§4. Абстрактные группы и гомоморфизмы.

4.1. Гомоморфизмы групп. Отображение групп $G \xrightarrow{\varphi} H$ называется *гомоморфизмом*, если оно переводит композицию преобразований в композицию, т. е. для любых двух преобразований $g_1, g_2 \in G_1$ в группе G_2 выполняется соотношение $\varphi(g_1 \circ g_2) = \varphi(g_1) \circ \varphi(g_2)$. Начиная с этого момента термины *эпиморфизм*, *мономорфизм* и *изоморфизм* применительно к отображениям групп будут для нас по умолчанию означать, что отображение, к которому они относятся, является *гомоморфизмом*. В частности, $\mathrm{Aut}\,(G)$ будет обозначать множество всех биективных гомоморфизмов из G в себя, $\mathrm{Hom}(G,H)$ — множество всевозможных гомоморфизмов из G в H и т. д. Если же мы захотим рассматривать не только гомоморфные, но любые отображения, мы будем писать $\mathrm{Aut}_{\,\mathrm{set}}(G)$, $\mathrm{Hom}_{\mathrm{set}}(G,H)$, где индекс set показывает, что в данном контексте группы рассматриваются просто как множества, без учёта композиции.

Наличие между группами изоморфизма означает, что эти группы можно отождествить друг с другом с сохранением таблицы умножения элементов. Простейшими примерами таких изоморфизмов являются построенные в (n° 2.1.4), (n° 2.1.5) отождествления группы треугольника с симметрической группой $\mathfrak{S}_3$ и полной группы тетраэдра с $\mathfrak{S}_4$, а также отождествления бесконечной циклической группы с группой сдвигов, конечной циклической группы — с группой поворотов (см. (n° 3.3.3)), а конечной группы, порождённой двумя инволюциями, — с группой диэдра (см. (n° 3.3.5)). Вот ещё несколько примеров гомоморфизмов.

4.1.1. Пример: изоморфизм собственной группы куба с $\mathfrak{S}_4$. Собственная группа куба состоит из 24 поворотов (см. рис. 4◇1): тождественного, $3 \cdot 3 = 9$ поворотов на углы, кратные 90° вокруг осей, проходящих через центры противоположных граней, $4 \cdot 2 = 8$ поворотов на углы, кратные 120° вокруг диагоналей, соединяющих противоположные вершины, и 6 поворотов на 180° вокруг осей, проходящих через середины противоположных рёбер. Чтобы убедиться, что других собственных движений нет, достаточно рассмотреть действие группы куба на восьми его вершинах, составляющих, очевидно, одну орбиту, и воспользоваться формулой для длины орбиты (n° 3.1.3).

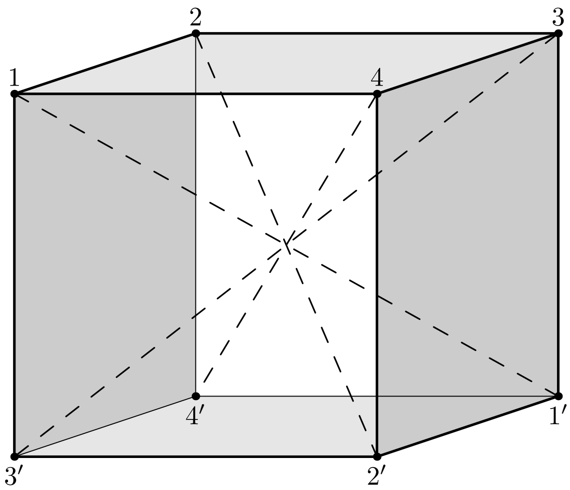

Рис. 4◇1. К действию группы куба на 4 диагонали (1, 2, 3, 4) и 3 пары противоположных граней (прозрачную, светлую, тёмную).

Упражнение 4.1. Убедитесь, что стабилизатор вершины в собственной группе куба состоит из трёх поворотов на углы, кратные 120°, вокруг проходящей через эту вершину внутренней диагонали куба.

