§13. Немного о строении групп

13.1. Свободные группы и соотношения. С произвольным множеством M связана группа F_M, которая называется *свободной группой*, порождённой множеством M. Она состоит из классов эквивалентных слов, написанных буквами x и x^{-1}, $x \in M$, по наименьшему отношению эквивалентности, отождествляющему между собою слова, которые отличаются 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 $w = x_1x_2 \ldots x_m$ является класс слова $w^{-1} = x_m^{-1} \ldots x_2^{-1}x_1^{-1}$, где каждое x_i — имеет вид x или x^{-1} с $x \in M$ и $\left(x^{-1}\right)^{-1} \stackrel{\text{def}}{=} x$.

Упражнение 13.1. 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 4-буквенного алфавита x, y, x^{-1}, y^{-1} уже довольно трудно обозрима.

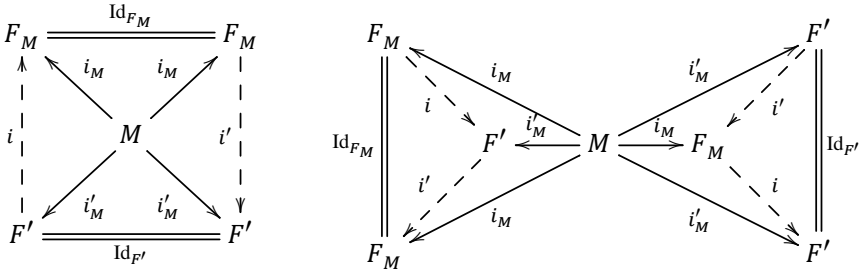
Упражнение 13.2. Постройте инъективный гомоморфизм групп $F_{\mathbb{N}} \hookrightarrow F_2$.

Предложение 13.1 (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 любой группы G и любого отображения множеств $\varphi_M : M \to G$ существует единственный гомоморфизм групп $\varphi : F_M \to G$, такой 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 изоморфизм групп $i' : F_M \xrightarrow{\sim} F'$, такой что $i'_M = i' \circ i_M$.

Доказательство. Гомоморфизм φ единствен, поскольку обязан переводить слово

$$w = x_1^{\varepsilon_1}x_2^{\varepsilon_2} \cdots x_m^{\varepsilon_m} \in F_M \qquad (x_\nu \in M\,, \quad \varepsilon_\nu = \pm 1)$$

в произведение $\varphi_M(x_1)^{\varepsilon_1}\varphi_M(x_2)^{\varepsilon_2} \cdots \varphi_M(x_m)^{\varepsilon_m} \in G$. 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. 13.1, то существуют единственные гомоморфизмы $i' : F_M \to F'$ и $i : F' \to F_M$, встраивающиеся в коммутативные диаграммы



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

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 $i' \circ i = \mathrm{Id}_{F'}$, $i \circ i' = \mathrm{Id}_{F_M}$. □

13.1.1. Задание групп образующими и соотношениями. Если гомоморфизм групп

$$\varphi : F_M \twoheadrightarrow G\,, \tag{13-1}$$

заданный отображением $\varphi_M : M \to G$, $m \mapsto g_m$, множества M в группу G, оказывается *сюръективным*, то говорят, что группа G *порождается* элементами $g_m = \varphi_M(m)$, $m \in M$, а сами эти элементы называются *образующими* группы G. В этом случае G исчерпывается всевозможными произведениями $g_1^{\varepsilon_1} g_2^{\varepsilon_2} \cdots g_k^{\varepsilon_k}$, $\varepsilon = \pm 1$, образующих и обратных к ним элементов. Группа G называется *конечно порождённой*, если она допускает конечное множество образующих. Ядро $\ker \varphi \lhd F_M$ эпиморфизма (13-1) 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 часто позволяет прояснить строение группы, явно строить её гомоморфизмы в другие группы и т. п. Однако в общем случае выяснить, изоморфны ли две группы, заданные своими образующими и определяющими соотношениями, и даже определить, отлична ли группа, заданная образующими и соотношениями, от тривиальной группы $\{e\}$, бывает непросто. Более того, даже в классе конечно определённых групп обе эти задачи являются *алгоритмически неразрешимыми*[1].

Предложение 13.2
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

$$x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_m^{\varepsilon_m} \mapsto \varphi(x_1)^{\varepsilon_1} \varphi(x_2)^{\varepsilon_2} \cdots \varphi(x_m)^{\varepsilon_m}\,,$$

когда для каждого слова $w = x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_m^{\varepsilon_m} \in R$ в группе G_2 выполняется соотношение

$$\varphi(x_1)^{\varepsilon_1} \varphi(x_2)^{\varepsilon_2} \cdots \varphi(x_m)^{\varepsilon_m} = 1\,.$$

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 $N_R \lhd F_M$ — наименьшая нормальная подгруппа, содержащая R, тогда и только тогда, когда $N_R \subset \ker \psi$. Так как $\ker \psi \lhd F_M$, для этого необходимио и достаточно включения $R \subset \ker \psi$. □

[1] в формальном смысле, принятом в математической логике

Пример 13.1 (образующие и соотношения группы диэдра)
Покажем, что группа диэдра D_n задаётся двумя образующими x_1, x_2 и соотношениями

$$x_1^2 = x_2^2 = (x_1x_2)^n = e\,. \tag{13-2}$$

Оси симметрии правильного n-угольника разбивают его на $2n$ конгруэнтных прямоугольных треугольников (см. рис. 13⋄1). Выберем один из них и обозначим через e. Поскольку любое движение плоскости однозначно задаётся своим действием на треугольник e, $2n$ движений $g \in D_n$ взаимно однозначно соответствуют треугольникам $g(e)$, в которые они переводят треугольник e. Пометим треугольник $g(e)$ преобразованием g. Обозначим через ℓ_1 и ℓ_2 стороны треугольника e, а через σ_1 и σ_2 — отражения плоскости относительно этих сторон. Тогда треугольники, получающиеся из e последовательными «перекатываниями» через стороны в направлении против ЧС пометятся элементами σ_2, $\sigma_2\sigma_1$, $\sigma_2\sigma_1\sigma_2$, $\sigma_2\sigma_1\sigma_2\sigma_1$, … , а треугольники, получающиеся «перекатываниями» по ЧС — элементами σ_1, $\sigma_1\sigma_2$, $\sigma_1\sigma_2\sigma_1$, $\sigma_1\sigma_2\sigma_1\sigma_2$, …

