Мультипликативная группа отличных от нуля действительных чисел разлагается в прямое произведение мультипликативной группы положительных действительных чисел и группы по умножению, составленной из чисел 1 *и* -1.

Действительно, в пересечении указанных двух подгрупп нашей группы содержится лишь число 1 — единичный элемент этой группы. С другой стороны, всякое положительное число является произведением самого себя на число 1, всякое отрицательное число — произведением своей абсолютной величины на число -1.

§ 67. Конечные абелевы группы

Если мы возьмем любой конечный набор примарных циклических групп, некоторые из которых могут относиться к одному и тому же простому числу или даже иметь один и тот же порядок, т. е. быть изоморфными, то прямая сумма этих групп будет конечной абелевой группой. Оказывается, что этим исчерпываются все конечные абелевы группы:

Основная теорема о конечных абелевых группах. *Всякая конечная абелева группа G, не являющаяся нулевой группой, разлагается в прямую сумму примарных циклических подгрупп.*

Доказательство этой теоремы начнем с замечания, что *в группе G непременно найдутся ненулевые элементы, порядки которых являются степенями простых чисел.* Действительно, если некоторый ненулевой элемент x группы G имеет порядок l, $lx=0$, и если p^k, $k>0$, есть такая степень простого числа p, на которую число l делится,

$$l=p^k m,$$

то элемент mx отличен от нуля и имеет порядок p^k.

Пусть

$$p_1,\ p_2,\ \ldots,\ p_s \tag{1}$$

будут все различные простые числа, некоторые степени которых служат порядками некоторых элементов группы G. Обозначим через p любое из этих чисел, а через P совокупность элементов группы G, имеющих своими порядками степени числа p.

Множество P является подгруппой группы G. Действительно, в P входит элемент 0, так как его порядок есть $1=p^0$. Далее, если $p^k x=0$, то и $p^k(-x)=0$. Наконец, если $p^k x=0$, $p^l y=0$ и если, например, $k\geqslant l$, то

$$p^k(x+y)=0,$$

т. е. порядком элемента $x+y$ служит или число p^k, или делитель этого числа, т. е. во всяком случае некоторая степень числа p.

Беря в качестве p поочередно каждое из чисел (1), мы получим s ненулевых подгрупп

$$P_1,\ P_2,\ \ldots,\ P_s. \tag{2}$$

Группа G является прямой суммой этих подгрупп,

$$G = P_1 + P_2 + \ldots + P_s. \tag{3}$$

Действительно, если x — произвольный элемент группы G, то его порядок l может делиться лишь на некоторые простые числа из системы (1),

$$l = p_1^{k_1} p_2^{k_2} \ldots p_s^{k_s},$$

где $k_i \geqslant 0$, $i = 1, 2, \ldots, s$. Поэтому, как показано в конце предшествующего параграфа, циклическая подгруппа $\{x\}$ разлагается в прямую сумму примарных циклических подгрупп, имеющих соответственно порядки $p_1^{k_1}, p_2^{k_2}, \ldots, p_s^{k_s}$. Эти примарные циклические подгруппы лежат в соответственных подгруппах (2), и, следовательно, элемент x представляется в виде суммы элементов, взятых по одному во всех или некоторых из подгрупп (2). Этим доказано равенство

$$G = \{P_1,\ P_2,\ \ldots,\ P_s\},$$

аналогичное равенству (6) из предшествующего параграфа.

Для доказательства равенства, аналогичного равенству (7) из того же параграфа, возьмем любое i, $2 \leqslant i \leqslant s$. Тогда любой элемент y из подгруппы $\{P_1,\ P_2,\ \ldots,\ P_{i-1}\}$ имеет вид

$$y = a_1 + a_2 + \ldots + a_{i-1},$$

где элемент a_j, $j = 1, 2, \ldots, i-1$, лежит в подгруппе P_j, т. е. имеет порядок $p_j^{k_j}$. Тогда

$$(p_1^{k_1} p_2^{k_2} \ldots p_{i-1}^{k_{i-1}})\, y = 0,$$

т. е. порядком элемента y служит некоторый делитель числа $p_1^{k_1} p_2^{k_2} \ldots p_{i-1}^{k_{i-1}}$ и, следовательно, элемент y, если он отличен от нуля, не может содержаться в подгруппе P_i. Этим доказано, что

$$\{P_1,\ P_2,\ \ldots,\ P_{i-1}\} \cap P_i = 0,$$

что и требовалось доказать.

