Независимый Московский Университет

Алгебра

Первый курс, весенний семестр 2004/05 г.
Лекции 1–2

Отображения множеств

Рассмотрим два множества M и N.

Определение 1. *Отображением* φ множества M во множество N

$$\varphi : M \to N \qquad (\text{или} \quad M \xrightarrow{\varphi} N)$$

называется любое правило, сопоставляющее каждому элементу $m \in M$ некоторый единственный элемент $\varphi(m) \in N$. Этот элемент $\varphi(m)$ называется *образом* элемента m при отображении φ. Вместо $n = \varphi(m)$ пишут также

$$\varphi : m \mapsto n \qquad \text{или} \qquad m \overset{\varphi}{\mapsto} n.$$

Если S — какое-нибудь подмножество в M, то можно рассмотреть в N подмножество, состоящее из образов всех элементов из S при отображении φ. Это подмножество называется *образом* множества S при отображении φ и обозначается через $\varphi(S)$. Запишем это формулой: $\varphi(S) = \{\varphi(m) \mid m \in S\}$.

Наоборот, пусть T — какое-нибудь подмножество в N. Рассмотрим в M подмножество, состоящее из всех элементов множества M, образы которых при отображении φ лежат в T. Это подмножество называется *прообразом* множества T при отображении φ и обозначается через $\varphi^{-1}(T)$ (формальная запись: $\varphi^{-1}(T) = \{m \in M \mid \varphi(m) \in T\}$).

Мы можем, в частности, рассмотреть случай, когда T состоит из одного элемента $n \in N$. В этом случае прообраз $\varphi^{-1}(n)$ элемента n при отображении φ часто называют слоем отображения φ над точкой n.

Из определения отображения сразу следует, что каждый элемент множества M содержится ровно в одном слое отображения φ. Иначе говоря, слои отображения φ покрывают множество M, попарно не пересекаясь.

Пример 1. Пусть $M = \mathbb{C}$ — множество комплексных чисел, $N = \mathbb{R}$, а отображение $\varphi : M \to M$ задается формулой $\varphi(z) = |z|$. Тогда $\varphi(M) = \mathbb{R}_+$ — множество всех неотрицательных вещественных чисел, а слой над числом $r \in N$ пуст, если $r < 0$, и является окружностью с центром в нуле и радиусом r, если $r \geqslant 0$.

Пример 2. Пусть M — произвольное множество. Отображение $\varphi : M \to M$, заданное формулой $\varphi(m) = m$, называется *тождественным отображением* множества M в себя, и обозначается через id_M, 1_M или e_M.

В зависимости от свойств слоев принято выделять несколько специальных типов отображений.

Определение 2. Отображение $\varphi : M \to N$ называется *сюръективным* (или *сюръекцией*), *инъективным* (или *инъекцией*), *биективным* (или *биекцией*), если, соответственно, каждый слой не пуст, каждый слой состоит не более, чем из одного элемента, каждый слой состоит ровно из одного элемента.

Пример 3. Пусть $M = N = \mathbb{R}$, а отображение $\varphi : M \to M$ задается функцией $y = x^2$. Тогда φ не является ни сюръекцией, ни инъекцией (и, значит, ни биекцией). Если рассмотреть функцию $y = \begin{cases} \ln|x|, & x \neq 0, \\ 0, & x = 0, \end{cases}$ то мы получим пример сюръекции, не являющейся инъекцией, а если взять функцию $y = e^x$, то, наоборот, пример инъекции, не являющейся сюръекцией. Функция $y = x^3$ определяет биекцию.

Отметим, что тождественное отображение всегда является биекцией.

Предположим, что заданы три множества M, N и K и два отображения $\varphi : M \to N$ и $\psi : N \to K$. Тогда можно определить отображение $\chi : M \to K$ с помощью формулы $\chi(m) = \psi(\varphi(m))$.

Таким образом, χ является результатом последовательного выполнения отображений φ и ψ. Определенное таким образом отображение χ называется композицией отображений φ и ψ и обозначается через $\psi \circ \varphi$.

Непосредственно проверяется, что для любых четырех множеств M, N, K и L и любых трех отображений $\varphi : M \to N$, $\psi : N \to K$ и $\theta : K \to L$ выполнено равенство:

$$\theta \circ (\psi \circ \varphi) = (\theta \circ \psi) \circ \varphi,$$

то есть операция композиции *ассоциативна*.

Пример 4. Пусть $\varphi, \psi : \mathbb{R} \to \mathbb{R}$ — отображения, заданные формулами $\varphi(x) = x^3$ и $\psi(x) = x^2 + x$. Проверьте, что $(\varphi \circ \psi)(x) = x^6 + 3x^5 + 3x^4 + x^3$, а $(\psi \circ \varphi)(x) = x^6 + x^3$. Таким образом, операция композиции, вообще говоря, не коммутативна.

Пусть $M_0, M_1, \ldots, M_n$ — произвольные множества, $\varphi_i : M_{i-1} \to M_i$ — отображения между ними. Рассмотрим выражение $\varphi_n \circ \varphi_{n-1} \circ \cdots \circ \varphi_1$. Каждой расстановке скобок в этом выражении отвечает некоторое отображение $M_0 \to M_n$. Из ассоциативности композиции с помощью индукции по n легко вывести, что все эти отображения совпадают (Проделайте это!). Для всех этих совпадающих отображений используется обозначение $\varphi_n \circ \varphi_{n-1} \circ \cdots \circ \varphi_1$.

Факторизация отображений

Кроме операций в алгебре рассматриваются еще отношения. Для любых двух множеств M и N всякое подмножество $R \subseteq M \times N$ называется *бинарным отношением* между M и N (или просто на M, если $N = M$). Обычно для отношения выбирают какой-нибудь символ (например $*$) и пишут $x * y$ для всех пар $(x, y) \in R$ (и только для них). Бинарное отношение на множестве M называется *отношением эквивалентности*, (для такого отношения обычно используется символ $\sim$), если для всех $x, x', x'' \in M$ выполнены следующие свойства:

1) $x \sim x$ (*рефлексивность*),

2) $x \sim x' \Rightarrow x' \sim x$ (*симметричность*),

3) $x \sim x', x' \sim x'' \Rightarrow x \sim x''$ (*транзитивность*).

Подмножество

$$\bar{x} = \{x' \in M \mid x' \sim x\} \subseteq M$$

всех элементов, эквивалентных данному x, называется *классом эквивалентности*, содержащим x.

Ясно, что классы эквивалентности покрывают множество M, попарно не пересекаясь (Почему?), т. е. образуют *разбиение* множества M. Множество классов эквивалентности называется *фактормножеством* M по отношению $\sim$ и обозначается через $M/\!\sim$. Сюръективное отображение $\pi : x \mapsto \bar{x}$ называется *канонической проекцией* M на $M/\!\sim$.

