— гомоморфизм, переводящий каждый элемент x_i в себя, а все другие элементы из S — в единичный элемент группы G. Наше утверждение теперь очевидно.

Следствие 2. *Пусть S — множество из n элементов $x_1, \ldots, x_n$, $n \geqslant 1$, и $G_1, \ldots, G_n$ — бесконечные циклические группы, порожденные этими элементами. Тогда отображение*

$$F(S) \to G_1 \circ \ldots \circ G_n,$$

переводящее каждое x_i в себя, является изоморфизмом.

Доказательство. Это отображение, очевидно, сюръективно и инъективно.

Следствие 3. *Пусть $G_1, \ldots, G_n$ — группы. Гомоморфизм*

$$G_1 \coprod \ldots \coprod G_n \to G_1 \circ \ldots \circ G_n$$

их копроизведения в $G_1 \circ \ldots \circ G_n$, индуцированный естественными вложениями $G_i \to G_1 \circ \ldots \circ G_n$, является изоморфизмом.

Доказательство. Опять-таки очевидно, что этот гомоморфизм инъективен и сюръективен.

§ 9. Прямые суммы и свободные абелевы группы

Абелевы группы образуют категорию, которую можно обозначить символом Ab. Заметим, что если $\{A_i\}_{i \in I}$ — семейство абелевых групп, то их произведение в категории групп является также произведением в категории абелевых групп, т. е. если мы образуем теоретико-множественное произведение

$$\prod_{i \in I} A_i$$

и наделим его структурой группы с помощью покомпонентного умножения, то оно станет абелевой группой, обладающей необходимым свойством универсальности.

Копроизведение в категории абелевых групп обычно называется прямой суммой.

Предложение 10. *Прямые суммы в категории абелевых групп существуют.*

Доказательство. Пусть $\{A_i\}_{i \in I}$ — семейство абелевых групп. Рассмотрим подмножество A прямого произведения $\prod A_i$, состоящее из всех семейств $(x_i)_{i \in I}$, $x_i \in A_i$, таких, что $x_i = 0$ для всех, кроме

конечного числа индексов i. Ясно, что A — подгруппа в произведении. Для каждого индекса $j \in I$ мы определим отображение

$$\lambda_j\colon A_j \to A,$$

положив $\lambda_j(x)$ равным элементу из A, j-я компонента которого есть x, а все остальные компоненты равны 0. Очевидно, λ_j — инъективный гомоморфизм. Мы утверждаем, что A вместе с семейством отображений $\{\lambda_i\}_{i \in I}$ есть прямая сумма семейства $\{A_i\}$. Пусть $\{f_i\colon A_i \to B\}$ — произвольное семейство гомоморфизмов в абелеву группу B. Определим отображение

$$f\colon A \to B$$

формулой

$$f((x_i)_{i \in I}) = \sum_{i \in I} f_i(x_i).$$

Сумма справа в действительности конечная, так как в ней все члены, кроме конечного числа, равны 0. Непосредственно проверяется, что отображение f — гомоморфизм. Кроме того, ясно, что $f \circ \lambda_j(x) = f_j(x)$ для всякого j и всякого $x \in A_j$. Таким образом, f удовлетворяет необходимому условию коммутативности. Ясно также, что отображение f однозначно определено, чем доказательство и завершено.

Заметим, что в случае конечного множества I прямая сумма и прямое произведение совпадают.

Пусть A — абелева группа и B, C — её подгруппы. Если $B + C = A$ и $B \cap C = 0$, то отображение

$$B \times C \to A,$$

задаваемое правилом $(x, y) \mapsto x + y$, является изоморфизмом (мы уже отмечали это в некоммутативном случае). Вместо записи $A = B \times C$ мы будем писать

$$A = B \oplus C$$

и говорить, что A — *прямая сумма* B и C. Аналогичное обозначение используется и для прямой суммы любого конечного числа подгрупп $B_1, \ldots, B_n$, таких, что $B_1 + \ldots + B_n = A$ и

$$B_{i+1} \cap (B_1 + \ldots + B_i) = 0.$$

В этом случае пишем

$$A = B_1 \oplus \ldots \oplus B_n.$$

Пусть теперь S — множество и $\mathscr{C}$ — категория, объектами которой являются отображения $f\colon S \to A$ множества S в абелевы группы, с очевидным образом определяемыми морфизмами: если $f\colon S \to A$ и $f'\colon S \to A'$ — два отображения в абелевы группы, то морфизм из f

в f' — это гомоморфизм (групп) g: $A \to A'$, такой, что коммутативна обычная диаграмма, т. е. $g \circ f = f'$. Универсальный объект этой категории $\mathscr{C}$ называется *свободной абелевой группой*, порожденной множеством S. Мы увидим, что *такой объект всегда существует*.

