§3. Орбиты.

3.1. Орбиты. Орбитой точки $x \in X$ относительно группы преобразований $G \subset \mathrm{Aut}\,(X)$ называется множество

$$G(x) \stackrel{\text{def}}{=} \{g(x) \mid g \in G\}\,,$$

состоящее из всех точек, которые можно получить из точки x, применяя к ней всевозможные преобразования из группы G. Заметим, что орбиты двух различных точек $x_1, x_2 \in X$ или не пересекаются или совпадают. В самом деле, если $g_1(x_1) = g_2(x_2)$ для некоторых $g_1, g_2 \in G$, то $x_1 = g_1^{-1}g_2(x_2)$, и стало быть, $G(x_1) \subset G(x_2)$. Вместе с тем $g_2^{-1}g_1(x_1) = x_2$, и поэтому $G(x_2) \subset G(x_1)$. Мы приходим к такому выводу:

3.1.1. ПРЕДЛОЖЕНИЕ. *Произвольное множество X, на котором действует произвольная группа преобразований $G \subset \mathrm{Aut}\,(X)$, разбивается в дизъюнктное объединение орбит.* □

3.1.2. Длины орбит. Разбиение множества X на орбиты устроено не так регулярно, как разбиение группы на смежные классы, и разные орбиты могут состоять из разного числа точек. Количество точек в орбите (если оно конечно) называется *длиной* этой орбиты.

Чтобы найти длину орбиты $G(x)$ произвольно заданной точки $x \in X$, заметим, что преобразования $g \in G$, которые переводят точку x в себя, образуют в группе G подгруппу

$$\mathrm{Stab}(x) \stackrel{\text{def}}{=} \{f \in G \mid f(x) = x\} \subset G\,.$$

Эта подгруппа называется *стабилизатором* точки x. Преобразования, переводящие точку x в точку $y = g(x) \in G(x)$ (лежащую в той же орбите, что и x) составляют смежный класс $g \cdot \mathrm{Stab}(x)$ этой подгруппы. В самом деле, если $f(x) = x$, то $gf(x) = y$, и наоборот, если $h(x) = y$, то h записывая h в виде $g \cdot g^{-1} \cdot h = g(g^{-1} \cdot h)$ мы будем иметь $g^{-1}h \in \mathrm{Stab}(x)$, поскольку $g^{-1}h(x) = g^{-1}(y) = x$.

Упражнение 3.1. Проверьте, что построенное нами соответствие $g(x) \leftrightsquigarrow g \cdot \mathrm{Stab}(x)$ задаёт биекцию между точками орбиты $G(x)$ и смежными классами подгруппы $\mathrm{Stab}(x)$.

Таким образом, длина орбиты $G(x)$ точки $x \in X$ равна индексу $[G : \mathrm{Stab}(x)]$ её стабилизатора. Из теоремы Лагранжа (n° 2.2.1) вытекает:

3.1.3. СЛЕДСТВИЕ (ФОРМУЛА ДЛЯ ДЛИНЫ ОРБИТЫ). $|G(x)| = |G| : |\mathrm{Stab}(x)|$. □

3.1.4. Пример: ещё раз о порядках групп платоновых тел. Наше вычисление порядков групп пяти платоновых тел, а также порядка общей группы диэдра $\mathfrak{D}_n$ (см. примеры (n° 2.1.4)–(n° 2.1.6), было в сущности ни чем иным, как применением формулы для длины орбиты. В самом деле, все вершины платонова тела образуют одну орбиту группы G этого тела, и стабилизатор $\mathrm{Stab}(в_1)$ вершины 1 — это в точности рассматривавшийся нами класс C_1, откуда $|G| = |\mathrm{Stab}(в_1)| \cdot$ (число вершин). С тем же успехом в качестве точки x, через которую проходит орбита, можно было бы взять не вершину, а центр какой-нибудь грани, скажем, центр $г_1$ первой грани. Тогда мы могли бы вычислить порядок группы как $|G| = |\mathrm{Stab}(г_1)| \cdot$ (число граней). Обратите внимание, что орбиты $G(в_1)$ и $G(г_1)$ имеют разную длину.

Упражнение 3.2. Для каждого из пяти платоновых тел найдите длины орбит всех точек этого тела при действии на них собственной и несобственной группы тела. Есть ли среди орбит такие, длина которых равна порядку группы?

