak{A}_n$.

Определим теперь все подгруппы циклической группы. Пусть $\mathfrak{G}$ — произвольная циклическая группа с образующей a и $\mathfrak{g}$ — подгруппа, состоящая не только из единицы. Если $\mathfrak{g}$ содержит элемент a^{-m} с отрицательным показателем, то и обратный к нему элемент лежит в $\mathfrak{g}$. Пусть a^m — элемент в $\mathfrak{g}$ с наименьшим положительным показателем. Докажем, что все элементы из $\mathfrak{g}$ являются степенями элемента a^m. Действительно, если a^s — произвольный элемент из $\mathfrak{g}$, то можно вновь считать, что

$$s=qm+r \qquad (0\leqslant r<m).$$

Тогда $a^s(a^m)^{-q}=a^{s-mq}=a^r$ — элемент из $\mathfrak{g}$ с $r<m$. Отсюда следует, что $r=0$ в силу выбора числа m и, следовательно, $s=qm$ и $a^s=(a^m)^q$. Таким образом, все элементы подгруппы $\mathfrak{g}$ являются степенями элемента a^m.

Если элемент a имеет конечный порядок n, т. е. $a^n=e$, то элемент $a^n=e$ должен лежать в $\mathfrak{g}$, а потому число n должно

делиться на m: $n = qm$. Подгруппа $\mathfrak{g}$ состоит в таком случае из элементов $a^m, a^{2m}, \ldots, a^{qm} = e$ и имеет порядок q. Но если a имеет бесконечный порядок, то и группа $\mathfrak{g}$, состоящая из элементов, $e, a^{\pm m}, a^{\pm 2m}, \ldots$, имеет бесконечный порядок. Тем самым мы доказали следующее:

Подгруппа циклической группы снова циклическая. Она состоит либо из единицы, либо из степеней элемента a^m с наименьшим возможным положительным показателем m. Другими словами, она состоит из m-х степеней элементов исходной группы. При этом для бесконечной циклической группы число m произвольно, в то время как для циклической группы конечного порядка n число m должно быть некоторым делителем числа n. В этом случае подгруппа имеет порядок $q = \frac{n}{m}$. Для каждого такого числа m существует одна и только одна подгруппа порядка $\frac{n}{m}$ в группе $\{a\}$, а именно $\{a^m\}$.

§ 8. Операции над комплексами. Смежные классы

Под *комплексом* в теории групп подразумевается произвольное множество элементов группы $\mathfrak{G}$.

Под *произведением* $\mathfrak{g}\mathfrak{h}$ *двух комплексов* $\mathfrak{g}$ *и* $\mathfrak{h}$ понимается множество всех произведений gh, где g — элемент из $\mathfrak{g}$, а h — элемент из $\mathfrak{h}$. Если в произведении $\mathfrak{g}\mathfrak{h}$ один из комплексов, скажем, $\mathfrak{g}$, состоит из единственного элемента g, то вместо $\mathfrak{g}\mathfrak{h}$ пишут просто $g\mathfrak{h}$.

Очевидно, имеет место равенство

$$\mathfrak{g}(\mathfrak{h}\mathfrak{f}) = (\mathfrak{g}\mathfrak{h})\mathfrak{f}.$$

Таким образом, в сложных произведениях комплексов мы можем опускать скобки (ср. § 6, (1)).

Если комплекс $\mathfrak{g}$ является группой, то

$$\mathfrak{g}\mathfrak{g} = \mathfrak{g}.$$

Пусть $\mathfrak{g}$ и $\mathfrak{h}$ — подгруппы группы $\mathfrak{G}$. При каких условиях произведение $\mathfrak{g}\mathfrak{h}$ снова является группой? Совокупностью элементов, обратных к элементам из $\mathfrak{g}\mathfrak{h}$, является $\mathfrak{h}\mathfrak{g}$, так как обратным к gh служит элемент $h^{-1}g^{-1}$. Таким образом, если $\mathfrak{g}\mathfrak{h}$ — группа, то

$$\mathfrak{h}\mathfrak{g} = \mathfrak{g}\mathfrak{h}, \tag{1}$$

т. е. $\mathfrak{g}$ и $\mathfrak{h}$ должны быть перестановочными. Но это условие является и достаточным, так как если оно выполнено, то $\mathfrak{g}\mathfrak{h}$ содержит вместе с каждым элементом gh обратный к нему элемент $h^{-1}g^{-1}$ и вместе с любыми двумя элементами — их произведение, потому что

$$\mathfrak{g}\mathfrak{h}\mathfrak{g}\mathfrak{h} = \mathfrak{g}\mathfrak{g}\mathfrak{h}\mathfrak{h} = \mathfrak{g}\mathfrak{h}.$$