Занумеруем теперь диагонали куба, соединяющие противоположные вершины (помеченные на рис. 4◇1 одинаковыми числами) соответствующими цифрами 1, 2, 3, 4 и сопоставим каждому вращению куба осуществляемую им перестановку диагоналей. Ясно, что мы получим гомоморфизм из собственной группы куба в симметрическую группу $\mathfrak{S}_4$. Он переводит 6 поворотов на $\pm 90°$ в 6 циклов длины 4 циклового типа , 8 поворотов на $\pm 120°$ — в 8 циклов длины 3 циклового типа , 3 поворота на $\pm 180°$ вокруг осей, проходящих через центры противоположных граней, — в 3 пары независимых транспозиций циклового типа , а 6 поворотов на 180° вокруг осей, проходящих через середины противоположных рёбер, — в 6 простых транспозиций циклового типа . Тем самым, собственная группа куба, как и полная группа тетраэдра, изоморфна симметрической группе $\mathfrak{S}_4$.

4.1.2. Пример: эпиморфизм $\mathfrak{S}_4 \twoheadrightarrow \mathfrak{S}_3$. Если в предыдущем примере вместо четырёх диагоналей куба рассмотреть три пары его противоположных граней (на рис. 4◇1 — прозрачную, светлую и тёмню) или, что то же самое — три отрезка, соединяющие центры противоположных граней, то сопоставляя каждому вращению куба осуществляемую им перестановку этих пар (соотв. отрезков) мы получим гомоморфизм из собственной группы куба в симметрическую группу $\mathfrak{S}_3$, состоящую из 6 элементов. Он эпиморфен, причём прообраз каждой перестановки из $\mathfrak{S}_3$ состоит в точности из четырёх поворотов куба:

тождественное преобразование и 3 поворота на $\pm 180^\circ$ вокруг осей, проходящих через центры противоположных граней, перейдут в тождественное отображение $\ydiagram{1,1,1}$, 8 поворотов на $\pm 120^\circ$ вокруг диагоналей перейдут в 2 цикла различных цикла $\ydiagram{1,1,1}$, а 6 поворотов на 180° вокруг осей, проходящих через середины противоположных рёбер и 6 поворотов на $\pm 90^\circ$ перейдут в транспозиции $\ydiagram{2,1}$.

Упражнение 4.2. Покажите, что тождественное преобразование куба и 3 поворота на $\pm 180^\circ$ вокруг осей, проходящих через центры противоположных граней, составляют в собственной группе куба подгруппу, изоморфную группе диэдра-двуугольника $\mathfrak{D}_2$, и что полные прообразы всевозможных элементов из $\mathfrak{S}_3$ относительно построенного в предыдущем примере (n° 4.1.2) эпиморфизма — это в точности смежные классы собственной группы куба по этой подгруппе.

Упражнение 4.3. Постройте сюрьективный гомоморфизм $\mathfrak{S}_3 \twoheadrightarrow \mathfrak{S}_2$.

4.1.3. Пример: знак перестановки. В этом примере мы построим *гомоморфизм знака*

$$\operatorname{sgn} : \mathfrak{S}_n \xrightarrow{g \mapsto \operatorname{sgn}(g)} \{\pm 1\}, \tag{4-1}$$

сопоставляющий каждой перестановке $g \in \mathfrak{S}_n$ её *знак* $\operatorname{sgn}(g) = \pm 1$ так, что

$$\forall\, g_1, g_2 \in \mathfrak{S}_n \quad \operatorname{sgn}(g_1 g_2) = \operatorname{sgn}(g_1)\operatorname{sgn}(g_2). \tag{4-2}$$

Напомним (см. (n° 3.3.5)), что мы называем цикл длины два $\langle i, j \rangle \in \mathfrak{S}_n$ (меняющий местами i-тый и j-тый элементы с сохранением на месте всех остальных) *транспозицией* элементов i и j. Согласно упр. 3.7 всякая перестановка может быть разложена в композицию транспозиций, причём сделать это можно многими разными способами. Нам бы хотелось задать гомоморфизм (4-1) требованиями $\operatorname{sgn}(\mathrm{Id}) = 1$ и $\operatorname{sgn}(\langle i, j \rangle) = -1\ \forall\, i \neq j$, а затем продолжить его на произведения транспозиций по формуле (4-2). Тогда все перестановки, представимые в виде композиции чётного числа транспозиций[1], будут иметь знак $+1$, а перестановки, раскладывающиеся в композицию нечётного числа транспозиций[2], получат знак -1, и свойство (4-2) будет автоматически выполнено. Однако, мы должны проверить, что такое построение не приведёт нас к противоречию: поскольку разложение перестановки в композицию транспозиций не единственно, следует убедиться, что никакая перестановка, являющаяся композицией чётного числа транспозиций, не может одновременно быть композицией нечётного числа транспозиций, и наоборот. Иными словами, нам надо доказать, что чётность числа транспозиций, на которые раскладывается произвольная перестановка $g \in \mathfrak{S}_n$, зависит только от g, но не от способа разложения.

