Глава 4.

Начала теории групп

4.1. Определение и примеры

В первой главе читатель познакомился с понятием абелевой группы. Абелевыми группами являются, в частности, аддитивная группа любого кольца, мультипликативная группа любого поля и аддитивная группа любого векторного пространства. Важнейшие примеры неабелевых групп появляются как группы преобразований.

Назовем преобразованием множества X всякое его отображение в самого себя.

Определение 1. Группой преобразований множества X называется всякая совокупность G его биективных преобразований, удовлетворяющая следующим условиям:

1) если $\varphi, \psi \in G$, то $\varphi\psi \in G$;

2) если $\varphi \in G$, то $\varphi^{-1} \in G$;

3) $\mathrm{id} \in G$.

(Здесь $\varphi\psi$ обозначает произведение (композицию) преобразований φ и ψ, id — тождественное преобразование.)

Пример 1. Совокупность $S(X)$ всех биективных преобразований множества X является группой преобразований. Если множество X бесконечно, эта группа слишком велика, чтобы быть интересной. Если X конечно, то можно считать, что $X = \{1, 2, \ldots, n\}$; в этом случае группа $S(X)$ называется группой подстановок, или симметрической группой, степени n и обозначается через S_n. Подстановка $\sigma \in S_n$ может быть записана в виде таблицы

$$\sigma = \begin{pmatrix} i_1 & i_2 & \dots & i_n \\ j_1 & j_2 & \dots & j_n \end{pmatrix},$$

в первой строке которой выписаны в каком-то порядке числа $1, 2, \dots, n$, а во второй строке — их образы, т. е. $j_k = \sigma(i_k)$. Фиксируя расположение чисел в первой строке (например, располагая их в порядке возрастания), мы видим, что число подстановок равно числу перестановок (см. §2.4), т. е. $n!$. При этом каждая подстановка может быть записана $n!$ способами. Приведем пример на умножение подстановок:

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = \\ = \begin{pmatrix} 4 & 3 & 2 & 1 \\ 2 & 1 & 4 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}.$$

(Здесь мы в начале для удобства переписали первую подстановку таким образом, чтобы первая строка в ее записи совпала со второй строкой в записи второй подстановки.)

Пример 2. Движения евклидовой плоскости E^2 (соотв. евклидова пространства E^3) образуют группу преобразований, обозначаемую через $\operatorname{Isom} E^2$ (соотв. $\operatorname{Isom} E^3$). Это свойство является аксиомой в той версии аксиоматики евклидовой геометрии, в которой понятие движения является одним из неопределяемых понятий. В другой версии, берущей за основу понятие расстояния между точками, движение определяется как преобразование, сохраняющее расстояния, а сформулированное выше свойство является очевидной теоремой.

Замечание 1. В предыдущих главах мы обозначали через E^2 (соотв. E^3) множество векторов евклидовой плоскости (соотв. пространства). Здесь же символ E^2 (соотв. E^3) использован для обозначения самой евклидовой плоскости (соотв. пространства). Впрочем, если в плоскости (соотв. в пространстве) фиксирована некоторая точка o (которую мы будем в дальнейшем называть началом координат), то можно договориться отождествлять точки с их радиусами-векторами относительно точки o. Это соглашение часто будет подразумеваться в дальнейшем.

Замечание 2. В той версии аксиоматики евклидовой геометрии, которая берет за основу понятие движения, утверждение о том, что всякое биективное преобразование, сохраняющее расстояния, является движением, является (несложной) теоремой.

Пример 3. Ввиду свойств линейных отображений, доказанных в §2.3, биективные линейные преобразования векторного пространства V образуют группу преобразований. Она называется полной линейной группой пространства V и обозначается через $GL(V)$.

Пример 4. Назовем параллельным переносом векторного пространства V на вектор $a \in V$ преобразование

$$t_a \colon x \mapsto x + a.$$

Легко видеть, что

$$t_a t_b = t_{a+b}, \quad t_a^{-1} = t_{-a}, \quad \mathrm{id} = t_0. \tag{73}$$

Эти формулы показывают, что совокупность $\mathrm{Tran}(V)$ всех параллельных переносов пространства V является группой преобразований.

Задача 1. Доказать, что совокупность всех возрастающих непрерывных функций на отрезке [0,1], удовлетворяющих условиям $f(0) = 0$, $f(1) = 1$, является группой преобразований отрезка $[0, 1]$.

Анализируя свойства операции умножения в группах преобразований, мы приходим к следующему понятию группы, которое отличается от понятия абелевой группы отсутствием требования коммутативности.

Определение 2. Группой называется множество G с операцией умножения, обладающей следующими свойствами:

1) $(ab)c = a(bc)$ $\forall a, b, c \in G$ (ассоциативность);

2) существует такой элемент $e \in G$ (единица), что $ae = ea = a$ $\forall a \in G$;

3) для всякого элемента $a \in G$ существует такой элемент $a^{-1} \in G$ (обратный элемент), что $aa^{-1} = a^{-1}a = e$.

Группа называется абелевой, или коммутативной, если

$$ab = ba \quad \forall a, b \in G.$$

Данное определение группы использует мультипликативную терминологию. Аддитивная терминология обычно используется только для абелевых групп (хотя в принципе операция в группе может называться и обозначаться как угодно).

Аналогично тому, как это было сделано для абелевых групп, доказывается единственность единицы и обратного элемента в любой группе. Что касается деления, то в неабелевой группе следует различать левое и правое деления. А именно, для любых $a, b \in G$ уравнение $ax = b$ имеет единственное решение, равное $a^{-1}b$, и уравнение $xa = b$ имеет единственное решение, равное ba^{-1}.

В любой группе

$$(ab)^{-1} = b^{-1}a^{-1}.$$

В самом деле,

$$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aa^{-1} = e.$$

Всякая группа преобразований является группой относительно операции умножения преобразований. Действительно, ассоциативность этой операции известна, единицей служит тождественное преобразование, а обратным элементом — обратное преобразование.

Пример 5. Невырожденные квадратные матрицы порядка n над полем K образуют группу по умножению, обозначаемую $GL_n(K)$. Поскольку имеется взаимно однозначное соответствие между квадратными матрицами порядка n и линейными преобразованиями пространства K^n, причем невырожденным матрицам отвечают обратимые линейные преобразования, а умножению матриц соответствует умножение линейных преобразований, группа $GL_n(K)$ изоморфна группе $GL(K^n)$ (и, тем самым, группе $GL(V)$, где V — любое n-мерное векторное пространство над полем K).

Пример 6. Как показывают формулы (73), группа $\mathrm{Tran}(V)$ изоморфна аддитивной группе пространства V.

Пример 7. Конечная группа может быть задана своей таблицей умножения. Так, множество $G = \{e, a, b, c\}$ с таблицей умножения

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

является абелевой группой. В самом деле, элемент e служит ее единицей и каждый элемент обратен сам себе. Далее, легко видеть, что любая перестановка элементов a, b, c является автоморфизмом множества G с указанной операцией. Поэтому, если исключить тривиальные случаи с участием единицы и принять во внимание коммутативность, доказательство ассоциативности сводится к проверке следующих соотношений:

$$a^2b = a(ab) = b, \quad (ab)c = a(bc) = e.$$

Задача 2. Доказать, что множество $G = \{А, Б, В, Г, Д, Е\}$ с операцией, заданной таблицей

	$А$	$Б$	$В$	$Г$	$Д$	$Е$
$А$	$Е$	$Д$	$Г$	$В$	$Б$	$А$
$Б$	$В$	$Г$	$Д$	$Е$	$А$	$Б$
$В$	$Б$	$А$	$Е$	$Д$	$Г$	$В$
$Г$	$Д$	$Е$	$А$	$Б$	$В$	$Г$
$Д$	$Г$	$В$	$Б$	$А$	$Е$	$Д$
$Е$	$А$	$Б$	$В$	$Г$	$Д$	$Е$

является группой, изоморфной S_3.

Определение 3. Подгруппой группы G называется всякое подмножество $H \subset G$, удовлетворяющее следующим условиям:

1) если $a, b \in H$, то $ab \in H$;

2) если $a \in H$, то $a^{-1} \in H$;

3) $e \in H$.

Замечание 3. Так как $aa^{-1} = e$, то условие 3) можно заменить требованием непустоты подмножества H.

Очевидно, что всякая подгруппа сама является группой относительно той же операции.

Сравнивая определения 1 и 3, мы видим, что группа преобразований множества X — это не что иное, как подгруппа группы $S(X)$.

Пример 8. Пусть f — какой-либо многочлен от n переменных. Тогда

$$\operatorname{Sym} f = \{\, \sigma \in S_n : f(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)}) = f(x_1, x_2, \ldots, x_n) \,\}$$

есть подгруппа группы S_n. В самом деле, пусть $\sigma, \tau \in \operatorname{Sym} f$. Положим $x_{\sigma(i)} = y_i$; тогда

$$\begin{aligned} &f(x_{\sigma\tau(1)}, x_{\sigma\tau(2)}, \ldots, x_{\sigma\tau(n)}) = f(y_{\tau(1)}, y_{\tau(2)}, \ldots, y_{\tau(n)}) = \\ &= f(y_1, y_2, \ldots, y_n) = f(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)}) = f(x_1, x_2, \ldots, x_n). \end{aligned}$$

Остальные две аксиомы подгруппы выполнены очевидным образом. Определение симметрического многочлена, данное в §3.8, означает, что $\operatorname{Sym} f = S_n$. В качестве примера многочлена с менее богатой, но не тривиальной симметрией рассмотрим многочлен $f = x_1x_2 + x_3x_4$ (от 4 переменных). Легко видеть, что группа $\operatorname{Sym} f$ состоит из 8 подстановок, сохраняющих разбиение множества $\{1, 2, 3, 4\}$ на два подмножества $\{1, 2\}$ и $\{3, 4\}$. (Допускается перестановка этих подмножеств и перестановка элементов в каждом из них; см. по этому поводу также пример 5.11).