Пример 5. Пусть $M = \mathbb{Z}$. Зафиксируем натуральное число n. Введем на M отношение эквивалентности, полагая $k \sim m$ в том и только в том случае, когда $m-k$ делится на n. Классы эквивалентности в этом случае называются классами вычетов по модулю n.

Пример 6. Пусть M — это плоскость. Введем на ней декартову систему координат. Скажем, что точки (a_1, a_2) и (b_1, b_2) эквивалентны, если $a_1 - b_1 \in \mathbb{Z}$ и $a_2 - b_2 \in \mathbb{Z}$. Геометрически каждый класс эквивалентности представляет собой «решетку» на плоскости.

Попробуем построить естественную модель фактормножества M по этому отношению эквивалентности. Нетрудно убедиться, что полуоткрытый единичый квадрат $\{(a_1, a_2) \in M \mid 0 \leqslant a_1 < 1, 0 \leqslant a_2 < 1\}$ пересекается с каждым классом эквивалентности ровно по одной точке, так что фактормножество может быть отождествлено с таким квадратом. Эта модель обладает тем недостатком, что близким решеткам могут отвечать далекие друг от друга точки квадрата (например, если $\varepsilon > 0$ мало, то решетки $\overline{(0,0)}$ и $\overline{(-\varepsilon, -\varepsilon)}$ близки, а соответствующие точки квадрата $(0, 0)$ и $(1-\varepsilon, 1-\varepsilon)$ – далеки). Этого недостатка можно избежать, рассмотрев замкнутый квадрат $\{(a_1, a_2) \in M \mid 0 \leqslant a_1 \leqslant 1, 0 \leqslant a_2 \leqslant 1\}$, а затем «склеив» (т. е. отождествив) точки, лежащие на противоположных сторонах. Склеив вертикальные сторон квадрата мы получим трубку, а склеив между собой верхнюю и нижнюю окружности, в которые превратились горизонтальные стороны квадрата после склеивания вертикальных, мы получим *тор*.

Теорема 1. *Пусть $\varphi : M \to N$ — произвольное отображение. Введем на M отношение эквивалентности $\sim_\varphi$, полагая $x \sim_\varphi y \Leftrightarrow \varphi(x) = \varphi(y)$. Пусть $Q = M/\!\sim_\varphi$, а $\pi : M \to Q$ — каноническая проекция. Тогда существует единственное отображение $\psi : Q \to N$, для которого $\varphi = \psi \circ \pi$, или, как говорят, для которого коммутативна следующая диаграмма:*

$$\begin{array}{ccc} M & \xrightarrow{\varphi} & N \\ & {\scriptstyle\pi}\searrow \quad \nearrow{\scriptstyle\psi} & \\ & Q & \end{array}$$

Отображение ψ инъективно, а если φ сюръективно, то ψ биективно.

Доказательство этой теоремы я оставляю в качестве упражнения.

Группы преобразований

Из определения следует, что для любых двух отображений φ и ψ множества M в себя определена их композиция $\varphi \circ \psi$, причем для любого отображения $\varphi : M \to M$ выполнены равенства $1_M \circ \varphi = \varphi$ и $\varphi \circ 1_M = \varphi$. Это оправдывает обозначение 1_M.

Предположим, что отображения φ и ψ множества M в себя являются биекциями. Тогда, как нетрудно проверить, их композиция $\varphi \circ \psi$ тоже является биекцией. Другими словами, множество $S(M)$ биективных отображений M в себя *замкнуто относительно взятия композиции.* Другое важное свойство множества $S(M)$ таково: для любой биекции $\varphi \in S(M)$ найдется, и притом только одна, биекция $\psi \in S(M)$, для которой

$$\varphi \circ \psi = 1_M,$$

т. е. ψ является *правым обратным отображением* к отображению φ, и

$$\psi \circ \varphi = 1_M,$$

т. е. ψ является *левым обратным отображением* к отображению φ. Эта биекция называется *обратной* к φ и обозначается φ^{-1}.

Элементы множества $S(M)$ называются *преобразованиями* множества M.

Если $\varphi \in S(M)$, а n — элемент множества целых чисел $\mathbb{Z}$, то по определению полагают

$$\varphi^n = \begin{cases} \underbrace{\varphi \circ \dots \circ \varphi}_{n \text{ раз}}, & \text{если } n > 0; \\ 1_M, & \text{если } n = 0; \\ \underbrace{\varphi^{-1} \circ \dots \circ \varphi^{-1}}_{-n \text{ раз}}, & \text{если } n < 0. \end{cases}$$

Упражнение 1. Доказать, что для любых $m, n \in \mathbb{Z}$ выполнены равенства:

$$\varphi^{m+n} = \varphi^m \circ \varphi^n \quad \text{и} \quad (\varphi^n)^m = \varphi^{mn}.$$

Пусть $M = \{1, \dots, n\}$. В этом случае множество $S(M)$ обозначается через S_n. Элементы S_n мы будем называть *перестановками* (иногда их называют подстановками).

Перестановки обычно задают таблицами вида:

$$\begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix},$$

где под каждым элементом множества $\{1, \dots, n\}$ стоит его образ при преобразовании σ.

Определение 3. Непустое подмножество $G \subseteq S(M)$ называется *группой преобразований* множества M, если G замкнуто относительно композиции и взятия обратного преобразования, то есть если $\varphi \circ \psi \in G$ и $\varphi^{-1} \in G$ для любых $\varphi, \psi \in G$.

Из этого определения сразу следует, что если G — группа преобразований множества M, то $1_M \in G$.

Множество $S(M)$ является, конечно, группой преобразований множества M; оно называется *симметрической группой* множества M. Другой пример группы преобразований получается, если рассмотреть для произвольно заданного $\varphi \in S(M)$ множество $\langle\varphi\rangle = \{\psi \in S(M) \mid \psi = \varphi^n \text{ для некоторого } n \in \mathbb{Z}\}$. То, что $\langle\varphi\rangle$ является группой преобразований, следует из упражнения 1. Такая группа преобразований называется *циклической* группой преобразований, порожденной φ.

Приведем еще несколько примеров.

Пример 7. Пусть M — плоскость, $X \subseteq M$ — какая-либо геометрическая фигура. Рассмотрим множество G движений плоскости, переводящих фигуру X в себя. Легко проверить, что это — группа преобразований множества M. Она называется *группой симметрий* фигуры X.

Упражнение 2. Сколько элементов в группе симметрий правильного n-угольника?

Пример 8. Пусть M — трехмерное пространство, $X \subseteq M$ — правильный многогранник. Рассмотрим множество G вращений (вокруг некоторой оси) пространства M, переводящих X в себя. Поскольку композиция вращений вновь является вращением (Проверьте это!), то G — группа преобразований множества M. Она называется *группой вращений* многогранника X. Часто вместо «группа вращений куба (тетраэдра, икосаэдра)» говорят просто «группа куба (соответственно тетраэдра или икосаэдра)».

Вложенный в пространство правильный многоугольник можно считать вырожденным правильным многогранником с двумя гранями — *диэдром*. Группа его вращений называется *группой диэдра*.

