§12. О строении групп

12.1. Свободные группы и соотношения. С любым множеством M можно связать группу F_M, которая называется *свободной группой*, порождённой множеством M. Она состоит из классов эквивалентных слов, которые можно написать буквами x и x^{-1}, где $x \in M$, по наименьшему отношению эквивалентности, отождествляющему между собою слова, отличающиеся друг от друга вставкой или удалением[1] двубуквенного фрагмента xx^{-1} или $x^{-1}x$. Композиция определяется как приписывание одного слова к другому. Единицей служит пустое слово. Обратным к классу слова $w = x_1 \dots x_M$ является класс слова $w^{-1} = x_m^{-1} \dots x_1^{-1}$, где каждая из букв x_i равна x или x^{-1}, где $x \in M$, и $\left(x^{-1}\right)^{-1} \stackrel{\text{def}}{=} x$.

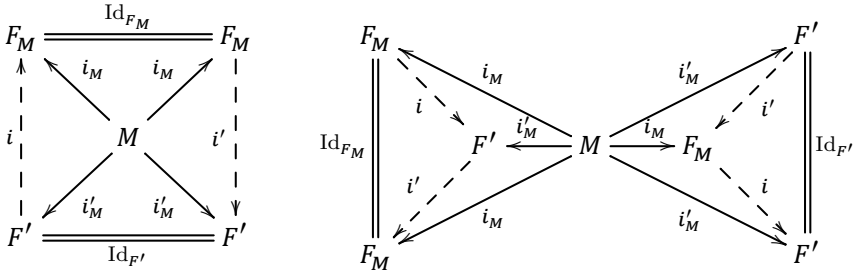
Упражнение 12.1. Убедитесь, что композиция корректно определена на классах эквивалентности слов и что в каждом классе содержится ровно одно *несократимое*[2] слово, которое одновременно является и самым коротким словом в своём классе.

Элементы множества M называются *образующими* свободной группы F_M. Свободная группа с k образующими обозначается F_k. Группа $F_1 \simeq \mathbb{Z}$ — это циклическая группа бесконечного порядка. Группа F_2 классов слов на четырёхбуквенном алфавите x, y, x^{-1}, y^{-1} уже трудно обозрима.

Упражнение 12.2. Постройте инъективный гомоморфизм групп $F_{\mathbb{N}} \hookrightarrow F_2$.

Предложение 12.1 (универсальное свойство свободных групп)
Отображение $i_M : M \to F_M$, переводящее элемент $x \in M$ в класс однобуквенного слова $x \in F_M$, обладает следующим свойством: для любых группы G и отображения множеств $\varphi_M : M \to G$ существует единственный такой гомоморфизм групп $\varphi : F_M \to G$, что $\varphi_M = \varphi \circ i_M$. Для любого обладающего этим свойством отображения $i'_M : M \to F'$ множества M в группу F' имеется единственный такой изоморфизм групп $i' : F_M \xrightarrow{\sim} F'$, что $i'_M = i' \circ i_M$.

Доказательство. Гомоморфизм φ единствен, так как обязан переводить слово $x_1^{\varepsilon_1} \dots x_m^{\varepsilon_m} \in F_M$, где $x_\nu \in M$, $\varepsilon_\nu = \pm 1$, в произведение $\varphi_M(x_1)^{\varepsilon_1} \dots \varphi_M(x_m)^{\varepsilon_m} \in G$. С другой стороны, это правило корректно задаёт гомоморфизм групп, что доказывает первое утверждение. Если отображение $i' : M \to F'$ множества M в группу F' обладает универсальным свойством из предл. 12.1, то существуют единственные гомоморфизмы $i' : F_M \to F'$ и $i : F' \to F_M$, встраивающиеся в коммутативные диаграммы



Разложения вида $i_M = \varphi \circ i_M$, $i'_M = \psi \circ i'_M$ в силу их единственности возможны только с $\varphi = \mathrm{Id}_{F_M}$, $\psi = \mathrm{Id}_{F'}$. Поэтому $i' \circ i = \mathrm{Id}_{F'}$, $i \circ i' = \mathrm{Id}_{F_M}$. □

[1] В начале, в конце, или же между произвольными двумя последовательными буквами слова.
[2] Т. е. не содержащее двубуквенных фрагментов xx^{-1} и $x^{-1}x$.

12.1.1. Задание групп образующими и соотношениями. Если гомоморфизм групп

$$\varphi : F_M \twoheadrightarrow G\,, \tag{12-1}$$

заданный отображением $\varphi_M : M \to G$ множества M в группу G, является *сюръективным*, то говорят, что группа G *порождается* элементами $g_m = \varphi_M(m)$, $m \in M$, а сами элементы g_m называются *образующими* группы G. В этом случае G исчерпывается всевозможными произведениями $g_1^{\varepsilon_1} g_2^{\varepsilon_2} \dots g_k^{\varepsilon_k}$, $\varepsilon = \pm 1$, образующих и обратных к ним элементов. Группа G называется *конечно порождённой*, если она допускает конечное множество образующих. Ядро $\ker\varphi \rtimes F_M$ эпиморфизма (12-1) называется *группой соотношений* между образующими g_m. Набор слов $R \subset \ker\varphi$ называется набором *определяющих соотношений*, если $\ker\varphi$ — это наименьшая нормальная подгруппа в F_M, содержащая R. Это означает, что любое соотношение можно получить из слов множества R конечным числом умножений, обращений и сопряжений произвольными элементами из свободной группы F_M. Группа, допускающая конечное число образующих с конечным набором определяющих соотношений называется *конечно определённой*.

Всякую группу можно задать образующими и соотношениями, например, взяв в качестве M множество всех элементов группы. Удачный выбор образующих с простыми определяющими соотношениями может значительно прояснить устройство группы и её гомоморфизмов в другие группы. Однако в общем случае выяснить, изоморфны ли две группы, заданные своими образующими и определяющими соотношениями, или даже определить, отлична ли группа, заданная образующими и соотношениями, от тривиальной группы $\{e\}$, бывает очень непросто. Более того, обе эти задачи являются *алгоритмически неразрешимыми*[1] даже в классе конечно определённых групп.

Предложение 12.2
Пусть группа G_1 задана множеством образующих M и набором определяющих соотношений R, а G_2 — произвольная группа. Отображение $\varphi : M \to G_2$ тогда и только тогда корректно задаёт гомоморфизм групп $G_1 \to G_2$ правилом $x_1^{\varepsilon_1}\dots x_m^{\varepsilon_m} \mapsto \varphi(x_1)^{\varepsilon_1}\dots\varphi(x_m)^{\varepsilon_m}$, когда для каждого слова $y_1^{\varepsilon_1}\dots y_m^{\varepsilon_m} \in R$ в группе G_2 выполняется соотношение $\varphi(y_1)^{\varepsilon_1}\dots\varphi(y_m)^{\varepsilon_m} = 1$.

Доказательство. Отображения множеств $\varphi_M : M \to G_2$ биективно соответствуют гомоморфизмам групп $\varphi : F_M \to G_2$. Такой гомоморфизм φ факторизуется до гомоморфизма из группы $G_1 = F_M/N_R$, где $N_R \rtimes F_M$ — наименьшая нормальная подгруппа, содержащая R, тогда и только тогда, когда $N_R \subset \ker\psi$. Так как $\ker\psi \rtimes F_M$, для этого необходимио и достаточно включения $R \subset \ker\psi$. □

Пример 12.1 (образующие и соотношения группы диэдра)
Покажем, что группа диэдра D_n задаётся двумя образующими x_1, x_2 и соотношениями

$$x_1^2 = x_2^2 = (x_1x_2)^n = e\,. \tag{12-2}$$

Оси симметрии правильного n-угольника разбивают его на $2n$ конгруэнтных прямоугольных треугольников как на рис. 12⋄1 ниже. Обозначим один из них через e. Поскольку любое движение плоскости однозначно задаётся своим действием на треугольник e, треугольники разбиения находятся в биекции с движениями $g \in D_n$, и каждый из них можно однозначно пометить

[1] В формальном смысле, принятом в математической логике.

тем единственным преобразованием g, которое переводит треугольник e в этот треугольник. При этом каждое преобразование $h \in D_n$ переводит каждый треугольник g в треугольник hg.

Упражнение 12.3. Для любого движения F евклидова пространства $\mathbb{R}^n$ и отражения σ_π в произвольной гиперплоскости $\pi \subset \mathbb{R}^n$ докажите соотношения

$$\sigma_{F(\pi)} = F \circ \sigma_\pi \circ F^{-1} \quad \text{и} \quad \sigma_{F(\pi)} \circ F = F \circ \sigma_\pi\,. \tag{12-3}$$

Обозначим через ℓ_1 и ℓ_2 боковые стороны треугольника e, а отражения плоскости в этих сторонах обозначим через $\sigma_1 = \sigma_{\ell_1}$ и $\sigma_2 = \sigma_{\ell_2}$. Тогда по второму из равенств (12-3) треугольники, получающиеся из e последовательными отражениями в направлении часовой стрелки пометятся элементами

$$\begin{aligned}
\sigma_{\ell_1} &= \sigma_1\,,\\
\sigma_{\sigma_1(\ell_2)}\sigma_1 &= \sigma_1\sigma_2\,,\\
\sigma_{\sigma_1\sigma_2(\ell_1)}\sigma_1\sigma_2 &= \sigma_1\sigma_2\sigma_1\,,\\
\sigma_{\sigma_1\sigma_2\sigma_1(\ell_2)}\sigma_1\sigma_2\sigma_1 &= \sigma_1\sigma_2\sigma_1\sigma_2\,,\ \ldots
\end{aligned}$$

а треугольники, получающиеся из e последовательными отражениями против часовой стрелки пометятся элементами

$$\begin{aligned}
\sigma_{\ell_2} &= \sigma_2\,,\\
\sigma_{\sigma_2(\ell_1)}\sigma_2 &= \sigma_2\sigma_1\,,\\
\sigma_{\sigma_2\sigma_1(\ell_2)}\sigma_2\sigma_1 &= \sigma_2\sigma_1\sigma_2\,,\\
\sigma_{\sigma_2\sigma_1\sigma_2(\ell_1)}\sigma_2\sigma_1\sigma_2 &= \sigma_2\sigma_1\sigma_2\sigma_1\,,\ \ldots
\end{aligned}$$

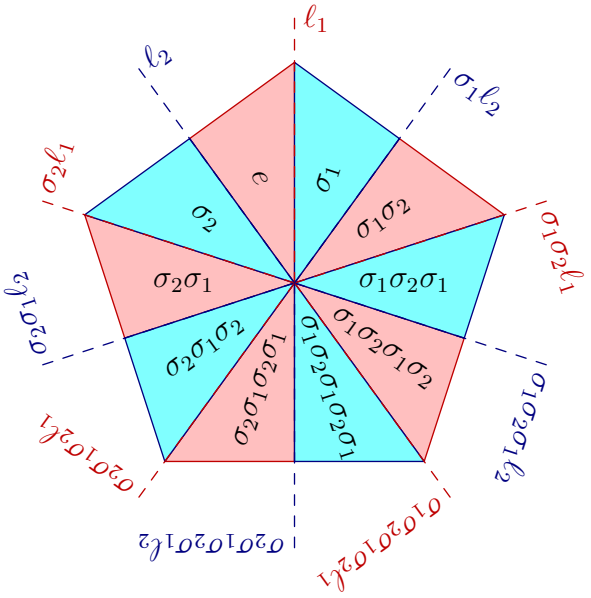


Рис. 12◇1. Образующие группы диэдра.