Итак: *произведение* $\mathfrak{g}\mathfrak{h}$ *двух подгрупп* $\mathfrak{g}$ *и* $\mathfrak{h}$ *некоторой группы* $\mathfrak{G}$

является группой тогда и только тогда, когда подгруппы $\mathfrak{g}$ *и* $\mathfrak{h}$ *перестановочны.* При этом, конечно, не требуется, чтобы каждый элемент из $\mathfrak{g}$ был перестановочен с каждым элементом из $\mathfrak{h}$. Если условие перестановочности (1) выполнено, то произведение $\mathfrak{g}\mathfrak{h}$ является подгруппой, порожденной $\mathfrak{g}$ и $\mathfrak{h}$.

В любой абелевой группе равенство (1) выполняется. Если абелева группа записана аддитивно, то $\mathfrak{g}$ и $\mathfrak{h}$ являются подмодулями некоторого модуля и пишут $(\mathfrak{g}, \mathfrak{h})$ вместо $\mathfrak{g}\mathfrak{h}$, так как обозначение $\mathfrak{g}+\mathfrak{h}$ предназначается для частного случая «прямой суммы» комплексов, о которой речь впереди.

Если $\mathfrak{g}$ — подгруппа и a — элемент группы $\mathfrak{G}$, то комплекс $a\mathfrak{g}$ называется *левым смежным классом*, а комплекс $\mathfrak{g}a$ — *правым смежным классом* группы $\mathfrak{G}$ по подгруппе $\mathfrak{g}$. Если a лежит в $\mathfrak{g}$, то $a\mathfrak{g}=\mathfrak{g}$; таким образом, всегда одним из левых (равно как и одним из правых) смежных классов по подгруппе $\mathfrak{g}$ является сама эта подгруппа.

В дальнейшем будут в основном рассматриваться левые смежные классы, хотя проводимые рассмотрения приводят к тем же выводам и в случае правых смежных классов.

Два смежных класса $a\mathfrak{g}$, $b\mathfrak{g}$ могут быть равными, даже если a и b не равны. Это происходит тогда, когда $a^{-1}b$ лежит в $\mathfrak{g}$:

$$b\mathfrak{g}=aa^{-1}b\mathfrak{g}=a(a^{-1}b\mathfrak{g})=a\mathfrak{g}.$$

Два *различных* смежных класса не имеют ни одного общего элемента. Если бы смежные классы $a\mathfrak{g}$ и $b\mathfrak{g}$ содержали общий элемент, скажем,

$$ag_1=bg_2,$$

то отсюда следовало бы, что

$$g_1g_2^{-1}=a^{-1}b,$$

и получилось бы, что $a^{-1}b$ лежит в $\mathfrak{g}$. В силу сказанного выше это означает, что $a\mathfrak{g}$ и $b\mathfrak{g}$ совпадают.

Каждый элемент a принадлежит некоторому смежному классу, а именно классу $a\mathfrak{g}$: этот класс содержит элемент $ae=a$. В силу доказанного выше элемент a принадлежит только одному смежному классу. Поэтому мы можем рассматривать каждый элемент a как *представитель* содержащего его смежного класса $a\mathfrak{g}$.

В соответствии со сказанным выше смежные классы образуют *разбиение группы* $\mathfrak{G}$ *на классы.* Каждый элемент принадлежит одному и только одному (смежному) классу [1]).

---

[1]) В литературе можно часто найти обозначение, введенное Галуа:

$$\mathfrak{G}=a_1\mathfrak{g}+a_2\mathfrak{g}+\dots,$$

которое говорит о том, что классы $a_\nu\mathfrak{g}$ попарно не пересекаются и все вместе составляют группу $\mathfrak{G}$. Этого способа записи мы избегаем, потому что оставляем символ $+$ для прямой суммы, которая будет введена позднее.