Симметрическая группа

Операцию композиции в группе перестановок обозначают как умножение — точкой (или пустым местом); соответственно результат композиции двух перестановок часто называют их произведением. Тождественную перестановку мы будем обозначать буквой e.

Пусть $i_1, \dots, i_k$ — попарно различные элементы множества M. Обозначим через $(i_1, \dots, i_k)$ перестановку $\sigma \in S_n$, переводящую i_1 в i_2, i_2 в i_3,..., i_{k-1} в i_k, i_k в i_1, а все остальные элементы множества M оставляющую на месте. Такая перестановка называется *циклом*. Число k называется длиной цикла. Из определения ясно, что все циклы длины 1 равны между собой и равны тождественному отображению. Мы будем называть циклы длины 1 тривиальными.

Орбитами цикла $\sigma = (i_1, \dots, i_k)$ (то есть $\langle\sigma\rangle$-орбитами) являются множество $\{i_1, \dots, i_k\}$ и одноэлементные множества $\{i\}$, где $i \in M \setminus \{i_1, \dots, i_k\}$.

Пусть $\sigma = (i_1, \dots, i_k)$ и $\tau = (j_1, \dots, j_l)$ — циклы, причем $\{i_1, \dots, i_k\} \cap \{j_1, \dots, j_l\} = \varnothing$. Тогда $\sigma\tau = \tau\sigma$ (Почему?). Такие циклы называются *независимыми*.

Рассмотрим теперь произвольную перестановку φ. Пусть $I^1, \ldots, I^m$ — все ее орбиты, содержащие более одного элемента. Выберем в каждой орбите I^α по элементу i_1^α. Пусть k_α — минимальное натуральное число, для которого $\varphi^{k_\alpha}(i_1^\alpha) = i_1^\alpha$ (если таких натуральных чисел нет, то положим $k_\alpha = \infty$).

Докажем, что $\varphi^r(i_1^\alpha) \neq \varphi^s(i_1^\alpha)$ при $1 \leqslant r < s < k_\alpha$. Действительно, если $\varphi^r(i_1^\alpha) = \varphi^s(i_1^\alpha)$, то $\varphi^{s-r}(i_1^\alpha) = i_1^\alpha$. Согласно определению k_α такого быть не может, поскольку $0 < s - r < k_\alpha$.

Отсюда, в частности, следует, что $k_\alpha < \infty$, поскольку все элементы вида $\varphi^r(i_1^\alpha)$ лежат в конечном множестве I^α.

Положим $i_r^\alpha = \varphi^{r-1}(i_1^\alpha)$ для $r = 2, \ldots, k_\alpha$. Как мы показали, все эти элементы попарно различны (и не равны i_1^α). Кроме того, $I^\alpha = \{i_1^\alpha, \ldots, i_{k_\alpha}^\alpha\}$. Действительно, по определению, любой элемент $\langle\varphi\rangle$-орбиты числа i_1^α имеет вид $\varphi^t(i_1^\alpha)$ при некотором целом t. Поделим с остатком t на k_α: $t = qk_\alpha + r$, $0 \leqslant r < k_\alpha$. Тогда

$$\varphi^t(i_1^\alpha) = \varphi^r \cdot \varphi^{qk_\alpha}(i_1^\alpha) = \varphi^r \cdot (\varphi^{k_\alpha})^q(i_1^\alpha) = \varphi^r(i_1^\alpha) = i_{r+1}^\alpha.$$

Из всего сказанного следует, что перестановка φ действует на элементы из I^α так же, как цикл $\sigma_\alpha = (i_1^\alpha, \ldots, i_{k_\alpha}^\alpha)$. Более того, имеет место равенство $\varphi = \sigma_1 \cdot \cdots \cdot \sigma_m$. Порядок сомножителей в этом произведении не важен, поскольку входящие в него циклы попарно независимы.

Таким образом, доказана

Теорема 2. *Каждая перестановка разлагается в произведение независимых нетривиальных циклов.*

Упражнение 3. Доказать, что представление перестановки в виде произведения независимых нетривиальных циклов единственно с точностью до порядка следования сомножителей.

Определение 4. Цикл длины 2 называется *транспозицией.*

Рассмотрим следующие транспозиции: $s_1 = (1,2)$, $s_2 = (2,3)$, $\ldots$, $s_{n-1} = (n-1, n)$. Каждая из этих перестановок меняет местами какие-нибудь два соседние элемента, оставляя остальные на местах.

Определение 5. *Длиной* $l(\sigma)$ перестановки σ называется число ее инверсий, то есть таких пар (i,j), что $i < j$, но $\sigma(i) > \sigma(j)$.

Теорема 3. *Каждая перестановка $\sigma \in S_n$ может быть представлена в виде произведения:*

$$\sigma = s_{i_1} s_{i_2} \ldots s_{i_l},$$

где $l = l(\sigma)$, а $(i_1, \ldots, i_l)$ — некоторая последовательность элементов множества $\{1, \ldots, n-1\}$ (члены последовательности могут повторяться).

Доказательство: Воспользуемся индукцией по $l(\sigma)$.

Если $l(\sigma) = 0$, то, очевидно, $\sigma = e$ и доказывать нечего.

Пусть $l(\sigma) = l > 0$ и для всех перестановок длины меньшей l утверждение теоремы верно. Докажем его для σ.

Поскольку $l(\sigma) > 0$, то найдутся $i, j \in M$ такие, что $i < j$ и $\sigma(i) > \sigma(j)$. Выберем такую пару (i,j) с минимальной разностью $j - i$. Если $j - i > 1$, то либо $\sigma(i+1) > \sigma(i) > \sigma(j)$, но $i + 1 < j$, либо $\sigma(i) > \sigma(i+1)$ но $i < i+1$. В обоих случаях получаем противоречие с минимальностью $j - i$. Поэтому $j - i = 1$, то есть $\sigma(i) > \sigma(i+1)$.

Рассмотрим перестановку $\sigma' = \sigma s_i$. Нетрудно убедиться, что $l(\sigma') = l - 1$ (Почему?). По предположению индукции имеется разложение

$$\sigma' = s_{i_1} s_{i_2} \ldots s_{i_{l-1}}.$$

Поскольку $s_i^2 = e$, то $\sigma' s_i = \sigma s_i^2 = \sigma$. Отсюда мы получаем искомое разложение

$$\sigma = s_{i_1} s_{i_2} \ldots s_{i_l},$$

где $i_l = i$. □

Замечание: Разложение, построенное в теореме 3, не является однозначным. Рассмотрим, например, перестановку $\sigma = (1,3) \in S_3$. Проверьте, что $l(\sigma) = 3$ и существуют два разложения: $\sigma = s_1 s_2 s_1$ и $\sigma = s_2 s_1 s_2$.

Определение 6. *Знаком* перестановки σ называется число

$$\varepsilon(\sigma) = (-1)^{l(\sigma)}.$$

Перестановка σ называется *четной*, если $\varepsilon(\sigma) = 1$, и *нечетной*, если $\varepsilon(\sigma) = -1$.