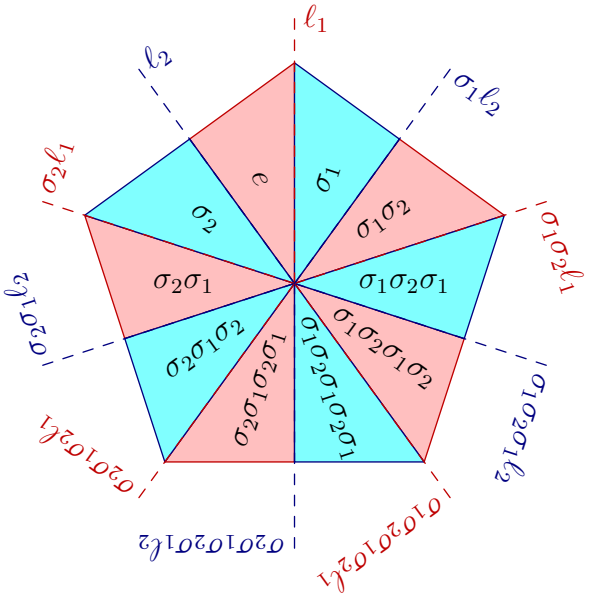


Рис. 13⋄1. Группа диэдра порождается отражениями.

Упражнение 13.3. Пусть F — произвольное движение плоскости, а σ_ℓ — отражение относительно прямой ℓ. Убедитесь, что $F \circ \sigma_\ell \circ F^{-1} = \sigma_{F(\ell)}$ или, что то же самое, $\sigma_{F(\ell)} \circ F = F \circ \sigma_\ell$.

Так как композиция $\sigma_1 \circ \sigma_2$ является поворотом в направлении от ℓ_2 к ℓ_1 на удвоенный угол между ℓ_2 и ℓ_1, равный $2\pi/n$, в группе D_n выполняются соотношения

$$\sigma_1^2 = \sigma_2^2 = (\sigma_1\sigma_2)^n = e\,. \tag{13-3}$$

По предл. 13.2 правило $x_1 \mapsto \sigma_1$, $x_2 \mapsto \sigma_2$ корректно задаёт сюръективный гомоморфизм $\varphi : F_2/H \twoheadrightarrow D_n$ из фактора свободной группы F_2 с образующими x_1, x_2 по наименьшей нормальной подгруппе $H \lhd F_2$, содержащей слова x_1^2, x_2^2 и $(x_1x_2)^n$. Каждое слово в алфавите $\{x_1, x_2\}$ по модулю соотношений (13-2) записывается словом $x_1x_2x_1\ldots$ или $x_2x_1x_2\ldots$ длины $< 2n$. Два таких слова переводятся гомоморфизмом φ в один и тот же элемент $g \in D_n$, если и только если сумма их длин равна[1] $2n$:

$$\varphi(\underbrace{x_1x_2x_1\ldots}_{k}) = \underbrace{\sigma_1\sigma_2\sigma_1\ldots}_{k} = g = \underbrace{\sigma_2\sigma_1\sigma_2\ldots}_{2n-k} = \varphi(\underbrace{x_2x_1x_2\ldots}_{2n-k})\,. \tag{13-4}$$

Упражнение 13.4. Убедитесь, что $\underbrace{x_1x_2x_1\ldots}_{k} = \underbrace{x_2x_1x_2\ldots}_{2n-k} \iff (x_1x_2)^n = e$.

Таким образом, гомоморфизм $\varphi : F_2/H \xrightarrow{\sim} D_n$ биективен.

[1] этому отвечают два способа «перекатить» треугольник e в треугольник g — двигаясь против ЧС и по ЧС, как на рис. 13⋄1)

