Пусть f: $A \to \mathbf{Z}x_1$ — проекция, т. е. гомоморфизм, для которого

$$f(m_1x_1 + \ldots + m_nx_n) = m_1x_1,$$

каковы бы ни были $m_i \in \mathbf{Z}$. Пусть B_1 — ядро ограничения f на B. Тогда B_1 содержится в свободной подгруппе $\langle x_2, \ldots, x_n \rangle$. По индукции B_1 свободна и имеет базис из $\leqslant n-1$ элементов. В силу леммы в B существует подгруппа C_1, изоморфная подгруппе в $\mathbf{Z}x_1$ (а именно, образу $f(B)$), такая, что

$$B = B_1 \oplus C_1.$$

Таким образом, $f(B)$ — либо 0, либо бесконечная циклическая группа, т. е. свободная группа с одной образующей, Это доказывает, что группа B — свободная.

(В случае когда A не является конечно порожденной, можно использовать аналогичное рассуждение с трансфинитной индукцией; мы предоставляем это читателю.)

Заметим, далее, что из предыдущего следует, что существует по меньшей мере один базис подгруппы B, мощность которого $\leqslant n$. Поэтому доказательство будет закончено, если мы покажем, что любые два базиса в B имеют одинаковую мощность. Пусть S — один базис с конечным числом элементов m, T — другой базис, содержащий по крайней мере r элементов. Достаточно доказать, что $r \leqslant m$ (затем можно воспользоваться симметрией). Пусть p — простое число. Тогда факторгруппа B/pB есть прямая сумма циклических групп порядка p, причем в сумме имеется m членов. Значит, порядок этой факторгруппы равен p^m. Используя базис T вместо S, заключаем, что B/pB содержит r-кратное произведение циклических групп порядка p, а потому $p^r \leqslant p^m$ и $r \leqslant m$, что и требовалось показать. (Отметим, что мы не предполагали a priori, что базис T конечен.)

§ 10. Конечно порожденные абелевы группы

Группы, названные в заглавии этого параграфа, встречаются так часто, что стоит установить теорему, полностью описывающую их структуру. В этом параграфе мы записываем наши абелевы группы аддитивно.

Пусть A — абелева группа. Элемент $a \in A$ называется *периодическим*, если он имеет конечный период. Подмножество всех периодических элементов из A является подгруппой в A, называемой *подгруппой кручения* группы A (если a имеет период m и b имеет период n, то $a \pm b$ имеет период, делящий mn).

Конечно порожденная периодическая абелева группа (группа, совпадающая со своей подгруппой кручения), очевидно, конечна. Мы начнем с изучения конечных абелевых групп. Пусть A — абелева группа и p — простое число. Мы обозначаем через $A(p)$ подгруппу

всех элементов $x \in A$, период которых есть степень p. Тогда $A(p)$ — периодическая группа, являющаяся p-группой, если она конечна.

Теорема 5. *Пусть A — конечная абелева группа. Тогда A является прямым произведением своих подгрупп $A(p)$ по всем простым p, таким, что $A(p) \neq 0$.*

Доказательство. Сначала рассмотрим случай абелевой группы A, показатель которой n может быть записан в виде произведения $n = mm'$, где m, m' — взаимно простые целые числа > 1. Существуют целые числа r, s, такие, что

$$rm + sm' = 1.$$

Поэтому

$$A = rmA + sm'A \subset mA + m'A \subset A,$$

откуда следует, что все символы включения нужно заменить на равенства. Если $a \in mA \cap m'A$, то $m'a = 0$ и $ma = 0$, откуда $a = rma + sm'a = 0$. Следовательно, A — прямое произведение подгрупп mA и $m'A$.

Пусть A_m обозначает подгруппу в A, состоящую из всех x, для которых $mx = 0$. Тогда $m'A \subset A_m$, так как $mm'A = 0$. Обратно, если $x \in A_m$, то $x = rmx + sm'x = m'sx$, так что $x \in m'A$. Следовательно, $m'A = A_m$ и аналогично $mA = A_{m'}$, так что окончательно

$$A = A_m \times A_{m'}.$$

По индукции заключаем, что A есть прямое произведение своих подгрупп $A(p)$, что и утверждается в теореме.