В результате каждый треугольник пометится словом вида $\sigma_1\sigma_2\sigma_1\sigma_2\ldots$ или $\sigma_2\sigma_1\sigma_2\sigma_1\ldots$ Так как композиция $\sigma_1 \circ \sigma_2$ является поворотом на угол $2\pi/n$, в группе D_n имеются соотношения

$$\sigma_1^2 = \sigma_2^2 = (\sigma_1\sigma_2)^n = e\,. \tag{12-4}$$

Последнее из них равносильно вытекающему из рис. 12◇1 равенству

$$\underbrace{\sigma_1\sigma_2\sigma_1\ldots}_{k} = \underbrace{\sigma_2\sigma_1\sigma_2\ldots}_{2n-k}\,. \tag{12-5}$$

Из сказанного вытекает, что правило $x_1 \mapsto \sigma_1$, $x_2 \mapsto \sigma_2$ корректно задаёт сюръективный гомоморфизм $\varphi\colon F_2/H \twoheadrightarrow D_n$ из фактора свободной группы F_2 с образующими x_1, x_2 по наименьшей нормальной подгруппе $H \rtimes F_2$, содержащей слова x_1^2, x_2^2 и $(x_1x_2)^n$. Каждое слово в алфавите $\{x_1, x_2\}$ по модулю соотношений (12-2) записывается содержащим меньше $2n$ букв словом $x_1x_2x_1\ldots$ или $x_2x_1x_2\ldots$, и два таких слова переводятся гомоморфизмом φ в один и тот же элемент $g \in D_n$ если и только если выполняется равенство (12-5), т. е. при

$$\underbrace{x_1x_2x_1\ldots}_{k} = \underbrace{x_2x_1x_2\ldots}_{2n-k}\,, \tag{12-6}$$

а это тождество является следствием тождества $(x_1x_2)^n = e$. Мы заключаем, что гомоморфизм $\varphi : F_2/H \twoheadrightarrow D_n$ биективен.

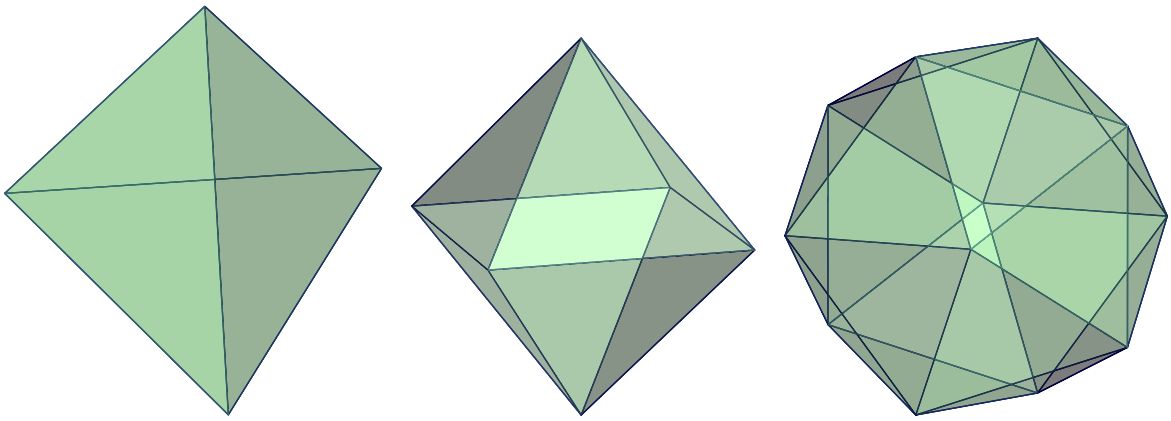


Рис. 12⋄2. Тетраэдр, октаэдр и икосаэдр.

Пример 12.2 (группы тетраэдра, октаэдра и икосаэдра)
Обозначим через M платоново тело с треугольными гранями, т. е. правильный *тетраэдр*, *октаэдр* или *икосаэдр* (см. рис. 12⋄2). Плоскости симметрии многогранника M задают *барицентрическое разбиение* каждой грани на 6 треугольников с вершинами в вершине M, в середине примыкающего к этой вершине ребра и центре примыкающей к этому ребру грани, как на рис. 12⋄3. Все эти треугольники конгруэнтны друг другу и сходятся по $2m_1 = 6$ штук в центрах граней, по $2m_2 = 4$ штуки в серединах рёбер и по $2m_3$ штук в вершинах, где числа m_i, а также число γ граней у M и общее число треугольников $N = 6\gamma$ представлены в таблице[1]:

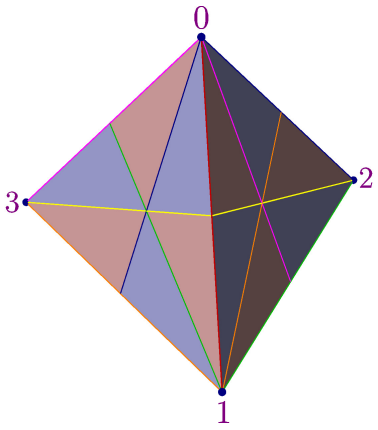


Рис. 12⋄3. Барицентрическое разбиение тетраэдра плоскостями симметрии.

M	m_1	m_2	m_3	γ	N
тетраэдр	3	2	3	4	24
октаэдр	3	2	4	8	48
икосаэдр	3	2	5	20	120 .

Пометим один из этих треугольников буквой e и назовём высекающие его плоскости симметрии буквами π_1, π_2, π_3 так, чтобы для всех циклических перестановок (i, j, k) тройки индексов $(1, 2, 3)$ двугранный угол между плоскостями π_i и π_j равнялся π/m_k, и обозначим через σ_i отражение в плоскости π_i. Так как каждое преобразование из группы O_M однозначно определяется своим действием на тройку векторов с концами в углах треугольника e, каждый треугольник триангуляции является образом треугольника e при одном и ровно одном преобразовании $g \in O_M$. Надпишем каждый треугольник тем преобразованием $g \in O_M$, которое переводит в него треугольник e, и надпишем стороны треугольника g, высекаемые плоскостями $g(\pi_1)$, $g(\pi_2)$, $g(\pi_3)$ соответствующими номерами 1, 2, 3. Отметим, что каждое преобразование $h \in O_M$ переводит каждый треугольник g в треугольник hg.

[1] Обратите внимание, что помещённый в пространство n-угольный диэдр из прим. 12.1 тоже можно включить в этот список со значениями $m_1 = n$, $m_2 = 2$, $m_3 = 2$, $\gamma = 2$ и $N = 4n$, если условиться, что плоский диэдр имеет две двумерные грани: «верхнюю» и «нижнюю».

На рис. 12⋄4 изображена стереографическая проекция картинки, которую 24 трёхгранных угла барицентрического разбиения тетраэдра с рис. 12⋄3 высекают на описанной около этого тетраэдра сфере. На каждом сферическом треугольнике написана композиция отражений $\sigma_1, \sigma_2, \sigma_3$, переводящая треугольник e в этот треугольник. Стороны треугольников, помеченные номерами 1, 2 и 3, изображены на рисунке в синим, зелёным и лиловым цветом.

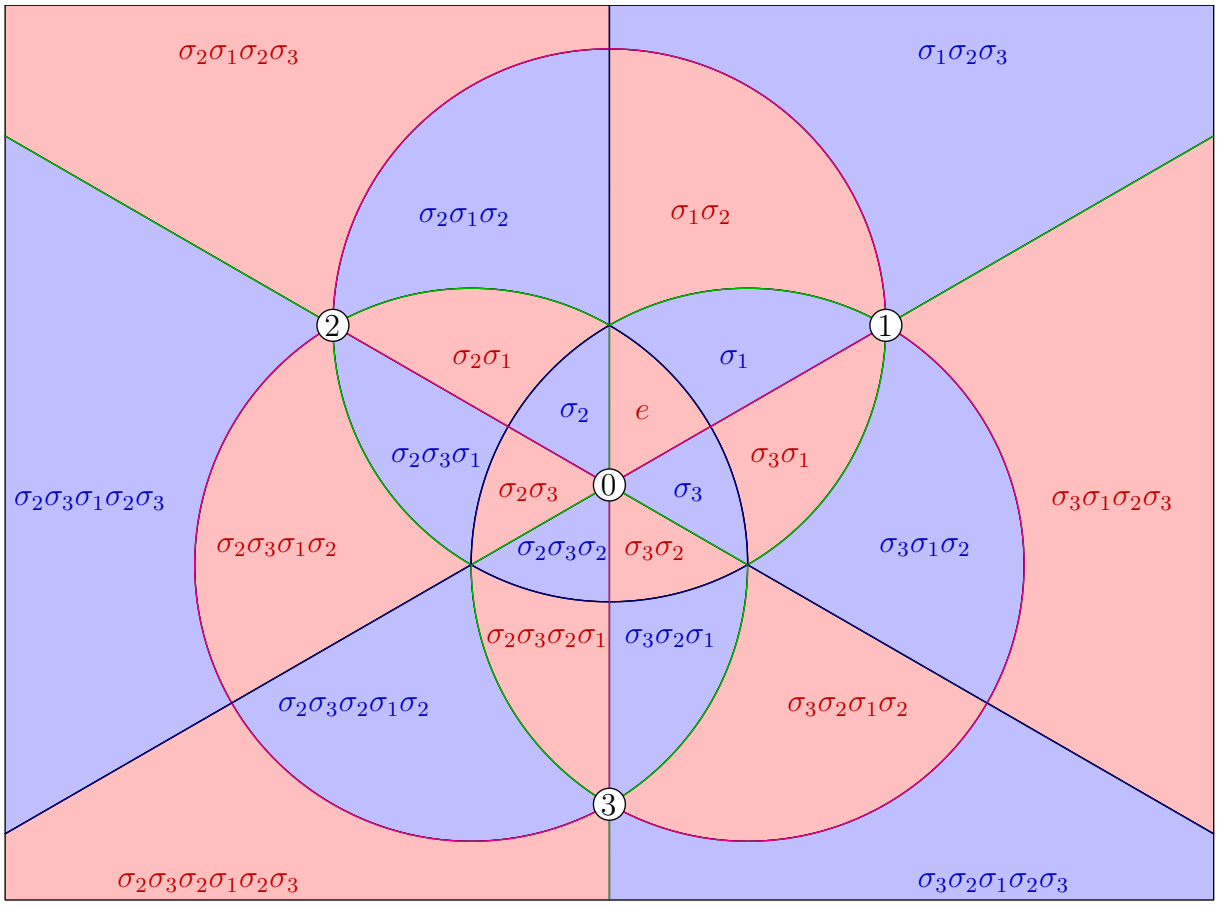


Рис. 12⋄4. Триангуляция описанной сферы плоскостями симметрии тетраэдра в стереографической проекции из диаметрально противоположного к вершине «0» полюса сферы на экваториальную плоскость, параллельную грани «123».