Любые два смежных класса равномощны: сопоставление $ag \longmapsto bg$ определяет взаимно однозначное отображение из $a\mathfrak{g}$ на $b\mathfrak{g}$.

За исключением самой подгруппы $\mathfrak{g}$, смежные классы не являются группами, потому что группа должна содержать единицу.

Число различных смежных классов группы $\mathfrak{G}$ по подгруппе $\mathfrak{g}$ называется *индексом* подгруппы $\mathfrak{g}$ в $\mathfrak{G}$. Индекс может быть конечным и бесконечным.

Если N — порядок (конечной) группы $\mathfrak{G}$, n — порядок и j — индекс подгруппы $\mathfrak{g}$, то имеет место соотношение:

$$N = jn; \tag{2}$$

действительно, $\mathfrak{G}$ распадается на j классов, состоящих из n элементов [1]).

Для конечных групп из равенства (2) можно выразить индекс j:

$$j = N/n.$$

Следствие. *Порядок подгруппы конечной группы является делителем порядка всей группы.*

В частности, если в качестве подгруппы взять циклическую группу, порожденную некоторым элементом c, то отсюда получится:

Порядок элемента конечной группы является делителем порядка всей группы.

Вот непосредственное следствие этого утверждения: *в любой группе из n элементов для произвольного элемента a имеет место равенство $a^n = e$.*

Может оказаться, что все левые смежные классы $a\mathfrak{g}$ равны правым смежным классам. Если это так, то тот левый смежный класс, который содержит элемент a, должен совпадать с правым смежным классом, содержащим тот же элемент a, т. е. для любого элемента a должно иметь место равенство комплексов:

$$a\mathfrak{g} = \mathfrak{g}a. \tag{3}$$

Подгруппу $\mathfrak{g}$, удовлетворяющую равенствам (3), т.е. перестановочную с любым элементом a из $\mathfrak{G}$, называют *нормальной* или *инвариантной подгруппой* группы $\mathfrak{G}$.

Если $\mathfrak{g}$ — нормальная подгруппа, то произведение двух смежных классов снова является смежным классом:

$$a\mathfrak{g} \cdot b\mathfrak{g} = a \cdot \mathfrak{g}b \cdot \mathfrak{g} = ab\mathfrak{g}\mathfrak{g} = ab\mathfrak{g}.$$

Задача 1. Найти для подгрупп группы $\mathfrak{S}_3$ правые и левые смежные классы. Какие из этих подгрупп являются нормальными?

---

[1]) Это соотношение остается верным и тогда, когда N бесконечно; только в этом случае для придания смысла произведению нужно ввести произведения кардинальных чисел, чего мы не сделали.

Задача 2. Показать, что элементы, обратные к элементам левого смежного класса по произвольной подгруппе, составляют правый смежный класс. Сделать отсюда вывод: индекс подгруппы можно также определить и как число правых смежных классов по ней.

Задача 3. Показать, что каждая подгруппа индекса 2 является нормальной. Пример: знакопеременная группа в симметрической группе на n символах.

Задача 4. Любая подгруппа абелевой группы всегда является нормальной.

Задача 5. Если $\mathfrak{G}$ — циклическая группа, порожденная элементом a, $\mathfrak{g}$ — ее произвольная подгруппа, отличная от $\mathfrak{G}$, порожденная степенью a^m при минимальном m (ср. § 7), то элементы $1, a, a^2, \ldots, a^{m-1}$ являются представителями смежных классов и число m равно индексу подгруппы $\mathfrak{g}$ в группе $\mathfrak{G}$.

Задача 6. Если произведение двух любых левых смежных классов группы $\mathfrak{G}$ по подгруппе $\mathfrak{g}$ снова является левым смежным классом, то $\mathfrak{g}$ — нормальная подгруппа в $\mathfrak{G}$.