Действительно, пусть $\mathbf{Z}\langle S\rangle$ — множество всех отображений φ: $S \to \mathbf{Z}$, таких, что $\varphi(x) = 0$ для почти всех $x \in S$. Тогда $\mathbf{Z}\langle S\rangle$ — абелева группа (сложением в которой служит обычное сложение отображений). Пусть k — целое число и x — некоторый элемент из S. Мы обозначаем через $k \cdot x$ отображение φ, для которого $\varphi(x) = k$ и $\varphi(y) = 0$ при $y \neq x$. Очевидно, что всякий элемент φ из $\mathbf{Z}\langle S\rangle$ может быть записан в виде

$$\varphi = k_1 \cdot x_1 + \ldots + k_n \cdot x_n,$$

где k_i — некоторые целые числа и $x_i \in S$ $(i = 1, \ldots, n)$, причем все элементы x_i различны. Кроме того, φ *допускает единственное такое представление*, так как если

$$\varphi = \sum_{x \in S} k_x \cdot x = \sum_{x \in S} k'_x \cdot x,$$

то

$$0 = \sum_{x \in S} (k_x - k'_x) \cdot x,$$

откуда $k'_x = k_x$ для всех $x \in S$.

Вложим S в $\mathbf{Z}\langle S\rangle$ посредством отображения $f_S = f$, для которого $f(x) = 1 \cdot x$. Ясно, что f инъективно и что $f(S)$ порождает $\mathbf{Z}\langle S\rangle$. Для всякого отображения g: $S \to B$ множества S в абелеву группу B определим отображение

$$g_*\colon \mathbf{Z}\langle S\rangle \to B$$

формулой

$$g_*\left(\sum_{x \in S} k_x \cdot x\right) = \sum_{x \in S} k_x g(x).$$

Это отображение — гомоморфизм (тривиально), для которого соответствующая диаграмма коммутативна, т. е. $g_* \circ f = g$ (тоже тривиально). Это единственный гомоморфизм, обладающий указанным свойством, так как для всякого такого гомоморфизма g_* должно выполняться условие $g_*(1 \cdot x) = g(x)$. Таким образом, наш универсальный объект построен.

Обычно отождествляют S с его образом в $\mathbf{Z}\langle S\rangle$; иногда мы будем опускать точку и писать просто $k_x x$ или $\sum k_x x$.

Для всякого отображения λ: $S \to S'$ *одного множества в другое существует единственный гомоморфизм* $\bar{\lambda}$, *для которого*

коммутативна следующая диаграмма:

$$\begin{tikzcd} S \arrow[r, "f_S"] \arrow[d, "\lambda"'] & \mathbf{Z}\langle S\rangle \arrow[d, "\bar{\lambda}"] \\ S' \arrow[r, "f_{S'}"'] & \mathbf{Z}\langle S'\rangle \end{tikzcd}$$

Действительно, $\bar{\lambda}$ есть не что иное, как $(f_{S'} \circ \lambda)_*$ в обозначениях предыдущего параграфа. Доказательство этого утверждения предоставляется читателю в качестве тривиального упражнения.

Положим $F_{\mathrm{ab}}(S) = \mathbf{Z}\langle S\rangle$ и $\bar{\lambda} = F_{\mathrm{ab}}(\lambda)$. Очевидно, что F_{ab} есть функтор из категории множеств в категорию абелевых групп.

В качестве упражнения покажите, что всякая абелева группа A есть факторгруппа некоторой свободной абелевой группы F. Если A — конечно порожденная группа, то покажите, что и F можно выбрать конечно порожденной.

Если множество S состоит из n элементов, то мы будем говорить, что свободная абелева группа $F_{\mathrm{ab}}(S)$ есть свободная абелева группа с n образующими. Если S — множество из n символов $x_1, \ldots, x_n$, то мы скажем, что $F_{\mathrm{ab}}(S)$ — свободная абелева группа со свободными образующими $x_1, \ldots, x_n$.

Абелева группа называется *свободной*, если она изоморфна свободной абелевой группе $F_{ab}(S)$ для некоторого множества S. Пусть A — абелева группа, и пусть S — такое подмножество в A, что для любого данного $z \in A$ существует единственный набор целых чисел n_x, по одному для каждого $x \in S$, такой, что почти все $n_x = 0$ и

$$z = \sum_{x \in S} n_x x.$$

Тогда ясно, что группа A изоморфна свободной абелевой группе $F_{\mathrm{ab}}(S)$; мы называем S множеством *свободных образующих* группы A или также ее *базисом*. Аналогичным образом определяется понятие семейства свободных образующих.

Несколько слов об обозначениях. Если A — абелева группа и T — подмножество элементов из A, то мы обозначаем через $\langle T\rangle$ подгруппу, порожденную всеми элементами из T, т. е. наименьшую подгруппу в A, содержащую T.