Пример 9. Аналогично, линейные преобразования пространства K^n, сохраняющие какой-либо заданный многочлен от n переменных, образуют подгруппу группы $GL_n(K)$. Линейные преобразования пространства $\mathbb{R}^n$, сохраняющие многочлен $x_1^2 + x_2^2 + \ldots + x_n^2$, называются ортогональными преобразованиями; они образуют подгруппу группы $GL_n(\mathbb{R})$, которая называется ортогональной группой и обозначается через O_n. Так как в декартовых координатах пространства E^2 (соотв.

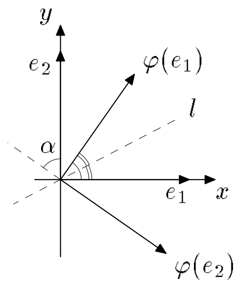

Рис. 20.

E^3) многочлен x^2+y^2 (соотв. $x^2+y^2+z^2$) выражает квадрат длины вектора, то ортогональные преобразования пространства E^2 (соотв. E^3) — это не что иное, как линейные преобразования, сохраняющие длину вектора. Дадим геометрическое описание ортогональных преобразований пространства E^2. Условие

$$\varphi = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in O_2$$

означает, что

$$(ax+by)^2 + (cx+dy)^2 = x^2+y^2,$$

т. е.

$$a^2+c^2 = b^2+d^2 = 1, \quad ab+cd = 0.$$

Из уравнения $a^2+c^2=1$ следует, что существует такой угол α, что

$$a = \cos\alpha, \quad c = \sin\alpha.$$

Оставшиеся два уравнения показывают, что

$$b = \pm\sin\alpha, \quad d = \mp\cos\alpha.$$

Таким образом,

$$\varphi = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} \quad \text{или} \quad \begin{pmatrix} \cos\alpha & \sin\alpha \\ \sin\alpha & -\cos\alpha \end{pmatrix}.$$

В первом случае, как мы уже знаем (см. пример 2.3.5) φ есть поворот на угол α. Во втором случае φ — зеркальное отражение относительно прямой l, образующей угол $\frac{\alpha}{2}$ с осью x (см. рис. 20). Эти два случая отличаются друг от друга тем, что в первом случае φ сохраняет ориентацию плоскости, а во втором — меняет. В курсе линейной алгебры доказывается, что всякое ортогональное преобразование пространства E^3, сохраняющее ориентацию, есть поворот вокруг некоторой прямой.

Пример 10. Движения евклидовой плоскости, оставляющие на месте начало координат o, образуют подгруппу группы $\operatorname{Isom} E^2$. Обозначим ее через H. Так как сложение векторов и их умножение на числа определяются в инвариантных геометрических терминах, то всякое движение, оставляющее на месте точку o, является линейным преобразованием. Более того, так как оно сохраняет длины векторов, то оно является ортогональным преобразованием. Обратно, поскольку расстояние между точками a и b есть длина вектора $a - b$, то всякое ортогональное преобразование сохраняет расстояние между точками и, значит, является движением. Таким образом, $H = O_2$. Аналогично, группа движений евклидова пространства, оставляющих на месте начало координат, совпадает с O_3.

Пример 11. Пусть F — какая-либо фигура на евклидовой плоскости. Тогда

$$\operatorname{Sym} F = \{\, \varphi \in \operatorname{Isom} E^2 : \varphi(F) = F \,\}$$

есть подгруппа группы $\operatorname{Isom} E^2$; она называется группой симметрии фигуры F. Так, группа симметрии окружности с центром в начале координат o есть группа O_2. Группа симметрии правильного n-угольника с центром в точке o есть подгруппа группы O_2, состоящая из поворотов вокруг точки o на углы, кратные $\frac{2\pi}{n}$, и отражений относительно прямых, проходящих через o и одну из вершин или середину одной из сторон. Таким образом, эта группа содержит $2n$ элементов (n поворотов и n отражений); она называется группой диэдра и обозначается через D_n.

Пример 12. В силу формулы умножения определителей матрицы с определителем 1 образуют подгруппу в группе $GL_n(K)$. Эта подгруппа называется унимодулярной группой и обозначается через $SL_n(K)$.

Пример 13. Целочисленные матрицы с определителем 1 образуют подгруппу в группе $SL_n(\mathbb{R})$, обозначаемую через $SL_n(\mathbb{Z})$ (см. задачу 2.5.3).

Пример 14. Множество невырожденных диагональных матриц порядка n является абелевой подгруппой группы $GL_n(K)$.

Задача 3. Доказать, что множество строго треугольных квадратных матриц порядка n является подгруппой группы $GL_n(K)$.

4.2. Группы в геометрии и физике

Цель этого параграфа — дать общее представление о роли групп в геометрии и физике.

В XIX веке математики осознали, что евклидова геометрия не является единственной мыслимой геометрией. Даже если принять, что «пространство, в котором мы живем», подчиняется законам евклидовой геометрии (что на самом деле верно лишь в первом приближении), имеет смысл изучать геометрию и других пространств, которые возникают в результате математических построений. В связи с этим возникает вопрос, что же в таком случае следует понимать под геометрией. Обобщая различные понятия, рассматриваемые в евклидовой геометрии, можно сформулировать различные ответы на этот вопрос.

В частности, обобщая понятие группы движений евклидовой геометрии, немецкий математик Клейн в своей лекции 1872 г., получившей известность под названием «Эрлангенская программа», дал определение геометрии как изучения свойств фигур, инвариантных относительно заданной группы преобразований.

Более подробно, пусть задано некоторое множество X и некоторая группа G его преобразований. Фигуру $F_1 \subset X$ будем считать эквивалентной (или равной, как говорят в элементарной геометрии) фигуре $F_2 \subset X$ относительно группы G и писать $F_1 \underset{G}{\sim} F_2$, если существует такой преобразование $\varphi \in G$, что $F_2 = \varphi(F_1)$. Проверим, что это действительно отношение эквивалентности:

1)$F \underset{G}{\sim} F$, так как $F = \mathrm{id}(F)$ и $\mathrm{id} \in G$;

2) если $F_1 \underset{G}{\sim} F_2$, т.е. $F_2 = \varphi(F_1)$, где $\varphi \in G$, то $F_2 \underset{G}{\sim} F_1$, так как $F_1 = \varphi^{-1}(F_2)$ и $\varphi^{-1} \in G$;

3) если $F_1 \underset{G}{\sim} F_2$ и $F_2 \underset{G}{\sim} F_3$, т.е. $F_2 = \varphi(F_1)$ и $F_3 = \psi(F_2)$,

где $\varphi, \psi \in G$, то $F_1 \underset{G}{\sim} F_3$, так как $F_3 = \psi\varphi(F_1)$ и $\psi\varphi \in G$.

Мы видим, таким образом, что три аксиомы отношения эквивалентности в точности соответствуют трем аксиомам группы преобразований.

Одной из задач геометрии является нахождение необходимых и достаточных условий эквивалентности фигур (вспомните признаки равенства треугольников в евклидовой геометрии). Этой цели служат величины, инвариантные относительно преобразований из группы G (такие, как расстояние между точками или мера угла в евклидовой геометрии). Соотношения между этими инвариантами суть геометрические теоремы (например, теорема Пифагора или теорема о том, что медианы треугольника пересекаются в одной точке).

Конечно, далеко не любая группа преобразований приводит к интересной и важной для приложений геометрии. Все такие геометрии связаны с достаточно богатыми группами преобразований, которых не так много. Минимальным требованием здесь является транзитивность.

Определение. Группа G преобразований множества X называется транзитивной, если для любых $x, y \in X$ существует такое преобразование $\varphi \in G$, что $y = \varphi(x)$.

(Это означает, что в соответствующей геометрии все точки эквивалентны в смысле данного выше определения эквивалентности фигур.)

Пример. Группа $\mathrm{Tran}(V)$ параллельных переносов векторного пространства V (см. пример 1.4) транзитивна. В самом деле, для любых $x, y \in V$ имеем

$$y = t_{y-x}x.$$

Однако группа $\mathrm{Tran}(V)$ все еще слишком мала, чтобы определять интересную геометрию. В качестве примера интересной геометрии, отличной от евклидовой, приведем аффинную геометрию.

Пусть V — какое-либо векторное пространство, $\varphi \in GL(V)$ и $a \in V$. Тогда

$$\varphi t_a \varphi^{-1} = t_{\varphi(a)}. \tag{74}$$

В самом деле, для любого $x \in V$ имеем:

$$(\varphi t_a \varphi^{-1})(x) = \varphi(\varphi^{-1}(x) + a) = x + \varphi(a) = t_{\varphi(a)}x.$$

Предложение 1. Для любой подгруппы $G \subset GL(V)$ множество

$$\mathrm{Tran}(V) \cdot G = \{t_a\varphi : a \in V,\ \varphi \in G\}$$

является транзитивной группой преобразований пространства V.

Доказательство. При $a, b \in V,\ \ \varphi, \psi \in GL(V)$ имеем ввиду формул (73) и (74):

$$(t_a\varphi)(t_b\psi) = t_a(\varphi t_b \varphi^{-1})\varphi\psi = t_{a+\varphi(b)}\varphi\psi \in \mathrm{Tran}(V) \cdot G.$$

Отсюда следует, что

$$(t_a\varphi)^{-1} = t_{-\varphi^{-1}(a)}\varphi^{-1} \in \mathrm{Tran}(V) \cdot G.$$

Таким образом, $\mathrm{Tran}(V) \cdot G$ — группа преобразований. Она транзитивна, поскольку уже ее подгруппа $\mathrm{Tran}(V)$ транзитивна.