Наша следующая задача — описать структуру конечных абелевых p-групп. Пусть $r_1, \ldots, r_s$ — целые числа $\geqslant 1$. Конечная p-группа A называется группой *типа* $(p^{r_1}, \ldots, p^{r_s})$, если она изоморфна прямому произведению циклических групп порядков p^{r_i} $(i = 1, \ldots, s)$.

Теорема 6. *Всякая конечная абелева p-группа изоморфна прямому произведению циклических p-групп. Если она есть группа типа $(p^{r_1}, \ldots, p^{r_s})$, причем*

$$r_1 \geqslant r_2 \geqslant \ldots \geqslant r_s \geqslant 1,$$

то последовательность $(r_1, \ldots, r_s)$ определена однозначно.

Доказательство. Пусть A — конечная абелева p-группа. Нам потребуется следующее замечание. Пусть b — элемент из A, $b \neq 0$, k — целое число $\geqslant 0$, такое, что $p^k b \neq 0$, и пусть p^m — период элемента $p^k b$. Тогда b имеет период p^{k+m}. Доказательство: разумеется,

$p^{k+m}b=0$, а если $p^n b=0$, то, во-первых, $n \geqslant k$, а, во-вторых, $n \geqslant k+m$, так как иначе период элемента $p^k b$ был бы меньше, чем p^m.

Теперь докажем существование искомого прямого произведения по индукции. Пусть $a_1 \in A$ — некоторый элемент максимального периода. Не теряя общности, мы можем предполагать, что группа A — не циклическая. Пусть A_1 — циклическая подгруппа, порожденная элементом a_1, периода, скажем, p^{r_1}. Нам нужна лемма.

Лемма. *Пусть $\bar{b}$ — некоторый элемент из A/A_1 периода p^r. Тогда в A существует представитель a класса $\bar{b}$, также имеющий период p^r.*

Доказательство. Пусть b — произвольный представитель класса $\bar{b}$ в A. Тогда $p^r b$ лежит в A_1, скажем, $p^r b = na_1$, где n — некоторое целое число. Заметим, что период $\bar{b} \leqslant$ периода b. Запишем $n = p^k \mu$, где μ взаимно просто с p. Тогда μa_1 также является образующей подгруппы A_1 и, следовательно, имеет период p^{r_1}. Мы можем предполагать, что $k \leqslant r_1$. Тогда $p^k \mu a_1$ имеет период p^{r_1-k}. В силу нашего предыдущего замечания элемент b имеет период

$$p^{r+r_1-k},$$

откуда по предположению $r+r_1-k \leqslant r_1$ и $r \leqslant k$. Это доказывает, что существует элемент $c \in A_1$, такой, что $p^r b = p^r c$. Пусть $a=b-c$. Тогда a есть представитель для $\bar{b}$ в A и $p^r a = 0$. Так как период $(a) \geqslant p^r$, то заключаем, что a имеет период, равный p^r.

Возвращаемся к основному доказательству. По индукции фактор-группа A/A_1 допускает представление в виде произведения

$$A/A_1 = \bar{A}_2 \times \ldots \times \bar{A}_s$$

циклических подгрупп порядков $p^{r_2}, \ldots, p^{r_s}$ соответственно; мы можем предполагать, что $r_2 \geqslant \ldots \geqslant r_s$. Пусть $\bar{a}_i$ — образующая для $\bar{A}_i$ $(i=2, \ldots, s)$ и a_i — ее представитель в A, имеющий тот же период, что и $\bar{a}_i$. Пусть A_i — циклическая подгруппа, порожденная элементом a_i. Мы утверждаем, что A есть прямое произведение подгрупп $A_1, \ldots, A_s$.