3.1.5. Пример: другой вывод явной формулы для мультиномиального коэффициента. Применим формулу для длины орбиты (n° 3.1.3) для подсчёта количества слов, которые можно получить переставляя буквы в слове

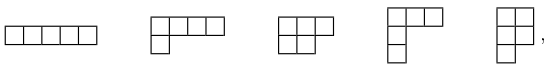
$$w = \underbrace{a_1, a_1, \ldots, a_1}_{m_1 \text{ букв } a_1}, \underbrace{a_2, a_2, \ldots, a_2}_{m_2 \text{ букв } a_2}, \ \ldots\ \ldots\ \ldots\ , \underbrace{a_k, a_k, \ldots, a_k}_{m_k \text{ букв } a_k}, \tag{3-1}$$

состоящем из $n = m_1 + m_2 + \cdots + m_k$ букв. Симметрическая группа $\mathfrak{S}_n$ действует на всевозможных n-буквенных словах перестановками букв. Искомое число — это в точности длина орбиты $\mathfrak{S}_n(w)$ слова (3-1)

относительно этого действия. Стабилизатор $\mathrm{Stab}(w)$ состоит из всевозможных перестановок одинаковых букв друг с другом и имеет порядок $|\mathrm{Stab}(w)| = m_1! \cdot m_2! \cdot \dots \cdot m_k!$. Поэтому

$$|\mathfrak{S}_n(w)| = |\mathfrak{S}_n| / |\mathrm{Stab}(w)| = \frac{(m_1 + m_2 + \dots + m_k)!}{m_1! \cdot m_2! \cdot \dots \cdot m_k!}\,.$$

3.1.6. Пример: раскладки соломинок по стаканам. Подсчитаем, сколькими способами можно разложить пять разноцветных соломинок по трём одинаковым стаканам, если требуется разложить все пять соломинок, но разрешается, чтобы некоторые из стаканов оставались пустыми. Будем обозначать цвета соломинок цифрами 1 , 2 , 3 , 4 , 5. На множестве всех раскладок действует симметрическая группа $\mathfrak{S}_5$, переставляющая соломинки между собою. Это действие не изменяет количества соломинок, находящихся в каждом из стаканов, и его орбиты взаимно однозначно соответствуют различным количественным распределениям соломинок по стаканам. Каждое количественное распределение удобно изображать диаграммой[1], на которой соломинки, находящиеся в одном стакане, рисуются полоской из клеток (число клеток равно числу соломинок), и эти полоски располагаются друг под другом в порядке убывания количества соломинок. В нашем случае получается 5 таких диаграмм[2]:



т. е. группа $\mathfrak{S}_5$ имеет 5 орбит, и каждая орбита состоит из всевозможных заполнений клеток соответствующей диаграммы цифрами 1 , 2 , 3 , 4 , 5 (каждая цифра используется ровно один раз). Стабилизатор раскладки, изображаемой такой заполненной цифрами диаграммой, состоит из всевозможных перестановок цифр, стоящих в одной строке (т. е. из произвольных перестановок соломинок внутри одного стакана), а также всевозможных перестановок между собою строк одинаковой длины (т. е. перестановок между собою стаканов, содержащих одинаковое число соломинок). Читателю предлагается убедиться, что

$$\left|\mathrm{Stab}\left(\begin{array}{|c|c|c|c|c|}\hline 1&2&3&4&5\\\hline\end{array}\right)\right| = 5! = 120 \qquad \left|\mathrm{Stab}\left(\begin{array}{|c|c|c|c|}\hline 1&2&3&4\\\hline 5\\\cline{1-1}\end{array}\right)\right| = 4! = 24 \cdot 1!$$

$$\left|\mathrm{Stab}\left(\begin{array}{|c|c|c|}\hline 1&2&3\\\hline 4&5\\\cline{1-2}\end{array}\right)\right| = 3! \cdot 2! = 12 \qquad \left|\mathrm{Stab}\left(\begin{array}{|c|c|c|}\hline 1&2&3\\\hline 4\\\cline{1-1} 5\\\cline{1-1}\end{array}\right)\right| = 3! \cdot 1! \cdot 1! \cdot 2! = 12$$

$$\left|\mathrm{Stab}\left(\begin{array}{|c|c|}\hline 1&2\\\hline 3&4\\\cline{1-2} 5\\\cline{1-1}\end{array}\right)\right| = 2! \cdot 2! \cdot 1! \cdot 2! = 8\,,$$