Чтобы явно написать композицию отражений $\sigma_1, \sigma_2, \sigma_3$, переводящую треугольник e в треугольник g, выберем внутри опирающихся на эти треугольники трёхгранных углов векторы u и w с концами на описанной вокруг M сфере так, чтобы $w \neq -u$ и натянутая на них плоскость Π_{uw} не содержала линий пересечения плоскостей симметрии многогранника M, и пройдём из u в w по кратчайшей дуге окружности, высекаемой на описанной сфере плоскостью Π_{uw}. Пусть мы при этом последовательно побываем в треугольниках $g_1 = e, g_2, g_3, \dots, g_{m+1} = g$. Обозначим через $\nu_i \in \{1, 2, 3\}$ номер, надписанный на той стороне треугольника g_i, сквозь которую осуществляется проход из g_i в g_{i+1}. Это означает, что общая сторона треугольников g_i и g_{i+1} высекается плоскостью $g_i(\pi_{\nu_i})$, т. е. образом плоскости π_{ν_i} при отображении g_i. По второму из равенств форм. (12-3) на стр. 170, $g_2 = \sigma_{\nu_1}$, $g_3 = \sigma_{g_2(\pi_{\nu_2})} g_2 = \sigma_{\nu_1}\sigma_{\nu_2}$, $g_4 = \sigma_{g_3(\pi_{\nu_3})} g_3 = \sigma_{\nu_1}\sigma_{\nu_2}\sigma_{\nu_3}$ и т. д. Таким образом, последовательность индексов $\nu_i \in \{1, 2, 3\}$ в разложении $g = \sigma_{\nu_1} \dots \sigma_{\nu_m}$

состоит из выписанных по порядку номеров сторон, которые приходится пересекать по пути из $e = g_1$ в $g = g_{m+1}$ по дуге uw, как на рис. 12⋄5, где стороны с номерами 1, 2, 3 изображены соответственно красным, зелёным и жёлтым цветами. Отметим, что полученное нами разложение элемента $g \in \mathrm{O}_M$ в композицию отражений $\sigma_1, \sigma_2, \sigma_3$ не единственно и зависит от выбора векторов u и w внутри трёхгранных углов e и g. При изменении любого из этих векторов последовательность $\nu_1, \ldots, \nu_m$ номеров зеркал, пересекаемых по дороге из u в w, не меняется до тех пор, пока натянутая на эти векторы плоскость Π_{uw} не натолкнётся на линию пересечения зеркал, а в момент пересечения такой линии в последовательности $\nu_1, \ldots, \nu_m$ некоторый фрагмент вида $\sigma_i\sigma_j\sigma_i\sigma_j \ldots$ длины m_k заменяется симметричным фрагментом $\sigma_j\sigma_i\sigma_j\sigma_i \ldots$ той же самой длины m_k, как показано на рис. 12⋄5.

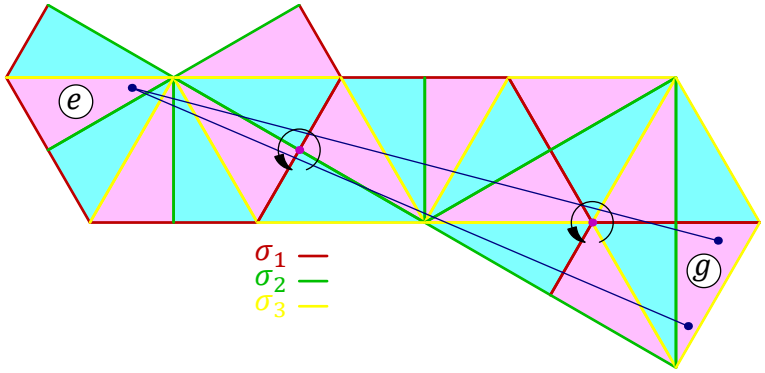


Рис. 12⋄5. $\sigma_2\sigma_3\sigma_2\sigma_3\boldsymbol{\sigma_1\sigma_2}\sigma_3\sigma_2\sigma_3\sigma_2\boldsymbol{\sigma_3\sigma_1\sigma_3}\sigma_2 = g = \sigma_2\sigma_3\sigma_2\sigma_3\boldsymbol{\sigma_2\sigma_1}\sigma_3\sigma_2\sigma_3\sigma_2\boldsymbol{\sigma_1\sigma_3\sigma_1}\sigma_2$.

Разложения, отвечающие верхней и нижней траекториям на рис. 12⋄5 отличаются друг от друга тем, что линии пересечения зеркал обходятся в противоположных направлениях. Композиции возникающих при этом отражений удовлетворяют соотношениям

$$\sigma_1\sigma_2 = \sigma_2\sigma_1 \quad \text{и} \quad \sigma_1\sigma_3\sigma_1 = \sigma_3\sigma_1\sigma_3$$

той же самой природы, что соотношения (12-4) в группе диэдра: так как композиция отражений $\sigma_i \circ \sigma_j$ является поворотом вокруг прямой $\pi_i \cap \pi_j$ на угол $2\pi/m_k$, равный удвоенному углу между плоскостями π_i и π_j, в группе O_M выполняются соотношения $\sigma_i^2 = e$ и $(\sigma_i\sigma_j)^{m_k} = e$, где $i = 1, 2, 3$, а тройка (i, j, k) пробегает три циклические перестановки номеров $(1, 2, 3)$. Отсюда вытекает, во-первых, что длина представления $g = \sigma_{\nu_1} \cdots \sigma_{\nu_m}$, считанного вдоль кратчайшей из двух дуг, соединяющих векторы u и w, не зависит от выбора этих векторов внутри трёхгранных углов, опирающихся на треугольники e и g, при условии, что плоскость Π_{uw} не проходит через линии пересечения зеркал, а во-вторых, что правило $x_i \mapsto \sigma_i$ задаёт сюръективный гомоморфизм $\varphi : F_3/H \twoheadrightarrow \mathrm{O}_M$ из фактора свободной группы F_3 на алфавите $\{x_1, x_2, x_3\}$ по наименьшей нормальной подгруппе $H \rtimes F_3$, содержащей шесть слов

$$x_i^2 \qquad \text{и} \qquad (x_ix_j)^{m_k}. \tag{12-7}$$

Для проверки того, что этот гомоморфизм является изоморфизмом, достаточно показать, что кратчайшее по модулю соотношений (12-7) представление каждого элемента $w \in F_3/H$ в виде $w = x_{\nu_1} \ldots x_{\nu_k}$ имеет в качестве набора индексов $\nu_1, \ldots \nu_k$ одну из возможных последовательностей номеров сторон, которые придётся пересечь, идя из треугольника e в треугольник $g = \sigma_{\nu_1} \ldots \sigma_{\nu_k}$ по дуге $[u, w]$, где $u \in e$, $w \in g$, так, как это объяснялось выше. Сделаем

это индукцией по длине k кратчайшего по модулю соотношений (12-7) слова $x_{\nu_1} \dots x_{\nu_k}$, представляющего данный элемент $y \in F_3 / H$. Для однобуквенных слов $y = x_1, x_2, x_3$ утверждение очевидно. Пусть оно верно для всех $y \in F_3 / H$, представимых словами из $\leqslant k$ букв. Рассмотрим произвольный такой y и проверим утверждение для всех элементов yx_j, $j = 1, 2, 3$, которые нельзя по модулю соотношений (12-7) записать словом из $\leqslant k$ букв. Пусть $g = \varphi(y)$ и $h = \varphi(yx_j) = g\sigma_j$. Рассмотрим плоскость $H = g(\pi_j)$.

Если треугольники e и g лежат по одну сторону от плоскости H, как на рис. 12⋄6, выберем векторы $u \in e$ и $w \in g$ так, чтобы продолжение дуги $[u, w]$ дальше за точку w уходило из треугольника g сквозь высекаемую плоскостью H сторону с номером j, и обозначим через v какой-нибудь вектор, лежащий в пересечении трёхгранного угла над треугольником h с продолжением дуги $[u, w]$. По предположению индукции в кратчайшем по модулю соотношений (12-7) представлении $y = x_{\nu_1} \dots x_{\nu_m}$ число букв $m \leqslant k$ и $\nu_1, \dots, \nu_m$ суть номера рёбер, которые приходится пересекать по пути из u в w по дуге $[u, w]$. При этом $h = \varphi(yx_j) = g\sigma_j = \sigma_{i_1} \dots \sigma_{i_m}\sigma_j$, и представление $yx_j = x_{\nu_1} \dots x_{\nu_m}x_j$ по нашему предположению состоит, как минимум, из $k + 1$ букв. Мы заключаем, что $m = k$, представление $yx_j = x_{\nu_1} \dots x_{\nu_k}x_j$ является одним из кратчайших для элемента yx_j и считывается с дуги $[u, v]$, как и требуется.

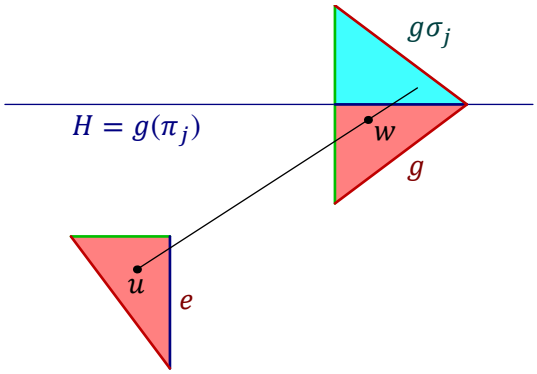


Рис. 12⋄6. H не разделяет e и g.

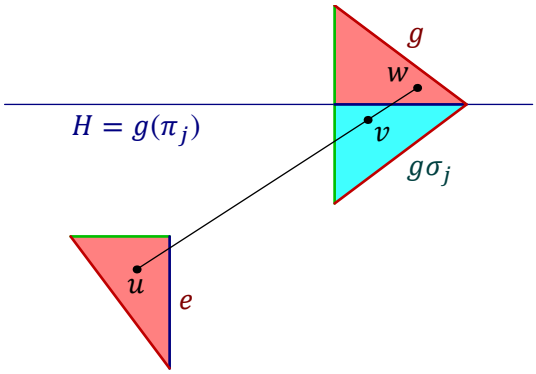


Рис. 12⋄7. H разделяет e и g.

Если треугольники e и g лежат по разные стороны от плоскости H, как на рис. 12⋄7, выберем вектор u в трёхгранном угле над e и вектор w в трёхгранном угле над g так, чтобы дуга $[u, w]$ входила в трёхгранный угол над треугольником g сквозь плоскость H, и обозначим через v какую-нибудь точку этой дуги, лежащую в трёхгранном угле над предыдущим треугольником $\sigma_{g(\pi_j)}g = g\sigma_j g^{-1} g = g\sigma_j = h$. По предположению индукции в кратчайшем по модулю соотношений (12-7) представлении $y = x_{\nu_1} \dots x_{\nu_m}$ число букв $m \leqslant k$ и $\nu_1, \dots, \nu_m$ суть номера рёбер, которые приходится пересекать по пути из u в w по дуге $[u, w]$. В частности, последняя буква $x_{\nu_m} = x_j$. Поэтому элемент $yx_j = x_{\nu_1} \dots x_{\nu_{m-1}}$ записывается более коротким словом, чем y, и утверждение для него верно по индуктивному предположению.

Итак, группа O_M платонова тела M с треугольными гранями порождается тремя элементами x_1, x_2, x_3, связанными шестью образующими соотношениями (12-7).

12.1.2. Образующие и соотношения симметрической группы S_{n+1}. Обозначим числами от 0 до n концы стандартных базисных векторов $e_0, e_1, \dots, e_n$ в $\mathbb{R}^{n+1}$ и рассмотрим n-мерный правильный симплекс $\Delta \subset \mathbb{R}^{n+1}$ с вершинами в этих точках. Поскольку каждое аффинное преобразование n-мерной гиперплоскости $x_0 + x_1 + \dots + x_n = 1$, в которой лежит симплекс Δ,

однозначно задаётся своим действием на вершины симплекса Δ, полная группа O_Δ симплекса Δ изоморфна симметрической группе S_{n+1} перестановок его вершин $0,\ 1,\ \dots,\ n$. Каждая k-мерная грань симплекса Δ является правильным k-мерным симплексом и представляет собою выпуклую оболочку каких-либо $k+1$ вершин симплекса Δ, и наоборот, выпуклая оболочка $[i_0, i_1, \dots, i_k]$ любых $k+1$ различных вершин $\{i_0, i_1, \dots, i_k\} \subset \{0, 1, \dots, n\}$ является k-мерной гранью симплекса Δ. Симплекс Δ симметричен относительно $n(n+1)/2$ гиперплоскостей π_{ij}, проходящих через середину ребра $[i, j]$ и противолежащую этому ребру грань коразмерности 2 с вершинами $\{0,\ 1,\ \dots\ ,\ n\}\setminus\{i, j\}$. Гиперплоскость π_{ij} перпендикулярна вектору $e_i - e_j$ и отражение $\sigma_{ij} \in \mathrm{O}_\Delta$ в этой гиперплоскости отвечает транспозиции элементов i и j в симметрической группе S_{n+1}.