§ 9. Изоморфизмы и автоморфизмы

Пусть даны два множества: $\mathfrak{M}$ и $\overline{\mathfrak{M}}$, в каждом из которых определены какие-то соотношения между элементами. Например, можно считать, что $\mathfrak{M}$ и $\overline{\mathfrak{M}}$ — группы, а соотношения в них — это равенства $a \cdot b = c$, выражающие групповое свойство. Или же можно считать, что $\mathfrak{M}$ и $\overline{\mathfrak{M}}$ — упорядоченные множества, а соотношения — это неравенства $a > b$.

Предположим, что можно установить взаимно однозначное отображение множеств $\mathfrak{M}$ и $\overline{\mathfrak{M}}$ друг на друга, при котором сохраняются соотношения; это означает, что если элементу a из $\mathfrak{M}$ взаимно однозначно соответствует элемент $\bar{a}$ из $\overline{\mathfrak{M}}$, то соотношения, выполняющиеся для произвольных элементов $a, b, \ldots$ из $\mathfrak{M}$, выполняются и для элементов $\bar{a}, \bar{b}, \ldots$ и наоборот. В этом случае множества $\mathfrak{M}$ и $\overline{\mathfrak{M}}$ называют *изоморфными* (относительно данных соотношений) и пишут $\mathfrak{M} \cong \overline{\mathfrak{M}}$. Само отображение называется *изоморфизмом*.

Таким образом, можно говорить об *изоморфных группах*, изоморфных упорядоченных или *подобных упорядоченных множествах* и т. д. Изоморфизм двух групп — это, следовательно, взаимно однозначное отображение $a \longmapsto \bar{a}$, при котором из $ab = c$ следует, что $\bar{a}\bar{b} = \bar{c}$ (и наоборот), так что произведению ab сопоставляется $\bar{a}\bar{b}$.

Подобно тому как в общей теории множеств равномощные множества считаются равнозначными, так в теории групп изоморфные группы рассматриваются как несущественно различные. Все понятия и предложения, которые определяются и доказываются на основе соотношений, заданных на некотором множестве, могут быть непосредственно перенесены на любое изоморфное множество. Например, если множество, на котором определено произведение, изоморфно некоторой группе, то оно само является группой; при этом изоморфизме единица, обратные элементы и подгруппы переходят в единицу, обратные элементы и подгруппы,

Если, в частности, множества $\bar{\mathfrak{M}}$ и $\mathfrak{M}$ совпадают, то мы рассматриваем взаимно однозначное сопоставление элементам a элементов $\bar{a}$ того же самого множества, сохраняющее соотношения; такое сопоставление называется *автоморфизмом*.

Автоморфизмы множества до некоторой степени выявляют его свойства симметрии. В самом деле, что означает симметрия, скажем, геометрической фигуры? Она означает, что при известных преобразованиях (отражениях, переносах и т. д.) фигура переходит в себя, при этом заданные соотношения (расстояния, углы, взаимное расположение) сохраняются, или, на нашем языке, фигура допускает автоморфизм относительно своих метрических свойств.

Очевидно, произведение двух автоморфизмов (в смысле произведения преобразований — см. § 6) является автоморфизмом и взятие обратного преобразования по отношению к автоморфизму вновь дает автоморфизм. Отсюда следует в силу § 6, что автоморфизмы произвольного множества (с любыми соотношениями между элементами) образуют группу преобразований — так называемую *группу автоморфизмов* множества.

В частности, автоморфизмы группы вновь составляют группу. Некоторые из этих автоморфизмов мы рассмотрим подробнее.

Если a — фиксированный элемент группы, то сопоставление элементу x элемента

$$\bar{x} = axa^{-1} \tag{1}$$

является автоморфизмом, потому что, во-первых, равенство (1) разрешимо относительно x:

$$x = a^{-1}\bar{x}a,$$

и, следовательно, отображение взаимно однозначно, а во-вторых,

$$\bar{x}\bar{y} = axa^{-1} \cdot aya^{-1} = a(xy)a^{-1} = \overline{xy},$$

и, следовательно, отображение изоморфно.

Элемент axa^{-1} называют *элементом, полученным из x трансформированием с помощью элемента a*, а сами элементы x и axa^{-1} называют *сопряженными в данной группе*. Автоморфизмы группы, порожденные элементами a по правилу $x \longmapsto axa^{-1}$, называются *внутренними*. Все остальные автоморфизмы (если они существуют) называются *внешними*.