и длины соответствующих орбит, тем самым, равны

$$\left|\mathfrak{S}_5\left(\begin{array}{|c|c|c|c|c|}\hline 1&2&3&4&5\\\hline\end{array}\right)\right| = \frac{120}{120} = 1 \qquad \left|\mathfrak{S}_5\left(\begin{array}{|c|c|c|c|}\hline 1&2&3&4\\\hline 5\\\cline{1-1}\end{array}\right)\right| = \frac{120}{24} = 5$$

$$\left|\mathfrak{S}_5\left(\begin{array}{|c|c|c|}\hline 1&2&3\\\hline 4&5\\\cline{1-2}\end{array}\right)\right| = \frac{120}{12} = 10 \qquad \left|\mathfrak{S}_5\left(\begin{array}{|c|c|c|}\hline 1&2&3\\\hline 4\\\cline{1-1} 5\\\cline{1-1}\end{array}\right)\right| = \frac{120}{12} = 10$$

$$\left|\mathfrak{S}_5\left(\begin{array}{|c|c|}\hline 1&2\\\hline 3&4\\\cline{1-2} 5\\\cline{1-1}\end{array}\right)\right| = \frac{120}{8} = 15\,.$$

Итого, имеется 41 способ раскладки пяти разных соломинок по трём одинаковым стаканам.

3.2. Цикловой тип перестановки. Пусть $X = \{1, 2, \dots, n\}$ и $g \in \mathfrak{S}_n = \mathrm{Aut}(X)$ — какая-то перестановка. Применяя автоморфизм g к произвольному элементу $x \in X$, мы получим последовательность точек

$$x \overset{g}{\longmapsto} g(x) \overset{g}{\longmapsto} g^2(x) \overset{g}{\longmapsto} g^3(x) \overset{g}{\longmapsto} \dots\,.$$

[1] такие диаграммы называют *диаграммами Юнга*

[2] на первой диаграмме все соломинки попали в один стакан; на второй: четыре — в один, и ещё одна — в другой, на третьей: три — в один, две — в другой; на четвёртой: три — в один, и ещё по одной — в два оставшихся стакана; на последней: по две — в два стакана, и одна — в третий

В силу конечности множества X в этой последовательности будут повторяющиеся элементы, и поскольку отображение g биективно, самым первым из повторившихся элементов будет стартовый элемент[1] x:

$$x \longmapsto g(x) \longmapsto g^2(x) \longmapsto \cdots \longmapsto g^{k-1}(x) \longmapsto x = g^k(x)\ . \tag{3-2}$$

Более того, из биективности отображения G вытекает, что любые два таких цикла (начинающиеся из разных точек x и y) либо не пересекаются, либо состоят из одних и тех же элементов.

Таким образом, множество X распадётся в дизъюнктное объединение циклов вида (3-2). Это разбиение можно иначе описать как разбиение множества X на непересекающиеся орбиты группы, состоящей из всевозможных итераций перестановки g и обратной к ней. Эта группа называется *циклической группой*, порождённой перестановкой g и обозначается

$$\langle g\rangle \stackrel{\text{def}}{=} \{\dots, g^{-2}, g^{-1}, \mathrm{Id}, g, g^2, \dots\}\ , \quad \text{где } g^{-k} \stackrel{\text{def}}{=} \underbrace{g^{-1}g^{-1}\cdots g^{-1}}_{k \text{ раз}} \text{ при } k \in \mathbb{N}\ . \tag{3-3}$$

Например[2], $g = (6, 5, 4, 1, 8, 3, 9, 2, 7) \in \mathfrak{S}_9$ разбивает множество $\{1, 2, \dots, 9\}$ на три цикла:

$$\begin{aligned} &1 \overset{g}{\longmapsto} 6 \overset{g}{\longmapsto} 3 \overset{g}{\longmapsto} 4 \overset{g}{\longmapsto} 1\\ &2 \overset{g}{\longmapsto} 5 \overset{g}{\longmapsto} 8 \overset{g}{\longmapsto} 2\\ &7 \overset{g}{\longmapsto} 9 \overset{g}{\longmapsto} 7\ , \end{aligned} \tag{3-4}$$