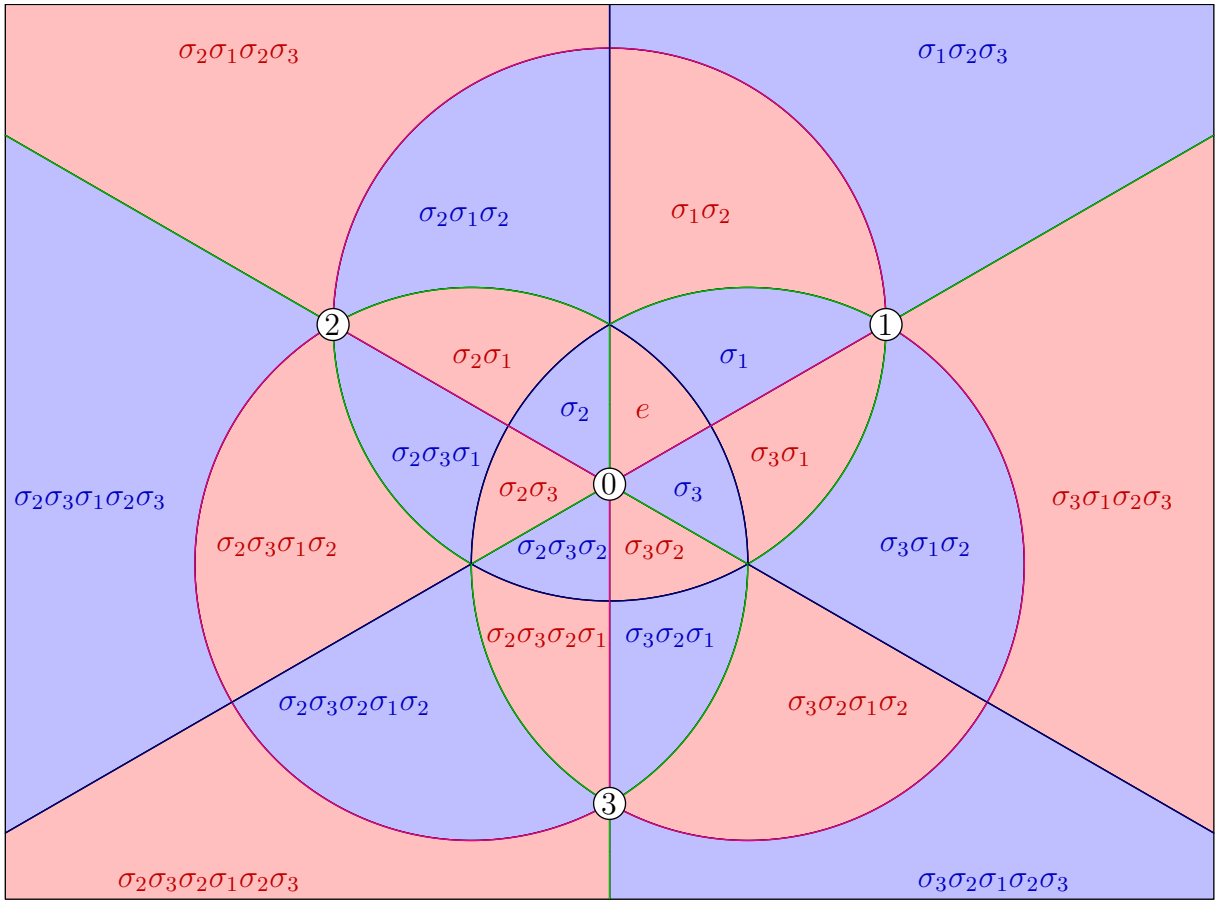


Рис. 13◇2. Триангуляция сферы плоскостями симметрии тетраэдра в стереографической проекции из диаметрально противоположной к вершине «0» точки на плоскость, параллельную грани «123».

Пример 13.2 (образующие и соотношения несобственных групп платоновых тел)
Рассмотрим платоново тело M с треугольными гранями — тетраэдр, октаэдр или икосаэдр. Плоскости симметрии многогранника M барицентрически разбивают каждую из граней на 6 треугольников, которые сходятся по $2m_1$ штук в вершинах M, по $2m_2$ штук в серединах рёбер M и по $2m_3$ штук в центрах граней M. Значения m_1, m_2, m_3 и общее число треугольников N для различных M таковы[1]:

M	m_1	m_2	m_3	N
тетраэдр	2	3	3	24
октаэдр	2	3	4	48
икосаэдр	2	3	5	120

Пересечения плоскостей симметрии с описанной около M сферой задают её триангуляцию N конгруэнтными сферическими треугольниками с углами[2] π/m_1, π/m_2, π/m_3

[1] n-угольный диэдр из предыдущего прим. 13.1 тоже вписывается в эту схему с $m_1 = 2$, $m_2 = 2$, $m_3 = n$ и $N = 4n$, если считать, что две его грани различны — скажем, покрашены в разные цвета, так что отражение в плоскости n-угольника является *нетривиальным* преобразованием

[2] они равны углам, под которыми пересекаются соответствующие плоскости симметрии

(см. рис. 13⋄2 на стр. 201). Поскольку любое линейное преобразование $\mathbb{R}^3$ однозначно задаётся своим действием на базисные векторы с концами в вершинах какого-нибудь сферического треугольника, который мы пометим буквой e, преобразования несобственной группы O_M тела M взаимно однозначно соответствуют N треугольникам триангуляции[1]. Мы пометим каждый треугольник тем преобразованием $g \in \mathrm{O}_M$, которое переводит в него треугольник e. Назовём плоскости, высекающие стороны треугольника e, буквами π_1, π_2, π_3 так, чтобы угол между плоскостями π_i и π_j равнялся π/m_k, и обозначим отражение в плоскости π_i через σ_i. Согласно предыдущему прим. 13.1 эти отражения удовлетворяют шести соотношениям:

$$\sigma_i^2 = e \qquad \text{и} \qquad (\sigma_i\sigma_j)^{m_k} = e\,, \tag{13-5}$$

в которых $i = 1, 2, 3$, а (i, j, k) пробегает циклические перестановки номеров $(1, 2, 3)$.

Упражнение 13.5. Убедитесь в этом.

Так как из треугольника e можно попасть в любой треугольник g последовательными отражениями относительно сторон, правило $x_i \mapsto \sigma_i$ задаёт сюръективный гомоморфизм из свободной группы F_3 на алфавите $\{x_1, x_2, x_3\}$ в группу O_M. В силу соотношений (13-5) он корректно факторизуется до эпиморфизма $\varphi : F_3/H \twoheadrightarrow \mathrm{O}_M$, где $H \lhd F_3$ — наименьшая нормальная подгруппа, содержащая 6 слов

$$x_i^2 \qquad \text{и} \qquad (x_ix_j)^{m_k}\,. \tag{13-6}$$

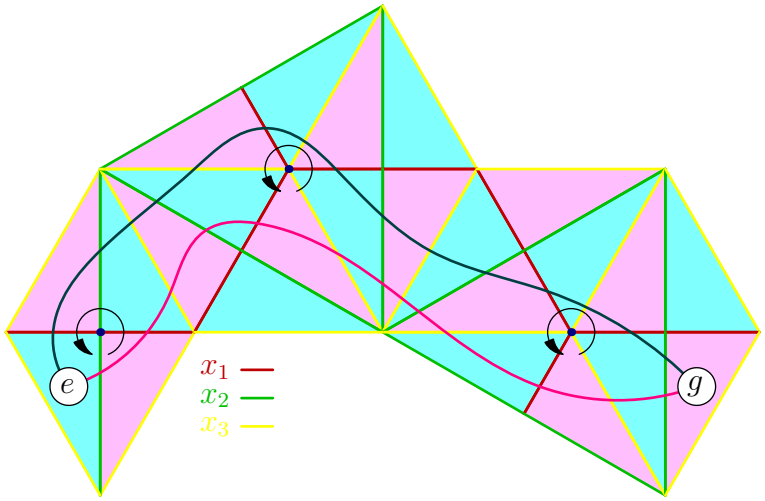


Рис. 13⋄3. $\boldsymbol{x_1x_2}x_3x_2\boldsymbol{x_3x_1x_3x_1}x_2x_3x_2\boldsymbol{x_1x_3x_1}x_2 = g = \boldsymbol{x_2x_1}x_3x_2\boldsymbol{x_1x_3}x_2x_3x_2\boldsymbol{x_3x_1x_3}x_2$

Чтобы показать, что φ — изоморфизм, достаточно проверить, что любые два слова w_1, w_2 в алфавите $\{x_1, x_2, x_3\}$, переходящие в один и тот же элемент $g \in \mathrm{O}_M$, эквивалентны по модулю слов (13-6). Каждое слово $\sigma_{i_1}\sigma_{i_2}\cdots\sigma_{i_m} = g$ задаёт последовательность треугольников $e = g_0, g_1, g_2, \ldots, g_m = g$, в которой треугольник $g_{k+1} = g_k\sigma_{k+1}$ получается из треугольника g_k отражением относительно их общей стороны, высекаемой на сфере плоскостью $g_k(\pi_{i_{k+1}})$ — образом плоскости $\pi_{i_{k+1}}$ при преобразовании g_k.