Теорема 4. *Знак произведения двух перестановок равен произведению их знаков.*

Доказательство: Прежде всего отметим, что для любой перестановки $\sigma \in S_n$ и любого $i \in \{1, \dots, n-1\}$

$$l(\sigma s_i) = \begin{cases} l(\sigma) + 1, & \text{если } \sigma(i) < \sigma(i+1); \\ l(\sigma) - 1, & \text{если } \sigma(i) > \sigma(i+1). \end{cases}$$

(Это очевидно из определения длины перестановки как числа инверсий.) Поэтому всегда $\varepsilon(\sigma s_i) = -\varepsilon(\sigma)$. Отсюда следует, что для любого разложения $\sigma = s_{i_1} \cdot \dots \cdot s_{i_m}$, где m не обязано совпадать с $l(\sigma)$, выполнено равенство $\varepsilon(\sigma) = (-1)^m$.

Пусть теперь у нас есть две перестановки σ и σ', длины которых $l(\sigma) = l$ и $l(\sigma') = l'$. По теореме 3 существуют разложения $\sigma = s_{i_1} \cdot \dots \cdot s_{i_l}$ и $\sigma' = s_{i'_1} \cdot \dots \cdot s_{i'_{l'}}$. Тогда $\sigma\sigma' = s_{i_1} \cdot \dots \cdot s_{i_l} \cdot s_{i'_1} \cdot \dots \cdot s_{i'_{l'}}$, следовательно, $\varepsilon(\sigma\sigma') = (-1)^{l+l'} = \varepsilon(\sigma)\varepsilon(\sigma')$. $\square$

Определение 7. Обозначим через A_n подмножество симметрической группы S_n, состоящее из всех четных перестановок. Из теоремы 4 легко следует, что A_n является группой преобразований множества M. Она называется *знакопеременной группой*.

Группы

Определение 8. Пусть G — некоторое множество, на котором задана бинарная операция $*$ (то есть правило, сопоставляющее каждой упорядоченной паре элементов $g_1, g_2 \in G$ элемент $g_1 * g_2 \in G$), так, что выполнены следующие аксиомы:

1) Ассоциативность: $(g_1 * g_2) * g_3 = g_1 * (g_2 * g_3)$ для любых $g_1, g_2, g_3 \in G$;

2) Существование нейтрального элемента: существует такой элемент $e \in G$, что $e * g = g * e = g$ для любого $g \in G$;

3) Существование обратного элемента: для любого $g \in G$ существует такой элемент $h \in G$, что $h*g = g*h = e$.

В этом случае G называется *группой* (относительно операции $*$).

Группа называется *коммутативной* или *абелевой*, если в ней дополнительно выполнена аксиома коммутативности: $g_1 * g_2 = g_2 * g_1$ для любых $g_1, g_2 \in G$.

Из аксиом группы легко следует единственность нейтрального и обратных элементов.

Пример 9. Произвольная группа преобразований является группой.

Пример 10. Произвольное кольцо A относительно операции сложения является абелевой группой.

Пример 11. Множество A^* обратимых элементов ассоциативного кольца A с единицей относительно умножения является группой.

Замечание: Как правило, для групп используют либо *мультипликативную* форму записи, либо *аддитивную* форму записи. А именно, в мультипликативном случае вместо $*$ либо не используют вообще никакого знака, либо используют знак умножения. Саму групповую операцию при этом называют умножением, а результат операции $g_1 g_2$ — произведением g_1 и g_2. При этом нейтральный элемент e называют единицей. Обратный элемент к g обозначают через g^{-1}.

В аддитивном случае вместо $*$ пишут $+$, операцию называют сложением, нейтральный элемент называют нулем и обозначают 0, и вообще используют привычную для сложения терминологию. Аддитивную форму записи используют почти исключительно для абелевых групп.

Пусть G — конечное множество. Как задать на G структуру группы? Проще всего составить таблицу такого вида:

$\cdot$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

На пересечении строки, озаглавленной $x \in G$, и столбца, озаглавленного $y \in G$, ставится их произведение xy. В данном случае $G = \{e, a, b\}$. Такая таблица называется *таблицей Кэли*.

Легко проверить, что приведенная нами таблица задает группу, изоморфную группе μ_3 комплексных корней третей степени из единицы (это записывается так: $G \cong \mu_3$).

Упражнение 4. Составьте таблицу Кэли для группы S_3.

Определение 9. Подмножество $H \subseteq G$ называется подгруппой, если оно непусто и замкнуто относительно умножения и взятия обратного элемента, то есть для любых $h_1, h_2 \in H$ их произведение $h_1 h_2$ и обратные к ним h_1^{-1}, h_2^{-1} лежат в H.

Пример 12. Любая группа преобразований множества M является, по определению, подгруппой симметрической группы $S(M)$.

Определение 10. Пусть H — подгруппа группы G. *Левым смежным классом группы G по подгруппе H* называется множество вида $gH = \{gh \mid h \in H\}$, где $g \in G$. Аналогично, *правым смежным классом группы G по подгруппе H* называется множество вида $Hg = \{hg \mid h \in H\}$, где $g \in G$.

Упражнение 5. Пусть H — подгруппа группы G. Определим на G отношение $\sim$, полагая $g_1 \sim g_2$, если $g_1^{-1}g_2 \in H$. Доказать, что это отношение эквивалентности, причем классами эквивалентности являются в точности левые смежные классы G по H. Какому отношению эквивалентности отвечают правые смежные классы?

Обозначим через G/H множество левых смежных классов G по H. Это фактормножество G по отношению эквивалентности, введенному в упражнении 5. Аналогично, через $H\backslash G$ обозначается множество правых смежных классов G по H.

Теорема 5 (Лагранжа). *Пусть G — конечная группа и H — ее подгруппа. Тогда*

$$|G| = |H| \cdot |G/H| = |H| \cdot |H\backslash G|.$$

Доказательство: Достаточно заметить, что в каждом смежном классе столько же элементов, сколько и в H, и воспользоваться упражнением 5. $\square$

Число элементов группы называется *порядком* группы. В качестве следствия из теоремы Лагранжа мы получаем, что порядок подгруппы всегда делит порядок конечной группы.

Определение 11. Пусть H — подгруппа группы G. Число $(G{:}H)$ левых смежных классов G по H называется *индексом* H в G.

Отметим, что индекс $(G{:}H)$ может быть конечен, даже если группа G бесконечна.

Упражнение 6. Найти индекс подгруппы $\mathbb{Q}^*_+$ положительных рациональных чисел в группе $\mathbb{Q}^*$.

Упражнение 7. Доказать, что число правых смежных классов по подгруппе конечного индекса тоже конечно и равно индексу.