представляющие собою орбиты действия группы (3-3), которая в данном случае состоит из 12 преобразований

$$\begin{aligned} g &= (6, 5, 4, 1, 8, 3, 9, 2, 7) = g^{-11}\\ g^2 &= (3, 8, 1, 6, 2, 4, 7, 8, 9) = g^{-10}\\ g^3 &= (4, 2, 6, 3, 5, 1, 9, 2, 7) = g^{-9}\\ g^4 &= (1, 5, 3, 4, 8, 6, 7, 5, 9) = g^{-8}\\ g^5 &= (6, 8, 4, 1, 2, 3, 9, 2, 7) = g^{-7}\\ g^6 &= (3, 2, 1, 6, 5, 4, 7, 8, 9) = g^{-6}\\ g^7 &= (4, 5, 6, 3, 8, 1, 9, 5, 7) = g^{-5}\\ g^8 &= (1, 8, 3, 4, 2, 6, 7, 2, 9) = g^{-4}\\ g^9 &= (6, 2, 4, 1, 5, 3, 9, 8, 7) = g^{-3}\\ g^{10} &= (3, 5, 1, 6, 8, 4, 7, 5, 9) = g^{-2}\\ g^{11} &= (4, 8, 6, 3, 2, 1, 9, 2, 7) = g^{-1}\\ \mathrm{Id} = g^{12} &= (1, 2, 3, 4, 5, 6, 7, 8, 9) \end{aligned} \tag{3-5}$$

(обратите внимание, что циклы (3-4) стоят в правых частях этих формул по столбцам).

Будем называть перестановку, которая переставляет по кругу какие-либо m попарно различных элементов[3]

$$i_1 \longmapsto i_2 \longmapsto i_3 \longmapsto \cdots \longmapsto i_{m-1} \longmapsto i_m \longmapsto i_1\ , \tag{3-6}$$

а все остальные элементы оставляет на месте, *циклом* длины m и обозначать такой цикл через

$$\langle i_1, i_2, \dots, i_m\rangle\ .$$

Упражнение 3.3. Покажите, что два цикла $c_1, c_2 \in \mathfrak{S}_n$ *коммутируют* друг с другом (т. е. удовлетворяют соотношению $c_1c_2 = c_2c_1$) ровно в двух случаях: когда $c_1^m = c_2$ для некоторого $m \in \mathbb{N}$, или когда множества участвующих в них элементов не пересекаются.

[1] более формально: если $g^m(x) = g^k(x)$ при $m > k$, то применяя к обеим частям g^{-k} получим $g^{m-k}(x) = x$

[2] мы используем обозначения n° 1.3.1

[3] числа $i_1, i_2, \dots, i_m$ могут быть любыми, не обязательно соседними или возрастающими

Циклы, переставляющие непересекающиеся множества элементов, называются *независимыми*. Из сказанного выше вытекает, что произвольная перестановка g распадается в композицию независимых коммутирующих между собою циклов, причём такое разложение единственно и совпадает с разложением множества X на орбиты циклической группы, порождённой g.

Набор длин циклов, на которые разлагается данная перестановка g называется её *цикловым типом* и обозначается через $\lambda(g)$. Цикловой тип удобно представлять себе в виде *диаграммы Юнга* — выровненного по левому краю набора горизонтальных клетчатых полосок, невозрастающей сверху вниз длины. Каждая такая полоска символизирует соответствующий цикл. Так, рассмотренная выше перестановка

$$g = (6,\,5,\,4,\,1,\,8,\,3,\,9,\,2,\,7) = \langle 1,6,3,4\rangle\langle 2,5,8\rangle\langle 7,9\rangle = \begin{array}{|c|c|c|c|}\hline 1&6&3&4\\\hline 2&5&8\\\cline{1-3} 7&9\\\cline{1-2}\end{array}$$

имеет цикловой тип $\lambda(g) =$  . Вместо того, чтобы полностью рисовать диаграмму Юнга, мы для экономии бумаги иногда будем просто выписывать в строчку длины её строк. Так, запись

$$\lambda(g) = (\lambda_1, \lambda_2, \dots, \lambda_m)\ , \quad \text{где } \lambda_1 \geqslant \lambda_2 \geqslant \dots \geqslant \lambda_m \geqslant 0$$