Для заданного элемента $x \in A$ обозначим через $\bar{x}$ его класс вычетов в A/A_1. Существуют целые числа m_i $(i=2, \ldots, s)$, для которых

$$\bar{x} = m_2 \bar{a}_2 + \ldots + m_s \bar{a}_s.$$

Следовательно, $x - m_2a_2 - \ldots - m_sa_s$ лежит в A_1 и существует целое число m_1, такое, что

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

откуда $A_1 + \ldots + A_s = A$.

Предположим далее, что $m_1, \ldots, m_s$ — целые числа $\geqslant 0$, такие, что

$$0 = m_1a_1 + m_2a_2 + \ldots + m_sa_s.$$

Так как a_i имеет период p^{r_i} $(i = 1, \ldots, s)$, то мы можем считать, что $m_i < p^{r_i}$. Проводя черту над членами этого уравнения, получаем

$$0 = m_2\bar{a}_2 + \ldots + m_s\bar{a}_s.$$

Так как A/A_1 — прямое произведение подгрупп $\bar{A}_2, \ldots, \bar{A}_s$, то заключаем, что каждое $m_i = 0$ для $i = 2, \ldots, s$. Но тогда также и $m_1 = 0$ и, следовательно, все $m_i = 0$. Отсюда вытекает немедленно, что

$$(A_1 + \ldots + A_i) \cap A_{i+1} = 0$$

для каждого $i \geqslant 1$ и, следовательно, A — прямое произведение подгрупп $A_1, \ldots, A_s$, что и требовалось установить.

Единственность доказываем по индукции. Предположим, что группа A записана двумя способами в виде произведения циклических групп, т. е. имеет одновременно типы, скажем,

$$(p^{r_1}, \ldots, p^{r_s}) \quad \text{и} \quad (p^{m_1}, \ldots, p^{m_k}),$$

где $r_1 \geqslant \ldots \geqslant r_s \geqslant 1$ и $m_1 \geqslant \ldots \geqslant m_k \geqslant 1$. Тогда pA — также p-группа порядка, строго меньшего, чем порядок A, и типов

$$(p^{r_1-1}, \ldots, p^{r_s-1}) \quad \text{и} \quad (p^{m_1-1}, \ldots, p^{m_k-1}),$$

причем подразумевается, что если некоторый показатель r_i или m_j равен 1, то множитель, соответствующий

$$p^{r_i-1} \quad \text{или} \quad p^{m_j-1}$$

в pA, будет просто тривиальной группой 0. По индукции подпоследовательность в

$$(r_1 - 1, \ldots, r_s - 1),$$

состоящая из тех целых чисел, которые $\geqslant 1$, однозначно определена, и то же самое справедливо для соответствующей подпоследовательности в

$$(m_1 - 1, \ldots, m_k - 1).$$

Другими словами, мы имеем $r_i - 1 = m_i - 1$ для всех таких номеров i, что $r_i - 1$ или $m_i - 1 \geqslant 1$. Следовательно, $r_i = m_i$ для всех этих номеров i и две последовательности

$$(p^{r_1}, \ldots, p^{r_s}) \quad \text{и} \quad (p^{m_1}, \ldots, p^{m_k})$$

могут отличаться только своими последними членами, равными p. Эти члены, соответствующие множителям типа $(p, \ldots, p)$, встречаются, скажем, ν раз в первой последовательности и μ раз во второй последовательности. Тогда для некоторого целого n группа A имеет типы

$$(p^{r_1}, \ldots, p^{r_n}, \underbrace{p, \ldots, p}_{\nu \text{ раз}}) \quad \text{и} \quad (p^{r_1}, \ldots, p^{r_n}, \underbrace{p, \ldots, p}_{\mu \text{ раз}}).$$

Таким образом, ее порядок равен

$$p^{r_1 + \cdots + r_n} p^{\nu} = p^{r_1 + \cdots + r_n} p^{\mu},$$

откуда $\nu = \mu$, и наша теорема доказана.

Группа G называется *группой, свободной от кручения*, или *группой без кручения*, если единичный элемент является единственным элементом в G, имеющим конечный период.