Определение 12. Пусть G — группа, $g_1, \ldots, g_k$ — некоторые ее элементы. *Подгруппой, порожденной элементами $g_1, \ldots, g_k$* назовем минимальную (по включению) подгруппу H группы G, их содержащую. Такая подгруппа обозначается через $\langle g_1, \ldots, g_k \rangle$. (Слова «минимальная по включению» означают, что любая подгруппа $H' \subset H$, $H' \neq H$ уже не содержит какого-то из элементов $g_1, \ldots, g_k$.)

Подгруппа, порожденная одним элементом, называется *циклической*. *Порядком элемента* $g \in G$ называется порядок порожденной g циклической подгруппы.

Если $G = \langle g_1, \ldots, g_k \rangle$, то элементы $g_1, \ldots, g_k$ называются *образующими* группы G.

Очевидно, что для любых элементов $g_1, \ldots, g_k$ группы G порожденная ими подгруппа содержит всевозможные произведения вида $g_{i_1}^{n_1} g_{i_2}^{n_2} \ldots g_{i_r}^{n_r}$, где $n_1, \ldots, n_r \in \mathbb{Z}$ и $i_1, \ldots, i_r \in \{1, \ldots, k\}$. С другой стороны, множество всех элементов группы G, которые можно представить в виде произведений такого вида, является подгруппой. Поэтому

$$\langle g_1, \ldots, g_k \rangle = \{g_{i_1}^{n_1} \ldots g_{i_r}^{n_r} \mid i_1, \ldots, i_r \in \{1, \ldots, k\}; n_1, \ldots, n_r \in \mathbb{Z}\}$$

Пример 13. Элементы $s_1, \ldots, s_{n-1}$ являются образующими симметрической группы S_n (см. теорему 3).

Упражнение 8. Доказать, что порядок элемента $g \in G$ равен минимальному натуральному числу k, для которого $g^k = e$.

Упражнение 9. Доказать теорему Эйлера: для любых взаимно простых натуральных чисел m и n выполнено сравнение $m^{\varphi(n)} \equiv 1 \pmod{n}$, где $\varphi(n)$ — количество натуральных чисел, меньших n и взаимно простых с ним (функция Эйлера).

Действие группы на множестве

Определение 13. Пусть G — группа, а M — произвольное множество. Скажем, что задано *действие группы G на множестве M*, если для каждого $g \in G$ и для каждого $m \in M$ определен элемент $g(m) \in M$, причем $e(m) = m$ для любого m (e — единица группы G) и $g_1g_2(m) = g_1(g_2(m))$ для любых $g_1, g_2 \in G$ и $m \in M$.

Пусть G — произвольная группа, действующая на множестве M. Сопоставим каждому элементу $m \in M$ множество $G_m = \{g \in G \mid g(m) = m\}$ элементов группы G, оставляющих m на месте. Ясно, что для любого фиксированного элемента $m \in M$ произведение элементов G_m вновь лежит в G_m, и обратные к элементам G_m принадлежат G_m. Таким образом, G_m является подгруппой группы G. Она называется *стационарной подгруппой* или *стабилизатором* элемента m.

Если $g \in G_m$, то m называется *неподвижной точкой* элемента g. Множество неподвижных точек элемента g обозначается через $Fix\, g$.

С другой стороны, рассмотрим для каждого $m \in M$ множество $G(m) = \{g(m) \mid g \in G\}$ всех элементов множества M, в которые m переходит под действием элементов G. Это множество называется G*-орбитой* элемента m.

Замечание. G-орбиты называют также орбитами относительно группы G, или просто орбитами группы G. Говорят даже «орбиты элемента $g \in G$», имея в виду $\langle g \rangle$-орбиты. Как правило, путаница при этом не возникает.

Пример 14. Пусть M — плоскость, G — группа движений плоскости. Тогда стабилизатор G_m точки $m \in M$ состоит из всевозможных вращений вокруг точки m, а также отражений относительно всевозможных прямых, проходящих через m.

Поскольку G_m тоже является группой, действующей на плоскости, мы можем рассматривать ее орбиты. G_m-орбитой точки n является окружность с центром в точке m, проходящая через n.

Упражнение 10. Доказать, что G-орбита элемента $g(m)$ совпадает с G-орбитой элемента m для любых $m \in M$, $g \in G$.

Упражнение 11. Доказать, что $G_{g(m)} = \{ghg^{-1} \mid h \in G_m\}$ для любых $m \in M$, $g \in G$.

Теорема 6. *Пусть G — конечная группа, действующая на множестве M. Тогда $|G| = |G(m)|\cdot|G_m|$ для любого $m \in M$.*

Доказательство: Отображение $\varphi : G \to M$, заданное формулой $\varphi(g) = g(m)$, отображает G на $G(m)$. Слоями этого отображения являются, как легко проверить, левые смежные классы по подгруппе G_m. По теореме о факторизации отображений мы получаем биекцию между G/G_m и $G(m)$. Осталось применить теорему Лагранжа. □

Действие группы G на множестве M называется *транзитивным*, если всё множество M является G-орбитой. В этом случае для конечной группы G получаем

$$|G| = |M| \cdot |G_m|, \tag{1}$$

для произвольного элемента $m \in M$.

Из упражнения 10 следует, что каждая группа G, действующая на множестве M, задает на M отношение эквивалентности, классами эквивалентности по которому являются G-орбиты (а именно, $m \sim n$, если найдется $g \in G$, для которого $n = g(m)$). Рассмотрим фактормножество по этому отношению эквивалентности. Оно называется *пространством орбит* и обозначается через $G\backslash M$.

Теорема 7 (Формула Бернсайда). *Пусть G — конечная группа, действующая на конечном множестве M. Тогда*

$$|G\backslash M| = \frac{1}{|G|}\sum_{g\in G} |Fix\, g|\,.$$

Доказательство: Рассмотрим множество $\tilde{M} = \{(g,m) \in G \times M \mid g(m) = m\}$. Подсчитаем число элементов этого множества.

С одной стороны,

$$\left|\tilde{M}\right| = \sum_{g\in G} |Fix\, g|\,. \tag{2}$$

С другой стороны,

$$\left|\tilde{M}\right| = \sum_{m\in M} |G_m| = \sum_{X\in G\backslash M} \Big(\sum_{m\in X} |G_m|\Big), \tag{3}$$

поскольку G-орбиты образуют разбиение множества M. Из упражнения 11 следует, что для любых элементов $m, n \in M$, лежащих в одной G-орбите, $|G_m| = |G_n|$. Поэтому для любой G-орбиты $X = G(n)$

$$\sum_{m\in X} |G_m| = |X| \cdot |G_n|\,,$$

что, по теореме 6, равно $|G|$. Поэтому (3) можно переписать следующим образом:

$$\left|\tilde{M}\right| = \sum_{X\in G\backslash M} |G| = |G| \cdot |G\backslash M|\,. \tag{4}$$

Сравнивая (2) и (4), получаем утверждение теоремы. □

Пример 15. Рассмотрим следующую комбинаторную задачу: сколько существует различных ожерелий из шести бусин, каждая из которых либо красная, либо зеленая, либо синяя. Разумеется, ожерелья, получаемые друг из друга циклической перестановкой бусин или обращением их порядка, считаются одинаковыми. Для решения этой задачи нужно рассмотреть действие группы D_6 на множестве всех раскрасок вершин правильного 6-угольника тремя цветами.