Для этого мы укажем способ отыскания чётности перестановки g, не использующий разложения g в композицию транспозиций. Назовём упорядоченную пару чисел (i, j), такую что $1 \leqslant i < j \leqslant n$, *инверсной парой* перестановки g, если $g(i) > g(j)$. Таким образом, мы разбиваем множество всех упорядоченных пар чисел $\{i < j\} \subset \{1, 2, \ldots, n\}$ (состоящее из $n(n-1)/2$ элементов) на два непересекающихся подмножества, образованные, соответственно, инверсными и неинверсными парами, причём это разбиение зависит только от g, «ничего не зная» про то, каким образом g раскладывается в произведение транспозиций.

Покажем теперь, что чётность числа инверсных пар произвольной перестановки совпадает с чётностью количества транспозиций, на которые её можно разложить. Для этого вначале проверим, что при композиции произвольной перестановки g с произвольной транспозицией $\langle i, j \rangle$ чётность числа инверсных пар меняется. Перестановки g и $g \circ \langle i, j \rangle$ отличаются друг от друга перестановкой элементов $g_i = g(i)$ и $g_j = g(j)$, стоящих на i-том и j-том местах в нашей стандартной записи перестановки g словом:

$$\begin{aligned} g &= (g_1, \ldots, g_{i-1}, \boldsymbol{g_i}, g_{i+1}, \ldots, g_{i-1}, \boldsymbol{g_j}, g_{j+1}, \ldots, g_n) \\ g \circ \langle i, j \rangle &= (g_1, \ldots, g_{i-1}, \boldsymbol{g_j}, g_{i+1}, \ldots, g_{i-1}, \boldsymbol{g_i}, g_{j+1}, \ldots, g_n)\,. \end{aligned} \tag{4-3}$$

Упражнение 4.4. Проверьте, что у двух перестановок (4-3) инверсность пары (i, j), а также $2(j - i - 1)$ пар вида (i, m) и (m, j) с произвольным m из промежутка $i < m < j$ противоположна[3], а инверсность всех остальных пар одинакова.

Тем самым, количество инверсных пар в этих перестановках разнится на нечётное число, и стало быть, мы показали, что композиция с транспозицией изменяет чётность числа инверсных пар. Если представить теперь перестановку g в виде композиции транспозиций:

$$g = \langle i_1, j_1 \rangle \circ \langle i_2, j_2 \rangle \circ \cdots \circ \langle i_k, j_k \rangle = \mathrm{Id} \circ \langle i_1, j_1 \rangle \circ \langle i_2, j_2 \rangle \circ \cdots \circ \langle i_k, j_k \rangle$$

[1] такие перестановки называются *чётными*

[2] такие перестановки называются *нечётными*

[3] т. е. если были инверсными в g, то являются неинверсными в $g \circ \langle i, j \rangle$ и наоборот, если были неинверсными в g, то стали инверсными в $g \circ \langle i, j \rangle$

то чётность числа инверсных пар в ней будет отличаться от нуля (равного чётности числа инверсных пар в тождественной перестановке) в точности на чётность числа k. Следовательно, чётность числа транспозиций, на которые раскладывается g, равна чётности числа инверсных пар перестановки g, и стало быть, не зависит от способа разложения.

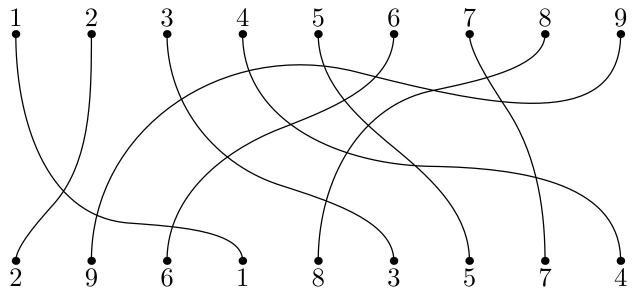

Рис. 4◇2. $\mathrm{sgn}(2,\,9,\,6,\,1,\,8,\,3,\,5,\,7,\,4) = +1$ (всего 18 пересечений)