Упражнение 12.4. Убедитесь, что гиперплоскости π_{ij} и π_{km} с $\{i, j\}\cap\{k, m\} = \varnothing$ ортогональны, а плоскости π_{ij} и π_{jk} с различными i, j, k пересекаются под углом $\pi/3 = 60^\circ$.

Плоскости π_{ij} осуществляют *барицентрическое разбиение* симплекса Δ на $(n+1)!$ меньших симплексов с вершинами в центрах граней симплекса Δ и в центре самого симплекса. Если обозначить через $\langle i_0 i_1\ \dots\ i_m\rangle$ центр m-мерной грани с вершинами в $i_0, i_1, \dots, i_m$, то каждый симплекс барицентрического разбиения будет иметь одну из вершин в какой-либо вершине $\langle i_0\rangle$ симплекса Δ, следующую вершину — в центре $\langle i_0 i_1\rangle$ какого-либо примыкающего к вершине i_0 ребра $[i_0, i_1]$, следующую вершину — в центре $\langle i_0 i_1 i_2\rangle$ какой-либо примыкающей к ребру $[i_0, i_1]$ двумерной треугольной грани $[i_0, i_1, i_2]$ и т. д. вплоть до центра $\langle i_0 i_1\ \dots\ i_n\rangle$ самого симплекса Δ. Таким образом, симплексы барицентрического разбиения симплекса Δ, осуществляемого гиперплоскостями π_{ij}, находятся в естественной биекции с перестановками $g \in S_{n+1}$: перестановке $g = (g_0, g_1,\ \dots,\ g_n) \in S_{n+1}$ отвечает симплекс с вершинами[1]

$$\langle g_0\rangle,\ \langle g_0, g_1\rangle,\ \langle g_0, g_1, g_2\rangle,\ \dots,\ \langle g_0 g_1\ \dots\ g_{n-1}\rangle,\ \langle g_0 g_1\ \dots\ g_n\rangle\,. \tag{12-8}$$

Этот симплекс является образом начального симплекса

$$e = \big[\langle 0\rangle,\ \langle 01\rangle,\ \langle 012\rangle,\ \dots,\ \langle 0,\ 1,\ \dots\ ,\ n-1\rangle,\ \langle 0,\ 1,\ \dots\ ,\ n\rangle\big] \tag{12-9}$$

под действием ортогонального преобразования $g \in S_{n+1} = \mathrm{O}_M$. Как и выше, пометим каждый симплекс (12-8) соответствующим преобразованием g и спроектируем поверхность симплекса Δ из его центра на описанную сферу. Мы получим разбиение $(n-1)$-мерной сферы S^{n-1} на $(n+1)!$ надписанных элементами $g \in S_{n+1}$ попарно конгруэнтных $(n-1)$-мерных симплексов, грани которых высекаются из сферы гиперплоскостями π_{ij}. При $n = 3$ получится представленная на рис. 12⋄4 на стр. 172 триангуляция двумерной сферы S^2 двадцатью четырьмя сферическими треугольниками с углами $\pi/3$, $\pi/3$ и $\pi/2$. Помеченному тождественным преобразованием e начальному симплексу (12-9) отвечает сферический симплекс, высекаемый из сферы n гиперплоскостями $\pi_i \stackrel{\text{def}}{=} \pi_{i-1,i}$ с $1 \leqslant i \leqslant n$. Обозначим через $\sigma_i = \sigma_{i-1,i}$ отражения в этих гиперплоскостях. В симметрической группе S_{n+1} эти отражения суть транспозиции $|i-1, i\rangle$ пар соседних элементов. В силу упр. 12.4 они удовлетворяют соотношениям[2]

$$\sigma_i^2 = e\,,\quad \sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1} \quad\text{и}\quad \sigma_i\sigma_j = \sigma_j\sigma_i\,,\quad \text{где}\quad |i-j| \geqslant 2\,. \tag{12-10}$$

[1] Первой вершиной служит вершина g_0 симплекса Δ, второй — середина выходящего из g_0 ребра $[g_0, g_1]$, третьей — центр примыкающей к этому ребру треугольной грани $[g_0, g_1, g_2]$ и т. д. вплоть до последней вершины, расположенной в центре симплекса Δ.

[2] Соотношение $\sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}$ является более употребительной в данном контексте записью циклического соотношения $(\sigma_i\sigma_{i+1})^3 = e$ на поворот $\sigma_i\sigma_{i+1}$ на 120° вокруг $(n-2)$-мерного подпространства $\pi_i \cap \pi_{i+1}$.

Упражнение 12.5. Убедитесь напрямую, что транспозиции $\sigma_i = |i-1, i\rangle \in S_{n+1}$ удовлетворяют соотношениям (12-10).

В силу этих соотношений, гомоморфизм свободой группы на алфавите $\{x_1, x_2, \dots, x_n\}$, переводящий x_i в σ_i, факторизуется до гомоморфизма $\varphi : F_n / H \to S_{n+1}$, где $H \rtimes F_n$ — наименьшая нормальная подгруппа, содержащая слова

$$x_i^2\,, \quad (x_i x_{i+1})^3 \quad \text{и} \quad (x_i x_j)^2\,, \quad \text{где} \quad |i-j| \geqslant 2\,. \tag{12-11}$$

Чтобы убедиться в его сюрьективности, выберем в симплексах e и g точки a и b так, чтобы они не были диаметрально противоположны и соединяющая их геодезическая[1] не пересекала граней коразмерности[2] 2. Пройдя из a в b по этой геодезической, мы получим разложение

$$g = \sigma_{i_1} \dots \sigma_{i_m}\,, \tag{12-12}$$

в котором каждое $i_\nu \in \{1, \dots, n\}$ равно номеру того зеркала $g_\nu(\pi_\nu)$, через которое осуществляется переход из ν-того встреченного по дороге симплекса $g_\nu = \sigma_1 \dots \sigma_{\nu-1}$ в следующий симплекс $g_{\nu+1} = \sigma_{g_\nu(\pi_{i_\nu})} g_\nu = g_\nu \sigma_{i_\nu}$. Дословно также как и в прим. 12.2 проверяется, что длина представления (12-12), полученного с помощью дуги $[a, b]$ не зависит от выбора её концов $a \in e$ и $b \in g$ при условии, что они не диаметрально противоположны и плоскость π_{ab} не проходит через пересечения зеркал π_{ij}: если при перемещении точек a и b внутри симплексов e и g дуга $[a, b]$ пройдёт через грань коразмерности 2 вида $g_k(\pi_i \cap \pi_j)$ с $|i-j| \geqslant 2$, вдоль которой пересекаются перпендикулярные гиперграни $g_k(\pi_i)$, $g_k(\pi_j)$, или через грань вида $g_k(\pi_i \cap \pi_{i+1})$, вдоль которой под углом 60° пересекаются гиперграни $g_k(\pi_i)$, $g_k(\pi_{i+1})$, то в представлении $g = \sigma_1 \dots \sigma_m$ стоящий на k-том месте фрагмент $\sigma_i \sigma_j$ или $\sigma_i \sigma_{i+1} \sigma_i$ заменится, соответственно, равным ему в группе O_Δ фрагментом $\sigma_j \sigma_i$ или $\sigma_{i+1} \sigma_i \sigma_{i+1}$. В ортогональной проекции вдоль $(n-2)$-мерного подпространства $g_k(\pi_i \cap \pi_j)$ или $g_k(\pi_i \cap \pi_{i+1})$ на ортогональную ему двумерную плоскость мы при этом увидим картину вроде показанной на рис. 12⋄5 на стр. 173. Как и в прим. 12.2, индукция по длине кратчайшего представления элемента $w \in F_n / H$ показывает, что последовательность индексов $i_1, \dots, i_m$ в каждом кратчайшем по модулю соотношений (12-11) представлении $w = x_{i_1} \dots x_{i_m}$ совпадает с последовательностью индексов в представлении (12-12) элемента $g = \varphi(w) \in \mathrm{O}_\Delta$, полученном при помощи подходящей дуги $[a, b]$ с $a \in e$, $b \in g$. Таким образом, симметрическая группа S_{n+1} задаётся n образующими x_i, $1 \leqslant i \leqslant n$, связанными соотношениями (12-11).

Разумеется, эту геометрическую картину можно выхолостить до сугубо комбинаторного рассуждения, что мы сделаем в n° 12.1.3 ниже.

Упражнение 12.6. Покажите, что знакопеременная группа A_{n+1} порождается а) парами непересекающихтранспозиций б) 3-циклами $|k-2, k-1, k\rangle$, где $2 \leqslant k \leqslant n$.

12.1.3. Порядок Брюа на S_{n+1}. Будем называть количество всех инверсных пар[3] в перестановке $g = (g_0, g_1, \dots, g_n) \in S_{n+1}$ *длиной* перестановки g и обозначать его $\ell(g)$.

Упражнение 12.7. Убедитесь, что $0 \leqslant \ell(g) \leqslant n(n+1)/2$ для всех $g \in S_{n+1}$, причём имеется ровно по одной перестановке длин 0 и $n(n+1)/2$. Что это за перестановки?

[1] Кратчайшая из двух дуг ab большой окружности, высекаемой из сферы двумерной плоскостью, проходящей через точки a, b и центр сферы.

[2] Т. е. пересечений всевозможных пар зеркал π_{ij}.

[3] Напомню, пара (i, j), где $1 \leqslant i < j \leqslant n$ называется *инверсной парой* перестановки $g \in S_n$, если $g_i = g(i) > g(j) = g_j$, см. n° 8.1.2 на стр. 108.

Правое умножение перестановки g на транспозицию $\sigma_i = |i-1, i\rangle$ приводит к перестановке $g\sigma_i$, отличающейся от g транспозицией $(i-1)$-того и i-го символов g_{i-1} и g_i:

$$\big(g_0, \ldots, g_{i-2}, \boldsymbol{g_{i-1}}, \boldsymbol{g_i}, g_{i+1}, \ldots, g_n\big) \circ \sigma_i = \big(g_0, \ldots, g_{i-2}, \boldsymbol{g_i}, \boldsymbol{g_{i-1}}, g_{i+1}, \ldots, g_n\big)\,,$$

причём $\ell(g\sigma_i) = \ell(g) + 1$, если $g_{i-1} < g_i$, и $\ell(g\sigma_i) = \ell(g) - 1$, если $g_{i-1} > g_i$. Поэтому любая перестановка g длины $\ell(g) = m$ может быть записана словом $g = \sigma_{i_1} \cdots \sigma_{i_m}$, в котором каждый переход от перестановки $h = \sigma_{i_1} \cdots \sigma_{i_{k-1}} = (h_0, \ldots, h_n)$ к перестановке $h\sigma_{i_k}$ заключается в транспозиции пары соседних возрастающих элементов $h_{i_v - 1} < h_{i_v}$. Частичный порядок на S_{n+1}, в котором $g < h$, если h получается из g увеличивающими длину транспозициями соседних элементов, называется *порядком Брюа*. Слово $w = x_{i_1} \cdots x_{i_m}$ в свободной группе F_n с образующими $x_1, \ldots, x_n$ называется *минимальным словом* перестановки $g \in S_{n+1}$, если $m = \ell(g)$ и $g = \sigma_{i_1} \cdots \sigma_{i_m}$. Начальные фрагменты минимального слова задают строго возрастающую в смысле порядка Брюа последовательность элементов $h_v = \sigma_{i_1}\sigma_{i_2} \cdots \sigma_{i_v} \in S_{n+1}$. Перестановка g может иметь много разных минимальных слов, однако не может быть записана никаким более коротким словом.

