Для случая конечных групп существование разложений группы по подгруппе приводит к следующей важной теореме:

Теорема Лагранжа. *Во всякой конечной группе порядок любой подгруппы является делителем порядка самой группы.*

В самом деле, пусть в конечной группе G порядка n дана подгруппа A порядка k. Рассмотрим левостороннее разложение группы G по подгруппе A. Пусть оно состоит из j классов; число j называется *индексом* подгруппы A в группе G. Каждый левый класс xA состоит ровно из k элементов, так как если

$$xa_1 = xa_2,$$

где a_1 и a_2 — элементы из A, то $a_1 = a_2$. Таким образом,

$$n = kj, \tag{7}$$

что и требовалось доказать.

Так как порядок элемента совпадает с порядком его циклической подгруппы, то из теоремы Лагранжа следует, что *порядок всякого элемента конечной группы является делителем порядка группы.*

Из теоремы Лагранжа следует также, что *всякая конечная группа, порядок которой есть простое число, будет циклической.* Действительно, эта группа должна совпадать с циклической подгруппой, порожденной любым ее элементом, отличным от единицы. Отсюда вытекает, ввиду полученного выше описания циклических групп, что *для всякого простого числа p существует единственная, с точностью до изоморфизма, конечная группа порядка p.*

§ 65. Нормальные делители, фактор-группы, гомоморфизмы

Подгруппа A группы G называется *нормальным делителем* этой группы (или *инвариантной подгруппой*), если левостороннее разложение группы G по подгруппе A совпадает с правосторонним.

Таким образом, все подгруппы абелевой группы являются в ней нормальными делителями. С другой стороны, во всякой группе G и единичная подгруппа, и сама эта группа будут нормальными делителями: оба разложения группы G по единичной подгруппе совпадают с разложением группы на отдельные элементы, оба разложения группы G по самой этой группе состоят из одного класса G.

Укажем более интересные примеры нормальных делителей в некоммутативных группах. В симметрической группе 3-й степени S_3 циклическая подгруппа элемента (123), состоящая из тождественной подстановки и подстановок (123) и (132), будет нормальным делителем: в обоих разложениях группы S_3 по этой подгруппе второй смежный класс состоит из подстановок (12), (13) и (23).

Вообще в симметричной группе n-й степени S_n знакопеременная группа n-й степени A_n будет нормальным делителем. Действительно, группа A_n имеет порядок $\frac{1}{2}n!$, поэтому всякий смежный класс

группы S_n по подгруппе A_n должен состоять из стольких же элементов и, следовательно, такой класс имеется еще только один, а именно совокупность нечетных подстановок.

В мультипликативной группе невырожденных квадратных матриц порядка n с элементами из поля P те матрицы, определитель которых равен 1, составляют, очевидно, подгруппу. Это будет даже нормальный делитель, так как смежным классом по этой подгруппе, одновременно левым и правым, порождаемым матрицей M, является класс всех матриц, определитель которых равен определителю матрицы M — достаточно вспомнить, что при умножении матриц их определители перемножаются.

Определению нормального делителя, приведенному выше, можно придать такую форму:

Подгруппа A группы G называется нормальным делителем этой группы, если для всякого элемента x из G

$$xA = Ax, \tag{1}$$

т. е. для всякого элемента x из G и элемента a из A можно подобрать в A такие элементы a' и a'', что

$$xa = a'x, \quad ax = xa''. \tag{2}$$

Можно указать и другие определения нормального делителя, равносильные исходному. Так, назовем элементы a и b группы G *сопряженными*, если в G существует хотя бы один такой элемент x, что

$$b = x^{-1}ax, \tag{3}$$

т. е., как говорят, элемент b получается из элемента a *трансформированием* элементом x. Из (3) следует, очевидно, равенство

$$a = xbx^{-1} = (x^{-1})^{-1}bx^{-1}.$$

Подгруппа A группы G тогда и только тогда будет нормальным делителем в G, если вместе со всяким своим элементом a она содержит и все элементы, сопряженные с ним в G.