Интерпретация чётности перестановки как чётности числа инверсных пар даёт практический способ отыскания чётности, известный как *правило ниточек*. А именно, напишем друг под другом исходные числа $1,\,2,\,\dots\,,n$ и их перестановку $g = (g_1, g_2, \dots, g_n)$ и соединим одинаковые числа нитями так, чтобы ни одна из нитей не вылезала изнутри четырёхугольника $1\,n\,g_n\,g_1$ (см. рис. 4◇2) и чтобы все точки пересечения нитей были простыми двойными[1]. Тогда чётность числа инверсных пар будет равна чётности числа точек пересечения нитей.

Упражнение 4.5. Докажите это и найдите при помощи правила ниточек чётность *тасующей перестановки* $(i_1, i_2, \dots, i_k,\, j_1, j_2, \dots, j_m)$, в которой наборы номеров $\{i_\nu\}, \{j_\mu\} \subset \{1,\,2,\,\dots\,,n\}$ не пересекаются, и каждый из них строго возрастают слева направо.

Другим эффективным способом отыскания чётности является разложение перестановки в композицию независимых циклов (см. n° 3.2).

Упражнение 4.6. Докажите, что перестановка чётна тогда и только тогда, когда количество циклов чётной длины в её цикловом типе чётно.

Например для перестановки с рис. 4◇2 получаем $(2,\,9,\,6,\,1,\,8,\,3,\,5,\,7,\,4) = \langle 1,\,2,\,9,\,4\rangle \circ \langle 3,\,6\rangle \circ \langle 5,\,8,\,7\rangle$, откуда тоже видно, что она чётна.

4.2. Знакопеременные группы $\mathfrak{A}_n \subset \mathfrak{S}_n$. Чётные перестановки образуют в симметрической группе $\mathfrak{S}_n$ подгруппу порядка $n!/2$. В самом деле, обратная к чётной подстановке подстановка также чётна, поскольку её разложение в произведение транспозиций будет состоять ровно из тех же самых транспозиций, но записанных в обратном порядке:

Упражнение 4.7. Докажите следующую формулу для вычисления обратного элемента к произведению:
$$(g_1 g_2 \,\cdots\, g_k)^{-1} = g_k^{-1} \,\cdots\, g_2^{-1} g_1^{-1}\,.$$

Композиция чётных перестановок также, очевидно, чётна. Таким образом, чётные перестановки действительно составляют подгруппу. Поскольку для любых двух нечётных перестановок $g_1,\, g_2$ перестановка $g_1 g_2^{-1}$ является чётной, все нечётные перестановки лежат в одном смежном классе этой подгруппы. Таким образом, вся группа перестановок представляет собой объединение в точности двух смежных классов, и так как смежные классы состоят из одинакового числа элементов, чётных и нечётных перестановок имеется поровну.

По историческим причинам, которые мы обсудим позже, когда будем изучать теорию Галуа, подгруппа чётных подстановок называется *знакопеременной группой* и обозначается[2] $\mathfrak{A}_n \subset \mathfrak{S}_n$.

Упражнение 4.8. Убедитесь, что при изоморфизме полной группы тетраэдра с $\mathfrak{S}_4$, построенном в примере (n° 2.1.5), собственная подгруппа тетраэдра отождествляется со знакопеременной подгруппой $\mathfrak{A}_4 \subset \mathfrak{S}_4$.

[1] это означает, что в каждой точке пересечения встречается ровно две нити, причём пересечение происходит трансверсально: , а не по касательной:

[2] готическая буква «A», участвующая в этом обозначении, происходит от *alternate*

4.2.1. Пример: эпиморфизм группы додекаэдра на $\mathfrak{A}_5$. Знакопеременная группа $\mathfrak{A}_5$ допускает геометрическую реализацию, похожую на геометрическую реализацию группы $\mathfrak{A}_4$ из упр. 4.8. На поверхности додекаэдра (см. рис. 4◇3) можно нарисовать ровно 5 кубов с вершинами в вершинах додекаэдра.