Упражнение 13.6. Удостоверьтесь, что

$$\sigma_{g_k(\pi_{i_{k+1}})} \circ \sigma_{g_{k-1}(\pi_{i_k})} \circ \cdots \circ \sigma_{g_1(\pi_{i_2})} \circ \sigma_{\pi_{i_1}} = \sigma_{i_1}\sigma_{i_2}\cdots\sigma_{i_k}\sigma_{i_{k+1}}\,.$$

[1] что ещё раз позволяет вычислить порядок этой группы

Эта последовательность отражений однозначно считывается по любой гладкой кривой, соединяющей e с g внутри образованной треугольниками ленты и трансверсально пересекающей внутренние рёбра этой ленты, как на рис. 13⋄3). Две такие кривые, производящие слова w_1 и w_2, можно продеформировать одну в другую по поверхности сферы. При прохождении через вершину триангуляции, в которой сходятся $2n$ треугольников, в задаваемом кривой слове некоторый фрагмент вида $x_1x_2x_1\ldots$ длины k заменятся равным ему в F_3/H фрагментом вида $x_2x_1x_2\ldots$ «дополнительной» длины $2n-k$ — как это происходило в форм. (13-4) и упр. 13.4 на стр. 200. Например, слова, отвечающие верхней и нижней траекториям на рис. 13⋄3 выше

$$\boldsymbol{x_1x_2}x_3x_2\boldsymbol{x_3x_1x_3x_1}x_2x_3x_2\boldsymbol{x_1x_3x_1}x_2 \mapsto g$$
$$\boldsymbol{x_2x_1}x_3x_2\boldsymbol{x_1x_3}x_2x_3x_2\boldsymbol{x_3x_1x_3}x_2 \mapsto g\,,$$

преобразуются одно в другое применением циклических соотношений

$$x_1x_2 = x_2x_1\,,\quad x_3x_1x_3x_1 = x_1x_3 \quad\text{и}\quad x_3x_1x_3 = x_1x_3x_1$$

в трёх отмеченных на (13-4) вершинах. Таким образом, любые два слова, ведущие из e в g лежат в одном классе группы F_3/H.

Упражнение 13.7. Выберем в треугольнике e точку a, а в треугольнике g — точку b так, чтобы они не были диаметрально противоположными и соединяющая их *геодезическая*[1] не проходила через вершины триангуляции. Покажите, что:
а) длина представляющего g слова, считанного с этой геодезической, не зависит от удовлетворяющего предыдущим условиям выбора точек a и b
б) все считываемые с таких геодезических слова имеют наименьшую возможную длину, среди всех слов, представляющих g
в) любое представляющее g слово минимальной длины считывается с некоторой геодезической.

Пример 13.3 (образующие и соотношения симметрической группы)
Симметрическая группа S_{n+1} изоморфна несобственной группе O_Δ правильного n-мерного симплекса[2] $\Delta = [0,\,1,\,\ldots\,,\,n] \subset \mathbb{R}^n$, поскольку каждая перестановка вершин однозначно определяет ортогональное преобразование пространства $\mathbb{R}^n$, осуществляющее такую перестановку. Все грани симплекса Δ тоже являются правильными симплексами и взаимно однозначно соответствуют собственным подмножествам в $\{1,\,2,\,\ldots\,,\,n\}$. Симплекс Δ симметричен относительно $n(n+1)/2$ гиперплоскостей π_{ij}, проходящих через середину ребра $[i,j]$ и противоположную ему грань коразмерности 2 с вершинами $\{0,\,1,\,\ldots\,,\,n\}\smallsetminus\{i,j\}$. Отражение $\sigma_{ij}\in\mathrm{O}_\Delta$ в этой плоскости отвечает в S_{n+1} транспозиции элементов i и j.

Упражнение 13.8. Убедитесь, что любые две плоскости 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 60°.

[1] или прямая в *сферической* геометрии, т. е. кратчайшая из двух дуг большого круга, высекаемого на сфере плоскостью, проходящей через точки a, b и центр сферы

[2] здесь и далее мы обозначаем вершины симплекса числами от 0 до n, как на рис. 13⋄2 на стр. 201, и считаем, что симметрическая группа S_{n+1} переставляет символы $0,\,1,\,\ldots\,,\,n$

Плоскости π_{ij} осуществляют *барицентрическое разбиение* симплекса Δ на $n!$ меньших симплексов с вершинами в центрах граней симплекса Δ. Обозначим через $\langle i_0 i_1 \,\dots\, i_m\rangle$ центр m-мерной грани с вершинами в $i_0, i_1, \dots, i_m$ и сопоставим каждой перестановке

$$g = (g_0, g_1, \,\dots\,, g_n) \in S_{n+1}$$

симплекс барицентрического разбиения с вершинами в точках[1]

$$\big[\langle g_0\rangle,\, \langle g_0, g_1\rangle,\, \langle g_0, g_1, g_2\rangle,\, \dots,\, \langle g_0 g_1 \,\dots\, g_{n-1}\rangle,\, \langle g_0 g_1 \,\dots\, g_n\rangle\big]\,. \tag{13-7}$$

Это соответствие устанавливает такую биекцию между симплексами барицентрического разбиения и элементами группы $S_{n+1} \simeq \mathrm{O}_\Delta$, что симплекс (13-7) является образом «начального» симплекса

$$\big[\langle 0\rangle,\, \langle 01\rangle,\, \langle 012\rangle,\, \dots,\, \langle 0,\, 1,\, \dots\,,\, n-1\rangle,\, \langle 0,\, 1,\, \dots\,,\, n\rangle\big]\,. \tag{13-8}$$