Действительно, если A — нормальный делитель в G, то, по (2), для выбранного нами элемента a из A и любого элемента x из G можно подобрать в A такой элемент a'', что

$$ax = xa''.$$

Отсюда

$$x^{-1}ax = a'',$$

т. е. всякий элемент, сопряженный с a, содержится в A. Обратно, если подгруппа A содержит вместе со всяким своим элементом a и все элементы, ему сопряженные, то в A содержится, в частности, элемент

$$x^{-1}ax = a'',$$

откуда следует второе из равенств (2). По той же причине в A содержится и элемент

$$(x^{-1})^{-1}ax^{-1}=xax^{-1}=a',$$

откуда следует и первое из равенств (2).

Пользуясь этим результатом, легко доказать, что *пересечение любых нормальных делителей группы G само будет нормальным делителем этой группы.* В самом деле, если A и B — нормальные делители группы G, то, как показано в предыдущем параграфе, пересечение $A\cap B$ будет подгруппой группы G. Пусть c — любой элемент из $A\cap B$, x — любой элемент группы G. Тогда элемент $x^{-1}cx$ должен содержаться и в A, и в B, так как оба этих нормальных делителя содержат элемент c. Отсюда следует, что элемент $x^{-1}cx$ входит в пересечение $A\cap B$.

Фактор-группа. Значение понятия нормального делителя основано на том, что из смежных классов по нормальному делителю — ввиду (1) левые и правые смежные классы можно в этом случае не различать — некоторым весьма естественным способом может быть построена новая группа.

Заметим сначала, что если A — произвольная подгруппа группы G, то

$$AA=A, \tag{4}$$

так как произведение любых двух элементов из подгруппы A принадлежит к A и, вместе с тем, умножая все элементы из A на единицу, мы уже получим всю подгруппу A.

Пусть A будет теперь нормальным делителем группы G. *В этом случае произведение любых двух смежных классов G по A* (в смысле умножения подмножеств группы G) *само будет смежным классом по A.* Действительно, используя ассоциативность умножения подмножеств группы, равенство (4) и равенство

$$yA=Ay$$

(ср. (1)), мы для любых элементов x и y группы G получим:

$$xA\cdot yA=xyAA=xyA. \tag{5}$$

Равенство (5) показывает, что для того, чтобы найти произведение двух данных смежных классов группы G по нормальному делителю A, следует произвольным образом выбрать в этих смежных классах по одному представителю — напомним, что всякий смежный класс порождается любым из своих элементов — и взять тот смежный класс, в котором лежит произведение этих представителей.

Таким образом, в множестве всех смежных классов группы G по нормальному делителю A определена операция умножения. Покажем, что *при этом выполняются все требования, входящие в определение группы.* В самом деле, ассоциативность умножения

смежных классов следует из ассоциативности умножения подмножеств группы. Роль единицы играет сам нормальный делитель A, являющийся одним из смежных классов разложения G по A: именно, ввиду (4) и (1) для любого x из G будет

$$xA \cdot A = xA, \quad A \cdot xA = xAA = xA.$$

Наконец, для смежного класса xA обратным будет смежный класс $x^{-1}A$, так как

$$xA \cdot x^{-1}A = 1 \cdot A = A.$$

Построенная нами группа называется *фактор-группой* группы G по нормальному делителю A и обозначается через G/A.

Мы видим, что со всякой группой связывается целый набор новых групп — ее фактор-групп по различным нормальным делителям. При этом фактор-группа группы G по единичной подгруппе будет, понятно, изоморфной с самой группой G.

Всякая фактор-группа G/A абелевой группы G сама является абелевой, так как из $xy = yx$ следует

$$xA \cdot yA = xyA = yxA = yA \cdot xA.$$

Всякая фактор-группа G/A циклической группы G сама циклическая, так как если G порождается элементом g, $G = \{g\}$, и если дан произвольный смежный класс xA, то существует такое целое число k, что

$$x = g^k$$

и поэтому

$$xA = (gA)^k.$$

Порядок любой фактор-группы G/A конечной группы G является делителем порядка самой этой группы. Действительно, порядок фактор-группы G/A равен индексу нормального делителя A в группе G, а поэтому можно воспользоваться равенством (7) из предшествующего параграфа.