Предложение 12.3
При гомоморфизме $\varphi : F_n \to S_{n+1}$, $x_i \mapsto \sigma_i$, каждое слово $w \in F_n$ эквивалентно минимальному слову перестановки $\varphi(w) \in S_{n+1}$ по модулю соотношений

$$x_i^2 = e\,, \quad x_i x_{i+1} x_i = x_{i+1} x_i x_{i+1} \quad \text{и} \quad x_i x_j = x_j x_i \text{ при } |i-j| \geqslant 2\,,$$

а все минимальные слова перестановки $\varphi(w)$ эквивалентны между собой.

Доказательство. Индукция по количеству букв в слове $w \in F_{n-1}$. Для $w = \varnothing$ утверждение очевидно. Пусть для всех слов из $\leqslant m$ букв предложение доказано. Достаточно для каждого m-буквенного слова w и каждой буквы x_v проверить предложение для слова wx_v. Если слово w не является минимальным словом элемента $g = \varphi(w)$, то по индукции оно эквивалентно более короткому минимальному слову. Тогда и wx_v эквивалентно более короткому слову, и предложение справедливо по индукции. Поэтому мы будем далее считать, что слово w является минимальным словом элемента $g = \varphi(w) = (g_0, g_1, \ldots, g_n)$. Возможны два случая: либо $g_{v-1} > g_v$, либо $g_{v-1} < g_v$. В первом случае у перестановки g есть минимальное слово вида ux_v, по предположению индукции эквивалентное слову w. Тогда $wx_v \sim ux_vx_v \sim u$ и элемент $\varphi(wx_v) = \varphi(u)$ является образом более короткого, чем w слова u, эквивалентного слову wx_v. По индукции, слово u эквивалентно минимальному слову элемента $\varphi(wx_v)$ и все такие слова эквивалентны друг другу. Поэтому то же верно и для эквивалентного u слова wx_v.

Остаётся рассмотреть случай $g_{v-1} < g_v$. Здесь $\ell(g\sigma_v) = \ell(g) + 1$ и слово wx_v является минимальным словом для элемента $\varphi(wx_v)$. Мы должны показать, что любое другое минимальное слово w' этого элемента эквивалентно wx_v. Для самой правой буквы слова w' есть 3 возможности: либо она равна x_v, либо она равна $x_{v\pm1}$ либо она равна x_μ с $|\mu - v| \geqslant 2$. В пером случае $w' = ux_v$, где u, как и w, является минимальным словом элемента g. По индукции $u \sim w$, а значит, и $w' = ux_k \sim wx_k$.

Пусть теперь $w' = ux_{v+1}$ — ситуация, когда $w' = ux_{v-1}$, полностью симметрична. Поскольку оба слова wx_v и ux_{v+1} минимальны для перестановки $h = \varphi(wx_v) = \varphi(ux_{v+1})$, в перестановке h на местах с номерами $v-1$, v, $v+1$ стоят числа $g_v > g_{v-1} > g_{v+1}$, а в перестановке $g = (g_0, g_1, \ldots, g_n) = \varphi(w)$ на этих же местах — числа $g_{v-1} < g_v > g_{v+1}$ с

$g_{\nu-1} > g_{\nu+1}$. Поэтому у перестановки h имеется минимальное слово вида $sx_{\nu+1}x_\nu x_{\nu+1}$, а у перестановки g — минимальное слово вида $tx_\nu x_{\nu+1}$. Перестановка $h' = \varphi(s) = \varphi(t)$ отличается от h тем, что числа на местах с номерами $\nu-1$, ν, $\nu+1$ в ней возрастают и равны $g_{\nu+1} < g_{\nu-1} < g_\nu$. Поскольку $\ell(h') = \ell(h) - 3 = \ell(g) - 2$, оба слова t и s минимальны для h' и по индукции эквивалентны. Кроме того, по индукции w эквивалентно $tx_\nu x_{\nu+1}$. Поэтому $wx_\nu \sim tx_\nu x_{\nu+1}x_\nu \sim sx_\nu x_{\nu+1}x_\nu \sim sx_{\nu+1}x_\nu x_{\nu+1}$. Но $sx_{\nu+1}x_\nu \sim u$, поскольку оба слова минимальны для одной и той же перестановки[1] длины $m = \ell(h) - 1$. Таким образом, $wx_\nu \sim ux_{\nu+1}$.

Наконец, пусть $h = \varphi(wx_\nu) = \varphi(ux_\mu)$, где $|\mu - \nu| \geqslant 2$. Тогда в h есть два непересекающихся фрагмента $g_{\nu-1} > g_\nu$ и $g_{\mu-1} > g_\mu$. Поэтому у h есть минимальные слова вида $tx_\mu x_\nu$ и вида $sx_\nu x_\mu$, где t и s являются минимальными словами для перестановки $\varphi(t) = \varphi(s)$, отличающейся от h тем, что расматриваемые 2 фрагмента в ней имеют вид $g_\nu < g_{\nu-1}$ и $g_\mu < g_{\mu-1}$. Так как длина этой перестановки равна $\ell(h) - 2 = m - 1$, по индукции $t \sim s$. Поскольку tx_μ — минимальное слово для g, по индукции $w \sim tx_\mu$. Аналогично, т. к. sx_ν и u — минимальные слова для перестановки $\varphi(sx_\nu) = \varphi(u)$, отличающейся от h' транспозицией первого из двух фрагментов и потому имеющей длину $\ell(h) - 1 = m$, по индукции $sx_\nu \sim u$. Таким образом, $wx_\nu \sim tx_\mu x_\nu \sim sx_\mu x_\nu \sim sx_\nu x_\mu \sim ux_\mu$, что и требовалось. □

12.2. Простые группы и композиционные факторы. Группа G называется *простой*, если она не содержит нормальных подгрупп, отличных от $\{e\}$ и G. Например, любая группа простого порядка проста, поскольку по теореме Лагранжа вообще не содержит никаких подгрупп кроме $\{e\}$ и G. Согласно сл. 11.1 на стр. 156 простота группы G равносильна тому, что всякий гомоморфизм $G \to G'$ либо является вложением, либо отображает всю группу G в единицу.

Определение 12.1 (композиционный ряд)
Конечная строго убывающая последовательность подгрупп

$$G = G_0 \supsetneq G_1 \supsetneq G_2 \supsetneq \cdots \supsetneq G_{n-1} \supsetneq G_n = \{e\} \tag{12-13}$$

называется *композиционным рядом* или *рядом Жордана–Гёльдера* группы G, если при каждом i подгруппа G_{i+1} нормальна в G_i и фактор G_i / G_{i+1} прост. В этой ситуации неупорядоченный набор простых групп G_i / G_{i+1} (в котором возможны повторения) называется набором *композиционных факторов* (или *факторов Жордана–Гёльдера*) группы G. Число n называется *длиной* композиционного ряда (12-13).

Пример 12.3 (композиционные факторы S_4)
Выше мы видели, что симметрическая группа S_4 имеет композиционный ряд

$$S_4 \rhd A_4 \rhd V_4 \rhd \mathbb{Z}/(2) \rhd \{e\},$$

в котором $A_4 \rtimes S_4$ — подгруппа чётных перестановок, $V_4 \rtimes A_4$ — подгруппа Клейна, состоящая из тождественной перестановки и трёх перестановок циклового типа $\square\!\square$, а

$$\mathbb{Z}/(2) \rtimes V_4 \simeq \mathbb{Z}/(2) \oplus \mathbb{Z}/(2)$$

любая из трёх циклических подгрупп второго порядка, порождённых неединичными элементами. Таким образом, симметрическая группа S_4 имеет композиционные факторы $\mathbb{Z}/(2) = S_4/A_4$, $\mathbb{Z}/(3) = A_4/V_4$, $\mathbb{Z}/(2) = V_4/\big(\mathbb{Z}/(2)\big)$ и $\mathbb{Z}/(2) = \mathbb{Z}/(2)/\{e\}$.

[1] Она отличается от g, h и h' тем, что числа в позициях с номерами $\nu-1$, ν, $\nu+1$ в ней упорядочены как $g_\nu > g_{\nu+1} < g_{\nu-1}$, где $g_\nu > g_{\nu-1}$.

Упражнение 12.8. Убедитесь, что $A_4/V_4 \simeq \mathbb{Z}/(3)$.

Теорема 12.1 (теорема Жордана – Гёльдера)
Если группа G имеет конечный композиционный ряд, то неупорядоченный набор его композиционных факторов не зависит от выбора композиционного ряда. В частности, все композиционные ряды имеют одинаковую длину.

Доказательство. Пусть у группы G есть два композиционных ряда

$$G = P_0 \supsetneq P_1 \supsetneq P_2 \supsetneq \cdots \supsetneq P_{n-1} \supsetneq P_n = \{e\} \tag{12-14}$$

$$G = Q_0 \supsetneq Q_1 \supsetneq Q_2 \supsetneq \cdots \supsetneq Q_{m-1} \supsetneq Q_m = \{e\}\,. \tag{12-15}$$

Мы собираемся вставить между последовательными членами этих рядов дополнительные цепочки нестрого убывающих подгрупп так, чтобы получившиеся удлинённые последовательности состояли из одинакового числа элементов, и построить между последовательными факторами полученных цепочек такую биекцию, что соответствующие друг другу факторы будут изоморфны. Применяя предл. 11.5 на стр. 167 к нормальной подгруппе $P_{i+1} \rtimes P_i$ и подгруппам $Q_\nu \cap P_i \subset P_i$, мы для каждого i получаем цепочку

$$P_i \supseteq (Q_1 \cap P_i)P_{i+1} \supseteq (Q_2 \cap P_i)P_{i+1} \supseteq \cdots \supseteq (Q_{m-1} \cap P_i)P_{i+1} \supseteq P_{i+1}\,, \tag{12-16}$$

которая начинается с P_i, кончается в P_{i+1} и имеет $(Q_{k+1} \cap P_i)P_{i+1} \rtimes (Q_k \cap P_i)P_{i+1}$ с

$$\frac{(Q_k \cap P_i)P_{i+1}}{(Q_{k+1} \cap P_i)P_{i+1}} \simeq \frac{(Q_k \cap P_i)}{(Q_{k+1} \cap P_i)(Q_k \cap P_{i+1})}\,. \tag{12-17}$$

Упражнение 12.9. Для любой четвёрки подгрупп A, B, C, D, в которой $A \rtimes B$ и $C \rtimes D$, постройте изоморфизм $(B \cap D)C/(A \cap D)C \simeq (B \cap D)/(A \cap D)(B \cap C)$.

Группа P_{i+1} является нормальной подгруппой во всех группах цепочки (12-16). Факторизуя по ней, получаем цепочку

$$\frac{P_i}{P_{i+1}} \supseteq \frac{(Q_1 \cap P_i)P_{i+1}}{P_{i+1}} \supseteq \frac{(Q_2 \cap P_i)P_{i+1}}{P_{i+1}} \supseteq \cdots \supseteq \frac{(Q_{m-1} \cap P_i)P_{i+1}}{P_{i+1}} \supseteq \{e\}\,, \tag{12-18}$$

в которой каждая подгруппа нормальна в предыдущей, а последовательные факторы

$$\frac{(Q_k \cap P_i)P_{i+1}/P_{i+1}}{(Q_{k+1} \cap P_i)P_{i+1}/P_{i+1}} \simeq \frac{(Q_k \cap P_i)P_{i+1}}{(Q_{k+1} \cap P_i)P_{i+1}} \simeq \frac{(Q_k \cap P_i)}{(Q_{k+1} \cap P_i)(Q_k \cap P_{i+1})}$$

совпадают с (12-17). Так как группа P_i/P_{i+1} проста, мы заключаем, что в цепочке (12-18) имеется ровно одно нестрогое включение, а все остальные включения — равенства. Тем самым, ровно один из факторов (12-17) отличен от единицы и изоморфен P_i/P_{i+1}.