При внутреннем автоморфизме $x \longmapsto axa^{-1}$ произвольная подгруппа $\mathfrak{g}$ переходит в подгруппу $a\mathfrak{g}a^{-1}$, которую называют *сопряженной с подгруппой* $\mathfrak{g}$.

Если подгруппа $\mathfrak{g}$ совпадает со всеми своими сопряженными, т. е.

$$a\mathfrak{g}a^{-1} = \mathfrak{g} \quad \text{для всех } a, \tag{2}$$

то это означает не что иное, как ее перестановочность со всеми элементами a:

$$a\mathfrak{g} = \mathfrak{g}a,$$

или что $\mathfrak{g}$ — *нормальная подгруппа* (§ 8). Итак,

Инвариантные относительно всех внутренних автоморфизмов подгруппы являются нормальными.

Этой теоремой объясняется использование другого названия для нормальных подгрупп — «инвариантная подгруппа».

Требование (2) можно заменить на более слабое:

$$a\mathfrak{g}a^{-1} \subseteq \mathfrak{g}. \tag{3}$$

Но если (3) выполняется для всех a, то оно верно и для a^{-1}:

$$\begin{aligned} a^{-1}\mathfrak{g}a &\subseteq \mathfrak{g}, \\ \mathfrak{g} &\subseteq a\mathfrak{g}a^{-1}, \end{aligned} \tag{4}$$

а из (3) и (4) следует (2). Таким образом:

Подгруппа является нормальной, если вместе с каждым элементом b она содержит все сопряженные к нему элементы aba^{-1}.

Задача 1. Абелевы группы не имеют внутренних автоморфизмов, отличных от тождественного.

Задача 2. Доказать, что в группе подстановок элемент aba^{-1}, трансформированный из b, можно получить так: разложить b в произведение циклов (§ 7) и подействовать на символы в этих циклах подстановкой a. С помощью этой теоремы вычислить aba^{-1} для случая

$$a = (2\,3\,4\,5),$$
$$b = (1\,2)\,(3\,4\,5).$$

Задача 3. Доказать, что симметрическая группа $\mathfrak{S}_3$ имеет ровно шесть внутренних автоморфизмов. В этом случае группа внутренних автоморфизмов изоморфна самой группе $\mathfrak{S}_3$.

Задача 4. Симметрическая группа $\mathfrak{S}_4$ имеет, кроме себя самой и единичной подгруппы, лишь следующие нормальные подгруппы:

а) знакопеременную группу $\mathfrak{A}_4$;

б) «четверную группу Клейна» $\mathfrak{B}_4$, состоящую из подстановок:

$$(1),\ (1\,2)\,(3\,4),\ (1\,3)\,(2\,4),\ (1\,4)\,(2\,3).$$

Последняя группа абелева.

Задача 5. Если $\mathfrak{g}$ — нормальная подгруппа в группе $\mathfrak{G}$ и $\mathfrak{H}$ — «промежуточная группа»:

$$\mathfrak{g} \subseteq \mathfrak{H} \subseteq \mathfrak{G},$$

то $\mathfrak{g}$ — нормальная подгруппа и в $\mathfrak{H}$.

Задача 6. Все бесконечные циклические группы изоморфны аддитивной группе целых чисел

Задача 7. Отношение сопряженности симметрично, рефлексивно и транзитивно. Поэтому элементы произвольной группы можно разбить на классы сопряженных элементов.

§ 10. Гомоморфизмы, нормальные подгруппы и факторгруппы

Если в двух множествах $\mathfrak{M}$ и $\mathfrak{N}$ определены некоторые соотношения (например, $a < b$ или $ab = c$) и если каждому элементу a из $\mathfrak{M}$ так сопоставлен элемент $\bar{a} = \varphi a$ из $\mathfrak{N}$, что все соотношения между элементами в $\mathfrak{M}$ выполняются и для их образов в $\mathfrak{N}$ (например, из $a < b$ следует $\bar{a} < \bar{b}$, если рассматривается соотношение $<$), то φ называется *гомоморфизмом* или *гомоморфным отображением* из $\mathfrak{M}$ в $\mathfrak{N}$.