Определение 14. Пусть G, G' — группы. Отображение $\varphi : G \to G'$ называется *гомоморфизмом*, если $\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2)$ для любых $g_1, g_2 \in G$. Биективный гомоморфизм называется *изоморфизмом*.

Упражнение 12. Доказать, что при любом гомоморфизме $\varphi : G \to H$ образом единицы группы G является единица группы H.

Пусть $\varphi : G \to H$ — гомоморфизм групп. По определению, $\varphi(gg') = \varphi(g)\varphi(g')$ для любых $g, g' \in G$. Согласно упражнению 12, единица группы G отображается в единицу группы H. Отсюда сразу следует, что $\varphi(g^{-1}) = \varphi(g)^{-1}$ для любого $g \in G$. Тем самым образ $\varphi(G)$ гомоморфизма φ является подгруппой в H. Из тех же соображений очевидно, что множество $\operatorname{Ker} \varphi = \{g \in G \mid \varphi(g) = e\}$, называемое *ядром* гомоморфизма φ, является подгруппой в G.

Упражнение 13. Доказать, что при гомоморфизм $\varphi : G \to H$ инъективен тогда и только тогда, когда $\operatorname{Ker} \varphi = \{e\}$.

Пример 16. Пусть задано действие группы G на множестве M. Тогда для любого $g \in G$ определено отображение $m \mapsto g(m)$ множества M в себя. Это отображение имеет обратное: $m \mapsto g^{-1}(m)$, поэтому оно является преобразованием множества M.

Таким образом, каждому элементу группы G отвечает преобразование множества M, то есть мы получаем отображение группы G в симметрическую группу $S(M)$. Очевидно, что это отображение является гомоморфизмом, причем каждый гомоморфизм $G \to S(M)$ связан с некоторым действием группы G на множестве M.

Рассмотрим действие G на себе, определяемое формулой: $g(h) = gh$. Этому действию отвечает некоторый гомоморфизм $\varphi : G \to S(G)$. Обозначим через $\overline{G}$ образ гомоморфизма φ. Очевидно, что $\overline{G}$ является группой преобразований множества G.

Пусть $g_1, g_2 \in G$ таковы, что $g_1 g = g_2 g$ для любого $g \in G$. Тогда $g_1 = g_1 e = g_2 e = g_2$. Отсюда следует, что φ биективно отображает G на $\overline{G}$. Мы получили следующий удивительный результат:

Теорема 8 (Кэли). *Каждая группа изоморфна некоторой группе преобразований.*

Таким образом, группы преобразований, которые мы использовали в качестве мотивировки определения абстрактных групп, в действительности являются наиболее общим примером последних.

Определение 15. Пусть G — произвольная группа. Преобразование $\varphi \in S(G)$ называется *автоморфизмом*, если оно является изоморфизмом группы G на себя. Множество автоморфизмов группы G обозначается через $\operatorname{Aut} G$.

Упражнение 14. Доказать, что $\operatorname{Aut} G$ является подгруппой группы $S(G)$, то есть группой преобразований множества G.

Упражнение 15. Пусть G — группа и $g \in G$. Доказать, что отображение $\imath_g : G \to G$, заданное формулой $\imath_g(h) = ghg^{-1}$, является автоморфизмом.

Обозначим через f отображение G в $\operatorname{Aut} G$, переводящее g в $\imath_g$. Легко видеть, что f является гомоморфизмом. Ядро f называется *центром* группы G; его составляют элементы группы G, коммутирующие со всеми элементами G, то есть такие $g \in G$, что $gh = hg$ для любого $h \in G$. Автоморфизмы, составляющие образ f, называются *внутренними*. Общепринятые обозначения: $Z(G) = \operatorname{Ker} f$, $\operatorname{Int} G = f(G)$.

Отметим, что гомоморфизм f определяет действие группы G на себе; действие элемента $g \in G$ называется *сопряжением с помощью* g. Орбиты этого действия называются *классами сопряженных элементов*.

Упражнение 16. Пусть $\sigma \in S_n$ — цикл длины k, а $\tau \in S_n$ — произвольная перестановка. Доказать, что $\tau\sigma\tau^{-1}$ — цикл длины k. Какие элементы входят в этот цикл, если $\sigma = (1, 2, \dots, k)$?

Задача 1. Найти $Z(G)$, $\operatorname{Int} G$, $\operatorname{Aut} G$ и классы сопряженных элементов для $G = \mu_n$, D_n, S_n, A_n, где μ_n — группа комплексных корней из единицы степени n, D_n — группа диэдра, S_n — симметрическая, и A_n — знакопеременная группы. Постарайтесь решить эту задачу хотя бы для малых n.

Нормальные подгруппы и факторгруппы

Отметим, что любая подгруппа $K \subseteq H$ является образом некоторого гомоморфизма (в качестве такового можно взять ограничение на K тождественного отображения H в H). Выясним теперь, какие подгруппы $N \subseteq G$ могут являться ядрами гомоморфизмов.

Ядро $\operatorname{Ker}\varphi$ гомоморфизма $\varphi : G \to H$ является слоем отображения φ над единицей группы H. Выберем произвольный элемент $g \in G$ и положим $h = \varphi(g)$. Элемент $g' \in G$ принадлежит слою отображения φ над h тогда и только тогда, когда $\varphi\left(g^{-1}g'\right) = e$, то есть когда g' принадлежит тому же левому смежному классу группы G по подгруппе $N = \operatorname{Ker}\varphi$, что и g. Аналогично проверяется, что $g' \in \varphi^{-1}(h)$ тогда и только тогда, когда g' принадлежит тому же правому смежному классу G по N, что и g. Отсюда следует, что левые смежные классы группы G по подгруппе N совпадают с правыми, являясь в точности слоями отображения φ.

Определение 16. Подгруппа $N \subseteq G$ называется *нормальной* (или *инвариантной*, или *нормальным делителем*), если левые смежные классы группы G по подгруппе N совпадают с правыми, то есть если для любого $g \in G$ выполнено равенство $gH = Hg$ или, что равносильно, $gHg^{-1} = H$. То, что N является нормальной подгруппой группы G, часто обозначается так: $N \lhd G$.