Те же самые рассуждения с заменой P на Q позволяют вставить между последовательными группами $Q_k \rhd Q_{k+1}$ композиционного ряда (12-15) убывающую цепочку подгрупп

$$Q_k \supseteq (P_1 \cap Q_k)Q_{k+1} \supseteq (P_2 \cap Q_k)Q_{k+1} \supseteq \cdots \supseteq (P_{n-1} \cap Q_k)Q_{k+1} \supseteq Q_{k+1}\,, \tag{12-19}$$

каждая из которых нормальна в предыдущей, а последовательные факторы имеют вид

$$\frac{(P_i \cap Q_k)Q_{k+1}}{(P_{i+1} \cap Q_k)Q_{k+1}} \simeq \frac{(Q_k \cap P_i)}{(Q_{k+1} \cap P_i)(Q_k \cap P_{i+1})} \tag{12-20}$$

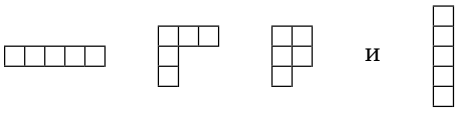
и изоморфны соответствующим факторам (12-17). Таким образом, вставляя между последовательными элементами композиционного ряда (12-14) цепочки (12-16), а между последовательными элементами ряда (12-15) — цепочки (12-19), мы получим цепочки одинаковой длины, в которых не все включения строгие, однако факторы которых биективно соответствуют друг другу так, что соответственные факторы (12-20) и (12-17) изоморфны. Остаётся заметить, что группа Q_{k+1} является нормальной подгруппой во всех группах цепочки (12-19), и то же рассуждение, что и с подгруппой P_{i+1} для цепочки (12-16), показывает, что при фиксированном k среди факторов (12-20) имеется ровно один отличный от единицы, и он изоморфен Q_k/Q_{k+1}. □

Замечание 12.1. Непростая группа может иметь несколько разных композиционных рядов с одинаковым набором факторов, а группы с одинаковыми наборами факторов Жордана-Гёльдера не обязательно изоморфны.

12.2.1. Конечные простые группы. Одним из крупных достижений математики XX века было создание полного списка всех конечных простых групп. Этот список состоит из нескольких бесконечных серий и 26 так называемых *спорадических групп*, не входящих в серии. Бесконечные серии делятся на три семейства: циклические группы $\mathbb{Z}/(p)$ простого порядка, знакопеременные группы A_n с[1] $n \geqslant 5$ и простые линейные алгебраические группы над конечными полями[2], такие как $\mathrm{PSL}_n(\mathbb{F}_q)$, $\mathrm{PSO}_n(\mathbb{F}_q)$, $\mathrm{PSp}_n(\mathbb{F}_q)$ и т. п. Эта классификация является итогом сотен работ десятков авторов по множеству напрямую несвязанных друг с другом направлений. Последние пробелы в ней, как принято считать, были устранены лишь в 2008 году. Какая-либо универсальная концепция, позволяющая единообразно классифицировать все конечные простые группы до сих пор не известна. Далее мы обсудим простоту знакопеременных групп.

Лемма 12.1
Знакопеременная группа A_5 проста.

Доказательство. В симметрической группе две перестановки сопряжены тогда и только тогда, когда у них одинаковый цикловой тип. Цикловые типы чётных перестановок из S_5 изображаются диаграммами



(12-21)

(5-циклы, 3-циклы, пары независимых транспозиций и тождественное преобразование). Эти классы сопряжённости в S_5 имеют мощность

$$5!/5 = 24 \qquad 5!/(3\cdot 2) = 20 \qquad 5!/(2^2\cdot 2) = 15 \qquad \text{и} \qquad 1\,.$$

Если перестановка относится к одному из последних трёх типов (12-21), то её централизатор содержит транспозицию пары неподвижных элементов или пары элементов, составляющих цикл длины 2. Поэтому две такие перестановки, сопряжённые в S_5, сопряжены и в A_5. Стало быть, перестановки каждого из трёх последних типов (12-21) образуют один класс сопряжённости

[1] Группа $A_3 \simeq \mathbb{Z}/(3)$ тоже проста.

[2] Описание и классификация таких групп даются в курсах линейных алгебраических и арифметических групп; представление о них можно получить по книге *Дж. Хамфри. Линейные алгебраические группы*. М., «Наука», 1980.

также и в A_5. Циклы длины 5 разбиваются в A_5 на два класса сопряжённости: 12 циклов, сопряжённых $|1,2,3,4,5\rangle$, и 12 циклов, сопряжённых $|2,1,3,4,5\rangle$. Поскольку любая нормальная подгруппа $H \rtimes A_5$ вместе с каждой перестановкой содержит и все ей сопряжённые,

$$|H| = 12\varepsilon_1 + 12\varepsilon_2 + 20\varepsilon_3 + 15\varepsilon_4 + 1\,,$$

где каждый из коэффициентов ε_k равен либо 1, либо 0. С другой стороны, $|H|$ является делителем $|A_5| = 60 = 3\cdot 4\cdot 5$.

Упражнение 12.10. Убедитесь, что такое возможно ровно в двух случаях: когда все $\varepsilon_k = 1$ или когда все $\varepsilon_k = 0$.

Таким образом, нормальные подгруппы в A_5 исчерпываются единичной подгруппой и всей группой A_5. □

Теорема 12.2
Все знакопеременные группы A_n с $n > 5$ тоже просты.

Доказательство. Индукция по n. Стабилизатор $\mathrm{Stab}_{A_n}(k)$ любого элемента $k \in \{1, 2, \dots, n\}$ изоморфен A_{n-1}. Если $N \rtimes A_n$, то пересечение $N \cap \mathrm{Stab}_{A_n}(k) \rtimes \mathrm{Stab}_{A_n}(k)$ по индукции либо совпадает со $\mathrm{Stab}_{A_n}(k)$ либо равно $\{e\}$. Поскольку стабилизаторы всех элементов сопряжены, подгруппа N либо содержит стабилизаторы всех элементов $1, 2, \dots, n$, либо тривиально пересекается с каждым из них. В первом случае N содержит все пары транспозиций и, стало быть, совпадает с A_n по упр. 12.6. Во втором случае если в N есть хоть одна перестановка, переводящая некое i в $j \neq i$, то в силу тривиальности $\mathrm{Stab}_N(j)$ эта перестановка является *единственной* в N перестановкой, переводящей i в j. Но при $n \geqslant 6$ у любой перестановки $g \in A_n$, переводящей i в j и не имеющей неподвижных точек, есть сопряжённые ей в A_n и отличные от неё перестановки, также переводящие i в j.

Упражнение 12.11. Убедитесь в этом.

Поскольку N нормальна, все эти перестановки тоже лежат в N. Противоречие. □

12.3. Полупрямые произведения. Для пары подгрупп N, H группы G положим

$$NH = \{xh \mid x \in N\,,\ h \in H\}\,.$$

Отображение $N \times H \to NH$, $(x,h) \mapsto xh$, биективно если и только если $N \cap H = \{e\}$. В самом деле, при $x_1h_1 = x_2h_2$ элемент $x_2^{-1}x_1 = h_2h_1^{-1} \in N \cap H$, и если $N \cap H = \{e\}$, то $x_2 = x_1$ и $h_2 = h_1$, а если в $N \cap H$ есть элемент $z \neq e$, то разные пары (e,e), $(z,z^{-1}) \in N \times H$ перейдут в один и тот же элемент $e \in NH$.

Будем называть подгруппы $N, H \subset G$ *дополнительными*, если $N \cap H = \{e\}$ и $NH = G$. В этом случае группа G как множество находится в биекции с прямым произведением $N \times H$. Если подгруппа $N \rtimes G$ при этом нормальна, то композиция элементов $g_1 = x_1h_1$ и $g_2 = x_2h_2$ может быть выражена в терминах пар (x_1,h_1), $(x_2,h_2) \in N \times H$. А именно, так как

$$g_1g_2 = x_1h_1x_2h_2 = x_1(h_1x_2h_1^{-1})\cdot h_1h_2 \quad \text{и} \quad h_1x_2h_1^{-1} \in N\,,$$

группу G можно *описать* как множество $N \times H$ с операцией

$$(x_1,h_1)\cdot(x_2,h_2) = (x_1\,\mathrm{Ad}_{h_1}(x_2), h_1h_2)\,, \tag{12-22}$$

где через $\mathrm{Ad}_h : N \xrightarrow{\sim} N$, $x \mapsto hxh^{-1}$, обозначено присоединённое действие элемента h на нормальной подгруппе N. В этой ситуации говорят, что группа G является *полупрямым произведением* нормальной подгруппы $N \rtimes G$ и дополнительной к ней подгруппы $H \subset G$ и пишут $G = N \rtimes H$. Если сопряжение элементами из подгруппы H действует на подгруппе N тривиально, что равносильно перестановочности $xh = xh$ любых двух элементов $x \in N$ и $h \in H$, то полупрямое произведение называется *прямым*. В этом случае

$$(x_1, h_1) \cdot (x_2, h_2) = (x_1 x_2, h_1 h_2)$$

для любых пар (x_1, h_1), $(x_2, h_2) \in N \times H$.

Пример 12.4 ($D_n = \mathbb{Z}/(n) \rtimes \mathbb{Z}/(2)$)
Группа диэдра D_n содержит нормальную подгруппу поворотов, изоморфную аддитивной группе $\mathbb{Z}/(n)$. Подгруппа второго порядка, порождённая любым отражением, дополнительна к группе поворотов и изоморфна аддитивной группе $\mathbb{Z}/(2)$. Присоединённое действие отражения на группе поворотов меняет знак у угла поворота. При отождествлении группы поворотов с $\mathbb{Z}/(n)$ это действие превращается в умножение на -1. Таким образом, $D_n = \mathbb{Z}/(n) \rtimes \mathbb{Z}/(2)$ и в терминах пар $(x, y) \in \mathbb{Z}/(n) \times \mathbb{Z}/(2)$ композиция на группе диэдра задаётся правилом

$$\big(x_1, y_1\big) \cdot \big(x_2, y_2\big) = \big(x_1 + (-1)^{y_1} x_2, y_1 + y_2\big)\,, \quad x_1, x_2 \in \mathbb{Z}/(n)\,, \quad y_1, y_2 \in \mathbb{Z}/(2)\,.$$

Пример 12.5 ($\mathrm{Aff}(V) = V \rtimes \mathrm{GL}(V)$, продолжение прим. 11.20 на стр. 165)
Аффинная группа[1] $\mathrm{Aff}(V)$ содержит нормальную подгруппу параллельных переносов, которая изоморфна аддитивной группе векторного пространства V и является ядром сюръективного гомоморфизма групп

$$D : \mathrm{Aff}(V) \twoheadrightarrow \mathrm{GL}(V)\,, \quad \varphi \mapsto D_\varphi\,, \tag{12-23}$$

сопоставляющего аффинному преобразованию $\varphi : \mathbb{A}(V) \to \mathbb{A}(V)$ его дифференциал

$$D_\varphi : V \to V\,, \quad \overrightarrow{pq} \mapsto \overrightarrow{\varphi(p)\varphi(q)}\,.$$

Если зафиксировать в $\mathbb{A}(V)$ какую-нибудь точку p, то ограничение гомоморфизма (12-23) на стабилизатор $\mathrm{Stab}_p \subset \mathrm{Aff}(V)$ задаст изоморфизм $D_p : \mathrm{Stab}_p \xrightarrow{\sim} \mathrm{GL}(V)$. Обратный изоморфизм сопоставляет линейному оператору $f : V \xrightarrow{\sim} V$ аффинное преобразование

$$\varphi_f : \mathbb{A}(V) \to \mathbb{A}(V)\,, \quad x \mapsto p + f(\overrightarrow{px})\,,$$

оставляющее на месте точку p. Поскольку каждое преобразование $\varphi \in \mathrm{Aff}(V)$ раскладывается в композицию $\varphi = \tau_v \circ (\tau_{-v} \circ \varphi)$ параллельного переноса τ_v на вектор $v = \overrightarrow{p\varphi(p)}$ и преобразования $\tau_{-v} \circ \varphi \in \mathrm{Stab}(p)$, группа $\mathrm{Aff}(V) = V \rtimes \mathrm{Stab}_p \simeq V \rtimes \mathrm{GL}(V)$. Согласно прим. 11.20 на стр. 165, композиция в группе $V \rtimes \mathrm{GL}(V)$ задаётся правилом $(u, f) \cdot (w, g) = (u + f(w),\ fg)$.