Например, пусть $\mathfrak{M}$ — группа и $\mathfrak{N}$ — произвольное множество, в котором определены произведения. Если сопоставление таково, что произведению ab всегда соответствует произведение $\bar{a}\bar{b}$, то отображение φ является *гомоморфизмом групп*. Примерами могут служить определенные выше (взаимно однозначные) изоморфизмы групп.

Если отображение φ *сюръективно*, т. е. каждый элемент из $\mathfrak{N}$ является образом по крайней мере одного элемента из $\mathfrak{M}$, то говорят о *гомоморфизме из* $\mathfrak{M}$ *на* $\mathfrak{N}$.

Гомоморфное отображение множества $\mathfrak{M}$ в себя называется *эндоморфизмом* этого множества.

При гомоморфном отображении множества $\mathfrak{M}$ на множество $\overline{\mathfrak{M}}$ можно объединить в один класс $\mathfrak{a}$ те элементы из $\mathfrak{M}$, которые имеют один и тот же образ $\bar{a}$ в $\overline{\mathfrak{M}}$. При этом окажется, что каждый элемент a будет принадлежать одному и только одному классу $\mathfrak{a}$, т. е. множество $\mathfrak{M}$ *разобьется на классы*, которые взаимно однозначно соответствуют элементам множества $\overline{\mathfrak{M}}$. Класс $\mathfrak{a}$ называется также *прообразом* элемента $\bar{a}$.

Примеры. Если сопоставить каждому элементу произвольно взятой группы ее единицу, то получится гомоморфизм этой группы на единичную группу. Точно так же получится гомоморфизм, если каждой подстановке произвольно взятой группы подстановок сопоставить число $+1$ или число -1 в зависимости от того, четна эта подстановка или нечетна. *Гомоморфным образом* здесь служит мультипликативная группа чисел $+1$ и -1.

Сопоставим каждому целому числу m степень a^m элемента a произвольной группы; тогда получится гомоморфизм аддитивной группы целых чисел в циклическую группу, порожденную элементом a, потому что сумме $m+n$ при этом сопоставляется произведение $a^{m+n} = a^m a^n$. Если a — элемент бесконечного порядка, то построенный гомоморфизм является изоморфизмом.

Рассмотрим отдельно гомоморфизмы групп.

Если в множестве $\overline{\mathfrak{G}}$ определены произведения (т. е. соотношения вида $\bar{a}\bar{b} = \bar{c}$) и группа $\mathfrak{G}$ гомоморфно отображается на $\overline{\mathfrak{G}}$, то и $\overline{\mathfrak{G}}$ является группой. Коротко: гомоморфный образ группы является группой.

Доказательство. Пусть сначала $\bar{a}$, $\bar{b}$, $\bar{c}$ — три элемента из $\overline{\mathfrak{G}}$, являющиеся образами элементов a, b, c из $\mathfrak{G}$. Из

$$ab \cdot c = a \cdot bc$$

следует, что

$$\bar{a}\bar{b} \cdot \bar{c} = \bar{a} \cdot \bar{b}\bar{c}.$$

Далее, из равенства

$$ae = a,$$

справедливого при всех a, следует, что для всех $\bar{a}$

$$\bar{a}\bar{e} = \bar{a},$$

и аналогично из

$$ba = e \qquad (b = a^{-1})$$

следует, что

$$\bar{b}\bar{a} = \bar{e}.$$

Таким образом, в $\overline{\mathfrak{G}}$ существует единичный элемент $\bar{e}$ и обратный элемент для каждого $\bar{a}$. Следовательно, $\overline{\mathfrak{G}}$ — группа. Одновременно мы доказали, что

Единичный элемент и обратные элементы при гомоморфизме переходят снова в единичный элемент и обратные элементы.

Изучим теперь подробнее разбиение на классы, которое задается гомоморфным отображением $\mathfrak{G} \to \overline{\mathfrak{G}}$. При этом мы установим очень важное взаимно однозначное соответствие между гомоморфизмами и нормальными подгруппами.