Отметим следующее важное, хотя и очевидное, следствие определения;

Утверждение 1. *Подгруппа $N \subseteq G$ является нормальной тогда и только тогда, когда она является объединением классов сопряженности группы G.*

Пусть N — нормальная подгруппа группы G. Тогда множество G/N (совпадающее с $N\backslash G$) можно наделить естественной структурой группы. Действительно, $(gN)(g'N) = g(Ng')N = g(g'N)N = gg'N$, то есть произведение двух смежных классов снова является смежным классом. Умножение смежных классов, очевидно, является ассоциативным, $N = eN$ является нейтральным элементом, а $g^{-1}N$ является обратным к gN. Отсюда сразу следует

Теорема 9. *Если N — нормальная подгруппа группы G, то операция $(gN)\cdot(g'N) = gg'N$ наделяет фактормножество G/N структурой группы, называемой факторгруппой G по N. При этом каноническая проекция $\pi : G \to G/N$ является гомоморфизмом групп, и $N = \operatorname{Ker}\pi$.*

Пусть $\varphi : G \to H$ — произвольный гомоморфизм групп. Положим $N = \operatorname{Ker}\varphi$. Мы уже проверили, что левые смежные классы группы G по N совпадает с правыми, то есть $N \lhd G$, при этом смежные классы G по N являются в точности слоями отображения φ. По теореме о факторизации отображений существует единственное отображение $\psi : G/N \to H$, делающее диаграмму

$$\begin{tikzcd} G \arrow[rr, "\varphi"] \arrow[dr, "\pi"'] & & H \\ & G/N \arrow[ur, "\psi"'] & \end{tikzcd}$$

коммутативной. Легко проверить, что ψ является гомоморфизмом групп. Таким образом, из теоремы о факторизации отображений следует

Теорема 10 (О гомоморфизмах групп). *Пусть $\varphi : G \to H$ — гомоморфизм групп с ядром N. Тогда существует единственный гомоморфизм $\psi : G/N \to H$ такой, что $\varphi = \psi\circ\pi$, где $\pi : G \to G/N$ — каноническая проекция. При этом ψ является изоморфизмом G/N на $\varphi(G)$.*

В частности, если гомоморфизм φ сюръективен, то факторгруппа G/N изоморфна H.

Пример 17. Группа $\mathbb{Z}$ — абелева, поэтому любая подгруппа в ней нормальна. Факторгруппа $\mathbb{Z}/n\mathbb{Z}$ называется *группой классов вычетов по модулю n*. Рассмотрим гомоморфизм $\varphi : \mathbb{Z} \to \mathbb{C}^*$, задаваемый формулой $\varphi(k) = e^{2\pi ik/n}$ ($n \in \mathbb{N}$ — фиксировано). Тогда $\operatorname{Ker}\varphi = n\mathbb{Z}$, $\varphi(\mathbb{Z}) = \mu_n$ и, согласно теореме 10, мы имеем изоморфизм групп $\mathbb{Z}/n\mathbb{Z} \cong \mu_n$.

Пример 18. Пусть $n > 1$. Функция «знак перестановки» представляет собой гомоморфизм симметрической группы S_n в группу $\mu_2 = \{\pm 1\}$. Знакопеременная группа — ядро этого гомоморфизма, а образом, очевидно, является вся группа μ_2. Мы получаем $S_n/A_n \cong \mu_2$.

Задание групп образующими и соотношениями

Мы уже встречались с понятием системы образующих группы. Например, симметрическая группа S_n порождается образующими $s_1 = (1,2), \ldots, s_{n-1} = (n-1,n)$. Между образующими группы могут быть соотношения. Так, в симметрической группе выполнены соотношения $s_i^2 = e$ ($i = 1,\ldots,n-1$), $s_is_{i+1}s_i = s_{i+1}s_is_{i+1}$ ($i = 1,\ldots,n-2$), $s_is_j = s_js_i$ ($i,j = 1,\ldots,n-1$; $|i-j| > 1$).

Из одних соотношений могут следовать другие; например, из соотношения $s_1^2 = e$ следует соотношение $s_1^{-4} = e$, а из соотношений $s_1^2 = e$, $s_2^2 = e$ и $s_1s_2s_1 = s_2s_1s_2$ следует соотношение $(s_1s_2)^3 = e$. Исходя из этого, можно попробовать дать логическое определение группы, порожденной образующими и соотношениями, как группы, имеющей предписанные образующие, между которыми выполняются предписанные соотношения и все их следствия (и только они). При этом встает естественный вопрос: как доказать существование такой группы? Следующая алгебраическая конструкция позволяет как избежать возни со строгим логическим определением следствий заданных соотношений, так и снимает вопрос существования группы, заданной образующими и соотношениями.

Построим сначала группу с заданным множеством образующих, но «без соотношений».

Определение 17. Пусть S — произвольное множество. Обозначим через A множество $S \sqcup \{s^{-1} \mid s \in S\}$. Рассмотрим множество всех *слов в алфавите* A, то есть множество всех конечных последовательностей $a_1 \dots a_k$, где k — неотрицательное целое число (подчеркнем, что среди прочих мы рассматриваем и *пустое слово*). Назовем *элементарным преобразованием* слова w любое слово, получающееся из w вставкой в него в произвольном месте двубуквенного слова вида ss^{-1} или $s^{-1}s$, где $s \in S$, или вычеркиванием двух букв ss^{-1} или $s^{-1}s$, идущих подряд. Два слова называются эквивалентными, если одно можно получить из другого цепочкой элементарных преобразований. *Свободной группой* $F(S)$ с множеством образующих S называется множество классов эквивалентности.

Произведением классов эквивалентности, содержащих слова $a_1 \dots a_k$ и $b_1 \dots b_l$, называется класс эквивалентности слова $a_1 \dots a_k b_1 \dots b_l$. Легко проверить, что это определение является корректным (то есть при замене исходных слов эквивалентными получается в качестве произведения тот же класс эквивалентности). Очевидно, что введенное таким образом произведение является ассоциативным, и класс эквивалентности пустого слова является единичным элементом. Кроме того, класс эквивалентности слова $a_k^{-1} \dots a_1^{-1}$ является обратным к классу эквивалентности слова $a_1 \dots a_k$ (мы полагаем $a^{-1} = s$ для $a = s^{-1}$, где $s \in S$).

Положим

$$s^k = \begin{cases} \underbrace{s \dots s}_{k \text{ раз}} & \text{при } k > 0, \\ \varnothing & \text{при } k = 0, \\ \underbrace{s^{-1} \dots s^{-1}}_{-k \text{ раз}} & \text{при } k < 0. \end{cases}$$

Очевидно, что любой элемент свободной группы $F(S)$ можно записать в виде $s_1^{k_1} s_2^{k_2} \dots s_m^{k_m}$, где $m \in \mathbb{N} \cup \{0\}$, $s_i \in S$, $s_i \neq s_{i+1}$, $k_i \in \mathbb{Z} \setminus \{0\}$ $(i = 1, \dots, m)$. Такая запись называется несократимой.

Пусть теперь нам задано некоторое подмножество $R \subset F(S)$. Мы хотели бы, говоря неформально, построить группу G, заданную образующими s из множества S и соотношениями $s_1^{k_1} \dots s_m^{k_m} = e$ для всех слов $s_1^{k_1} \dots s_m^{k_m} \in R$. Идея состоит в том, чтобы определить G как некоторую факторгруппу свободной группы $F(S)$.