12.3.1. Полупрямое произведение групп. Предыдущую конструкцию можно применить к двум абстрактным группам N и H как только задано действие группы H на группе N, т. е. гомоморфизм группы H в группу автоморфизмов группы N:

$$\psi : H \to \mathrm{Aut}\, N\,, \quad h \mapsto \psi_h : N \xrightarrow{\sim} N\,, \tag{12-24}$$

[1] См. прим. 11.20 на стр. 165.

По аналогии с форм. (12-22) на стр. 181 зададим на множестве $N \times H$ операцию правилом

$$(x_1, h_1) \cdot (x_2, h_2) \stackrel{\text{def}}{=} (x_1 \psi_{h_1}(x_2), h_1 h_2)\,. \tag{12-25}$$

Упражнение 12.12. Проверьте, что формула (12-25) задаёт на $N \times H$ структуру группы с единицей (e, e) и обращением $(x, h)^{-1} = \left(\psi_h^{-1}(x^{-1}), h^{-1}\right)$, где $\psi_h^{-1} = \psi_{h^{-1}}$ — автоморфизм, обратный к $\psi_h : N \xrightarrow{\sim} N$.

Полученная таким образом группа называется *полупрямым произведением* групп N и H по действию $\psi : N \to \operatorname{Aut} H$ и обозначается $N \rtimes_\psi H$. Подчеркнём, что результат зависит от выбора действия ψ. Если действие тривиально, т. е. $\psi_h = \mathrm{Id}_N$ для всех $h \in H$, мы получаем прямое произведение $N \times H$ с покомпонентными операциями.

Упражнение 12.13. Убедитесь, что подмножество $N' \stackrel{\text{def}}{=} \{(x, e) \mid x \in N\}$ является изоморфной группе N нормальной подгруппой в $G = N \rtimes_\psi H$ и фактор $G / N' \simeq H$, а подмножество $H' \stackrel{\text{def}}{=} \{(e, h) \mid h \in H\}$ (e, h) является изоморфной H и дополнительной к N' подгруппой в G, причём $G = N' \rtimes H'$ является полупрямым произведением своих подгрупп N' и H'.

12.4. p-группы и теоремы Силова. Группа порядка p^n, где $p \in \mathbb{N}$ — простое, называется *p-группой*. Поскольку все подгруппы p-группы также являются p-группами, длина любой орбиты p-группы при любом её действии на любом множестве либо делится на p, либо равна единице. Мы получаем простое, но полезное

Предложение 12.4
Пусть p-группа G действует на конечном множестве X, число элементов в котором не делится на p. Тогда G имеет на X неподвижную точку. □

Предложение 12.5
Любая p-группа имеет нетривиальный центр.

Доказательство. Рассмотрим присоединённое действие группы на себе. Центр группы представляет собой множество неподвижных точек этого действия. Поскольку и число элементов в группе, и длины всех орбит, содержащих более одной точки, делятся на p, кроме одноточечной орбиты e должны быть и другие одноточечные орбиты. □

Упражнение 12.14. Покажите, что любая группа G порядка p^2 (где p простое) абелева.

Определение 12.2 (силовские подгруппы)
Пусть G — произвольная конечная группа. Запишем её порядок в виде $|G| = p^n m$, где p — простое, $n \geqslant 1$, и m взаимно просто с p. Всякая подгруппа $S \subset G$ порядка $|S| = p^n$ называется *силовской p-подгруппой* в G. Количество силовских p-подгрупп в G обозначается через $N_p(G)$.

Теорема 12.3 (теорема Силова)
Для любого простого p, делящего $|G|$, силовские p-подгруппы в G существуют. Все они сопряжены друг другу, и любая p-подгруппа в G содержится в некоторой силовской p-подгруппе.

Доказательство. Пусть $|G| = p^n m$, где m взаимно просто с p. Обозначим через $\mathcal{E}$ множество p^n-элементных подмножеств в G и рассмотрим действие G на $\mathcal{E}$, индуцированное левым регулярным действием G на себе. Стабилизатор точки $F \in \mathcal{E}$ состоит из всех элементов $g \in G$, левое умножение на которые переводит множество $F \subset G$ в себя: $\operatorname{Stab}(F) = \{g \in G \mid gF \subset F\}$. Так

как $g_1 x \neq g_2 x$ при $g_1 \neq g_2$ в группе G, группа $\mathrm{Stab}(F)$ свободно действует на множестве F и все орбиты этого действия состоят из $|\mathrm{Stab}(F)|$ точек. Поэтому $|F| = p^n$ делится на $|\mathrm{Stab}(F)|$ и имеется следующая альтернатива: либо длина G-орбиты элемента $F \in \mathcal{E}$ делится на p, либо G-орбита элемента $F \in \mathcal{E}$ состоит из m элементов и $|\mathrm{Stab}(F)| = p^n$, т. е. подгруппа $\mathrm{Stab}(F) \subset G$ силовская. Во втором случае согласно предл. 12.4 каждая p-подгруппа $H \subset G$ (в частности, каждая силовская подгруппа), имеет на G-орбите элемента F неподвижную точку gF, а значит, содержится в силовской подгруппе $\mathrm{Stab}(gF) = g\,\mathrm{Stab}(F)\,g^{-1}$, сопряжённой к $\mathrm{Stab}(F)$ (и совпадает с ней, если H силовская). Таким образом, для доказательства теоремы остаётся убедиться, что в множестве $\mathcal{E}$ есть G-орбита, длина которой не делится на p. Это вытекает из следующей ниже леммы. □

Лемма 12.2
$|\mathcal{E}| = \binom{p^n m}{p^n} \equiv m \pmod p$ не делится на p.

Доказательство. Класс вычетов $\binom{p^n m}{p^n} \pmod p$ равен коэффициенту при x^{p^n}, возникающему при раскрытии бинома $(1+x)^{p^n m}$ над полем $\mathbb{F}_p = \mathbb{Z}/(p)$. Так как возведение в p-тую степень над $\mathbb{F}_p$ является аддитивным гомоморфизмом, $(1+x)^{p^n} = 1+x^{p^n}$, откуда $(1+x)^{p^n m} = \left(1 + x^{p^n}\right)^m =$
$= 1 + m x^{p^n} +$ старшие степени. □

Следствие 12.1 (дополнение к теореме Силова)
В условиях теоремы Силова число N_p силовских p-подгрупп в G делит m и сравнимо с единицей по модулю p.

Доказательство. Обозначим множество силовских p-подгрупп в G через $\mathcal{S}$ и рассмотрим действие G на $\mathcal{S}$, индуцированное присоединённым действием G на себе. По теореме Силова это действие транзитивно, откуда $|\mathcal{S}| = |G|/|\mathrm{Stab}(P)|$, где $P \in \mathcal{S}$ — произвольно взятая силовская p-подгруппа. Поскольку $P \subset \mathrm{Stab}(P)$, порядок $|\mathrm{Stab}(P)|$ делится на $|P| = p^n$, а значит $|\mathcal{S}|$ делит $|G|/p^n = m$, что доказывает первое утверждение.

Для доказательства второго утверждения достаточно проверить, что P, действуя сопряжениями на $\mathcal{S}$, имеет там ровно одну неподвижную точку, а именно, саму себя. Тогда порядки всех остальных P-орбит будут делиться на p, и мы получим $|\mathcal{S}| \equiv 1 \pmod p$.

Пусть силовская подгруппа $H \in \mathcal{S}$ неподвижна при сопряжении подгруппой P. Это означает, что $P \subset \mathrm{Stab}(H) = \{g \in G \mid gHg^{-1} \subset H\}$. Поскольку $H \subset \mathrm{Stab}(H) \subset G$, порядок $|\mathrm{Stab}(H)| = p^n m'$, где $m'|m$ взаимно просто с p. Таким образом, и P, и H являются силовскими p-подгруппами в $\mathrm{Stab}(H)$, причём H нормальна в $\mathrm{Stab}(H)$. Так как все силовские подгруппы сопряжены, мы заключаем, что $H = P$, что и требовалось. □

Пример 12.6 (группы порядка pq с простыми $p > q$)
Пусть $|G| = pq$, где $p > q$ простые. Тогда в G есть ровно одна силовская p-подгруппа $H_p \simeq \mathbb{Z}/(p)$, автоматически нормальная. Рассмотрим любую силовскую q-подгруппу $H_q \simeq \mathbb{Z}/(q)$. Поскольку H_p и H_q просты, $H_p \cap H_q = e$ и $G = H_p H_q$. Согласно n° 12.3 $G = \mathbb{Z}/(p) \rtimes_\psi \mathbb{Z}/(q)$ для некоторого гомоморфизма $\psi : \mathbb{Z}/(q) \to \mathrm{Aut}(\mathbb{Z}/(p))$.

Упражнение 12.15. Убедитесь, что $\mathrm{Aut}(\mathbb{Z}/(p)) \simeq \mathbb{F}_p^* \simeq \mathbb{Z}/(p-1)$.

Гомоморфизм $\psi : \mathbb{Z}/(q) \to \mathrm{Aut}(\mathbb{Z}/(p))$ однозначно задаётся своим значением на образующей $[1]_q$, которая является элементом порядка q. Поэтому элемент $\eta = \psi([1]_q) \in \mathrm{Aut}(\mathbb{Z}/(p))$ либо единичный, либо имеет порядок q. По упр. 12.15 последнее возможно только при $q \mid (p-1)$,

и в этом случае элементы q-го порядка образуют в $\mathbb{F}_p^*$ циклическую мультипликативную подгруппу порядка q.

Упражнение 12.16. Убедитесь в этом.

