Глава I

Группы

§ 1. Моноиды

Пусть S — множество. Отображение

$$S \times S \to S$$

называется иногда *законом композиции* (на S в себя). Если x и y — элементы из S, то образ пары (x, y) при этом отображении называется также их *произведением* относительно закона композиции и будет обозначаться через xy. (Иногда мы пишем также $x \cdot y$, а во многих случаях удобно использовать и аддитивное обозначение и писать, таким образом, $x+y$. В этом случае мы называем элемент $x+y$ *суммой* x и y. Обычно обозначение $x+y$ используют только в том случае, когда выполняется соотношение $x+y=y+x$.)

Пусть S — множество, наделенное законом композиции. Произведение элементов x, y, z из S можно составить двумя способами: $(xy)z$ и $x(yz)$. Если $(xy)z=x(yz)$ для всех x, y, z из S, то мы говорим, что закон композиции *ассоциативен*.

Элемент e из S, такой, что $ex=x=xe$ для всех $x \in S$, называется *единичным элементом*. (Когда закон композиции записывается аддитивно, единичный элемент обозначается через 0 и называется *нулевым элементом*.) Единичный элемент единствен, поскольку если e' — другой единичный элемент, то по предположению имеем

$$e=ee'=e'.$$

В большинстве случаев единичный элемент обозначают просто 1 (вместо e). В большей части этой главы, однако, мы будем писать e, чтобы избежать путаницы при доказательствах основных свойств.

Моноид — это множество G с ассоциативным законом композиции, обладающим единичным элементом (так что, в частности, G не пусто).

Пусть G — моноид и $x_1, \ldots, x_n$ — элементы из G (где n — целое число >1). Мы определим их произведение по индукции

$$\prod_{\nu=1}^{n} x_\nu = x_1 \ldots x_n = (x_1 \ldots x_{n-1})\, x_n.$$

Справедливо следующее правило

$$\prod_{\mu=1}^{m} x_\mu \cdot \prod_{\nu=1}^{n} x_{m+\nu} = \prod_{\nu=1}^{m+n} x_\nu,$$

утверждающее по существу, что мы можем любым способом расставлять скобки в нашем произведении, не изменяя его значения. Доказательство легко получается индукцией, и мы предоставляем его читателю в качестве упражнения.

Вместо $\prod_{\nu=1}^{n} x_{m+\nu}$ пишут также $\prod_{m+1}^{m+n} x_\nu$.

Удобно считать, что пустое произведение равно единичному элементу. Таким образом, по определению $\prod_{\nu=1}^{0} x_\nu = e$.

Можно было бы определить более общие законы композиции, т. е. отображения $S_1 \times S_2 \to S_3$ с произвольными множествами; можно, далее, определить ассоциативность и коммутативность в любой ситуации, для которой это имеет смысл. Например, для коммутативности нужен закон композиции

$$f\colon S \times S \to T,$$

где два исходных множества одинаковы. *Коммутативность* тогда означает, что $f(x, y) = f(y, x)$, или $xy = yx$, если опустить в обозначениях f. Что касается ассоциативности, то мы предоставляем читателю найти наиболее общую комбинацию множеств, при которой она работает. Ниже нам встретятся специальные случаи, связанные, например, с отображениями $S \times S \to S$ и $S \times T \to T$. Здесь произведение $(xy)z$ имеет смысл при $x \in S$, $y \in S$ и $z \in T$. Произведение $x(yz)$ также имеет смысл для таких элементов x, y, z, и, следовательно, имеет смысл говорить об ассоциативности нашего закона композиции, коль скоро для всех указанных выше элементов x, y, z выполнено равенство $(xy)z = x(yz)$.

Если закон композиции, определенный на G, коммутативен, то мы также будем говорить, что сам моноид G *коммутативен* (или *абелев*).

Пусть G — коммутативный моноид и $x_1, \ldots, x_n$ — элементы из G. Пусть ψ — биективное отображение множества целых чисел $(1, \ldots, n)$ на себя. Тогда

$$\prod_{\nu=1}^{n} x_{\psi(\nu)} = \prod_{\nu=1}^{n} x_\nu.$$

Мы докажем это утверждение по индукции. Для $n = 1$ оно очевидно. Предположим, что оно верно для $n - 1$. Пусть k — такое целое число, что $\psi(k) = n$. Тогда

$$\prod_{1}^{n} x_{\psi(\nu)} = \prod_{1}^{k-1} x_{\psi(\nu)} \cdot x_{\psi(k)} \cdot \prod_{1}^{n-k} x_{\psi(k+\nu)} = \prod_{1}^{k-1} x_{\psi(\nu)} \cdot \prod_{1}^{n-k} x_{\psi(k+\nu)} \cdot x_{\psi(k)}.$$

Определим отображение φ множества $(1, \ldots, n-1)$ в себя формулами

$$\varphi(\nu) = \psi(\nu), \qquad \text{если} \quad \nu < k,$$
$$\varphi(\nu) = \psi(\nu+1), \quad \text{если} \quad \nu \geqslant k.$$

Тогда

$$\prod_1^n x_{\psi(\nu)} = \prod_1^{k-1} x_{\varphi(\nu)} \cdot \prod_1^{n-k} x_{\varphi(k-1+\nu)} \cdot x_n = \prod_1^{n-1} x_{\varphi(\nu)} \cdot x_n,$$

что по индукции равно $x_1, \ldots, x_n$, как и требовалось.