Подгруппа, порожденная элементами множества R, не обязательно является нормальной, поэтому, вообще говоря, факторизовать по ней нельзя. Обозначим через $N(R)$ пересечение всех нормальных подгрупп группы $F(S)$, содержащих множество R. Подгруппа $N(R)$ уже является нормальной. Действительно, $N(R) = \bigcap N_\alpha$, где все подгруппы N_α нормальны в $F(S)$, то есть если $x \in N_\alpha$, то и $gxg^{-1} \in N_\alpha$ для любого $g \in F(S)$. Поэтому если $x \in \bigcap N_\alpha$, то и $gxg^{-1} \in \bigcap N_\alpha$ для любого $g \in F(S)$. Это означает, что $\bigcap N_\alpha = N(R) \lhd F(S)$.

Определение 18. Группой, заданной образующими $s \in S$ и соотношениями $r = e$, где $r \in R \subset F(S)$, *называется факторгруппа* $G = F(S)/N(R)$. *Часто используется обозначение* $G = \langle s_1, \dots, s_n \mid r_1 = e, \dots, r_m = e \rangle$, *где* $S = \{s_1, \dots, s_n\}$, *и* $R = \{r_1, \dots, r_m\}$.

Мы будем обозначать образ образующей $s \in S$ при канонической проекции $F(S) \to G$ той же буквой s. Группа G обладает следующим замечательным свойством универсальности:

Теорема 11. *Пусть H — любая группа, имеющая образующие $f(s)$, где $s \in S$, и такая, что для любого элемента $s_1^{k_1} \dots s_m^{k_m} \in R$ в группе H выполнено равенство $f(s_1)^{k_1} \dots f(s_m)^{k_m} = e$. Тогда существует сюръективный гомоморфизм $\varphi : G \to H$ такой, что $\varphi(s) = f(s)$.*

Доказательство: Отображение $f : S \to H$ можно, очевидно, продолжить до сюръективного гомоморфизма $f : F(S) \to H$. Условия теоремы означают, что R лежит в ядре этого гомоморфизма. Положим $\tilde{N} = \operatorname{Ker} f$. Поскольку ядро любого гомоморфизма является нормальной подгруппой, то $N(R) \subseteq \tilde{N}$. Поэтому формула $\varphi(xN(R)) = f(x)$ корректно определяет отображение $\varphi : G \to H$. То, что это отображение является сюръективным гомоморфизмом — очевидно. □

В действительности, конструкция группы, заданной образующими и соотношениями, через свободную группу нужна лишь для того, чтобы доказать существование группы G, обладающей указанным свойством универсальности. Во всех приложениях используется именно это свойство группы, заданной образующими и соотношениями.

Пример 19. Пусть $S = \{s\}$ — одноэлементное множество. Тогда $F(S)$ — бесконечная циклическая группа, то есть $F(S) \cong \mathbb{Z}$. Пусть $R = \{s^n\}$ для некоторого натурального n. Тогда $\langle s \mid s^n = e\} = F(S)/N(R) \cong \mathbb{Z}/n\mathbb{Z}$.

Пример 20. Пусть $S = \{s, t\}$, $R = \{s^2, t^n, stst\}$. Докажем, что $\langle s, t \mid s^2 = e, t^n = e, stst = e\rangle \cong D_n$, где D_n — группа диэдра (группа симметрий правильного n-угольника).

Докажем сперва, что в группе $G = \langle s, t \mid s^2 = e, t^n = e, stst = e\rangle$ не более $2n$ элементов. Действительно, поскольку $s^2 = e = t^n$ в G, то любой элемент группы G можно записать в виде $t^{k_0}st^{k_1}s\ldots t^{k_{m-1}}st^{k_m}$, где $m \geqslant 0$, $0 \leqslant k_i < n$ $(i = 0, 1, \ldots, m)$ и $k_i > 0$ при $0 < i < n$. Далее, поскольку $stst = e$, то $st = t^{-1}s^{-1} = t^{n-1}s$. Отсюда $st^k = t^{n-k}s$. Поэтому каждый элемент группы G можно записать в виде $t^k s^l$, где $k \in \{0, 1, \ldots, n-1\}$ и $l \in \{0, 1\}$. Следовательно $|G| \leqslant 2n$.

Заметим, что мы еще не доказали, что $|G| = 2n$ (для этого нам пришлось бы доказать, что из наших соотношений *не следует* никакое соотношение вида $t^{k_1}s^{l_1} = t^{k_2}s^{l_2}$, где $k_1, k_2 \in \{0, 1, \ldots, n-1\}$, $l_1, l_2 \in \{0, 1\}$ и $k_1 \neq k_2$ или $l_1 \neq l_2$). Вот здесь нам и нужно свойство универсальности.

Обозначим через τ поворот правильного n-угольника на угол $2\pi/n$, а через σ — произвольную осевую симметрию, переводящую n-угольник в себя. Легко проверить, что эти преобразования порождают группу D_n, причем выполнены соотношения $\sigma^2 = \tau^n = \sigma\tau\sigma\tau$. Поэтому существует сюръективный гомоморфизм $\varphi : G \to D_n$, переводящий s в σ, а t в τ. Поскольку $|G| \leqslant 2n = |D_n|$, то φ — изоморфизм, то есть $G \cong D_n$.

Отметим, что $D_3 \cong S_3$. Действительно, занумеруем вершины правильного треугольника числами $1, 2, 3$. Каждый элемент группы D_3 переставляет вершины, то есть задает перестановку из S_3. Мы получаем гомоморфизм $D_3 \to S_3$. Легко видеть, что этот гомоморфизм инъективен (движение плоскости, оставляющее все вершины треугольника неподвижными, является тождественным). Кроме того, $|D_3| = 6 = |S_3|$. Поэтому эти группы изоморфны. Следовательно, $S_3 \cong \langle s, t \mid s^2 = e, t^3 = e, stst = e\rangle$.

Подведем некоторые итоги. Мы видели, что группы возникают естественным образом как группы преобразований (группы симметрий). Кроме того, группы можно задавать таблицами Кэли, можно рассматривать подгруппы и факторгруппы уже известных групп и, наконец, можно задавать группы образующими и соотношениями. Я хочу привести еще один рецепт построения новых групп.

Пусть $H_1, \ldots, H_n$ — некоторые группы. Их *прямым произведением* называется группа, элементами которой являются всевозможные строчки вида $(h_1, \ldots, h_n)$, где $h_i \in H_i$, а умножение определяется «покоординатно»: $(g_1, \ldots, g_n)(h_1, \ldots, h_n) = (g_1h_1, \ldots, g_nh_n)$. Эта группа обозначается через $H_1 \times \cdots \times H_n$. В случае, если все группы H_i являются абелевыми и для них используется аддитивная форма записи, их прямое произведение называют *прямой суммой* и обозначают $H_1 \oplus \cdots \oplus H_n$.

Упражнение 17. Доказать, что $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/6\mathbb{Z}$, но $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \ncong \mathbb{Z}/8\mathbb{Z}$.