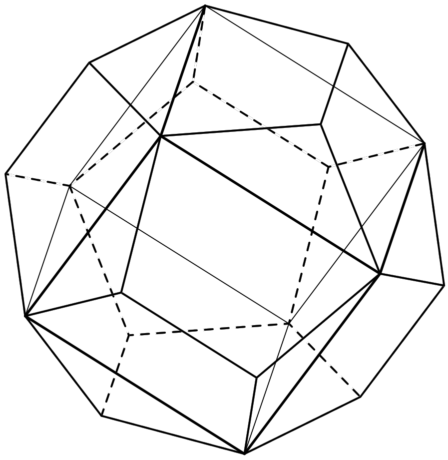

Рис. 4◇3. Один из пяти кубов, лежащих на додекаэдре.

Упражнение 4.9. Докажите, что восьмивершинный шестигранник, образованный изображёнными на рис. 4◇3 двенадцатью диагоналями граней додекаэдра, действительно является кубом, и убедитесь, что таких кубов и в самом деле пять.

Занумеруем эти кубы цифрами 1, 2, 3, 4, 5 и сопоставим каждому движению из группы додекаэдра осуществляемую им перестановку кубов. Мы получим гомоморфизм из группы додекаэдра в симметрическую группу $\mathfrak{S}_5$. Легко видеть, что образами 60 поворотов (ср. с (n° 2.1.6)) при этом будут в точности 60 чётных перестановок: $6 \cdot 4 = 24$ поворота на углы $2\pi k/5$ с $k = 1, 2, 3, 4$ вокруг осей, проходящих через центры противоположных граней додекаэдра, реализуют всевозможные циклы длины 5 (т. е. все 24 перестановки циклового типа), $10 \cdot 2 = 20$ поворотов на углы $\pm 2\pi/3$ вокруг осей, проходящих через противоположные вершины додекаэдра, реализуют всевозможные циклы длины 3 (т. е. все 20 перестановок циклового типа), 15 поворотов на 180° вокруг осей, проходящих через середины противоположных рёбер додекаэдра, реализуют всевозможные пары независимых транспозиций (т. е. все 10 перестановок циклового типа); наконец, тождественное преобразование перейдёт в тождественную перестановку. Согласно (n° 2.1.6) собственная группа додекаэдра исчерпывается шестьюдесятью перечисленными поворотами, а значит, построенный нами гомоморфизм устанавливает изоморфизм между собственной группой додекаэдра и знакопеременной группой $\mathfrak{A}_5$.

Однако в отличие от примера (n° 2.1.5) и упр. 4.8 переход от собственной группы к полной в случае додекаэдра не добавляет никаких новых перестановок кубов. В самом деле, по теореме Лагранжа полная группа додекаэдра G представляет собою объединение двух смежных классов: $G = H \sqcup gH$, где $H \subset G$ — подгруппа собственных движений, а $g \in G \smallsetminus H$ — любое несобственное движение. Беря в качестве g центральную симметрию относительно центра додекаэдра, переводящую каждый из кубов в себя, мы заключаем, что образ гомоморфизма $G \longrightarrow \mathfrak{S}_5$ совпадает с образом гомоморфизма $H \longrightarrow \mathfrak{S}_5$ и равен $\mathfrak{A}_5$. При этом прообраз каждой перестановки $g \in \mathfrak{A}_5$ состоит из одного из перечисленных выше поворотов и композиции этого поворота с центральной симметрией додекаэдра.

Упражнение 4.10*. Покажите, что симметрическая группа $\mathfrak{S}_5$ не изоморфна полной группе додекаэдра.

4.3. Абстрактные группы. Изоморфные группы преобразований, действующие на разных множествах, имеют одинаковую таблицу умножения, и поэтому любое алгебраическое соотношение на композиции преобразований, справедливое в одной из них, будет справедливо для соответствующих композиций и в другой. Чтобы иметь возможность точно формулировать и изучать такие соотношения не прибегая к явной реализации группы в виде совокупности конкретных симметрий того-или иного объекта, удобно ввести абстрактное понятие группы.