В частности, мы можем взять $G = GL(V)$. Полученная группа

$$GA(V) = \mathrm{Tran}(V) \cdot GL(V) \tag{75}$$

называется полной аффинной группой пространства V, а ее элементы — (биективными) аффинными преобразованиями. Связанная с ней геометрия называется аффинной геометрией.

В случае $V = E^2$ мы получаем аффинную геометрию евклидовой плоскости.

Предложение 2. Группа движений евклидовой плоскости (соотв. пространства) есть подгруппа группы $GA(E^2)$, равная $\mathrm{Tran}(E^2) \cdot O_2$.

Доказательство. Прежде всего, заметим, что все параллельные переносы и все ортогональные преобразования являются движениями. Пусть теперь α — какое-либо движение. Положим $a = \alpha(o)$. Тогда движение $\varphi = t_a^{-1}\alpha$ оставляет на месте точку o и, значит, принадлежит группе O_2 (см. пример 1.10). Таким образом,

$$\alpha = t_a\varphi \in \mathrm{Tran}(E^2) \cdot O_2$$

Следствие. Если фигуры $F_1, F_2 \subset E^2$ равны в евклидовой геометрии, то они равны и в аффинной геометрии.

Группа $GA(E^2)$ не совпадает с группой движений. Примером аффинного преобразования, не являющегося движением, может служить гомотетия (с коэффициентом $\neq \pm 1$) или растяжение вдоль какой-либо оси. Таким образом, группа $GA(E^2)$ богаче группы движений, и фигуры, не равные в евклидовой геометрии, могут оказаться равными в аффинной геометрии. Так, в аффинной геометрии все окружности равны.

Задача 1. Доказать, что в аффинной геометрии все треугольники равны.

В аффинной геометрии отсутствует понятие расстояния между точками. Однако, как показывает следующая задача, имеется инвариант трех точек, лежащих на одной прямой.

Задача 2. Доказать, что при аффинных преобразованиях сохраняется отношение, в котором точка делит отрезок.

Аналогичным образом определяется аффинная геометрия евклидова пространства.

В рамках группового подхода могут быть построены также проективная и конформная геометрии, геометрия Лобачевского и другие геометрии, используемые в математике и ее приложениях.

Группы преобразований в физике описывают симметрию физических законов, в частности, симметрию пространства-времени.

Точка пространства-времени задается тремя пространственными координатами x, y, z и временно́й координатой t, так что пространство-время с фиксированной системой отсчета может быть отождествлено с $\mathbb{R}^4$. Переход к другой системе отсчета означает некоторое преобразование пространства $\mathbb{R}^4$. Как в классической, так и в релятивистской механике (точнее, в специальной теории относительности) существует понятие инерциальных систем отсчета, в которых все законы механики имеют одинаковый вид. Переходы от одной инерциальной системы отсчета к другим составляют некоторую группу преобразований пространства $\mathbb{R}^4$. Эта группа однозначно определяет законы механики. Отличие релятивистской механики от классической обусловлено тем, что она берет за основу другую группу преобразований.

Группа симметрии пространства-времени в классической механике есть группа Галилея, описываемая следующим образом:

$$G = \mathrm{Tran}(\mathbb{R}^4) \cdot H \cdot O_3,$$

где O_3 — группа ортогональных преобразований пространственных координат, а H — группа преобразований вида

$$(x, y, z, t) \mapsto (x + at, y + bt, z + ct, t),$$

соответствующих переходу к новой системе отсчета, равномерно и прямолинейно движущейся относительно старой. Из этого описания группы Галилея видно, что в классической механике время абсолютно в том смысле, что разность временны́х координат двух событий одинакова во всех инерциальных системах отсчета.

Согласно представлению релятивистской механики группа симметрии пространства-времени есть группа Пуанкаре

$$G = \mathrm{Tran}(\mathbb{R}^4) \cdot O_{3,1},$$

где $O_{3,1}$ — группа линейных преобразований, сохраняющих многочлен

$$x^2 + y^2 + z^2 - t^2$$

(в системе единиц, в которой скорость света равна 1). Группа $O_{3,1}$ содержит группу O_3, не затрагивающую временно́й координаты. Нетривиальным примером преобразований из $O_{3,1}$ могут служить преобразования Лоренца

$$(x, y, z, t) \mapsto (x \operatorname{ch} a + t \operatorname{sh} a, y, z, x \operatorname{sh} a + t \operatorname{ch} a),$$

перемешивающие пространственные и временные координаты. Вид этих преобразований показывает, что в релятивистской механике время не абсолютно.

Группа Пуанкаре была описана в работах Лоренца и Пуанкаре как группа симметрии законов электродинамики (уравнений Максвелла). Заслуга Эйнштейна состояла в том, что он имел смелость сделать вывод, что и законы механики должны иметь ту же группу симметрии.

Группы преобразований лежат также в основе кристаллографии и теории элементарных частиц. Так, в кристаллографии они описывают симметрию кристаллических структур и, тем самым, — физических свойств кристаллов.

4.3. Циклические группы

Так же, как в группе $\mathbb{R}^*$, в любой группе G могут быть определены степени элемента $g \in G$ с целыми показателями:

$$g^k = \begin{cases} \underbrace{gg\ldots g}_{k}, & \text{если } k > 0, \\ e, & \text{если } k = 0, \\ \underbrace{g^{-1}g^{-1}\ldots g^{-1}}_{-k}, & \text{если } k < 0. \end{cases}$$

Имеет место свойство

$$g^k g^l = g^{k+l}. \tag{76}$$

Это очевидно, если $k, l > 0$. Рассмотрим случай, когда $k > 0$, $l < 0$, $k + l > 0$. Тогда

$$g^k g^l = \underbrace{gg\ldots g}_{k}\underbrace{g^{-1}g^{-1}\ldots g^{-1}}_{-l} = \underbrace{gg\ldots g}_{k+l} = g^{k+l}.$$

Аналогично рассматриваются остальные случаи.

Из (76) следует, что

$$(g^k)^{-1} = g^{-k}.$$

Кроме того, $e = g^0$ по определению. Таким образом, степени элемента g образуют подгруппу в группе G. Она называется циклической подгруппой, порожденной элементом g, и обозначается через $\langle g \rangle$.

Возможны два принципиально разных случая: либо все степени элемента g различны, либо нет. В первом случае подгруппа $\langle g \rangle$ бесконечна. Рассмотрим более подробно второй случай.

Пусть $g^k = g^l$, $k > l$; тогда $g^{k-l} = e$. Наименьшее из натуральных чисел m, для которых $g^m = e$, называется в этом случае порядком элемента g и обозначается через $\operatorname{ord} g$.

Предложение 1. Если $\operatorname{ord} g = n$, то
1) $g^m = e \iff n \mid m$;
2) $g^k = g^l \iff k \equiv l \pmod{n}$.

Доказательство. 1) Разделим m на n с остатком:

$$m = qn + r, \quad 0 \leqslant r < n.$$

Имеем тогда в силу определения порядка:

$$g^m = (g^n)^q \cdot g^r = g^r = e \iff r = 0.$$

2) Имеем в силу предыдущего:

$$g^k = g^l \iff g^{k-l} = e \iff n \mid (k-l) \iff k \equiv l \pmod n.$$

Следствие. Если $\operatorname{ord} g = n$, то подгруппа $\langle g\rangle$ содержит n элементов.

Доказательство. Действительно,

$$\langle g\rangle = \{e, g, g^2, \ldots, g^{n-1}\}, \tag{77}$$

причем все перечисленные элементы различны.

В том случае, когда не существует такого натурального m, что $g^m = e$ (т. е. имеет место первый из описанных выше случаев), полагают $\operatorname{ord} g = \infty$. Отметим, что $\operatorname{ord} e = 1$; порядки же всех остальных элементов группы больше 1.

В аддитивной группе говорят не о степенях элемента g, а о его кратных, которые обозначают через kg. Соответственно этому порядок элемента g аддитивной группы G — это наименьшее из натуральных чисел m (если такие существуют), для которых

$$mg \doteqdot \underbrace{g + g + \ldots + g}_{m} = 0.$$

Пример 1. Характеристика поля (см. §1.6) есть порядок любого ненулевого элемента в его аддитивной группе.

Пример 2. Очевидно, что в конечной группе порядок любого элемента конечен. Покажем, как вычисляются порядки элементов группы S_n. Подстановка $\tau \in S_n$ называется циклом длины p и обозначается через $(i_1 i_2 \ldots i_p)$, если она циклически переставляет $i_1, i_2, \ldots, i_p$, т. е.

$$\tau(i_1) = i_2,\ \tau(i_2) = i_3,\ \ldots,\ \tau(i_p) = i_1,$$

а все остальные числа оставляет на месте. Очевидно, что порядок цикла длины p равен p. Циклы τ_1 и τ_2 называются независимыми, если среди фактически переставляемых ими чисел нет общих; в этом случае $\tau_1\tau_2 = \tau_2\tau_1$. Всякая подстановка однозначно разлагается в произведение независимых циклов. Например,

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 6 & 7 & 4 & 8 & 3 & 2 & 1 \end{pmatrix} = (2637)(158),$$

что наглядно показано на рис. 21, где действие подстановки σ изображено стрелками. Если подстановка σ разлагается в произведение независимых циклов длин $p_1, p_2, \ldots, p_s$, то

$$\operatorname{ord} \sigma = \text{НОК}\{p_1, p_2, \ldots, p_s\}.$$

Например, для подстановки σ, изображенной на рис. 21, $\operatorname{ord} \sigma = 12$.