Класс $\mathfrak{e}$ группы $\mathfrak{G}$, который при гомоморфизме $\mathfrak{G} \to \overline{\mathfrak{G}}$ переходит в единичный элемент $\bar{e}$ группы $\overline{\mathfrak{G}}$, является нормальной подгруппой в $\mathfrak{G}$; остальные классы являются смежными классами по этой нормальной подгруппе.

Доказательство. Сначала покажем, что $\mathfrak{e}$ — подгруппа. Пусть a и b переходят при гомоморфизме в $\bar{e}$; тогда ab снова переходит в $\bar{e}^2 = \bar{e}$, так что $\mathfrak{e}$ содержит произведение двух любых своих элементов. Далее, элемент a^{-1} переходит также в $\bar{a}^{-1} = \bar{e}$, и класс $\mathfrak{e}$ содержит элементы, обратные ко всем своим элементам.

Все элементы произвольно взятого левого смежного класса $a\mathfrak{e}$ переходят в элемент $\bar{a}\bar{e} = \bar{a}$. Если, наоборот, элемент a' переходит в элемент $\bar{a}$, то определим x из уравнения

$$ax = a'.$$

Получается, что

$$\bar{a}\bar{x} = \bar{a},$$
$$\bar{x} = \bar{e}.$$

Следовательно, элемент x лежит в классе $\mathfrak{e}$, а элемент a' принадлежит классу $a\mathfrak{e}$.

Поэтому класс группы $\mathfrak{G}$, который соответствует элементу $\bar{a}$, является левым смежным классом $a\mathfrak{e}$.

Но точно так же можно показать, что класс, который соответствует элементу $\bar{a}$, должен быть правым смежным классом $\mathfrak{e}a$. Таким образом, налицо совпадение правых и левых смежных классов:

$$a\mathfrak{e} = \mathfrak{e}a,$$

и класс $\mathfrak{e}$ — нормальная подгруппа. Утверждение полностью доказано.

Нормальная подгруппа $\mathfrak{e}$, элементы которой переходят при гомоморфизме в единичный элемент e, называется *ядром гомоморфизма*.

Обратим теперь постановку вопроса: *пусть задана произвольная нормальная подгруппа* $\mathfrak{g}$ *группы* $\mathfrak{G}$. *Можно ли построить группу* $\overline{\mathfrak{G}}$ — *гомоморфный образ группы* $\mathfrak{G}$, — *элементам которой в точности соответствовали бы смежные классы группы* $\mathfrak{G}$ *по нормальной подгруппе* $\mathfrak{g}$?

Чтобы это сделать, возьмем попросту в качестве элементов конструируемой группы $\overline{\mathfrak{G}}$ смежные классы по нормальной подгруппе $\mathfrak{g}$. Согласно § 8 произведение двух любых смежных классов по нормальной подгруппе $\mathfrak{g}$ снова является смежным классом и если a — элемент смежного класса $a\mathfrak{g}$, а b — элемент смежного класса $b\mathfrak{g}$, то произведение ab принадлежит произведению смежных классов $ab\mathfrak{g} = a\mathfrak{g} \cdot b\mathfrak{g}$. Таким образом, смежные классы составляют множество, гомоморфное группе $\mathfrak{G}$, т. е. *гомоморфный образ группы* $\mathfrak{G}$. Группу, состоящую из этих смежных классов, называют *факторгруппой* группы $\mathfrak{G}$ по нормальной подгруппе $\mathfrak{g}$ и обозначают через

$$\mathfrak{G}/\mathfrak{g}.$$

Порядок группы $\mathfrak{G}/\mathfrak{g}$ равен индексу подгруппы $\mathfrak{g}$.

Здесь мы видим принципиальную важность нормальных подгрупп: они позволяют строить новые группы, гомоморфные данным группам.