Пусть G — коммутативный моноид, I — некоторое множество, и пусть $f\colon I \to G$ — такое отображение, что $f(i) = e$ для почти всех $i \in I$. (Здесь и ниже *почти все* означает *все, кроме конечного числа.*) Пусть I_0 — подмножество в I, состоящее из тех i, для которых $f(i) \neq e$. Под

$$\prod_{i \in I} f(i)$$

мы будем понимать произведение

$$\prod_{i \in I_0} f(i),$$

взятое в любом порядке (его значение не зависит от порядка по предыдущему замечанию). Разумеется, пустое произведение равно e.

Когда G записывается аддитивно, то вместо знака произведения мы пишем знак суммы $\sum$.

Имеется ряд формальных правил обращения с произведениями, которые было бы скучно полностью перечислять. Приведем только один пример. Пусть I, J — два множества и $f\colon I \times J \to G$ — отображение в коммутативный моноид, принимающее значение e для почти всех пар (i, j). Тогда

$$\prod_{i \in I} \Big[\prod_{j \in J} f(i, j) \Big] = \prod_{j \in J} \Big[\prod_{i \in I} f(i, j) \Big].$$

Доказательство предоставляем читателю в качестве упражнения.

Мы будем иногда писать $\prod f(i)$, опуская $i \in I$, если ясно, о каком множестве индексов идет речь.

Пусть x — элемент моноида G. Для всякого целого $n \geqslant 0$ мы определим x^n как

$$\prod_1^n x,$$

так что, в частности, $x^0 = e$, $x^1 = x$, $x^2 = xx$, ... Очевидно, $x^{n+m} = x^n x^m$ и $(x^n)^m = x^{nm}$. Кроме того, в силу ассоциативности для любых двух элементов x и y моноида G, таких, что $xy = yx$,

имеем $(xy)^n = x^n y^n$. Формальное доказательство предоставляем читателю в качестве упражнения.

Пусть S, S' — два подмножества моноида G. Мы понимаем под SS' подмножество, состоящее из всех элементов вида xy, где $x \in S$ и $y \in S'$. По индукции можно определить произведение любого конечного числа подмножеств, причем имеет место ассоциативность. Например, если S, S', S'' — подмножества в G, то $(SS')S'' = S(S'S'')$. Заметим, что $GG = G$ (потому что в G имеется единичный элемент). Для $x \in G$ мы определим xS как $\{x\}S$, где $\{x\}$ — множество, состоящее из одного элемента x. Таким образом, множество xS состоит из всех элементов вида xy, где $y \in S$.

Подмоноидом моноида G называется подмножество H в G, содержащее единичный элемент e и такое, что $xy \in H$, если x, $y \in H$ (мы говорим, что H *замкнуто* относительно закона композиции). Ясно, что подмоноид H сам является моноидом относительно закона композиции, индуцированного законом композиции на G.

Для всякого элемента x моноида G подмножество степеней x^n $(n = 0, 1, \ldots)$ есть подмоноид в G.

Пример моноида. Мы предполагаем, что читатель знаком с терминологией элементарной топологии. Пусть M — множество классов гомеоморфных друг другу компактных (связных) поверхностей. Определим сложение в M. Пусть S, S' — компактные поверхности, D — маленький диск в S и D' — маленький диск в S'. Пусть далее C, C' — окружности, образующие границы D и D', а D_0, D'_0 — внутренности дисков D и D' соответственно. Приклеим $S - D_0$ к $S' - D'_0$, отождествив C с C'. Можно показать, что получающаяся поверхность не зависит с точностью до гомеоморфизма от произвола в выборе, имеющегося в предыдущем построении. Если σ, σ' обозначают классы поверхностей, гомеоморфных поверхностям S и S' соответственно, то мы берем в качестве $\sigma + \sigma'$ класс поверхности, полученной указанным процессом склеивания. Можно показать, что так определенное сложение определяет на M структуру моноида, нулевым элементом которого будет класс обычной двумерной сферы. Кроме того, если τ обозначает класс тора, а π — класс проективной плоскости, то всякий элемент σ из M имеет единственное представление в виде

$$\sigma = n\tau + m\pi,$$

где n — целое число $\geqslant 0$, а $m = 0$, 1 или 2. Справедливо равенство $3\pi = \tau + \pi$.

(Предыдущий пример включен по двум причинам: во-первых, чтобы скрасить неизбежную скуку этого параграфа; во-вторых, чтобы показать читателю, что моноиды существуют в природе. Нет нужды говорить, что этот пример никоим образом не будет использоваться в остальной части книги.)