Приведем некоторые примеры фактор-групп. Так как в аддитивной группе целых чисел подгруппа чисел, кратных натуральному числу k, имеет, как показано в предшествующем параграфе, индекс k, то фактор-группа нашей группы по этой подгруппе будет конечной группой порядка k, притом циклической, так как сама рассматриваемая группа циклическая.

Фактор-группа симметричной группы n-й степени S_n по знакопеременной группе n-й степени A_n будет группой 2-го порядка, причем, ввиду простоты числа 2, циклической группой (см. конец предшествующего параграфа).

Выше приведено описание смежных классов мультипликативной группы невырожденных матриц порядка n с элементами из поля P по нормальному делителю, составленному из матриц, определитель

которых равен 1. Из этого описания следует, что соответствующая фактор-группа изоморфна мультипликативной группе отличных от нуля чисел поля P.

Гомоморфизмы. Понятия нормального делителя и фактор-группы тесно связаны со следующим обобщением понятия изоморфизма.

Отображение φ группы G на группу G', ставящее в соответствие всякому элементу a из G однозначно определенный элемент $a'=a\varphi$ из G', называется *гомоморфным отображением* G на G' (или просто *гомоморфизмом*), если всякий элемент a' из G' служит при этом отображении образом некоторого элемента a из G, $a'=a\varphi$, и если для любых элементов a, b группы G

$$(ab)\varphi=a\varphi\cdot b\varphi.$$

Очевидно, что, потребовав дополнительно взаимную однозначность отображения φ, мы получили бы уже известное нам определение изоморфизма.

Если φ — гомоморфизм группы G на группу G' и 1 и a — соответственно единица и произвольный элемент группы G, $1'$ — единица группы G', то

$$1\varphi=1',$$
$$(a^{-1})\varphi=(a\varphi)^{-1}.$$

Действительно, если $1\varphi=e'$ и x' — произвольный элемент группы G', то в G существует такой элемент x, что $x\varphi=x'$. Отсюда

$$x'=x\varphi=(x\cdot 1)\varphi=x\varphi\cdot 1\varphi=x'\cdot e'.$$

Аналогично

$$x'=e'x'$$

и, следовательно, $e'=1'$.

С другой стороны, если $(a^{-1})\varphi=b'$, то

$$1'=1\varphi=(aa^{-1})\varphi=a\varphi\cdot(a^{-1})\varphi=a\varphi\cdot b'$$

и, аналогично,

$$1'=b'\cdot a\varphi,$$

откуда $b'=(a\varphi)^{-1}$.

Назовем *ядром* гомоморфизма φ группы G на группу G' совокупность тех элементов группы G, которые отображаются при φ в единицу $1'$ группы G'.

Ядро всякого гомоморфизма φ группы G является нормальным делителем группы G.

Действительно, если элементы a, b группы G входят в ядро гомоморфизма φ, т. е.

$$a\varphi=b\varphi=1',$$

то

$$(ab)\varphi=a\varphi\cdot b\varphi=1'\cdot 1'=1',$$

т. е. и произведение ab содержится в ядре гомоморфизма φ. С другой стороны, если $a\varphi = 1'$, то

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

т. е. и a^{-1} входит в ядро гомоморфизма φ. Наконец, если $a\varphi = 1'$, а x — произвольный элемент группы G, то

$$(x^{-1}ax)\varphi = (x^{-1})\varphi \cdot a\varphi \cdot x\varphi = (x\varphi)^{-1} \cdot 1' \cdot x\varphi = 1'.$$

Ядро рассматриваемого гомоморфизма оказалось подгруппой группы G, содержащей вместе со всяким своим элементом и все элементы, с ним сопряженные; оно будет, следовательно, нормальным делителем.

Пусть теперь A — произвольный нормальный делитель группы G. Ставя в соответствие всякому элементу x группы G тот смежный класс xA по нормальному делителю A, в котором этот элемент лежит, мы получим отображение группы G на всю фактор-группу G/A. Из определения умножения в группе G/A (см. (5)) следует, что это отображение будет гомоморфным.