Если группа $\mathfrak{G}$ гомоморфно отображается на другую группу $\overline{\mathfrak{G}}$, то, как мы видели, элементы группы $\overline{\mathfrak{G}}$ взаимно однозначно соответствуют смежным классам по ядру $\mathfrak{e}$ в группе $\mathfrak{G}$. Это соответствие, конечно, является изоморфизмом, потому что если $a\mathfrak{g}$, $b\mathfrak{g}$ — два смежных класса, то $ab\mathfrak{g}$ — их произведение, а для соответствующих элементов $\bar{a}$, $\bar{b}$, $\overline{ab}$ из $\overline{\mathfrak{G}}$ в силу гомоморфизма имеет место равенство

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

Итак, мы имеем:

$$\mathfrak{G}/\mathfrak{e} \cong \overline{\mathfrak{G}},$$

а вместе с этим изоморфизмом и теорему о гомоморфизмах групп:

Каждая группа $\overline{\mathfrak{G}}$, на которую гомоморфно отображается группа $\mathfrak{G}$, изоморфна факторгруппе $\mathfrak{G}/\mathfrak{e}$; при этом нормальная подгруппа $\mathfrak{e}$ является ядром данного гомоморфизма. Обратно, группа $\mathfrak{G}$ гомоморфно отображается на любую свою факторгруппу $\mathfrak{G}/\mathfrak{e}$ (где $\mathfrak{e}$ — нормальная подгруппа).

Задача 1. Вот тривиальные факторгруппы любой группы $\mathfrak{G}$: $\mathfrak{G}/\mathfrak{E} \cong \mathfrak{G}$; $\mathfrak{G}/\mathfrak{G} \cong \mathfrak{E}$ ($\mathfrak{E}$ — единичная подгруппа).

Задача 2. Факторгруппа группы подстановок по знакопеременной подгруппе ($\mathfrak{S}_n/\mathfrak{A}_n$) является циклической группой второго порядка.

Задача 3. Факторгруппа $\mathfrak{S}_4/\mathfrak{A}_4$ по четверной группе Клейна (§ 9, задача 4) изоморфна группе подстановок $\mathfrak{S}_3$.

Задача 4. Элементы $aba^{-1}b^{-1}$ произвольной группы $\mathfrak{G}$ и их произведения (взятые в конечном числе) образуют группу, называемую *коммутантом* группы $\mathfrak{G}$. Эта подгруппа является нормальной и факторгруппа по ней абелева. Каждая нормальная подгруппа, факторгруппа по которой абелева, содержит коммутант.

Задача 5. Если $\mathfrak{G}$ — циклическая группа, a — порождающий ее элемент, а $\mathfrak{g}$ — подгруппа индекса m, то факторгруппа $\mathfrak{G}/\mathfrak{g}$ — циклическая группа порядка m.

В абелевой группе всякая подгруппа является нормальной (ср. § 8, задача 4). Если закон композиции записывать как сложение, то группы и подгруппы принято называть модулями, о чем упоминалось выше. Смежный класс $a+\mathfrak{M}$ (где $\mathfrak{M}$ — некоторый модуль) называется *классом вычетов по модулю* $\mathfrak{M}$ (или *классом вычетов* mod $\mathfrak{M}$), а факторгруппа $\mathfrak{G}/\mathfrak{M}$ называется *фактор-модулем* модуля $\mathfrak{G}$ по подмодулю $\mathfrak{M}$.

Два элемента a, b лежат в одном классе вычетов, если их разность лежит в $\mathfrak{M}$. Такие два элемента называют *сравнимыми по модулю* $\mathfrak{M}$ (или *сравнимыми* mod $\mathfrak{M}$) и пишут

$$a \equiv b \pmod{\mathfrak{M}}$$

или, кратко,

$$a \equiv b\,(\mathfrak{M}).$$

Тогда для элементов $\bar{a}$ и $\bar{b}$ модуля классов вычетов, соответствующих элементам a и b в силу гомоморфизма, имеет место равенство

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

Наоборот, из $\bar{a} = \bar{b}$ следует $a \equiv b\,(\mathfrak{M})$.

Например, в множестве целых чисел кратные фиксированного натурального числа m образуют модуль, и в соответствии с этим пишут

$$a \equiv b\,(m),$$

если разность $a-b$ делится на m. Классы вычетов могут быть представлены элементами $0, 1, 2, \ldots, m-1$ и, следовательно, модуль классов вычетов является циклической группой порядка m.

Задача 6. Каждая циклическая группа порядка m изоморфна модулю классов вычетов по целому числу m.