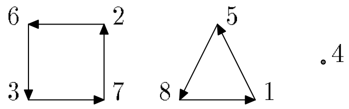

Рис. 21.

Задача 1. Доказать, что порядок любого элемента группы S_n не превосходит числа

$$e^{n/e} \approx 1{,}44^n.$$

Пример 3. Порядок комплексного числа c в группе $\mathbb{C}^*$ конечен тогда и только тогда, когда это число есть корень некоторой степени из единицы, что , в свою очередь, имеет место тогда и только тогда, когда $|c| = 1$, а $\arg c$ соизмерим с π, т. е. $\dfrac{\arg c}{\pi} \in \mathbb{Q}$.

Задача 2. Доказать, что $\operatorname{arctg} \dfrac{3}{4}$ несоизмерим с π.

Пример 4. Найдем элементы конечного порядка в группе $\operatorname{Isom} E^2$ движений плоскости. Пусть $\varphi \in \operatorname{Isom} E^2$, $\varphi^n = \mathrm{id}$. Для любой точки $p \in E^2$ точки

$$p, \varphi p, \varphi^2 p, \ldots, \varphi^{n-1} p$$

циклически переставляются движением φ, так что их центр тяжести o неподвижен относительно φ. Следовательно, φ — либо поворот на угол вида $\dfrac{2\pi k}{n}$ вокруг точки o, либо отражение относительно некоторой прямой, проходящей через o.

Пример 5. Найдем порядок матрицы

$$A = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$$

как элемента группы $GL_2(\mathbb{R})$. Имеем:

$$A^2 = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}, \quad A^3 = -E,$$

откуда

$$A^4 = -A, \quad A^5 = -A^2, \quad A^6 = -A^3 = E,$$

так что $\operatorname{ord} A = 6$. Конечно, этот пример специально подобран: вероятность того, что порядок наудачу выбранной матрицы $A \in GL_2(\mathbb{R})$ будет конечен, равна нулю.

Предложение 2. Если $\operatorname{ord} g = n$, то

$$\operatorname{ord} g^k = \frac{n}{(n,k)}. \tag{78}$$

Доказательство. Пусть

$$(n,k) = d, \quad n = n_1 d, \quad k = k_1 d,$$

так что $(n_1, k_1) = 1$. Имеем:

$$(g^k)^m = e \iff n \mid km \iff n_1 \mid k_1 m \iff n_1 \mid m.$$

Следовательно, $\operatorname{ord} g^k = n_1$.

Определение. Группа G называется циклической, если существует такой элемент $g \in G$, что $G = \langle g \rangle$. Всякий такой элемент называется порождающим элементом группы G.

Пример 6. Аддитивная группа $\mathbb{Z}$ целых чисел является циклической, так как порождается элементом 1.

Пример 7. Аддитивная группа $\mathbb{Z}_n$ вычетов по модулю n является циклической, так как порождается элементом $[1]$.

Пример 8. Мультипликативная группа C_n комплексных корней n-й степени из 1 является циклической. В самом деле, эти корни суть числа

$$\varepsilon_k = \cos\frac{2\pi k}{n} + i \sin\frac{2\pi k}{n} \quad (k = 0, 1, \ldots, n-1).$$

Ясно, что $\varepsilon_k = \varepsilon_1^k$. Следовательно, группа C_n порождается элементом ε_1.

Легко видеть, что в бесконечной циклической группе $G = \langle g \rangle$ порождающими элементами являются только g и g^{-1}. Так в группе $\mathbb{Z}$ порождающими элементами являются только 1 и -1.

Число элементов конечной группы G называется ее порядком и обозначается через $|G|$. Порядок конечной циклической группы равен порядку ее порождающего элемента. Поэтому из предложения 2 следует

Предложение 3. Элемент g^k циклической группы $G = \langle g \rangle$ порядка n является порождающим тогда и только тогда, когда $(n, k) = 1$.

Пример 9. Порождающие элементы группы C_n (см. пример 8) называются первообразными корнями n-й степени из 1. Это корни вида ε_k, где $(n, k) = 1$. Например, первообразные корни 12-й степени из 1 — это $\varepsilon_1, \varepsilon_5, \varepsilon_7, \varepsilon_{11}$.

Циклические группы — это наиболее простые группы, которые можно себе представить. (В частности, они абелевы.) Следующая теорема дает их полное описание.

Теорема 1. Всякая бесконечная циклическая группа изоморфна группе $\mathbb{Z}$. Всякая конечная циклическая группа порядка n изоморфна группе $\mathbb{Z}_n$.

Доказательство. Если $G = \langle g \rangle$ — бесконечная циклическая группа, то в силу формулы (76) отображение $f\colon \mathbb{Z} \to G,\ k \mapsto g^k$ есть изоморфизм.

Пусть $G = \langle g \rangle$ — конечная циклическая группа порядка n. Рассмотрим отображение

$$f\colon \mathbb{Z}_n \to G, \quad [k] \mapsto g^k \quad (k \in \mathbb{Z}).$$

Так как

$$[k] = [l] \iff k \equiv l \pmod{n} \iff g^k = g^l,$$

то отображение f корректно определено и биективно. Свойство

$$f(k + l) = f(k)f(l)$$

вытекает из той же формулы (76). Таким образом, f — изоморфизм.

Для понимания строения какой-либо группы важную роль играет знание ее подгрупп. Все подгруппы циклической группы могут быть легко описаны.

Теорема 2. 1) Всякая подгруппа циклической группы является циклической.

2) В циклической группе порядка n порядок любой подгруппы делит n и для любого делителя q числа n существует ровно одна подгруппа порядка q.

Доказательство. 1) Пусть $G = \langle g \rangle$ — циклическая группа и H — ее подгруппа, отличная от $\{e\}$. (Единичная подгруппа, очевидно, является циклической.) Заметим, что если $g^{-m} \in H$ для какого-либо $m \in \mathbb{N}$, то и $g^m \in H$. Пусть m — наименьшее из натуральных чисел, для которых $g^m \in H$. Докажем, что $H = \langle g^m \rangle$. Пусть $g^k \in H$. Разделим k на m с остатком:

$$k = qm + r, \quad 0 \leqslant r < m.$$

Имеем:

$$g^r = g^k (g^m)^{-q} \in H,$$

откуда в силу определения m следует, что $r = 0$ и, значит, $g^k = (g^m)^q$.

2) Если $|G| = n$, то предыдущее рассуждение, примененное к $k = n$ (в этом случае $g^k = e \in H$), показывает, что $n = qm$. Подгруппа H имеет вид

$$H = \{e, g^m, g^{2m}, \ldots, g^{(q-1)m}\} \tag{79}$$

и является единственной подгруппой порядка q в группе G. Обратно, если q — любой делитель числа n и $n = qm$, то подмножество H, определяемое равенством (79), является подгруппой порядка q.

Следствие. В циклической группе простого порядка любая неединичная подгруппа совпадает со всей группой.

Пример 10. В группе $\mathbb{Z}$ всякая подгруппа имеет вид $m\mathbb{Z}$, где $m \geqslant 0$.

Пример 11. В группе C_n корней n-й степени из 1 любая подгруппа есть группа C_q корней q-й степени из 1, где $q \mid n$.

4.4. Системы порождающих

Пусть S — какое-либо подмножество группы G. Обозначим через $\langle S \rangle$ совокупность всевозможных произведений вида

$$g_1^{\varepsilon_1} g_2^{\varepsilon_2} \ldots g_k^{\varepsilon_k} \quad (g_1, g_2, \ldots g_k \in S;\ \varepsilon_1, \varepsilon_2, \ldots, \varepsilon_k = \pm 1). \tag{80}$$

Это наименьшая подгруппа группы G, содержащая S. В самом деле, если какая-либо подгруппа содержит S, то она содержит и все указанные произведения. С другой стороны, само множество $\langle S\rangle$ является подгруппой, как показывают следующие равенства

$$(g_1^{\varepsilon_1} g_2^{\varepsilon_2} \dots g_k^{\varepsilon_k})(g_{k+1}^{\varepsilon_{k+1}} g_{k+2}^{\varepsilon_{k+2}} \dots g_{k+l}^{\varepsilon_{k+l}}) = g_1^{\varepsilon_1} g_2^{\varepsilon_2} \dots g_{k+l}^{\varepsilon_{k+l}},$$
$$(g_1^{\varepsilon_1} g_2^{\varepsilon_2} \dots g_k^{\varepsilon_k})^{-1} = g_k^{-\varepsilon_k} \dots g_2^{-\varepsilon_2} g_1^{-\varepsilon_1}.$$

Говорят, что $\langle S\rangle$ — подгруппа, порожденная подмножеством S. В частности, если S состоит из одного элемента g, то $\langle S\rangle = \langle g\rangle$ есть циклическая подгруппа, порожденная элементом g в том смысле, как это было определено в предыдущем параграфе.

Замечание. Удобно считать, что в число произведений (80) входит пустое произведение ($k = 0$), которое по определению равно e.

Определение. Говорят, что группа G порождается своим подмножеством S, или что S — система порождающих (элементов) группы G, если $G = \langle S\rangle$.

Конечно, любая группа G порождается подмножеством $S = G$, однако представляет интерес найти возможно меньшую систему порождающих.

Пример. Группа диэдра D_n (см. пример 1.11) порождается поворотом φ на угол $\dfrac{2\pi}{n}$ и (любым) отражением $\psi \in D_n$. В самом деле, φ порождает циклическую подгруппу C_n всех поворотов, содержащихся в группе D_n; умножая элементы этой подгруппы на ψ, мы получим все отражения, входящие в группу D_n.