под действием ортогонального преобразования, задаваемого перестановкой g. Как и в предыдущем примере, надпишем на каждом симплексе отвечающее ему преобразование g и спроектируем гиперповерхность симплекса Δ из его центра на описанную вокруг Δ сферу S^{n-1}, т. е. рассмотрим триангуляцию этой сферы её пересечениями гиперплоскостями π_{ij}. Эта триангуляция состоит из $n!$ конгруэнтных $(n-1)$-мерных симплексов, надписанных элементами группы S_{n+1}. При $n = 3$, т. е. для группы S_4, мы получим тетраэдрическую триангуляцию сферы S^2 треугольниками с углами $\pi/3$, $\pi/3$ и $\pi/2$, изображённую на рис. 13◇2 на стр. 201. Начальному симплексу (13-8), помеченному тождественным преобразованием e, отвечает симплекс триангуляции, высекаемый из сферы n гиперплоскостями $\pi_i = \pi_{i-1,i}$ 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. 13.8 они удовлетворяют соотношениям[2]

$$\sigma_i^2 = e\,, \quad \sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1} \quad \text{и} \quad \sigma_i\sigma_j = \sigma_j\sigma_i \quad \text{при} \quad |i-j| \geqslant 2\,. \tag{13-9}$$

Упражнение 13.9. Убедитесь непосредственно, что соотношения (13-9) выполняются для *транспозиций* σ_i в группе S_{n+1}.

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 $H \lhd F_n$ — наименьшая нормальная подгруппа, содержащая слова

$$x_i^2\,, \qquad (x_i x_{i+1})^3 \quad \text{и} \quad (x_i x_j)^2 \text{ с } |i-j| \geqslant 2\,. \tag{13-10}$$

Чтобы убедиться в его сюръективности, выберем в симплексах e и g точки a и b так, чтобы они не были диаметрально противоположны и соединяющая их геодезическая[3] не

[1] т. е. с первой вершиной в вершине g_0 самого симплекса Δ, следующей вершиной — в середине выходящего из g_0 ребра $[g_0, g_1]$, следующей — в центре примыкающей к этому ребру треугольной грани $[g_0, g_1, g_2]$ и т. д. последняя вершина является центром всего 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 $\pi_i \cap \pi_{i+1}$

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

пересекала граней коразмерности 2. Пройдя из a в b по этой геодезической, мы получим представление элемента g словом $x_1x_2\ \dots\ x_m$, где i_ν — это номер такой из плоскостей π_ν, что переход из ν-того встретившегося нам по дороге симплекса[1] g_ν к следующему $(\nu+1)$-му симплексу происходит сквозь гиперплоскость $g_\nu(\pi_\nu)$. Инъективность гомоморфизма φ устанавливается дословно так же, как в прим. 13.2. Каждому слову $w \in F_n$, переходящему в элемент $g \in \mathrm{O}_\Delta$, отвечает ведущая из e в g «трубка», образованная симплексами триангуляции. Слово w состоит из номеров гиперграней, разделяющих соседние симплексы этой трубки, и может быть считано при движении из e в g по любой идущей внутри трубки кривой, трансверсально пересекающей эти грани. Любые две такие кривые можно продеформировать по сфере друг в друга. Когда в процессе этой деформации кривая пересекает грань $g(\pi_i \cap \pi_j)$ коразмерности 2, происходит замена некоторого фрагмента слова либо при помощи циклического соотношения $(x_ix_j)^2 = e$, отвечающего перпендикулярным плоскостям с $|i-j| \geqslant 2$, либо при помощи циклического соотношения $(x_ix_{i+1})^3$, отвечающего плоскостям, пересекающимся под углом 60°. В ортогональной проекции вдоль $(n-2)$-мерного подпространства $g(\pi_i \cap \pi_j)$ на ортогональную ему двумерную плоскость мы увидим картину вроде показанной на рис. 13⋄3 на стр. 202. Таким образом, симметрическая группа S_{n+1} задаётся n транспозициями x_i пар соседних элементов с определяющими соотношениями (13-10).

Разумеется, эту геометрическую картину можно выхолостить до сугубо комбинаторного рассуждения, что мы сделаем в n° 13.1.2 ниже.

Упражнение 13.10. Покажите, что знакопеременная группа A_{n+1} порождается а) парами транспозиций б) 3-циклами $|k-2, k-1, k\rangle$, где $2 \leqslant k \leqslant n$.

13.1.2. Порядок Брюа на S_{n+1}. Будем называть число инверсных пар в перестановке[2] $g = (g_0, g_1, \dots, g_n) \in S_{n+1}$ *длиной* перестановки g и обозначать его $\ell(g)$.

Упражнение 13.11. Убедитесь, что длина перестановок из S_{n+1} лежит в пределах от 0 до $n(n+1)/2$, причём имеется ровно по одной перестановке минимальной и максимальной длины. Что это за перестановки?

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:

$$\big(g_1, \dots, g_{i-2}, \boldsymbol{g_{i-1}}, \boldsymbol{g_i}, g_{i+1}, \dots, g_n\big) \circ \sigma_i = \big(g_1, \dots, g_{i-2}, \boldsymbol{g_i}, \boldsymbol{g_{i-1}}, g_{i+1}, \dots, g_n\big)\ ,$$

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 дины m

$$g = \sigma_{i_1}\sigma_{i_2}\cdots\sigma_{i_m}\,, \quad \ell(g) = m\,, \tag{13-11}$$

в котором каждое умножение справа на очередное σ_{i_ν} переставляет между собой соседние возрастающие элементы $h_{i_\nu-1} < h_{i_\nu}$ перестановки $(h_0, h_1, \dots, h_n) = \sigma_{i_1}\sigma_{i_2}\ \cdots\ \sigma_{i_\nu-1}$. Частичный порядок на S_{n+1}, в котором $g < h$, если h получается из g увеличивающими длину транспозициями соседних элементов, называется *порядком Брюа*. Слово $w = x_{i_1}x_{i_2}\ \cdots\ x_{i_m}$

[1] как и в прим. 13.2 мы последовательно нумеруем встречающиеся симплексы так, что $e = g_0$, а $g = g_{m+1}$

[2] 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° 9.2 на стр. 133

в свободной группе F_n с образующими $x_1, x_2, \dots, x_n$ называется *минимальным словом* перестановки $g \in S_{n+1}$, если $m = \ell(g)$ и $g = \sigma_{i_1}\sigma_{i_2} \cdots \sigma_{i_m}$. Начальные фрагменты минимального слова задают строго возрастающую в смысле порядка Брюа последовательность элементов $h_\nu = \sigma_{i_1}\sigma_{i_2} \cdots \sigma_{i_\nu} \in S_{n+1}$. Перестановка g может иметь много разных минимальных слов, однако не может быть записана никаким более коротким словом.