Обозначим через $\eta \in \mathbb{F}_p^*$ одну из образующих этой подгруппы. Гомоморфизм

$$\psi : \mathbb{Z}/(p) \to \mathrm{Aut}(\mathbb{Z}/(p)), \quad [1]_q \mapsto \eta, \tag{12-26}$$

сопоставляет каждому элементу $[y]_q \in \mathbb{Z}/(q)$ автоморфизм $\psi_y : \mathbb{Z}/(p) \xrightarrow{\sim} \mathbb{Z}/(p)$, $[x]_p \mapsto [\eta^y x]_p$, и задаёт полупрямое произведение $\mathbb{Z}/(p) \rtimes_\psi \mathbb{Z}/(q)$ с операцией

$$\bigl([x_1]_p, [y_1]_q\bigr) \cdot \bigl([x_2]_p, [y_2]_q\bigr) = \bigl([x_1 + \eta^{y_1} x_2]_p, [y_1 + y_2]_q\bigr). \tag{12-27}$$

Любой другой гомоморфизм $\varphi : \mathbb{Z}/(q) \to \mathrm{Aut}(\mathbb{Z}/(p))$, $[1]_q \mapsto \eta^m$, с $1 \leqslant m \leqslant q-1$ является композицией гомоморфизма (12-26) и умножения на $m : \mathbb{Z}/(q) \xrightarrow{\sim} \mathbb{Z}/(q)$, $[y]_q \mapsto [my]_q$. Согласно упр. 12.17 ниже, полупрямые произведения $\mathbb{Z}/(p) \rtimes_\varphi \mathbb{Z}/(q)$ и $\mathbb{Z}/(p) \rtimes_\psi \mathbb{Z}/(q)$ изоморфны.

Упражнение 12.17. Для гомоморфизма $\psi : H \to \mathrm{Aut}(N)$, $h \mapsto \psi_h$, и автоморфизмов $\alpha : H \xrightarrow{\sim} H$ и $\beta : N \xrightarrow{\sim} N$ убедитесь, что отображения $(n, h) \mapsto (n, \alpha^{-1}h)$ и $(n, h) \mapsto (\beta n, h)$ задают, соответственно, изоморфизмы полупрямых произведений

$$N \rtimes_\psi H \xrightarrow{\sim} N \rtimes_{\psi\circ\alpha} H \quad \text{и} \quad N \rtimes_\psi H \xrightarrow{\sim} N \rtimes_{\mathrm{Ad}_\beta(\psi)} H,$$

где $\mathrm{Ad}_\beta(\psi) : H \to \mathrm{Aut}(N)$, $h \mapsto \beta\psi_h\beta^{-1}$.

Мы заключаем, что для простых $p > q$ при $q \nmid (p-1)$ группа порядка pq изоморфна $\mathbb{Z}/(p) \oplus \mathbb{Z}/(q)$, а при $q \mid (p-1)$ кроме абелевой есть ровно одна неабелева группа $\mathbb{Z}/(p) \rtimes \mathbb{Z}/(q)$ с операцией (12-27). В частности, для простого $p > 2$ имеется единственная с точностью до изоморфизма неабелева группа порядка $2p$, а именно, группа правильного p-угольника из прим. 12.4 на стр. 182.

Ответы и указания к некоторым упражнениям

Упр. 12.1. Первое очевидно, второе вытекает из того, что при вставке фрагментаЁ$x^{\varepsilon}x^{-\varepsilon}$ в произвольное слово w получится такое слово, в котором сокращение любого фрагмента вида $y^{\varepsilon}y^{-\varepsilon}$ приведёт либо обратно[1] к слову w, либо к слову, получающемуся из w сначала сокращением *того же самого фрагмента* $y^{\varepsilon}y^{-\varepsilon}$, а уже затем вставкой $x^{\varepsilon}x^{-\varepsilon}$ в *то же самое место*, что и в w.

Упр. 12.2. Отобразите $n \in \mathbb{N}$ в $x^n y x^n \in F_2$ и воспользуйтесь предл. 12.1 на стр. 168.

Упр. 12.3. Поскольку отображение $F\colon \mathbb{R}^n \to \mathbb{R}^n$ биективно, достаточно убедиться, что отображения $\sigma_{F(\pi)}$ и $F \circ \sigma_\pi \circ F^{-1}$ одинаково действуют на точку вида $F(p)$ с произвольным $p \in \mathbb{R}^n$.

Упр. 12.4. Обозначим через v_i вектор, идущий из центра симплекса Δ в вершину i. Вектор $n_{ij} = v_i - v_j$ ортогонален гиперплоскости π_{ij}, поскольку для любого $k \neq i, j$ скалярное произведение $\big(n_{ij}, v_k - (v_i + v_j)/2\big) = (v_i, v_k) - (v_j, v_k) + (v_i, v_i)/2 - (v_j, v_j)/2 = 0$, т. к. все произведения (v_i, v_j) с $i \neq j$ и все скалярные квадраты (v_i, v_i) одинаковы. Аналогичная выкладка показывает, что при $\{i, j\} \cap \{k, m\} = \varnothing$ векторы n_{ij} и n_{km} ортогональны. Векторы $v_i - v_k$ и $v_k - v_j$ образуют в натянутой на них двумерной плоскости стороны правильного треугольника с вершинами в концах векторов v_i, v_j и v_k, и угол между ними равен 60°.

Упр. 12.8. При эпиморфизме S_4 на группу треугольника из прим. 11.9 подгруппа чётных перестановок $A_4 \subset S_4$ переходит в группу вращений треугольника.

Упр. 12.9. Примените изоморфизм $HN/N \simeq H/H \cap N$ из предл. 11.5 на стр. 167 для $G = D$, $H = B \cap D$ и $N = (A \cap D)C$ и воспользуйтесь тем, что $HN = (B \cap D)(A \cap D)C = (B \cap D)C$ и $H \cap N = (B \cap D) \cap (A \cap D) = (A \cap D)(B \cap C)$ (последнее равенство вытекает из того, что любой элемент $d = ac \in (B \cap D) \cap (A \cap D)$ с $d \in B \cap D$, $a \in A \cap D$, и $c \in C$ имеет $c = a^{-1}d \in C \cap B$).

Упр. 12.10. Правая часть равенства $|H| = 12\varepsilon_1 + 12\varepsilon_2 + 20\varepsilon_3 + 15\varepsilon_4 + 1$, приведённая по модулям 3, 4 и 5, равна, соответственно, $1 - \varepsilon_3$, $1 - \varepsilon_4$ и $1 + 2(\varepsilon_1 + \varepsilon_2)$. Она может делиться на 3 или на 4 только если $\varepsilon_3 = 1$ или $\varepsilon_4 = 1$. В обоих случаях $|H| \geqslant 16$, так что $|H|$ не может быть ни 3, ни 4, ни $3 \cdot 4$, ни $3 \cdot 5$. Если $|H|$ делится на 5, то $\varepsilon_1 = \varepsilon_2 = 1$ и $|H| \geqslant 25$, так что $|H|$ не может быть ни 5, ни $4 \cdot 5$. Остаются ровно две возможности: $|H| = 1$ и $|H| = 3 \cdot 4 \cdot 5$.

Упр. 12.11. Рассмотрим любое $k \notin i, j, g^{-1}(i)$. Тогда $g(k) = m \notin \{i, j, k\}$. При $n \geqslant 6$ найдётся чётная перестановка h, оставляющая на месте i, j, k и переводящая m в $\ell \neq m$. Тогда hgh^{-1} переводит i в j, а k — в $\ell \neq m$.

Упр. 12.12. Проверка ассоциативности:

$$\big((x_1, h_1) \cdot (x_2, h_2)\big) \cdot (x_3, h_3) = \big(x_1\psi_{h_1}(x_2),\, h_1h_2\big) \cdot (x_3, h_3) = \big(x_1\psi_{h_1}(x_2)\psi_{h_1h_2}(x_3),\, h_1h_2h_3\big)$$
$$(x_1, h_1) \cdot \big((x_2, h_2) \cdot (x_3, h_3)\big) = (x_1, h_1) \cdot \big(x_2\psi_{h_2}(x_3),\, h_2h_3\big) = \Big(x_1\psi_{h_1}\big(x_2\psi_{h_2}(x_3)\big),\, h_1h_2h_3\Big).$$

Но $\psi_{h_1}\big(x_2\psi_{h_2}(x_3)\big) = \psi_{h_1}(x_2)\psi_{h_1} \circ \psi_{h_2}(x_3) = \psi_{h_1}(x_2)\psi_{h_1h_2}(x_3)$. Существование единицы: $(x, h) \cdot (e, e) = (x, \psi_h(e), he) = (x, h)$, поскольку $\psi_h(e) = e$ в силу того, что ψ_h гомоморфизм. Существование обратного: $\big(\psi_h^{-1}(x^{-1}),\, h^{-1}\big) \cdot (x, h) = \big(\psi_h^{-1}(x^{-1})\psi_h^{-1}(x^{-1}),\, h^{-1}h\big) = (e, e)$.

Упр. 12.13. Так как $\psi\colon H \to \operatorname{Aut} N$ — гомоморфизм, $\psi_e = \mathrm{Id}_N$ и

$$(x_1, e) \cdot (x_2, e) = (x_1\psi_e(x_2), e) = (x_1x_2, e),$$

[1] Обратите внимание, что такое происходит *не только* при сокращении того же самого фрагмента $x^{\varepsilon}x^{-\varepsilon}$, который был перед этим вставлен, но и при сокращении одной из букв $x^{\pm\varepsilon}$ с её соседкой.

т. е. элементы (x, e) образуют подгруппу, изоморфную N. Она нормальна, поскольку

$$(y,h)\cdot(x,e)\cdot\left(\psi_h^{-1}(y^{-1}),h^{-1}\right)=(y\psi_h(x),h)\cdot\left(\psi_h^{-1}(y^{-1}),h^{-1}\right)=\left(y\psi_h(x)y^{-1},e\right)\,.$$

Элементы (e, h) очевидно образуют дополнительную подгруппу, изоморфную H, и

$$\mathrm{Ad}_{(e,h)}(x,e)=(\psi_h(x),e)\,.$$

Упр. 12.14. Пусть центр $Z(G)=C$. Если $|C|=p$, то $C\simeq\mathbb{Z}/(p)\simeq G/C$. Пусть $a\in C$ — образующая центра, $b\in G$ — такой элемент, что смежный класс bC является образующей в G/C. Тогда любой элемент группы имеет вид $b^k a^m$. Так как a централен, любые два таких элемента коммутируют.

Упр. 12.15. Аддитивные автоморфизмы группы $\mathbb{Z}/(p)$ суть линейные автоморфизмы одномерного векторного пространства над полем $\mathbb{F}_p$. Они образуют группу $\mathrm{GL}_1(\mathbb{F}_p)\simeq\mathbb{F}_p^*$ ненулевых элементов поля $\mathbb{F}_p$ по умножению. Как и всякая конечная мультипликативная подгруппа поля, она циклическая.

Упр. 12.16. Корни многочлена x^q-1 образуют в поле $\mathbb{F}_p$ мультипликативную подгруппу из $\leqslant q$ элементов, автоматически циклическую[1]. При $q\mid(p-1)$ многочлен x^q-1 имеет ровно q корней $\eta=\zeta^{\alpha k}$, где $0\leqslant\alpha\leqslant q-1$, а $\zeta\in\mathbb{F}_p^*$ — любая образующая циклической мультипликативной группы $\mathbb{F}_p^*$.

Упр. 12.17. Отображение $(n,h)\mapsto(n,\alpha^{-1}h)$ переводит сомножители из левой части равенства $(n_1,h_1)(n_2,h_2)=(n_1\psi_{h_1}n_2,h_1h_2)$ в $(n_1,\alpha^{-1}h_1)$ и $(n_2,\alpha^{-1}h_2)$, произведение которых в $N\rtimes_{\psi\circ\alpha}H$ равно $(n_1\psi_{h_1}n_2,\alpha^{-1}(h_1h_2))$. Отображение $(n,h)\mapsto(\beta n,h)$ переводит те же самые сомножители в $(\beta n_1,h_1)$ и $(\beta n_2,h_2)$. Их произведение в $N\rtimes_{\mathrm{Ad}_\beta(\psi)}H$ равно $(\beta(n_1\psi_{h_1}n_2),h_1h_2)$.

[1] См. предл. 3.10 на стр. 49.