Два важных примера систем порождающих содержатся в приводимых ниже теоремах.

Подстановка, являющаяся циклом длины 2 (см. пример 3.2), называется транспозицией.

Теорема 1. Группа S_n порождается транспозициями.

Доказательство. Отметим, что каждая транспозиция обратна сама себе. Поэтому утверждение теоремы означает, что любая подстановка разлагается в произведение транспозиций.

Умножение подстановки

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ k_1 & k_2 & \dots & k_n \end{pmatrix} \tag{81}$$

слева на транспозицию (ij) вызывает перестановку i и j в нижней строке. Такая операция также называется транспозицией. Очевидно, что путем последовательных транспозиций любую перестановку $(k_1, k_2, \dots, k_n)$ можно привести к тривиальной: сначала, если $k_1 \neq 1$, меняем местами k_1 и 1, ставя тем самым 1 на первое место, затем ставим 2 на второе место и т. д. Таким образом, существуют такие транспозиции $\tau_1, \tau_2, \dots, \tau_s$, что

$$\tau_s \dots \tau_2 \tau_1 \sigma = \mathrm{id}$$

и, значит,

$$\sigma = \tau_1 \tau_2 \dots \tau_s.$$

Задача 1. Доказать, что группа S_n порождается смежными транспозициями $(12), (23), \dots, ((n-1)n)$, причем минимальное число смежных транспозиций, в произведение которых может быть разложена подстановка $\sigma \in S_n$, равно числу инверсий в нижней строке ее стандартной записи (81).

Теорема 2. Группа $GL_n(K)$ порождается элементарными матрицами.

(Определение элементарных матриц см. в §2.1)

Доказательство. Отметим, что матрица, обратная к элементарной, также элементарна (см. §2.1). Поэтому утверждение теоремы означает, что любая невырожденная матрица разлагается в произведение элементарных матриц.

Умножение матрицы $A \in GL_n(K)$ слева на элементарную матрицу вызывает соответствующее элементарное преобразование ее строк. Мы знаем, что с помощью элементарных преобразований строк любую невырожденную матрицу можно привести к единичной матрице. Таким образом, существуют такие элементарные матрицы $U_1, U_2, \dots, U_s$, что

$$U_s \dots U_2 U_1 A = E$$

и, значит,

$$A = U_1^{-1} U_2^{-1} \dots U_s^{-1}.$$

Задача 2. Доказать, что группа $SL_2(\mathbb{Z})$ (см. пример 1.13) порождается матрицами

$$R = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}, \quad S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Задача 3. Доказать, что группа движений плоскости порождается отражениями относительно прямых. (Указание: доказать вначале, что каждый поворот и каждый параллельный перенос являются произведением двух отражений.)

4.5. Разбиение на смежные классы

Пусть G — группа и H — ее подгруппа. Будем говорить, что элементы $g_1, g_2 \in G$ сравнимы по модулю H, и писать

$$g_1 \equiv g_2 \pmod{H},$$

если

$$g_1^{-1} g_2 \in H, \tag{82}$$

т. е. $g_2 = g_1 h$, где $h \in H$. Это определение обобщает определение сравнимости целых чисел по модулю n, которое получается в случае $G = \mathbb{Z}$, $H = n\mathbb{Z}$.

Докажем, что определенное таким образом отношение сравнимости по модулю H является отношением эквивалентности:

1) $g \equiv g \pmod{H}$, так как $g^{-1} g = e \in H$;

2) если $g_1 \equiv g_2 \pmod{H}$, т.е. $g_1^{-1} g_2 \in H$, то $g_2 \equiv g_1 \pmod{H}$, так как

$$g_2^{-1} g_1 = (g_1^{-1} g_2)^{-1} \in H;$$

3) если $g_1 \equiv g_2 \pmod{H}$ и $g_2 \equiv g_3 \pmod{H}$, т.е. $g_1^{-1} g_2$, $g_2^{-1} g_3 \in H$, то $g_1 \equiv g_3 \pmod{H}$, так как

$$g_1^{-1} g_3 = (g_1^{-1} g_2)(g_2^{-1} g_3) \in H.$$

Классы этой эквивалентности называются (левыми) смежными классами группы G по подгруппе H. Ясно, что смежный класс, содержащий элемент g, имеет вид

$$gH = \{gh : h \in H\}.$$

Одним из смежных классов является сама подгруппа H.

Поскольку умножение в группе не обязано быть коммутативным, мы получим, вообще говоря, другое отношение эквивалентности, взяв вместо условия (82) аналогичное ему условие

$$g_2 g_1^{-1} \in H. \tag{83}$$

Классы этой эквивалентности называются правыми смежными классами группы G по подгруппе H. Они имеют вид

$$Hg = \{hg : h \in H\}.$$

Заметим, что инверсия $g \mapsto g^{-1}$ устанавливает взаимно однозначное соответствие между множествами левых и правых смежных классов. А именно,

$$(gH)^{-1} = Hg^{-1}.$$

Пример 1. Смежные классы аддитивной группы $\mathbb{C}$ по подгруппе $\mathbb{R}$ изображаются на комплексной плоскости прямыми, параллельными действительной оси (рис. 22а).

Пример 2. Смежные классы мультипликативной группы $\mathbb{C}^*$ по подгруппе $\mathbb{R}_+^*$ положительных чисел — это лучи, исходящие из начала координат (рис. 22б).

Пример 3. Смежные классы группы $\mathbb{C}^*$ по подгруппе

$$\mathbb{T} = \{z \in \mathbb{C}^* : |z| = 1\}$$

— это окружности с центром в начале координат (рис. 22в).

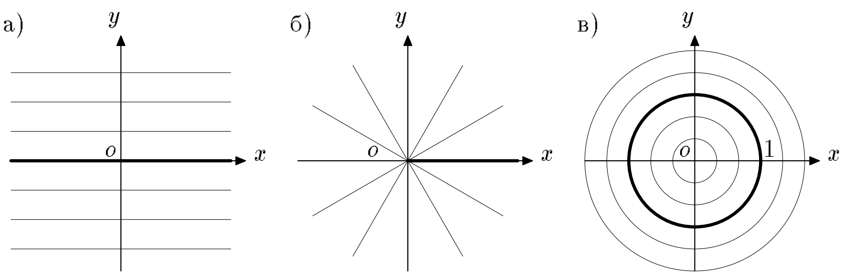

Рис. 22.

Пример 4. В случае $G = GL_n(K)$, $H = SL_n(K)$ (см. пример 1.12) условие (82), равно как и (83), означает, что $\det g_1 = \det g_2$. Поэтому левые смежные классы в данном случае совпадают с правыми (хотя группа $GL_n(K)$ не абелева); каждый из них представляет собой совокупность всех матриц с определителем, равным какому-либо фиксированному числу.

Пример 5. В группе $G = S_n$ рассмотрим подгруппу $H \simeq S_{n-1}$, состоящую из подстановок, оставляющих на месте число n. Подстановки $\sigma_1, \sigma_2 \in S_n$ принадлежат одному левому смежному классу по H, если $\sigma_1^{-1}\sigma_2(n) = n$, т.е. если

$$\sigma_1(n) = \sigma_2(n).$$

Следовательно, имеется n левых смежных классов $P_1, P_2, \ldots, P_n$, где

$$P_k = \{\sigma \in S_n : \sigma(n) = k\}.$$

В то же время подстановки $\sigma_1, \sigma_2 \in S_n$ принадлежат одному правому смежному классу, если $\sigma_2\sigma_1^{-1}(n) = n$, т.е. если

$$\sigma_1^{-1}(n) = \sigma_2^{-1}(n).$$

Следовательно, имеется n правых смежных классов $Q_1, Q_2, \ldots, Q_n$, где

$$Q_k = \{\sigma \in S_n : \sigma(k) = n\}.$$

Мы видим, что правые смежные классы отличны от левых (за исключением $Q_n = P_n = H$).

Множество левых смежных классов группы G по подгруппе H обозначается через G/H. Число смежных классов G по H (левых или правых, безразлично), если оно конечно, называется индексом подгруппы H и обозначается через $|G : H|$.

Теорема 1 (Лагранж). Если G — конечная группа и H — любая ее подгруппа, то

$$|G| = |G : H|\,|H|$$

Доказательство. Все смежные классы gH содержат содержат одно и то же число элементов, равное $|H|$. Поскольку они образуют разбиение группы G (как классы эквивалентности), порядок группы G равен произведению их числа на $|H|$.

Следствие 1. Порядок любой подгруппы конечной группы делит порядок группы.

Мы уже видели это в случае циклических групп (теорема 3.2).

Следствие 2. Порядок любого элемента конечной группы делит порядок группы.

Действительно, порядок элемента равен порядку порождаемой им циклической подгруппы.

Следствие 3. Всякая конечная группа простого порядка является циклической.

Д о к а з а т е л ь с т в о. В силу следствия 1 такая группа должна совпадать с циклической подгруппой, порожденной любым элементом, отличным от единицы.

Следствие 4. Если $|G| = n$, то $g^n = e$ для любого $g \in G$.

Д о к а з а т е л ь с т в о. Пусть $\operatorname{ord} g = m$. В силу следствия 2 $m \mid n$. Следовательно, $g^n = e$.

Пример 6. Если p — простое число, то мультипликативная группа $\mathbb{Z}_p^*$ поля $\mathbb{Z}_p$ есть (абелева) группа порядка $p-1$. Следовательно, $g^{p-1} = 1$ для любого элемента $g \in \mathbb{Z}_p^*$. Это означает, что

$$a^{p-1} \equiv 1 \pmod p$$

для любого целого числа a, не делящегося на p. Последнее утверждение есть так называемая малая теорема Ферма.