означает, что перестановка g состоит из $\leqslant m$ циклов, длины которых суть $\lambda_1, \lambda_2, \dots, \lambda_m$. Например,

$$\lambda(6,\,5,\,4,\,1,\,8,\,3,\,9,\,2,\,7) = (4,\,3,\,2)$$

Число клеток, из которого состоит диаграмма Юнга λ, называется её *весом* и обозначается $|\lambda|$. Таким образом, цикловые типы перестановок из $\mathfrak{S}_n$ изображаются диаграммами Юнга веса n. Единственной перестановкой с цикловым типом $\lambda = (1,\,1,\,\dots\,,\,1)$ (он изображается диаграммой-столбцом высоты n и ширины 1) является тождественная перестановка Id. Диаграмме $\lambda = (n)$ (состоящей из одной строки длины n) отвечают всевозможные циклы максимальной длины, переставляющие все элементы множества X по кругу в некотором порядке.

Упражнение 3.4. Сколько имеется в $\mathfrak{S}_n$ различных циклов длины n?

3.2.1. Пример: сколько различных перестановок из $\mathfrak{S}_n$ имеют заданный цикловой тип λ? Пусть диаграмма Юнга λ состоит из m_1 строк длины 1, m_2 строк длины 2, … , m_n строк длины[1] n. Заполним её клетки числами 1, 2, … , n так, чтобы каждое число использовалось ровно один раз, и интерпретируем строки как независимые циклы, слева направо сдвигающие стоящие в них числа.

Симметрическая группа $\mathfrak{S}_n$ действует на таких заполнениях перестановками цифр, а тем самым, действует и на множестве всех перестановок заданного циклового типа λ, причём последние образуют одну орбиту этого действия. Длина этой орбиты и есть искомое нами число. Стабилизатор данной перестановки, задаваемой каким-либо конкретным заполнением диаграммы λ числами, состоит из всевозможных перестановок циклов одинаковой длины между собою, а также циклических перестановок цифр в каждой строке, т. е. состоит из

$$|\mathrm{Stab}(\lambda)| = 1^{m_1}\cdot m_1!\cdot 2^{m_2}\cdot m_2!\cdot\ \dots\ \cdot n^{m_n}\cdot m_n! = \prod_{\alpha=1}^{n} \alpha^{m_\alpha} m_\alpha! \tag{3-7}$$

перестановок. Стоящее в правой части произведение принято обозначать z_λ. По формуле для длины орбиты (n° 3.1.3) число перестановок, распадающихся в произведение m_1 циклов длины 1, m_2 циклов длины 2, … , m_n циклов длины n (все циклы независимы) равно

$$\frac{n!}{z_\lambda} = \frac{n!}{1^{m_1}\cdot m_1!\cdot 2^{m_2}\cdot m_2!\cdot\ \dots\ \cdot n^{m_n}\cdot m_n!}\ ,$$

где $m_1\lambda_1 + m_2\lambda_2 + \dots + m_n\lambda_n = n$. Отметим, что число $n!/z_\lambda$, тем самым, всегда[2] является целым и

$$\sum_{|\lambda|=n} \frac{1}{z_\lambda} = 1$$

[1] отметим, что $m_1\lambda_1 + m_2\lambda_2 + \dots + m_n\lambda_n = n$ и среди чисел m_i с неизбежностью встречаются нулевые

[2] т. е. для любой диаграммы λ веса n

(суммирование происходит по всем диаграммам Юнга λ веса n).

3.3. Циклические группы и порядки элементов. Рассмотрим теперь произвольную группу преобразований G и произвольное преобразование $g \in G$. Наименьшая подгруппа группы G, содержащая g, обозначается через $\langle g\rangle$ и называется *циклической подгруппой, порождённой* g. Она состоит из всевозможных целых степеней[1] g^m преобразования g. Если все эти преобразования попарно различны, говорят, что элемент g имеет *бесконечный порядок*. Отметим, что элементы бесконечного порядка могут быть только в бесконечных группах G.

Если среди преобразований вида g^m встречаются одинаковые[2], скажем, $g^m = g^k$ для некоторых $m > k$, то применяя к обеим частям преобразование g^{-k}, мы приходим к равенству $g^{m-k} = \mathrm{Id}$. В этом случае говорят, что элемент g имеет конечный порядок, и наименьшее $n \in \mathbb{N}$, для которого $g^n = \mathrm{Id}$, называется *порядком* элемента g.