Пример. *Группа Гротендика. Пусть M — коммутативный моноид, записываемый аддитивно. Существуют коммутативная группа $K(M)$, называемая группой Гротендика моноида M, и гомоморфизм моноидов*

$$\gamma\colon M \to K(M),$$

обладающие свойством универсальности относительно гомоморфизмов моноида M в коммутативные группы.

Доказательство. Пусть $F_{ab}(M)$ — свободная абелева группа, порожденная M. Обозначим через $[x]$ образующую группы $F_{ab}(M)$, соответствующую элементу $x \in M$. Пусть B — подгруппа, порожденная всеми элементами вида

$$[x+y]-[x]-[y],$$

где $x, y \in M$. Положим $K(M) = F_{ab}(M)/B$. Пусть, далее,

$$\gamma\colon M \to K(M)$$

— отображение, являющееся композицией вложения моноида M в $F_{ab}(M)$, задаваемого соответствием $x \mapsto [x]$, и канонического отображения

$$F_{ab}(M) \to F_{ab}(M)/B.$$

Ясно, что γ — гомоморфизм, удовлетворяющий нужному свойству универсальности.

Будем говорить, что в M выполняется *закон сокращения*, если для любых $x, y, z \in M$, связанных соотношением $x+z=y+z$, имеем $x=y$.

Справедлив следующий важный критерий инъективности построенного выше универсального отображения γ.

Если в M выполняется закон сокращения, то каноническое отображение γ моноида M в его группу Гротендика инъективно.

Доказательство. Доказательство здесь по существу то же самое, что и при построении отрицательных целых чисел, исходя из натуральных. Рассмотрим пары (x, y), где $x, y \in M$, и скажем, что пара (x, y) эквивалентна паре (x', y'), если $y+x'=x+y'$. (Из справедливости закона сокращения вытекает, что это действительно отношение эквивалентности.) Сложение пар определим покомпонентно. Тогда классы эквивалентности пар образуют группу, нулевым элементом которой служит класс пары $(0, 0)$ [или класс пары (x, x) для любого $x \in M$]. Противоположным для элемента (x, y) является (y, x). Имеет место гомоморфизм

$$x \mapsto \text{класс пары } (0, x).$$

Из закона сокращения сразу следует, что он инъективен. Таким образом, мы построили инъективный гомоморфизм моноида M в некоторую группу. Отсюда вытекает, что универсальный гомоморфизм также должен быть инъективен.

Мы рассмотрим позже несколько примеров универсальных групп $K(M)$.

Для данных абелевой группы A и ее подгруппы B иногда бывает желательно найти подгруппу C, такую, что $A = B \oplus C$. Следующая лемма дает нам условие, при котором это возможно.

Лемма. *Пусть $A \xrightarrow{f} A'$ — сюръективный гомоморфизм абелевых групп и B — ядро f. Тогда, если группа A' свободна, то в A существует подгруппа, такая, что ограничение f на C индуцирует изоморфизм C на A', и $A = B \oplus C$.*

Доказательство. Пусть $\{x'_i\}_{i \in I}$ — базис группы A', и для каждого $i \in I$ пусть x_i — какой-либо элемент из A, для которого $f(x_i) = x'_i$. Пусть C — подгруппа в A, порожденная всеми элементами x_i, $i \in I$. Если

$$\sum_{i \in I} n_i x_i = 0$$

для некоторых целых n_i, из которых почти все равны 0, то, применяя f, получаем

$$0 = \sum_{i \in I} n_i f(x_i) = \sum_{i \in I} n_i x'_i,$$

откуда все $n_i = 0$. Следовательно, наше семейство $\{x_i\}_{i \in I}$ — базис подгруппы C. Аналогичным образом, если $z \in C$ и $f(z) = 0$, то $z = 0$. Следовательно, $B \cap C = 0$. Пусть $x \in A$. Так как $f(x) \in A'$, то существуют целые числа n_i, $i \in I$, такие, что

$$f(x) = \sum_{i \in I} n_i x'_i.$$

Применяя f к $x - \sum_{i \in I} n_i x_i$, находим, что последний элемент лежит в ядре f, скажем

$$x - \sum_{i \in I} n_i x_i = b \in B.$$

Отсюда видно, что $x \in B + C$, и, следовательно, $A = B \oplus C$, что и утверждалось.

Теорема 4. *Пусть A — свободная абелева группа, B — некоторая ее подгруппа. Тогда B — также свободная абелева группа и мощность базиса $B \leqslant$ мощности базиса A. Любые два базиса B имеют одинаковую мощность, называемую рангом B.*

Доказательство. Мы дадим доказательство только для случая, когда A конечно порождена, скажем, базисом $\{x_1, \ldots, x_n\}$ $(n \geqslant 1)$; проводим доказательство индукцией по n. Имеем представление A в виде прямой суммы

$$A = \mathbf{Z}x_1 \oplus \ldots \oplus \mathbf{Z}x_n.$$

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