Разбиение на смежные классы естественно возникает при изучении групп преобразований.

Пусть G — группа преобразований множества X. Будем говорить, что точки $x, y \in X$ эквивалентны относительно G, и писать $x \underset{G}{\sim} y$, если существует такой элемент $g \in G$, что $y = gx$. Это частный случай эквивалентности фигур, определенной в §2, и, следовательно, — отношение эквивалентности. Класс эквивалентности точки $x \in X$ называется ее орбитой. Иначе говоря, орбита точки x есть множество

$$Gx = \{gx : g \in G\}.$$

В частности, транзитивные группы преобразований (см. определение 2.1) — это группы преобразований, имеющие единственную орбиту.

Подгруппа

$$G_x = \{\, g \in G : gx = x \,\}$$

называется стабилизатором точки x.

Пример 7. Группа движений евклидовой плоскости транзитивна. Стабилизатором начала координат является ортогональная группа O_2 (см. пример 1.10).

Пример 8. Орбиты группы O_2 суть окружности с центром в начале координат o и сама точка o. Стабилизатор точки $p \neq o$ состоит из тождественного преобразования и отражения относительно прямой op, а стабилизатор точки o есть вся группа O_2.

Пример 9. Группа S_n транзитивна на множестве $\{1, 2, \ldots, n\}$. Стабилизатор числа n есть подгруппа $H \simeq S_{n-1}$, рассмотренная в примере 5.

Следующая теорема является обобщением (первой части) примера 5.

Теорема 2. Имеется взаимно однозначное соответствие между орбитой Gx и множеством смежных классов G/G_x, при котором точке $y = gx \in Gx$ соответствует смежный класс gG_x.

Доказательство. При $g_1, g_2 \in G$ имеем:

$$g_1 \equiv g_2 \pmod{G}_x \iff \\ \iff g_1^{-1}g_2 \in G_x \iff g_1^{-1}g_2x = x \iff g_1x = g_2x.$$

Таким образом, элементы одного смежного класса G по G_x характеризуются тем, что они переводят точку x в одну и ту же точку. Более точно, все элементы смежного класса gG_x, и только они, переводят точку x в точку $y = gx$. Тем самым и установлено искомое соответствие.

Число элементов орбиты Gx, если оно конечно, называется ее длиной и обозначается через $|Gx|$.

Следствие. Если G — конечная группа, то

$$|G| = |Gx|\,|G_x|. \tag{84}$$

Из этой формулы следует, что порядки стабилизаторов всех точек орбиты одинаковы. На самом деле имеется точная связь между стабилизаторами точек одной орбиты, не зависящая от конечности группы G. Мы сформулируем ее в виде задачи.

Задача 1. Доказать, что

$$G_{gx} = gG_xg^{-1}.$$

Пример 10. Пусть $K \subset E^3$ — куб. Рассмотрим группу его симметрии

$$G = \operatorname{Sym} K = \{ \varphi \in \operatorname{Isom} E^3 : \varphi(K) = K \}.$$

Очевидно, что это конечная группа. Более того, симметрия куба полностью определяется тем, как она переставляет его вершины. Поэтому мы можем рассматривать группу G как группу преобразований множества V вершин куба K. Ввиду того, что куб является правильным многогранником, любую вершину куба можно перевести в любую другую с помощью преобразования из группы G. Иначе говоря, группа G транзитивна на множестве V. Следовательно,

$$|G| = 8|G_v|,$$

где v — какая-либо вершина. Аналогичным образом, рассматривая группу G_v как группу преобразований множества ребер, выходящих из v, можно показать, что

$$|G_v| = 3|G_{v,e}|,$$

где $G_{v,e}$ — стабилизатор в группе G_v какого-либо ребра e, выходящего из v. Группа $G_{v,e}$ состоит из тождественного преобразования и отражения относительно плоскости, проходящей через центр куба и ребро e (см. рис. 23). Таким образом,

$$|\operatorname{Sym} K| = 8 \cdot 3 \cdot 2 = 48.$$

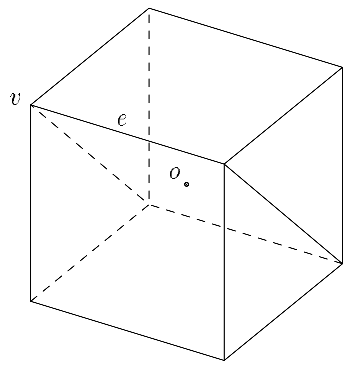

Рис. 23.

Задача 2. Получить тот же результат еще двумя способами, рассмотрев группу $\operatorname{Sym} K$ как группу преобразований множества граней и множества ребер куба соответственно.

Пример 11. Пусть G — группа преобразований алгебры многочленов $K[x_1, x_2, x_3, x_4]$, состоящая из всевозможных перестановок переменных x_1, x_2, x_3, x_4. Группа G изоморфна S_4 и, следовательно, $|G| = 4! = 24$. Рассмотрим многочлен $f = x_1x_2 + x_3x_4$. Перестановками переменных из него можно получить 3 многочлена

$$x_1x_2 + x_3x_4, \quad x_1x_3 + x_2x_4, \quad x_1x_4 + x_2x_3.$$

Это означает, что $|Gf| = 3$. По формуле (84) находим

$$|G_f| = \frac{|G|}{|Gf|} = \frac{24}{3} = 8.$$

Заметим, что, если отождествить группу G с группой S_4, то G_f будет не что иное, как подгруппа, обозначенная в примере 1.8 через $\operatorname{Sym} f$.

Отношение сравнимости по модулю n в аддитивной группе целых чисел согласовано с операцией сложения, что позволяет определить операцию сложения в фактормножестве. Аналогичным образом можно определить операцию в множестве смежных классов группы по подгруппе и в других случаях, но не всегда.

Определение. Подгруппа H группы G называется нормальной, если

$$gH = Hg \quad \forall g \in G \tag{85}$$

или, что эквивалентно,

$$gHg^{-1} = H \quad \forall g \in G. \tag{86}$$

В этом случае пишут $H \lhd G$ (или $G \rhd H$).

Для того чтобы подгруппа H была нормальна, достаточно (но не необходимо), чтобы каждый элемент группы G был перестановочен с каждым элементом из H. В частности, в абелевой группе любая подгруппа нормальна.

Теорема 3. Отношение сравнимости по модулю подгруппы H согласовано с операцией умножения в группе G тогда и только тогда, когда подгруппа H нормальна.

Доказательство. Согласованность отношения сравнимости по модулю H с операцией умножения означает, что

$$g_1 \equiv g_1' \pmod{H}, \quad g_2 \equiv g_2' \pmod{H} \implies \implies g_1 g_2 \equiv g_1' g_2' \pmod{H}$$

или, что эквивалентно, для любых $g_1, g_2 \in G$ и $h_1, h_2 \in H$

$$(g_1 h_1)(g_2 h_2) \equiv g_1 g_2 \pmod{H}.$$

Последнее условие согласно определению переписывается в виде

$$g_2^{-1} h_1 g_2 \in H.$$

Так как g_2 может быть любым элементом группы G, а h_1 — любым элементом подгруппы H, то это равносильно условию нормальности (86).

Задача 3. Доказать, что всякое отношение эквивалентности в группе, согласованное с операцией, есть отношение сравнимости по модулю некоторой подгруппы.

Таким образом, если $H \triangleleft G$, то операция умножения в группе G определяет операцию умножения в множестве G/H по правилу

$$(g_1 H)(g_2 H) = g_1 g_2 H.$$

Эта операция наследует ассоциативность операции в группе G. Для нее имеется единица — смежный класс eH. Каждый смежный класс gH имеет обратный, а именно, $g^{-1}H$. Следовательно, G/H — группа. Эта группа называется факторгруппой группы G по H.

Очевидно, что если группа абелева, то любая ее факторгруппа также абелева.

Пример 12. Факторгруппа $\mathbb{Z}/n\mathbb{Z}$ есть группа вычетов $\mathbb{Z}_n$.

Пример 13. Смежные классы $\mathbb{C}$ по $\mathbb{R}$ (см. пример 1) суть прямые $L_a = \{z : \operatorname{Im} z = a\}$ $(a \in \mathbb{R})$. Операция сложения в $\mathbb{C}/\mathbb{R}$ задается формулой $L_a + L_b = L_{a+b}$, так что

$$\mathbb{C}/\mathbb{R} \simeq \mathbb{R}.$$

Пример 14. Смежные классы $\mathbb{C}^*$ по $\mathbb{T}$ (см. пример 3) суть окружности $C_r = \{z \in \mathbb{C}^* : |z| = r\}$ $(r > 0)$. Операция умножения в $\mathbb{C}^*/\mathbb{T}$ задается формулой $C_r C_s = C_{rs}$, так что

$$\mathbb{C}^*/\mathbb{T} \simeq \mathbb{R}_+^*.$$

Пример 15. Как мы видели выше (см. пример 4), левые смежные классы $GL_n(K)$ по $SL_n(K)$ совпадают с правыми и имеют вид

$$M_a = \{ A \in GL_n(K) : \det A = a \} \quad (a \in K^*).$$

Следовательно, $SL_n(K)$ — нормальная подгруппа. Операция умножения в факторгруппе задается формулой $M_a M_b = M_{ab}$, так что

$$GL_n(K)/SL_n(K) \simeq K^*.$$

Пример 16. Подгруппа $H \simeq S_{n-1}$ группы S_n, рассмотренная в примере 5, не является нормальной при $n \geqslant 3$.