Упражнение 13.12. Проверьте, что в терминах прим. 13.3 проход из симплекса e в симплекс g по любой геодезической, не пересекающей граней коразмерности 2, задаёт минимальное слово элемента g и что каждое минимальное слово элемента g считывается с некоторой такой геодезической.

Предложение 13.3
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_ν проверить предложение для слова wx_ν. Если слово w не является минимальным словом элемента $g = \varphi(w)$, то по индукции оно эквивалентно более короткому минимальному слову. Тогда и wx_ν эквивалентно более короткому слову, и предложение справедливо по индукции. Поэтому мы будем далее считать, что слово w является минимальным словом элемента $g = \varphi(w) = (g_0, g_1, \dots, g_n)$. Возможны два случая: либо $g_{\nu-1} > g_\nu$, либо $g_{\nu-1} < g_\nu$. В первом случае у перестановки g есть минимальное слово вида ux_ν, по предположению индукции эквивалентное слову w. Тогда $wx_\nu \sim ux_\nu x_\nu \sim u$ и элемент $\varphi(wx_\nu) = \varphi(u)$ является образом более короткого, чем w слова u, эквивалентного слову wx_ν. По индукции, слово u эквивалентно минимальному слову элемента $\varphi(wx_\nu)$ и все такие слова эквивалентны друг другу. Поэтому то же верно и для эквивалентного u слова wx_ν.

Остаётся рассмотреть случай $g_{\nu-1} < g_\nu$. Здесь $\ell(g\sigma_\nu) = \ell(g) + 1$ и слово wx_ν является минимальным словом для элемента $\varphi(wx_\nu)$. Мы должны показать, что любое другое минимальное слово w' этого элемента эквивалентно wx_ν. Для самой правой буквы слова w' есть 3 возможности: либо она равна x_ν, либо она равна $x_{\nu\pm1}$ либо она равна x_μ с $|\mu-\nu| \geqslant 2$. В пером случае $w' = ux_\nu$, 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 $w' = ux_{\nu+1}$ — ситуация, когда $w' = ux_{\nu-1}$, полностью симметрична. Поскольку оба слова wx_ν и $ux_{\nu+1}$ минимальны для перестановки $h = \varphi(wx_\nu) = \varphi(ux_{\nu+1})$, в перестановке h на местах с номерами $\nu-1$, ν, $\nu+1$ стоят числа $g_\nu > g_{\nu-1} > g_{\nu+1}$, а в перестановке $g = (g_0, g_1, \dots, g_n) = \varphi(w)$ на этих же местах — числа $g_{\nu-1} < g_\nu > g_{\nu+1}$ 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. □

13.2. 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. 12.1 на стр. 186 простота группы G равносильна тому, что всякий гомоморфизм $G \to G'$ либо является вложением, либо отображает всю группу G в единицу.

Определение 13.1 (композиционный ряд)
Конечная строго убывающая последовательность подгрупп

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

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 (13-12).

Пример 13.4 (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 $A_4 \lhd S_4$ — подгруппа чётных перестановок, $V_4 \lhd A_4$ — подгруппа Клейна, состоящая из тождественной перестановки и трёх перестановок циклового типа  , а

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

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 $\mathbb{Z}/(2) = \mathbb{Z}/(2)/\{e\}$.

Упражнение 13.13. Убедитесь, что $A_4/V_4 \simeq \mathbb{Z}/(3)$.

[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 $g_\nu > g_{\nu-1}$

Теорема 13.1 (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

$$G = P_0 \supsetneq P_1 \supsetneq P_2 \supsetneq \cdots \supsetneq P_{n-1} \supsetneq P_n = \{e\} \tag{13-13}$$
$$G = Q_0 \supsetneq Q_1 \supsetneq Q_2 \supsetneq \cdots \supsetneq Q_{m-1} \supsetneq Q_m = \{e\}\,. \tag{13-14}$$

Мы собираемся вставить между последовательными членами этих рядов дополнительные цепочки нестрого убывающих подгрупп так, чтобы получившиеся удлинённые последовательности состояли из одинакового числа элементов, а между их последовательными факторами возникла бы такая естественная биекция, при которой соответствующие друг другу факторы будут изоморфны. Применяя предл. 12.5 на стр. 197 к нормальной подгруппе $P_{i+1} \lhd P_i$ и подгруппам $Q_\nu \cap P_i \subset P_i$, мы для каждого i получаем цепочку

$$P_i \supseteq (Q_1 \cap P_i)P_{i+1} \supseteq (Q_2 \cap P_i)P_{i+1} \supseteq \cdots \supseteq (Q_{m-1} \cap P_i)P_{i+1} \supseteq P_{i+1}\,, \tag{13-15}$$

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

$$\frac{(Q_k \cap P_i)P_{i+1}}{(Q_{k+1} \cap P_i)P_{i+1}} \simeq \frac{(Q_k \cap P_i)}{(Q_{k+1} \cap P_i)(Q_k \cap P_{i+1})}\,. \tag{13-16}$$

Упражнение 13.14. Убедитесь в этом, т. е. для любой четвёрки подгрупп A, B, C, D, таких что $A \lhd B$ и $C \lhd D$, 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 (13-15). Факторизуя по ней, получаем цепочку

$$\frac{P_i}{P_{i+1}} \supseteq \frac{(Q_1 \cap P_i)P_{i+1}}{P_{i+1}} \supseteq \frac{(Q_2 \cap P_i)P_{i+1}}{P_{i+1}} \supseteq \cdots \supseteq \frac{(Q_{m-1} \cap P_i)P_{i+1}}{P_{i+1}} \supseteq \{e\}\,, \tag{13-17}$$

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 (13-16). Так как группа P_i/P_{i+1} проста, мы заключаем, что в цепочке (13-17) имеется ровно одно нестрогое включение, а все остальные включения — равенства. Тем самым, ровно один из факторов (13-16) 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 (13-14) убывающую цепочку подгрупп

$$Q_k \supseteq (P_1 \cap Q_k)Q_{k+1} \supseteq (P_2 \cap Q_k)Q_{k+1} \supseteq \cdots \supseteq (P_{n-1} \cap Q_k)Q_{k+1} \supseteq Q_{k+1}\,, \tag{13-18}$$