Заметим, что абелева группа, порядки всех элементов которой являются степенями одного и того же простого числа p, называется *примарной* относительно числа p. Примарные циклические группы являются частным случаем примарных групп. Таким образом, подгруппы (2) примарны. Они называются *примарными компонентами* группы G, а прямое разложение (3) — *разложением этой группы в примарные компоненты.* Так как подгруппы (2) определены

в группе G однозначным образом, то и *разложение группы G в примарные компоненты определено однозначно.*

Разложимость всякой конечной абелевой группы в прямую сумму примарных групп сводит, понятно, доказательство основной теоремы на случай конечной примарной абелевой группы P, относящейся к некоторому простому числу p. Рассмотрим этот случай.

Пусть a_1 будет один из элементов группы P, имеющих в ней наивысший порядок. Если, далее, в группе P имеются ненулевые элементы, циклические подгруппы которых пересекаются с циклической подгруппой $\{a_1\}$ лишь по нулю, то через a_2 обозначим один из элементов наивысшего порядка среди элементов с этим свойством; таким образом

$$\{a_1\} \cap \{a_2\} = 0.$$

Пусть уже выбраны элементы $a_1, a_2, \ldots, a_{i-1}$. Подгруппу группы P, порожденную их циклическими подгруппами, обозначим через $\{a_1, a_2, \ldots, a_{i-1}\}$,

$$\{\{a_1\}, \{a_2\}, \ldots, \{a_{i-1}\}\} = \{a_1, a_2, \ldots, a_{i-1}\}. \tag{4}$$

Она состоит, очевидно, из всех элементов группы P, которые могут быть записаны в виде суммы элементов, кратных элементам $a_1, a_2, \ldots, a_{i-1}$; будем говорить, что эта подгруппа *порождается* элементами $a_1, a_2, \ldots, a_{i-1}$. Обозначим теперь через a_i один из элементов наивысшего порядка среди тех элементов группы P, циклические подгруппы которых имеют равное нулю пересечение с подгруппой $\{a_1, a_2, \ldots, a_{i-1}\}$; таким образом

$$\{a_1, a_2, \ldots, a_{i-1}\} \cap \{a_i\} = 0. \tag{5}$$

Ввиду конечности группы P этот процесс должен остановиться; пусть это произойдет после того, как будут выбраны элементы $a_1, a_2, \ldots, a_s$. Если через P' мы обозначим подгруппу, порожденную этими элементами,

$$P' = \{a_1, a_2, \ldots, a_s\},$$

т. е.

$$P' = \{\{a_1\}, \{a_2\}, \ldots, \{a_s\}\}, \tag{6}$$

то, следовательно, циклическая подгруппа любого ненулевого элемента группы P имеет с подгруппой P' ненулевое пересечение.

Равенство (6) и равенство (5), справедливое для $i = 2, 3, \ldots, s$, показывают, ввиду (4), что подгруппа P' является прямой суммой циклических подгрупп $\{a_1\}, \{a_2\}, \ldots, \{a_s\}$,

$$P' = \{a_1\} + \{a_2\} + \ldots + \{a_s\}. \tag{7}$$

Остается доказать, что подгруппа P' на самом деле совпадает со всей группой P.

Пусть x — любой элемент группы P, имеющий порядок p. Так как

$$P' \cap \{x\} \neq 0,$$

а подгруппа $\{x\}$ не имеет ненулевых подгрупп, отличных от нее самой — напомним, что порядок подгруппы является делителем порядка группы, а число p простое, — то в действительности подгруппа $\{x\}$ содержится в подгруппе P' и, следовательно, x принадлежит к P'. Таким образом, все элементы порядка p из группы P входят в подгруппу P'.

Пусть уже доказано, что в подгруппу P' входят все элементы группы P, порядок которых не превосходит числа p^{k-1}, и пусть x — любой элемент из P, имеющий порядок p^k. Как показывает выбор элементов $a_1, a_2, \ldots, a_s$, порядки их идут не возрастая и поэтому можно указать такое i, $1 \leqslant i-1 \leqslant s$, что порядки элементов $a_1, a_2, \ldots, a_{i-1}$ больше или равны p^k, а при $i-1 < s$ порядок элемента a_i строго меньше этого числа, т. е. меньше порядка элемента x. Отсюда следует, ввиду условий, которым подчинен выбор элемента a_i, что если

$$Q = \{a_1, a_2, \ldots, a_{i-1}\},$$

то

$$Q \cap \{x\} \neq 0.$$

В предшествующем параграфе было доказано, однако, что всякая ненулевая подгруппа примарной циклической группы $\{x\}$ порядка p^k содержит элемент

$$y = p^{k-1} x. \tag{8}$$

Элемент y входит, следовательно, в пересечение $Q \cap \{x\}$, а поэтому и в подгруппу Q. Это позволяет записать y в виде суммы элементов, кратных элементам $a_1, a_2, \ldots, a_{i-1}$,