Задача 4. Доказать, что всякая факторгруппа циклической группы является циклической.

Задача 5. Доказать, что группа диагональных матриц не является нормальной подгруппой группы $GL_n(K)$ при $n \geqslant 2$ и $|K| \geqslant 3$.

4.6. Гомоморфизмы

Связи между различными алгебраическими структурами одного типа устанавливаются при помощи гомоморфизмов. Понятие гомоморфизма отличается от понятия изоморфизма тем, что оно не требует биективности. В одном случае мы уже встречались с этим понятием. А именно, гомоморфизмы векторных пространств — это не что иное, как их линейные отображения.

Дадим точное определение гомоморфизма групп.

Определение. Гомоморфизмом группы G в группу H называется отображение $f\colon G \to H$, удовлетворяющее условию

$$f(ab) = f(a)f(b) \quad \forall a, b \in G.$$

Установим некоторые общие свойства гомоморфизмов групп.

1) $f(e) = e$. В самом деле, пусть $f(e) = h \in H$; тогда

$$h^2 = f(e)^2 = f(e^2) = f(e) = h,$$

откуда $h = e$.

2) $f(a^{-1}) = f(a)^{-1}$, ибо

$$f(a)f(a^{-1}) = f(aa^{-1}) = f(e) = e.$$

3) $\operatorname{Im} f = \{f(a) : a \in G\}$ есть подгруппа группы H (называемая образом гомоморфизма f). Это следует из определения гомоморфизма и предыдущих свойств.

4) $\operatorname{Ker} f = \{a \in G : f(a) = e\}$ есть нормальная подгруппа группы G (называемая ядром гомоморфизма f). Действительно,

$$a, b \in \operatorname{Ker} f \implies f(ab) = f(a)f(b) = e^2 = e \implies ab \in \operatorname{Ker} f,$$
$$a \in \operatorname{Ker} f \implies f(a^{-1}) = f(a)^{-1} = e^{-1} = e \implies a^{-1} \in \operatorname{Ker} f,$$
$$e \in \operatorname{Ker} f,$$

$$a \in \operatorname{Ker} f,\ g \in G \implies f(gag^{-1}) = f(g)f(a)f(g)^{-1} =$$
$$= f(g)ef(g)^{-1} = f(g)f(g)^{-1} = e \implies gag^{-1} \in \operatorname{Ker} f.$$

Гомоморфизм группы в саму себя называется ее эндоморфизмом. Изоморфизм группы на саму себя называется ее автоморфизмом.

Пример 1. Пусть K — произвольное кольцо. Свойство дистрибутивности $a(b + c) = ab + ac$ означает, что отображение $x \mapsto ax$ (умножение слева на a) является эндоморфизмом аддитивной группы кольца K. (Аналогичное утверждение справедливо и для умножения справа.)

Пример 2. Пусть G — произвольная аддитивная (соотв. мультипликативная) абелева группа. Тогда для любого $n \in \mathbb{Z}$ отображение $x \mapsto nx$ (соотв. $x \mapsto x^n$) является эндоморфизмом группы G. (Для неабелевой группы это, вообще говоря, неверно.) В случае $G = \mathbb{C}^*$ ядром этого гомоморфизма является группа C_n корней n-ой степени из 1.

Пример 3. Согласно основному свойству экспоненты отображение $x \mapsto e^x$ является гомоморфизмом аддитивной группы $\mathbb{R}$ в мультипликативную группу $\mathbb{R}^*$. Его образ есть подгруппа $\mathbb{R}^*_+$ положительных чисел, а ядро тривиально. Это отображение может быть продолжено до гомоморфизма $\mathbb{C} \to \mathbb{C}^*$ по формуле

$$z = x + yi \mapsto e^z = e^x(\cos y + i \sin y) \quad (x, y \in \mathbb{R}).$$

В самом деле, пусть $z_1 = x_1 + y_1 i,\ \ z_2 = x_2 + y_2 i$; тогда

$$e^{z_1+z_2} = e^{x_1+x_2}(\cos(y_1 + y_2) + i \sin(y_1 + y_2)) =$$
$$= [e^{x_1}(\cos y_1 + i \sin y_1)][e^{x_2}(\cos y_2 + i \sin y_2)] = e^{z_1}e^{z_2}.$$

Образ последнего гомоморфизма есть вся группа $\mathbb{C}^*$, а его ядро есть бесконечная циклическая подгруппа $2\pi i\mathbb{Z}$ группы $\mathbb{C}$.

Пример 4. Формула умножения определителей означает, что отображение

$$\det\colon GL_n(K) \to K^*, \quad A \mapsto \det A,$$

является гомоморфизмом. Его ядро — это унимодулярная группа $SL_n(K)$.

Пример 5. Назовем знаком подстановки $\sigma \in S_n$ и обозначим через $\operatorname{sgn}\sigma$ произведение знаков верхней и нижней перестановки в ее записи (см. пример 1.1):

$$\operatorname{sgn}\begin{pmatrix} i_1 & i_2 & \dots & i_n \\ j_1 & j_2 & \dots & j_n \end{pmatrix} = \operatorname{sgn}(i_1, i_2, \dots, i_n) \cdot \operatorname{sgn}(j_1, j_2, \dots, j_n).$$

Это произведение не зависит от способа записи подстановки σ, так как от любого способа записи можно перейти к любому другому последовательными транспозициями столбиков, а при каждой такой транспозиции одновременно меняются знаки верхней и нижней перестановок, так что их произведение сохраняется. Основное свойство знака состоит в том, что отображение

$$\operatorname{sgn}\colon S_n \to C_2 = \{\pm 1\}, \quad \sigma \mapsto \operatorname{sgn}\sigma,$$

является гомоморфизмом. В самом деле, перемножая подстановки σ и τ, мы можем считать, что верхняя перестановка в записи σ совпадает с нижней перестановкой в записи τ:

$$\sigma = \begin{pmatrix} j_1 & j_2 & \dots & j_n \\ k_1 & k_2 & \dots & k_n \end{pmatrix}, \quad \tau = \begin{pmatrix} i_1 & i_2 & \dots & i_n \\ j_1 & j_2 & \dots & j_n \end{pmatrix}.$$

Тогда

$$\sigma\tau = \begin{pmatrix} i_1 & i_2 & \dots & i_n \\ k_1 & k_2 & \dots & k_n \end{pmatrix},$$

так что

$$\begin{aligned} \operatorname{sgn}\sigma\tau = \operatorname{sgn}(i_1, i_2, \dots, i_n) \cdot \operatorname{sgn}(k_1, k_2, \dots, k_n) = \\ = [\operatorname{sgn}(i_1, i_2, \dots, i_n) \operatorname{sgn}(j_1, j_2, \dots, j_n)] \times \\ \times [\operatorname{sgn}(j_1, j_2, \dots, j_n) \operatorname{sgn}(k_1, k_2, \dots, k_n)] = \\ = \operatorname{sgn}\tau \cdot \operatorname{sgn}\sigma = \operatorname{sgn}\sigma \cdot \operatorname{sgn}\tau. \end{aligned}$$

Ядро гомоморфизма sgn называется знакопеременной группой и обозначается через A_n. Употребляется также следующая терминология: подстановки σ, для которых $\operatorname{sgn}\sigma = 1$ (соотв. $\operatorname{sgn}\sigma = -1$), называются четными (соотв. нечетными). Таким образом, A_n — это подгруппа четных подстановок.

Задача 1. Вывести следующую формулу для знака циклической подстановки:

$$\operatorname{sgn}(i_1 i_2 \ldots i_p) = (-1)^{p-1}.$$

Пользуясь этим, доказать, что знак любой подстановки равен $(-1)^{m-s}$, где m — число фактически переставляемых ею (т. е. не оставляемых на месте) элементов, а s — число независимых циклов, в произведение которых она разлагается.

Следующая теорема носит название теоремы о гомоморфизме групп.

Теорема 1. Пусть $f\colon G \to H$ — гомоморфизм групп. Тогда

$$\operatorname{Im} f \simeq G/\operatorname{Ker} f.$$

Более точно, имеется изоморфизм

$$\varphi\colon \operatorname{Im} f \to G/\operatorname{Ker} f,$$

сопоставляющий каждому элементу $h = f(g) \in \operatorname{Im} f$ смежный класс $g \operatorname{Ker} f$.

Доказательство. Доказательство этой теоремы аналогично доказательству теоремы 5.2. А именно,

$$g_1 \equiv g_2 \pmod{\operatorname{Ker} f} \iff g_1^{-1} g_2 \in \operatorname{Ker} f \iff \\ \iff f(g_1^{-1} g_2) = e \iff f(g_1) = f(g_2),$$

так что элементы одного смежного класса G по $\operatorname{Ker} f$ характеризуются тем, что их образом служит один и тот же элемент группы H (принадлежащий $\operatorname{Im} f$). Более точно, все элементы смежного класса $g \operatorname{Ker} f$, и только они, переходят при гомоморфизме f в элемент $h = f(g) \in \operatorname{Im} f$. Тем самым показано, что отображение φ, о котором идет речь в теореме, корректно определено и биективно. Остается проверить, что φ — гомоморфизм.

Пусть $g_1, g_2 \in G$, $f(g_1) = h_1$, $f(g_2) = h_2$. Тогда $f(g_1 g_2) = h_1 h_2$, и

$$\varphi(h_1 h_2) = g_1 g_2 \operatorname{Ker} f = (g_1 \operatorname{Ker} f)(g_2 \operatorname{Ker} f) = \varphi(h_1)\varphi(h_2),$$

что и требовалось доказать.