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

$$\frac{(P_i \cap Q_k)Q_{k+1}}{(P_{i+1} \cap Q_k)Q_{k+1}} \simeq \frac{(Q_k \cap P_i)}{(Q_{k+1} \cap P_i)(Q_k \cap P_{i+1})} \tag{13-19}$$

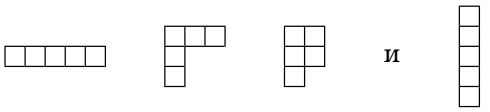
и изоморфны соответствующим факторам (13-16). Таким образом, вставляя между последовательными элементами композиционного ряда (13-13) цепочки (13-15), а между последовательными элементами ряда (13-14) — цепочки (13-18), мы получим цепочки одинаковой длины, в которых не все включения строгие, однако факторы которых находятся в естественной биекции, такой что соответственные факторы (13-19) и (13-16) изоморфны. Остаётся заметить, что группа Q_{k+1} является нормальной подгруппой во всех группах цепочки (13-18), и то же рассуждение, как с подгруппой P_{i+1} для цепочки (13-15), показывает, что при фиксированном k среди факторов (13-19) имеется ровно один отличный от единицы, и он изоморфен Q_k/Q_{k+1}. □

Замечание 13.1. Непростая группа может иметь несколько разных композиционных рядов с одинаковым набором факторов, а группы с одинаковыми наборами факторов Жордана-Гёльдера не обязательно изоморфны.

13.2.1. 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 13.1
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



(13-20)

(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 (13-20), то её централизатор содержит транспозицию пары неподвижных элементов или пары элементов, составляющих цикл длины 2. Поэтому две такие перестановки, сопряжённые в S_5, сопряжены

[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

и в A_5. Стало быть, перестановки каждого из трёх последних типов (13-20) образуют один класс сопряжённости 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 $H \lhd A_5$ 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 13.15. 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 13.2
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 $N \lhd A_n$, то пересечение $N \cap \mathrm{Stab}_{A_n}(k) \lhd \mathrm{Stab}_{A_n}(k)$ 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, … , 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. 13.10. 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 13.16. Убедитесь в этом.

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

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

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

Отображение множеств $N \times H \to NH$, $(x,h) \mapsto xh$, биективно тогда и только тогда, когда $N \cap H = \{e\}$. 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 это пересечение исчерпывается единичным элементом, то $x_2 = x_1$ и $h_2 = h_1$, а если в пересечении есть элемент $z \neq e$, то две различных 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 $N \lhd G$ 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, т. к.

$$g_1g_2 = x_1h_1x_2h_2 = x_1(h_1x_2h_1^{-1}) \cdot h_1h_2$$

и $h_1x_2h_1^{-1} \in N$, мы можем *описать* группу G как множество $N \times H$ с операцией композиции, заданной правилом

$$(x_1,h_1) \cdot (x_2,h_2) = (x_1\,\mathrm{Ad}_{h_1}(x_2), h_1h_2), \tag{13-21}$$

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 $N \lhd G$ и дополнительной к ней подгруппы $H \subset G$ и пишут $G = N \leftthreetimes H$. 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 13.5 ($D_n = \mathbb{Z}/(n) \leftthreetimes \mathbb{Z}/(2)$)
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, $D_n = \mathbb{Z}/(n) \leftthreetimes \mathbb{Z}/(2)$ и в терминах пар $(x, y) \in \mathbb{Z}/(n) \times \mathbb{Z}/(2)$ композиция на группе диэдра задаётся правилом

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

13.3.1. 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. имеется гомоморфизм

$$\psi : H \to \mathrm{Aut}\, N\,, \quad h \mapsto \psi_h : N \xrightarrow{\sim} N\,, \tag{13-22}$$

группы H в группу автоморфизмов группы N. По аналогии с формулой (13-21) зададим на декартовом произведении $N \times H$ операцию композиции правилом

$$(x_1, h_1) \cdot (x_2, h_2) = (x_1 \psi_{h_1}(x_2), h_1 h_2)\,. \tag{13-23}$$

Упражнение 13.17. Проверьте, что формула (13-23) задаёт на $N \times H$ структуру группы с единицей (e, e) и обращением $(x, h)^{-1} = \big(\psi_h^{-1}(x^{-1}), h^{-1}\big)$, 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 $\psi : N \to \mathrm{Aut}\, H$ и обозначается $N \underset{\psi}{\leftthreetimes} H$. 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 13.18. Убедитесь, что элементы вида (x, e) с $x \in N$ образуют в группе $G = N \underset{\psi}{\leftthreetimes} H$ нормальную подгруппу N', изоморфную N, и фактор $G/N' \simeq H$, а элементы вида (e, h) с $h \in H$ образуют подгруппу H', дополнительную к N', и G является полупрямым произведением подгрупп N' и H'.

13.4. 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 13.4
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 13.5
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 13.19. Покажите, что любая группа G порядка p^2 (где p простое) абелева.

13.4.1. 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 13.3 (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 $\operatorname{Stab}(F)$ свободно действует на множестве F и все орбиты этого действия состоят из $|\operatorname{Stab}(F)|$ точек. Поэтому $|F| = p^n$ делится на $|\operatorname{Stab}(F)|$ 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 $|\operatorname{Stab}(F)| = p^n$, т. е. подгруппа $\operatorname{Stab}(F) \subset G$ силовская. Во втором случае согласно предл. 13.4 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 $\operatorname{Stab}(gF) = g \operatorname{Stab}(F) g^{-1}$, сопряжённой к $\operatorname{Stab}(F)$ (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 13.2
$|\mathcal{E}| = \binom{p^n m}{p^n} \equiv m \pmod{p}$ 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 $(1+x)^{p^n m} = \left(1 + x^{p^n}\right)^m = 1 + mx^{p^n} +$ старшие степени. □

Следствие 13.1 (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 $m' | m$ и 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 13.6 (группы порядка pq с простыми $p > q$ и нод$(p-1, q) = 1$)
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 $H_q \simeq \simeq \mathbb{Z}/(q)$. Поскольку H_p и H_q просты, $H_p \cap H_q = e$ и $G = H_p H_q$. Согласно n° 13.3 $G = H_p \underset{\psi}{\leftthreetimes} H_q$ для некоторого гомоморфизма $\psi : H_q \to \mathrm{Aut}\, H_p$.