$$y = l_1 a_1 + l_2 a_2 + \ldots + l_{i-1} a_{i-1}. \tag{9}$$

Из (8) следует, что элемент y имеет порядок p. Поэтому

$$(pl_1) a_1 + (pl_2) a_2 + \ldots + (pl_{i-1}) a_{i-1} = 0,$$

т. е., ввиду существования прямого разложения (7),

$$(pl_j) a_j = 0, \qquad j = 1, 2, \ldots, i-1.$$

Число pl_j должно, следовательно, делиться на порядок элемента a_j, а поэтому и на число p^k, откуда вытекает, что l_j делится на p^{k-1},

$$l_j = p^{k-1} m_j, \qquad j = 1, 2, \ldots, i-1. \tag{10}$$

Пусть

$$z = m_1 a_1 + m_2 a_2 + \ldots + m_{i-1} a_{i-1}.$$

Это будет элемент из подгруппы Q, а поэтому и из подгруппы P', причем, ввиду (9) и (10),

$$y = p^{k-1} z. \tag{11}$$

Из (8) и (11) вытекает равенство

$$p^{k-1}(x-z)=0,$$

т. е. порядок элемента

$$t=x-z$$

не больше p^{k-1} и, следовательно, в силу индуктивного предположения t содержится в подгруппе P'. Поэтому и элемент x, как сумма двух элементов из P', $x=z+t$, принадлежит к подгруппе P'. Этим доказано, что все элементы порядка p^k из группы P содержатся в P'.

Наше индуктивное доказательство позволяет утверждать, следовательно, что все элементы группы P входят в подгруппу P', т. е. $P'=P$. Доказательство основной теоремы закончено.

В качестве побочного продукта мы получаем, что *конечная абелева группа тогда и только тогда будет примаркой относительно простого числа p, если ее порядок является степенью этого числа p.* В самом деле, было показано, что всякая конечная примарная (по p) абелева группа P разлагается в прямую сумму примарных (по p) циклических групп, а поэтому порядок группы P равен произведению порядков этих циклических групп, т. е. является степенью числа p. Обратно, если конечная абелева группа имеет порядок p^k, где p — простое число, то порядок любого ее элемента будет делителем этого числа, т. е. также некоторой степенью числа p, а поэтому группа оказывается примарной относительно p.

Основная теорема еще не исчерпывает вопроса о полном описании конечных абелевых групп, так как пока не исключена возможность того, что прямые суммы двух различных наборов циклических групп, примарных по некоторым простым числам, могут оказаться изоморфными группами. На самом деле это не имеет места, как показывает следующая теорема:

Если конечная абелева группа G разложена двумя способами в прямую сумму примарных циклических подгрупп,

$$G=\{a_1\}+\{a_2\}+\ldots+\{a_s\}=\{b_1\}+\{b_2\}+\ldots+\{b_t\}, \quad (12)$$

то оба прямых разложения обладают одним и тем же числом прямых слагаемых, $s=t$, и между прямыми слагаемыми этих разложений можно установить такое взаимно однозначное соответствие, что соответствующие слагаемые являются циклическими группами одного и того же порядка, т. е. изоморфны.

Заметим сначала, что если мы в первом, например, из прямых разложений (12) соберем прямые слагаемые, относящиеся к данному простому числу p, то их прямая сумма будет примарной (по p) подгруппой группы G и даже примарной компонентой этой группы, так как ее порядок равен наивысшей степени числа p, на которую делится порядок группы G. Объединяя этим способом прямые слагаемые в каждом из разложений (12), мы в обоих случаях получим

разложение группы G в примарные компоненты, единственность которого уже была отмечена выше.

Это позволяет доказывать нашу теорему в предположении, что группа G сама является примарной относительно простого числа p. Пусть нумерация прямых слагаемых в каждом из разложений (12) выбрана так, что порядки этих слагаемых идут не возрастая, т. е. элементы $a_1, a_2, \ldots, a_s$ имеют соответственно порядки

$$p^{k_1}, p^{k_2}, \ldots, p^{k_s},$$

причем

$$k_1 \geqslant k_2 \geqslant \ldots \geqslant k_s,$$

а элементы $b_1, b_2, \ldots, b_t$ — порядки

$$p^{l_1}, p^{l_2}, \ldots, p^{l_t},$$

причем

$$l_1 \geqslant l_2 \geqslant \ldots \geqslant l_t.$$

Если бы утверждение нашей теоремы не имело места, то нашлось бы такое i, $i \geqslant 1$, что

$$k_1 = l_1, \ \ldots, \ k_{i-1} = l_{i-1}, \tag{13}$$

но

$$k_i \neq l_i.$$

Понятно, что $i \leqslant \min(s, t)$, так как для каждого из разложений (12) произведение порядков всех прямых слагаемых равно порядку группы G. Покажем, что наше предположение приводит к противоречию.

Пусть, например,

$$k_i < l_i. \tag{14}$$

Обозначим через H совокупность элементов группы G, порядки которых не превосходят p^{k_i}. Это будет подгруппа группы G, так как если x и y — элементы из H, то и $x+y$, и $-x$ имеют порядки, не превосходящие числа p^{k_i}.