А именно, будем называть (*абстрактной*) *группой* произвольное множество G, на котором задана операция $G \times G \longrightarrow G$, сопоставляющая каждой паре элементов $(g_1, g_2) \in G \times G$ некоторый элемент $g_1 g_2 \in G$, так что при этом выполняются следующие три свойства:

$$(fg)h = f(gh) \quad \forall\, f, g, h \in G \qquad (\textit{ассоциативность}) \tag{4-4}$$

$$\exists\, e \in G \, : \, eg = ge = g \quad \forall\, g \in G \qquad (\textit{существование единицы}) \tag{4-5}$$

$$\forall\, g \in G \quad \exists\, g^{-1} \in G \, : \, gg^{-1} = g^{-1}g = e \quad \forall\, g \in G \qquad (\textit{существование обратного}) \tag{4-6}$$

Элемент e, существование которого постулируется в (4-5), автоматически единственен, поскольку для любых двух таких элементов e и e' выполняются равенства $e' = e'e'' = e''$. Как мы видели в n° 1.7.1, свойство (4-6) можно было бы ослабить до требования существования для каждого элемента $g \in G$ левого обратного f: $fg = e$ и правого обратного h: $gh = e$, не требуя при этом, чтобы они совпадали друг с другом — их совпадение будет автоматически следовать из выкладки $f = fe = f(gh) = (fg)h = eh = h$, которая заодно показывает, что обратный элемент

$g^{-1} = f = h$ единственен (для заданного g). Минимизировать набор условий, определяющих группу можно и дальше.

Упражнение 4.11. Любителям формальных выкладок предлагается убедиться, что в условии (4-5) достаточно требовать существования одной только левой единицы (т. е. такого элемента e, что $eg = g$ $\forall\, g \in G$), а в условии (4-6) — существования одного только левого обратного (решение можно подглядеть в сноске ([1])).

4.4. Реализация абстрактной группы группой преобразований. Всякая группа преобразований, рассматриваемая как множество отображений с операцией композиции, является абстрактной группой. Наоборот, для всякой абстрактной группы G можно строить гомоморфизмы $G \xrightarrow{\varphi} \mathrm{Aut}\,(X)$ в группы автоморфизмов различных множеств, позволяющие интерпретировать элементы абстрактной группы как отображения. Всякий такой гомоморфизм φ называется *представлением* (абстрактной) группы G автоморфизмами множества X или *действием* группы G на множестве X. Представление называется *точным*, если оно инъективно. В этом случае группу G можно отождествить с группой преобразований $\varphi(G) \subset \mathrm{Aut}\,(X)$.

4.4.1. Левое регулярное представление. Примером точного представления является *левое регулярное представление*, в котором в качестве X выступает сама группа G, рассматриваемая как множество. Это представление сопоставляет каждому элементу $g \in G$ отображение

$$\lambda_g : G \xrightarrow{h \mapsto gh} G\,, \tag{4-7}$$

умножающее все элементы группы G слева на g. Отображение λ_g биективно, поскольку отображение $\lambda_{g^{-1}} : G \xrightarrow{h \mapsto g^{-1}h} G$ является для него двусторонним обратным:

$$\forall\, h \in G \quad \lambda_g \lambda_{g^{-1}}(h) = \lambda_g(g^{-1}h) = gg^{-1}h = h \quad \text{и} \quad \lambda_{g^{-1}}\lambda_g(h) = \lambda_{g^{-1}}(gh) = g^{-1}gh = h\,.$$

Таким образом, мы получаем отображение[2]

$$\lambda : G \xrightarrow{g \mapsto \lambda_g} \mathrm{Aut}_{\,\mathrm{set}}(G)\,. \tag{4-8}$$

Оно является гомоморфизмом групп, т. е. переводит произведение в произведение:

$$\lambda_{g_1 g_2} = \lambda_{g_1}\lambda_{g_2}\,, \quad \text{т. к.} \;\; \forall\, h \in G \;\; \lambda_{g_1 g_2}(h) = g_1 g_2 h = \lambda_{g_1}(g_2 h) = \lambda_{g_1}\left(\lambda_{g_2}(h)\right) = \lambda_{g_1}\lambda_{g_2}(h)\,.$$

Этот гомоморфизм инъективен, ибо при $g_1 \neq g_2$ преобразования λ_{g_1} и λ_{g_2} различны: если $\lambda_{g_1}(h) = \lambda_{g_2}(h)$ хотя бы для одного $h \in G$, то умножая равенство $g_1 h = g_2 h$ справа на h^{-1}, мы получаем $g_1 = g_2$.