Упражнение 13.20. Убедитесь, что $\mathrm{Aut}(H_p)$ — циклическая группа порядка $p-1$.

Аддитивный гомоморфизм $\psi : \mathbb{Z}/(q) \to \mathbb{Z}/(p-1)$ однозначно задаётся своим значением на образующей $[1]_q$ $\mathbb{Z}$-модуля $\mathbb{Z}/(q)$. Поскольку $0 = \psi(0) = \psi(q \cdot [1]_q) = q \cdot \psi([1]_q)$, элемент $\psi([1]_q) \in \mathbb{Z}/(p-1)$ должен аннулироваться оператором умножения на $q : x \mapsto qx$. Но при нод$(p-1, q) = 1$ в $\mathbb{Z}$-модуле $\mathbb{Z}/(p-1)$ этот оператор обратим, откуда $\psi = 0$, т. е. в мультипликативной записи гомоморфизм $\psi : H_q \to \mathrm{Aut}\, H_p$ переводит H_q в тождественное преобразование. Поэтому $G = H_p \times H_q \simeq \mathbb{Z}/(p) \oplus \mathbb{Z}/(q)$ при простых $p > q$ с нод$(p-1, q) = 1$.

Пример 13.7 (группы порядка $2p$)
Пусть $|G| = 2p$, где $p > 2$ простое. Рассуждая как в предыдущем примере, заключаем, что $G = \mathbb{Z}/(p) \underset{\psi}{\leftthreetimes} \mathbb{Z}/(2)$ для некоторого действия $\psi : \mathbb{Z}/(2) \to \mathrm{Aut}\big(\mathbb{Z}/(p)\big) \simeq \mathbb{F}_p^*$, которое однозначно задаётся элементом $\psi([1]) \in \mathbb{F}_p^*$ с $\psi([1])^2 = 1$. Таких элементов имеется ровно два: $\psi([1]) = 1$ и $\psi([1]) = -1$. В первом случае действие ψ тривиально и $G \simeq \mathbb{Z}/(p) \oplus \mathbb{Z}/(q)$. Во втором случае $[0] \in \mathbb{Z}/(2)$ действует на $\mathbb{Z}/(p)$ тривиально, а $[1] \in \mathbb{Z}/(2)$ действует на $\mathbb{Z}/(p)$ сменой знака, т. е. $G \simeq D_p$ это группа правильного p-угольника.

Ответы и указания к некоторым упражнениям

Упр. 13.1. Первое очевидно, второе вытекает из того, что при вставке фрагмента $x^\varepsilon x^{-\varepsilon}$ 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. 13.2. Отобразите $n \in \mathbb{N}$ в $x^n y x^n \in F_2$ и воспользуйтесь предл. 13.1 на стр. 198.

Упр. 13.4. Так как $x_1^2 = x^2 = e$, $\underbrace{x_1 x_2 x_1 \dots}_{n} = \underbrace{x_2 x_1 x_2 \dots}_{n}$ и $(x_2 x_1)^n = e$.

Упр. 13.5. Композиция $\sigma_i \circ \sigma_j$ отражений в плоскостях π_i и π_j является поворотом на удвоенный угол $2\pi/m_k$ между этими плоскостями вокруг прямой $\pi_i \cap \pi_j$ в направлении от π_j к π_i.

Упр. 13.6. Это следует из упр. 13.3 на стр. 200.

Упр. 13.7. Первое вытекает из того, что геодезическая прямая, проходящая через вершину триангуляции, разбивает $2m_i$ рёбер, сходящихся в этой вершине, в точности пополам — тем самым, при прохождении геодезической через вершину в отвечающем ей слове один фрагмент длины n заменяется другим фрагментом длины n. Утверждения (б) и (в) доказываются индукцией по длине минимального слова, ведущего в g. Пусть они верны для элемента g. Достаточно убедиться, что они верны для всех элементов $g\sigma_i$. Проведём из e в g геодезическую так, чтобы она сама или её продолжение пересекало сторону $g(\pi_i)$ треугольника g и обозначим через $u = g$ считанное с этой геодезической минимальное слово для g. Если геодезическая входит в треугольник g через сторону $g(\pi_i)$, то $u = w\sigma_i$, а значит $g\sigma_i = w$ имеет более короткое минимальное слово и утверждения верны для него по индукции. Если продолжение геодезической выходит из g через $g(\pi_i)$, то оно попадает в $g\sigma_i$, и значит $g\sigma_i = u\sigma_i$. Либо это минимальное слово для $g\sigma_i$, и тогда утверждения (а) и (б) верны, либо $g\sigma_i$ можно записать более коротким словом, и тогда утверждения (а) и (б) верны для $g\sigma_i$ по индукции.

Упр. 13.8. 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. 13.12. Воспользуйтесь индукцией по длине минимального слова и тем же рассуждением, что в упр. 13.8.

Упр. 13.13. При эпиморфизме S_4 на группу треугольника из прим. 12.9 подгруппа чётных перестановок $A_4 \subset S_4$ переходит в группу вращений треугольника.

[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

Упр. 13.14. По предл. 12.5 $(A\cap D)C\lhd D$, поскольку $C\lhd D$. Изоморфизм $HN/N\simeq H/H\cap N$ из предл. 12.5 в случае $G=D$, $H=B\cap D$ и $N=(A\cap D)C$ имеет требуемый вид

$$(B\cap D)C/(A\cap D)C\simeq (B\cap D)/(A\cap D)(B\cap C)\,.$$

В самом деле, $A\subset B\Rightarrow HN=(B\cap D)(A\cap D)C=(B\cap D)C$. Равенство

$$H\cap N=(B\cap D)\cap(A\cap D)=(A\cap D)(B\cap C)$$

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. 13.15. Правая часть формулы $|H|=12\varepsilon_1+12\varepsilon_2+20\varepsilon_3+15\varepsilon_4+1$, приведённая по модулю 3, по модулю 4 и по модулю 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. 13.16. 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. 13.17. 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. 13.18. Так как $\psi:H\to\operatorname{Aut}N$ — гомоморфизм, $\psi_e=\mathrm{Id}_N$ и

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

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

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

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

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

Упр. 13.19. 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^ka^m. Так как a централен, любые два таких элемента коммутируют.

Упр. 13.20. 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.