Полученный гомоморфизм называется *естественным гомоморфизмом* группы G на фактор-группу G/A. Ядром этого гомоморфизма служит, очевидно, сам нормальный делитель A.

Отсюда следует, что *нормальные делители группы G и только они служат ядрами гомоморфизмов этой группы.* Этот результат можно рассматривать как еще одно определение нормального делителя.

Оказывается, что все группы, на которые группа G может гомоморфно отображаться, по существу исчерпываются фактор-группами этой группы, а все гомоморфизмы группы G — ее естественными гомоморфизмами на свои фактор-группы. Точнее, справедлива следующая

Теорема о гомоморфизмах. *Пусть дан гомоморфизм φ группы G на группу G' и пусть A — ядро этого гомоморфизма. Тогда группа G' изоморфна фактор-группе G/A, причем существует такое изоморфное отображение σ первой из этих групп на вторую, что результат последовательного выполнения отображений φ и σ совпадает с естественным гомоморфизмом группы G на фактор-группу G/A.*

В самом деле, пусть x' будет произвольный элемент группы G', а x — такой элемент группы G, что $x\varphi = x'$. Так как для любого элемента a из ядра A гомоморфизма φ имеет место равенство $a\varphi = 1'$, то

$$(xa)\varphi = x\varphi \cdot a\varphi = x' \cdot 1' = x',$$

т. е. все элементы смежного класса xA отображаются при φ в элемент x'.

С другой стороны, если z — любой такой элемент группы G, что $z\varphi = x'$, то

$$(x^{-1}z)\varphi = x^{-1}\varphi \cdot z\varphi = (x\varphi)^{-1} \cdot z\varphi = x'^{-1} \cdot x' = 1',$$

т. е. $x^{-1}z$ содержится в ядре A гомоморфизма φ. Если мы положим $x^{-1}z = a$, то $z = xa$, т. е. элемент z содержится в смежном классе xA. Таким образом, собирая все те элементы группы G, которые при гомоморфизме φ отображаются в фиксированный элемент x' группы G', мы получаем точно смежный класс xA.

Соответствие σ, относящее каждому элементу x' из G' тот смежный класс группы G по нормальному делителю A, который состоит из всех элементов группы G, имеющих x' своим образом при φ, будет взаимно однозначным отображением группы G' на группу G/A. Это отображение σ будет изоморфизмом, так как если

$$x'\sigma = xA, \quad y'\sigma = yA,$$

т. е.

$$x\varphi = x', \quad y\varphi = y',$$

то

$$(xy)\varphi = x\varphi \cdot y\varphi = x'y',$$

а поэтому

$$(x'y')\sigma = xyA = xA \cdot yA = x'\sigma \cdot y'\sigma.$$

Наконец, если x — произвольный элемент из G и $x\varphi = x'$, то

$$(x\varphi)\sigma = x'\sigma = xA,$$

т. е. последовательное выполнение гомоморфизма φ и изоморфизма σ на самом деле отображает элемент x в порождаемый им смежный класс xA. Теорема доказана.

§ 66. Прямые суммы абелевых групп

Мы хотим закончить главу одной теоретико-групповой теоремой, более глубокой, чем те элементарные свойства групп, которые излагались выше. Именно, опираясь на уже известное нам из § 64 описание циклических групп, мы получим в следующем параграфе полное описание конечных абелевых групп.

Как принято в теории абелевых групп, для групповой операции будет использоваться аддитивная запись: мы будем говорить о сумме $a+b$ элементов a и b группы, о нулевой подгруппе 0, о кратных ka некоторого элемента a и т. д.

В этом параграфе мы изучим одну конструкцию, которую будем излагать применительно к абелевым группам, хотя ее можно было бы вводить сразу для любых (т. е. не обязательно коммутативных) групп. Эта конструкция подсказывается следующими примерами. Плоскость, рассматриваемая как двумерное действительное линейное пространство, является абелевой группой относительно сложения