Следствие 1. Гомоморфизм f является изоморфизмом тогда и только тогда, когда $\operatorname{Im} f = H$ и $\operatorname{Ker} f = \{e\}$.

Следствие 2. Если группа G конечна, то

$$|G| = |\operatorname{Im} f|\,|\operatorname{Ker} f|.$$

(Интересно сравнить эту формулу с формулой (84))

Пример 6. Рассмотрим гомоморфизм

$$f\colon \mathbb{C} \to \mathbb{R}, \quad z \mapsto \operatorname{Im} z.$$

Имеем $\operatorname{Im} f = \mathbb{R}$, $\operatorname{Ker} f = \mathbb{R}$, так что

$$\mathbb{C}/\mathbb{R} \simeq \mathbb{R}$$

— результат, уже полученный нами в примере 5.13.

Пример 7. Рассмотрим гомоморфизм

$$f\colon \mathbb{C}^* \to \mathbb{R}^*_+, \quad z \mapsto |z|.$$

Имеем $\operatorname{Im} f = \mathbb{R}^*_+$, $\operatorname{Ker} f = \mathbb{T} = \{z \in \mathbb{C}^* : |z| = 1\}$, так что

$$\mathbb{C}^*/\mathbb{T} \simeq \mathbb{R}^*_+$$

— результат, уже полученный нами в примере 5.14.

Пример 8. Отображение

$$f\colon \mathbb{C}^* \to \mathbb{T}, \quad z \mapsto \frac{z}{|z|},$$

также является гомоморфизмом, причем $\operatorname{Im} f = \mathbb{T}$, $\operatorname{Ker} f = \mathbb{R}^*_+$. Следовательно,

$$\mathbb{C}^*/\mathbb{R}^*_+ \simeq \mathbb{T}.$$

(Соответствующее разбиение на смежные классы было описана в примере 5.2.)

Пример 9. Аналогичным образом рассмотрение гомоморфизма $\det$ из примера 4 приводит к тому, что

$$GL_n(K)/SL_n(K) \simeq K^*$$

— результат, уже полученный в примере 5.15.

Пример 10. Рассмотрение гомоморфизма sgn из примера 5 приводит к тому, что

$$S_n/A_n \simeq C_2.$$

В частности, отсюда следует, что

$$|A_n| = \frac{1}{2}n!$$

Пример 11. Согласно определению (см. §2) всякое аффинное преобразование α есть произведение параллельного переноса и линейного преобразования φ. Последнее называется линейной частью, или дифференциалом преобразования α, и обозначается через $d\alpha$. Формула

$$(t_a\varphi)(t_b\psi) = t_{a+\varphi(b)}\,\varphi\psi,$$

полученная при доказательстве предложения 2.1, показывает, что отображение

$$d\colon GA(V) \to GL(V), \quad \alpha \mapsto d\alpha,$$

является гомоморфизмом. Очевидно, что

$$\operatorname{Im} d = GL(V), \quad \operatorname{Ker} d = \operatorname{Tran}(V),$$

так что

$$GA(V)/\operatorname{Tran}(V) \simeq GL(V).$$

Пример 12. Пусть $\triangle = A_1A_2A_3$ — правильный треугольник. Сопоставив каждому движению $\varphi \in \operatorname{Sym}\triangle$ подстановку $\sigma \in S_3$ по правилу

$$\varphi(A_i) = A_{\sigma(i)},$$

мы получим гомоморфизм

$$f\colon \operatorname{Sym}\triangle \to S_3.$$

Поскольку всякое движение плоскости, оставляющее на месте 3 точки, не лежащие на одной прямой, тождественно, $\operatorname{Ker} f = \{\mathrm{id}\}$. Докажем, что $\operatorname{Im} f = S_3$. Так как $\operatorname{Im} f$ — подгруппа группы S_3 и группа S_3 порождается транспозициями, то достаточно проверить, что любая транспозиция принадлежит $\operatorname{Im} f$, т. е. может быть осуществлена некоторым движением $\varphi \in \operatorname{Sym}\triangle$. Но это действительно так: например, транспозиция (12) осуществляется отражением относительно прямой l, показанной на рис. 24. Таким образом,

$$\operatorname{Sym}\triangle \simeq S_3.$$

Аналогично доказывается, что группа симметрии правильного тетраэдра изоморфна S_4 (проделайте это!).

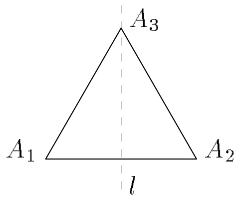

Рис. 24.

Пример 13. При перестановках переменных x_1, x_2, x_3, x_4 многочлены

$$x_1x_2 + x_3x_4,\ x_1x_3 + x_2x_4,\ x_1x_4 + x_2x_3 \tag{87}$$

переставляются между собой. Занумеровав их каким-либо образом, мы получим гомоморфизм

$$f\colon S_4 \to S_3.$$

Докажем, что $\operatorname{Im} f = S_3$. Для этого достаточно проверить, что любая транспозиция многочленов (87) может быть осуществлена некоторой перестановкой x_1, x_2, x_3, x_4. Но это действительно так: например, транспозиция первых двух многочленов (87) может быть осуществлена транспозицией x_2 и x_3.

Задача 2. Доказать, что для любого $n \in \mathbb{N}$ имеет место следующий «парадоксальный» изоморфизм:

$$\mathbb{C}^*/C_n \simeq \mathbb{C}^*.$$

Задача 3. Пусть p — простое число. Найти порядки групп $GL_2(\mathbb{Z}_p)$ и $SL_2(\mathbb{Z}_p)$.

Очевидно, что композиция гомоморфизмов $F \to G$ и $G \to H$ есть гомоморфизм $F \to H$.

Пример 14. Рассмотрим композицию гомоморфизмов

$$\det\colon GL_n(\mathbb{R}) \to \mathbb{R}^* \quad \text{и} \quad \operatorname{sgn}\colon \mathbb{R}^* \to C_2 = \{\pm 1\},$$

где sgn обозначает знак действительного числа. Мы получим таким образом гомоморфизм

$$\varepsilon\colon GL_n(\mathbb{R}) \to C_2.$$

При $n = 2$ он имеет следующий геометрический смысл: если $\varepsilon(A) = 1$ (соотв. $\varepsilon(A) = -1$), то линейное преобразование пространства E^2, определяемое матрицей A, сохраняет (соотв. меняет) ориентацию в том смысле, что любой положительно ориентированный базис оно переводит в положительно (соотв. отрицательно) ориентированный базис. Аналогичная интерпретация возможна и при $n = 3$.

Пример 15. Композиция гомоморфизмов

$$d\colon GA(\mathbb{R}^n) \to GL(\mathbb{R}^n) = GL_n(\mathbb{R}) \quad \text{и} \quad \varepsilon\colon GL_n(\mathbb{R}) \to C_2$$

есть гомоморфизм

$$GA(\mathbb{R}^n) \to C_2. \tag{88}$$

При $n = 2$ и 3 это позволяет распространить на аффинные преобразования евклидовой плоскости и евклидова пространства понятие сохранения или изменения ориентации. А именно, аффинное преобразование сохраняет (соотв. меняет) ориентацию, если его дифференциал сохраняет (соотв. меняет) ориентацию. В частности, можно говорить о движениях, сохраняющих или меняющих ориентацию (что мы уже делали раньше, не давая точного определения).

Пример 16. Пусть $G \subset \operatorname{Isom} E^n$ ($n = 2$ или 3) — какая-либо подгруппа, содержащая движения, меняющие ориентацию. Рассматривая ограничение на G гомоморфизма (88), мы получаем, что подмножество движений из G, сохраняющих ориентацию, есть подгруппа индекса 2. Мы будем обозначать эту подгруппу через G_+.

Пример 17. В частности, подгруппу $\operatorname{Sym}_+ K \subset \operatorname{Sym} K$ будем называть группой вращений куба K. Так как $|\operatorname{Sym} K| = 48$ (см. пример 5.10), а $\operatorname{Sym}_+ K$ есть подгруппа индекса 2, то

$$|\operatorname{Sym}_+ K| = 24.$$

Докажем, что

$$\operatorname{Sym}_+ K \simeq S_4.$$

Для этого занумеруем каким-либо образом 4 диагонали куба K и сопоставим каждому движению $\varphi \in \operatorname{Sym}_+ K$ подстановку, осуществляемую им на множестве диагоналей. Мы получим гомоморфизм

$$f\colon \operatorname{Sym}_+ K \to S_4.$$

Докажем, что $\operatorname{Im} f = S_4$, откуда уже будет следовать, что f — изоморфизм, поскольку $|\operatorname{Sym}_+ K| = |S_4|$. Для этого достаточно проверить, что любая транспозиция принадлежит $\operatorname{Im} f$.

Но это действительно так: например, транспозиция (12) осуществляется поворотом на π вокруг прямой l, изображенной на рис. 25.

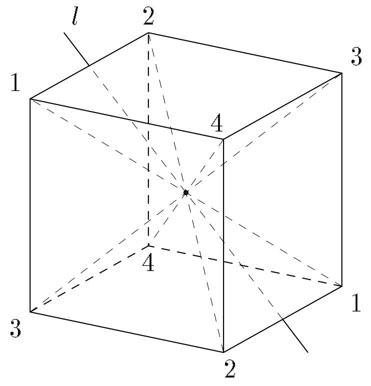

Рис. 25.

Задача 4. Доказать, что группа D_4 (группа симметрии квадрата) изоморфна группе $\mathrm{Sym}(x_1x_2 + x_3x_4)$ (см. примеры 1.8 и 5.11).

Задача 5. Доказать, что $SL_2(\mathbb{Z}_2) \simeq S_3$.