Группа $\langle g\rangle$ состоит в этом случае в точности n преобразований

$$\mathrm{Id},\ g,\ g^2,\ \ldots,\ g^{n-1} \tag{3-8}$$

В самом деле, представляя произвольную целую степень m в виде $m = q\cdot n + r$, где остаток r заключён в пределах $0 \leqslant r \leqslant (n-1)$, мы видим, что $g^m = (g^n)^q\, g^r = \mathrm{Id}^q g^r = g^r$. С другой стороны, все преобразования (3-8) попарно различны, поскольку из равенства $g^r = g^s$ с $0 \leqslant r < s < n$ получалось бы равенство $g^{s-r} = \mathrm{Id}$, в котором $0 < (s-r) < n$ вопреки определению порядка n элемента g.

Итак, в конечной группе преобразований порядок любого элемента $g \in G$ совпадает с порядком $|\langle g\rangle|$ порождённой им циклической подгруппы. Из теоремы Лагранжа вытекает

3.3.1. СЛЕДСТВИЕ. *Порядок любого элемента конечной группы нацело делит порядок группы. В частности* $g^{|G|} = \mathrm{Id}\quad \forall\, g \in G$. □

3.3.2. Пример: порядок перестановки $g \in \mathfrak{S}_n$ циклового типа $\lambda(g) = (\lambda_1, \lambda_2, \ldots, \lambda_m)$ равен

$$|\langle g\rangle| = \mathrm{НОК}(\lambda_1, \lambda_2, \ldots, \lambda_m)\ ,$$

т. е. наименьшему натуральному числу, нацело делящемуся на длины всех независимых циклов, из которых состоит g. Например, порядок перестановки

$$\mathfrak{S}_{12} \ni (3,\ 12,\ 7,\ 9,\ 10,\ 4,\ 11,\ 1,\ 6,\ 2,\ 8,\ 5) = \langle 1,\ 3,\ 7,\ 11,\ 8\rangle\langle 2,\ 12,\ 5,\ 10\rangle\langle 4,\ 9,\ 6\rangle$$

равен $5\cdot 4\cdot 3 = 60$.

3.3.3. Циклические группы. Группа G называется *циклической*, если $G = \langle g\rangle$ для некоторого $g \in G$. Примером бесконечной циклической группы является группа T_v параллельных переносов (плоскости или пространства) на всевозможные целые кратные заданного вектора v. Эта группа состоит из тождественного преобразования (сдвига на нулевой вектор $0 = 0\cdot v$) и бесконечной серии сдвигов на векторы $\pm v$, $\pm 2v$, $\pm 3v$, ...

Циклическая группа порядка n — это группа поворотов $\boldsymbol{\mu}_n$ из примеров (n° 2.1.2) и (n° 2.2.2). Ясно, что произвольную циклическую группу порядка n, порождённую элементом g можно отождествить с группой поворотов так, чтобы композиции элементов переходили в композиции — для этого надо отобразить элемент g^k в поворот на угол $2\pi k/n$. Таким образом, все циклические группы порядка n устроены «одинаково». Точный математический смысл этого мы обсудим ниже в §4, а сейчас рассмотрим ещё несколько примеров.

3.3.4. Пример: всякая группа простого порядка является циклической, причём в качестве порождающего её элемента можно взять любое преобразование $g \in G$, отличное от тождественного. В самом деле, в этом случае $|\langle g\rangle|$ будет больше единицы и по теореме Лагранжа должен нацело делить $|G|$, что возможно только если $|\langle g\rangle| = |G|$, т. е. $\langle g\rangle = G$.

---

[1] под g^{-n} с $n \in \mathbb{N}$ мы, как обычно, понимаем $\left(g^{-1}\right)^m$, а $g^0 = \mathrm{Id}$, по определению, означает тождественное преобразование

[2] что с неизбежностью произойдёт, если группа G конечна

Упражнение 3.5. Является ли циклической группа двуугольника $\mathfrak{D}_2$?

3.3.5. Пример: инволюции. Отличные от тождественного преобразования g порядка 2, т. е. такие что $g \neq \mathrm{Id}$, но $g^2 = \mathrm{Id}$, называются *инволюциями*. Иначе можно сказать, что инволюции — это преобразования, которые обратны сами себе: $g^2 = \mathrm{Id} \iff g = g^{-1}$. Для того чтобы перестановка $g \in \mathfrak{S}_n$ была инволюцией необходимо и достаточно, чтобы в её разложении в композицию независимых циклов не было циклов длины $\geqslant 3$. Циклы длины 2 называются *транспозициями*. Таким образом, всякая инволюция в $\mathfrak{S}_n$ является композицией независимых транспозиций.