Заметим, что к подгруппе H принадлежат, в частности, следующие элементы:

$$p^{k_1-k_i}a_1, \ p^{k_2-k_i}a_2, \ \ldots, \ p^{k_{i-1}-k_i}a_{i-1}, \ a_i, \ a_{i+1}, \ \ldots, \ a_s.$$

С другой стороны, если $1 \leqslant j \leqslant i-1$, то элемент $p^{k_j-k_i-1}a_j$ имеет порядок p^{k_i+1} и поэтому в H не входит. Отсюда следует, что смежный класс $a_j + H$ (напоминаем, что мы используем аддитивную запись!) имеет, как элемент фактор-группы G/H, порядок $p^{k_j-k_i}$; таков же порядок его циклической подгруппы $\{a_j + H\}$. Докажем, что группа

G/H является прямой суммой циклических подгрупп $\{a_j+H\}$, $j=1, 2, \ldots, i-1$,

$$G/H=\{a_1+H\}+\{a_2+H\}+\ldots+\{a_{i-1}+H\}, \tag{15}$$

и поэтому ее порядок равен числу

$$p^{(k_1-k_i)+(k_2-k_i)+\ldots+(k_{i-1}-k_i)}. \tag{16}$$

Если x — произвольный элемент группы G, то существует запись

$$x=m_1a_1+m_2a_2+\ldots+m_sa_s.$$

Пусть для $j=1, 2, \ldots, i-1$

$$m_j=p^{k_j-k_i}q_j+n_j,$$

где

$$0\leqslant n_j<p^{k_j-k_i}. \tag{17}$$

Тогда

$$m_ja_j=q_j(p^{k_j-k_i}a_j)+n_ja_j,$$

а так как первое слагаемое правой части содержится в H, то

$$m_ja_j+H=n_ja_j+H.$$

С другой стороны,

$$m_ia_i+H=H, \ \ldots, \ m_sa_s+H=H.$$

Поэтому

$$\begin{aligned} x+H&=(m_1a_1+H)+(m_2a_2+H)+\ldots+(m_sa_s+H)=\\ &=(n_1a_1+H)+(n_2a_2+H)+\ldots+(n_{i-1}a_{i-1}+H). \end{aligned} \tag{18}$$

Пусть существует еще одна такая запись,

$$x+H=(n_1'a_1+H)+(n_2'a_2+H)+\ldots+(n_{i-1}'a_{i-1}+H), \tag{19}$$

где

$$0\leqslant n_j'<p^{k_j-k_i}, \quad j=1, 2, \ldots, i-1. \tag{20}$$

Тогда элементы

$$n_1a_1+n_2a_2+\ldots+n_{i-1}a_{i-1}$$

и

$$n_1'a_1+n_2'a_2+\ldots+n_{i-1}'a_{i-1}$$

лежат в одном смежном классе по H, т. е. их разность принадлежит к H и поэтому

$$p^{k_i}[(n_1-n_1')a_1+(n_2-n_2')a_2+\ldots+(n_{i-1}-n_{i-1}')a_{i-1}]=0.$$

Отсюда следует (так как первое из разложений (12) — прямое), что

$$p^{k_i}(n_j-n_j')a_j=0, \quad j=1, 2, \ldots, i-1,$$

а поэтому число $p^{k_i}(n_j - n_j')$ должно делиться на порядок p^{k_j} элемента a_j и, следовательно, разность $n_j - n_j'$ делится на число $p^{k_j - k_i}$. Отсюда, ввиду (17) и (20), следует, что

$$n_j = n_j', \quad j = 1, 2, \ldots, i-1,$$

т. е. записи (18) и (19) тождественны. Этим доказано существование прямого разложения (15).

Аналогичные рассмотрения, проведенные для второго из прямых разложений (12), покажут, что эта же фактор-группа G/H обладает прямым разложением

$$G/H = \{b_1 + H\} + \{b_2 + H\} + \ldots + \{b_{i-1} + H\} + \{b_i + H\} + \ldots,$$

т. е., ввиду (13) и (14), ее порядок должен быть строго больше числа (16). Это противоречие доказывает теорему.

Полное обозрение конечных абелевых групп нами теперь уже получено. Именно, *берем всевозможные конечные наборы натуральных чисел*

$$(n_1, n_2, \ldots, n_k),$$

отличных от единицы, но не обязательно различных, причем каждое из этих чисел должно быть степенью некоторого простого числа. Каждому такому набору ставим в соответствие прямую сумму циклических групп, порядками которых служат числа из этого набора. Все полученные этим путем конечные абелевы группы будут попарно неизоморфными, а любая другая конечная абелева группа изоморфна одной из этих групп.