4.4.2. Правое регулярное представление. Наряду с левым регулярным представлением можно рассматривать *правое регулярное представление*

$$\varrho : G \xrightarrow{g \mapsto \varrho_g} \mathrm{Aut}_{\,\mathrm{set}}(G)\,,$$

которое сопоставляет каждому элементу $g \in G$ отображение ϱ_g правого умножения на g^{-1}:

$$\varrho_g : G \xrightarrow{h \mapsto hg^{-1}} G\,. \tag{4-9}$$

[1] РЕШЕНИЕ: пусть g^{-1} означает (какой-нибудь) левый обратный к g, а e — (какую-нибудь) левую единицу; тогда по их определению $g^{-1}gg^{-1} = eg^{-1} = g^{-1}$; умножая правую и левую часть слева на левый обратный к g^{-1}, получаем $gg^{-1} = e$, т. е. что g^{-1} автоматически является и правым обратным к g элементом; теперь легко увидеть, что e является также и правой единицей: $ge = g(g^{-1}g) = (gg^{-1})g = eg = g$

[2] напомним, что индекс set в обозначении $\mathrm{Aut}_{\,\mathrm{set}}(G)$ указывает на то, что мы рассматриваем произвольные биекции, не обязательно согласованные с композицией в G; отображение λ_g, как правило, *не является гомоморфизмом*, т. к. $\lambda_g(h_1h_2) = gh_1h_2$ обычно не равно $\lambda_g(h_1)\lambda_g(h_2) = gh_1gh_2$

Появление минус первой степени вызвано тем, что именно именно так заданное отображение ϱ будет являться гомоморфизмом групп, т. е. переводить произведение g_1g_2 в композицию $\varrho_{g_1}\varrho_{g_2}$:

$$\forall\, h\in G \;\; \varrho_{g_1g_2}(h) = h(g_1g_2)^{-1} = hg_2^{-1}g_1^{-1} = \varrho_{g_1}(hg_2^{-1}) = \varrho_{g_1}\left(\varrho_{g_2}(h)\right) = \varrho_{g_1}\varrho_{g_2}(h)\,,$$

тогда как наивное правило, которое мы обозначим $\varrho'_g : h \longmapsto hg$, удовлетворяло бы соотношению

$$\varrho'_{g_1g_2} = \varrho'_{g_2}\varrho'_{g_1}\,, \quad \text{т. к.} \;\; \forall\, h\in G \;\; \varrho'_{g_1g_2}(h) = hg_1g_2 = \varrho'_{g_2}(hg_1) = \varrho'_{g_2}\left(\varrho'_{g_1}(h)\right) = \varrho'_{g_2}\varrho'_{g_1}(h)\,,$$

т. е. переводило бы произведение в произведение, записанное в противоположном порядке[1].

Упражнение 4.12. Убедитесь в том, что отображение $G \xrightarrow{\varrho_g} G$ биективно $\forall\, g\in G$ и что $\varrho_{g_1} \neq \varrho_{g_2}$ при $g_1 \neq g_2$.

4.4.3. Пример: числовые группы. Хорошо знакомыми примерами абстрактных групп являются числовые множества $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ с операцией сложения[2]. При помощи левого регулярного представления из n° 4.4 мы можем воспринимать эти группы как группы сдвигов числовой прямой: каждое число $g \in \mathbb{R}$ в левом регулярном представлении превращается в преобразование сдвига $g : \mathbb{R} \xrightarrow{x\mapsto g+x} \mathbb{R}$. Аналогично, все ненулевые числа из $\mathbb{Q}$ и $\mathbb{R}$ являются группами с операцией умножения[3]. В этом случае левое регулярное представление интерпретирует каждое ненулевое число g как гомотетию[4] $g : \mathbb{R} \xrightarrow{x\mapsto gx} \mathbb{R}$. Рассмотренное в n° 4.1.3 множество знаков $\{\pm 1\}$ также является группой относительно операции умножения. Все эти группы замечательны тем, что (как и в группе поворотов из примера (n° 2.1.2)) их групповая операция помимо свойств (4-4)–(4-6) обладает ещё одним дополнительным свойством:

$$\forall\, g_1, g_2 \in G \quad g_1g_2 = g_2g_1 \qquad\qquad (\textit{коммутативность}) \tag{4-10}$$

Группы с коммутативной операцией называются *коммутативными* или *абелевыми*.

Упражнение 4.13. Проверьте, что из диэдральных групп и групп правильных многогранников абелевой является только группа двуугольника $\mathfrak{D}_2$ (ср. с упр. 4.2).