Теорема 7. *Пусть A — конечно порожденная абелева группа без кручения. Тогда A — свободная.*

Доказательство. Предположим, что $A \neq 0$. Пусть S — конечное множество образующих и $x_1, \ldots, x_n$ — максимальное подмножество в S, обладающее тем свойством, что, каковы бы ни были целые числа $\nu_1, \ldots, \nu_n$, из

$$\nu_1 x_1 + \ldots + \nu_n x_n = 0$$

вытекают равенства $\nu_j = 0$ для всех j (заметим, что $n \geqslant 1$, так как $A \neq 0$). Пусть B — подгруппа, порожденная элементами $x_1, \ldots, x_n$. Тогда B свободна. В силу предположения о максимальности $x_1, \ldots, x_n$ для заданного $y \in A$ существуют целые числа $m_1, \ldots, m_n, m$, не все равные нулю, такие, что

$$my + m_1 x_1 + \ldots + m_n x_n = 0.$$

При этом $m \neq 0$, иначе все $m_j = 0$. Следовательно, my лежит в B. Это справедливо для каждого элемента y из конечного множества образующих группы A, откуда вытекает, что существует целое число $m \neq 0$, для которого $mA \subset B$. Отображение

$$x \longmapsto mx$$

группы A в себя — гомоморфизм, имеющий тривиальное ядро, поскольку A без кручения. Следовательно, это изоморфизм группы A

на подгруппу в B. В силу теоремы 4 предыдущего параграфа заключаем, что mA свободна, откуда и A свободна.

Теорема 8. *Пусть A — конечно порожденная абелева группа и A_t — ее подгруппа, состоящая из всех элементов, имеющих конечный период. Тогда A_t конечна и A/A_t свободна. При этом в A существует свободная подгруппа B, такая, что A есть прямая сумма A_t и B.*

Доказательство. Напомним, что конечно порожденная периодическая абелева группа очевидным образом конечна. Пусть A порождается n элементами, и пусть F — свободная абелева группа с n образующими. В силу свойства универсальности существует сюръективный гомоморфизм

$$F \xrightarrow{\varphi} A$$

группы F на A. Подгруппа $\varphi^{-1}(A_t)$ в F конечно порождена в силу теоремы 4. Следовательно, A_t сама конечно порождена и потому конечна.

Далее, докажем, что A/A_t не имеет кручения. Пусть $\bar{x}$ — некоторый элемент в A/A_t, такой, что $m\bar{x}=0$ для некоторого целого $m \neq 0$. Тогда для любого представителя x класса $\bar{x}$ в A имеем $mx \in A_t$, откуда $qmx=0$ для некоторого целого $q \neq 0$. Следовательно, $x \in A_t$, так что $\bar{x}=0$ и A/A_t свободна от кручения. Значит, в силу теоремы 7 A/A_t свободна. Для завершения доказательства используем лемму к теореме 4.

Ранг факторгруппы A/A_t называется также *рангом* группы A.

§ 11. Дуальная группа

Пусть A — абелева группа показателя $m \geqslant 1$. Это означает, что $mx=0$ для каждого элемента $x \in A$. Пусть Z_m — циклическая группа порядка m. Будем обозначать через A^* или через $\mathrm{Hom}(A, Z_m)$ группу гомоморфизмов группы A в Z_m и называть ее *дуальной* к A.

Пусть $f\colon A \to B$ — гомоморфизм абелевых групп, причем обе группы имеют показатель m. Тогда f индуцирует гомоморфизм

$$f^*\colon B^* \to A^*.$$

Именно, для каждого $\psi \in B^*$ полагаем $f^*(\psi)=\psi \circ f$. Тривиально проверяется, что f^* — гомоморфизм. Можно рассматривать $\mathrm{Hom}(A, Z_m)$ как контравариантный функтор на категории абелевых групп показателя m. Действительно, свойства

$$\mathrm{id}^* = \mathrm{id} \quad \text{и} \quad (f \circ g)^* = g^* \circ f^*$$

проверяются тривиально.