Упражнение 3.6. Покажите, что произвольная перестановка может быть представлена в виде композиции двух инволюций.

Подсказка: сначала представьте в виде произведения двух инволюций произвольный цикл[1]

Упражнение 3.7. Покажите, что произвольная перестановка может быть (многими способами) представлена в виде композиции нескольких (не обязательно независимых) транспозиций.

Покажем, что в произвольной конечной группе G любая пара не равных друг другу инволюций g_1, g_2 порождает подгруппу[2], которую можно отождествить с группой диэдра. Пусть порядок композиции g_1g_2 равен n. Отметим, что $n \geqslant 2$, поскольку $g_1 \neq g_2 = g_2^{-1}$. Наименьшая подгруппа, содержащая g_1 и g_2 состоит из всевозможных чередующихся произведений $g_1g_2g_1g_2\ldots$ и $g_2g_1g_2g_1\ldots$. Домножая равенство

$$\mathrm{Id} = (g_1g_2)^n = \underbrace{g_1g_2g_1g_2\cdots g_1g_2}_{n \text{ пар}}$$

справа на g_2 (и пользуясь тем, что $g_2^2 = \mathrm{Id}$), мы получаем выражение $g_2 = g_1g_2g_1\ldots$, позволяющее переписать каждое произведение вида $g_2g_1g_2g_1\ldots$ как произведение вида $g_1g_2g_1g_2\ldots$ (для этого надо заменить первую букву g_2 выражением $g_2 = g_1g_2g_1\ldots$). Поскольку $(g_1g_2)^n = \mathrm{Id}$, любое произведение вида $g_1g_2g_1g_2\ldots$ может быть редуцировано до произведения, состоящего из не более чем $2n-1$ сомножителей. Покажем, что ни одно из этих произведений не равно Id.

В самом деле, если $g_1g_2g_1\cdots = \mathrm{Id}$, то произведение слева должно кончаться на g_1, т. к. иначе порядок элемента g_1g_2 был бы меньше n. Умножая обе части равенства слева и справа на g_1 мы получаем аналогичное равенство $g_2g_1g_2\ldots g_2 = \mathrm{Id}$ с на два меньшим числом сомножителей, обе части которого можно с двух сторон умножить на g_2 и т. д. Эта процедура в конце концов приведёт либо к равенству $g_1 = \mathrm{Id}$, либо к равенству $g_2 = \mathrm{Id}$, что не так.

Упражнение 3.8. Покажите аналогичным образом, что все $2n-1$ произведений $g_1g_2g_1g_2\ldots$ попарно различны.

Таким образом, порождённая двумя инволюциями подгруппа состоит из тождественного преобразования и $2n-1$ преобразований $g_1g_2g_1\ldots$. Сопоставим теперь инволюциям g_1 и g_2 симметрии n-угольника относительно двух соседних осей ℓ_1 и ℓ_2 (расположенных при чётном n под углом π/n, а при нечётном n — под углом $2\pi/n$ друг к другу), а их композиции — композицию этих двух симметрий, представляющую собою согласно упр. 1.12 при чётном n поворот на угол $2\pi/n$, а при нечётном n — на угол $2\cdot(2\pi/n)$ по направлению от ℓ_2 к ℓ_1.

Упражнение 3.9. Убедитесь, что отображая $2n-1$ произведений $g_1g_2g_1g_2\ldots$ в соответствующие композиции симметрий n-угольника мы получим сохраняющую композиции биекцию между группой диэдра $\mathfrak{D}_n$ и группой, порождённой инволюциями g_1 и g_2.

[1] это утверждение является аналогом того, что композиция двух осевых симметрий относительно пересекающихся прямых является поворотом вокруг точки пересечения этих прямых на удвоенный угол между прямыми, ср. с упр. 1.12

[2] подгруппой, *порождённой* элементами $g_1, g_2, \ldots, g_n \in G$, называется наименьшая по включению подгруппа $H \subset G$, содержащая все эти элементы; такая подгруппа состоит из всевозможных композиций преобразований g_i и обратных к ним преобразований g_i^{-1}