4.5. Подгруппы абстрактных групп. Непустое подмножество $H \subset G$ (абстрактной) группы G называется *подгруппой* в G, если обратные ко всем элементам из H, а также произведения любых двух элементов из H тоже лежат в H. Как и в (n° 2.1) из этих условий вытекает, что единица группы G лежит в H, поскольку $e = hh^{-1}$ для произвольно взятого $h \in H$.

Упражнение 4.14. Докажите, что подмножество H в группе G является подгруппой тогда и только тогда, когда $\forall\, h_1, h_2 \in H \;\, h_1h_2^{-1} \in H$.

Для подгрупп абстрактных групп справедливы все факты, установленные нами в §2 для подгрупп групп преобразований. А именно, с каждой подгруппой $H \subset G$ можно связать два разбиения группы G: в дизъюнктное объединение левых смежных классов[5] $gH = \{gh \mid h \in H\}$ и

---

[1]Отображение групп $G \xrightarrow{\psi} G'$, удовлетворяющее $\forall\; g_1, g_2 \in G_1$ условию $\psi(g_1g_2) = \psi(g_2)\psi(g_1)$ называется *антигомоморфизмом* Тут уместно сделать следующее

Важное отступление об обозначениях.

В алгебраической литературе равноправно употребляются две системы обозначений для композиции отображений. Обозначение, которое было введено нами в (n° 1.6) и которому мы всё время будем следовать, называется *левым действием*, поскольку в нём отображения применяются к своим аргументам слева и перемножаются справа налево: $fg(x) \overset{\text{def}}{=} f(g(x))$, $fgh(x) \overset{\text{def}}{=} f(g(h(x)))$, и т. д. Другая система обозначений — так называемое *правое действие* — определяет композицию так, что отображения применяются к своим аргументам справа и перемножаются слева направо: $[fg]_{\text{прав}} : x \overset{f}{\longmapsto} f(x) \overset{g}{\longmapsto} g(f(x))$, $[fgh]_{\text{прав}} : x \overset{f}{\longmapsto} f(x) \overset{g}{\longmapsto} g(f(x)) \overset{h}{\longmapsto} f(g(f(x)))$, и т. д. Следовать «правой» системе обозначений левое и правое регулярные представления пришлось бы задавать формулами, противоположными нашим, т. е. обращать g в левом регулярном представлении, и использовать само g, а не g^{-1} в правом. В этих записках мы практически никогда не будем использовать «правых» обозначений, но читатель, поглядывающий в другие учебники, должен следить за тем, какой стиль в них принят, и при необходимости переводить с правого языка на левый и наоборот.

[2]отметим, что натуральные числа группы не образуют

[3]на сей раз не только натуральные числа, но и целые числа не будут образовывать такой группы

[4]физики любят называть такие преобразования *пересκалированиями*

[5]напомним (см. n° 2.2 и упр. 2.12), что любые два левых смежных класса либо не пересекаются, либо совпадают

в дизъюнктное объединение правых смежных классов[1] $Hg = \{hg \mid h \in H\}$, причём каждый из этих классов будет биективен подгруппе H. Для любой конечной группы G выполняется теорема Лагранжа:

$$|G/H| = [G : H] = |G|/|H| = |H\backslash G| ,$$

где через G/H и $H\backslash G$ обозначены множества левых и правых смежных классов соответственно. С каждым элементом $g \in G$ можно связать циклическую подгруппу, образованную всеми целыми степенями g. Для конечной группы G эта подгруппа также будет конечна: $\langle g\rangle = \{1, g, g^2, \dots , g^{n-1}\} \subset G$, где $n = |\langle g\rangle|$ равно наименьшему натуральному числу, для которого $g^n = e$. Это число называется ***порядком*** элемента g. По теореме Лагранжа порядок любого элемента нацело делит порядок группы $|G|$. В частности, $\forall\, g\in G \;\; g^{|G|} = e$. Всё это доказывается либо непосредственным повторением рассуждений из предыдущего параграфа, либо точным представлением абстрактной группы G автоморфизмами какого-нибудь множества[2].

Упражнение 4.15. Обязательно ещё раз переговорите для себя все доказательства из §2.

[1]напомним (см. n° 2.2.3), что любые два правых смежных класса также либо не пересекаются, либо совпадают

[2]любое гомоморфное вложение $G \hookrightarrow \mathrm{Aut}\,(X)$ (скажем, левое регулярное представление (n° 4.4.1)) превращает все перечисленные выше факты в уже доказанные нами в §2 результаты о подгруппах групп преобразований