

§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 удалением¹ двубуквенного фрагмента xx^{-1} или $x^{-1}x$. Композиция определяется как приписывание одного слова к другому. Единицей служит пустое слово. Обратным к классу слова $w = x_1x_2 \dots x_m$ является класс слова $w^{-1} = x_m^{-1} \dots x_2^{-1}x_1^{-1}$, где каждое x_i — имеет вид x или x^{-1} с $x \in M$ и $(x^{-1})^{-1} \stackrel{\text{def}}{=} x$.

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 $F_{\mathbb{N}} \hookrightarrow F_2$.

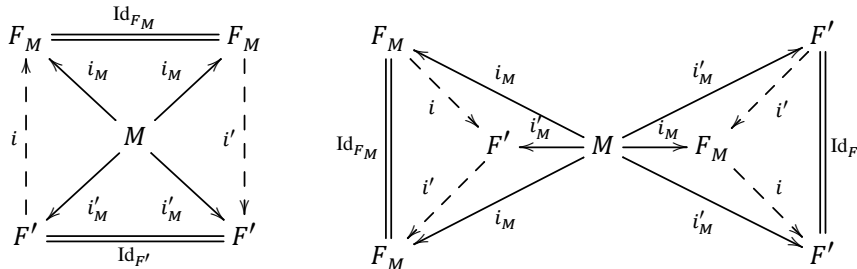
Предложение 13.1 (универсальное свойство свободных групп)

Отображение $i_M : M \rightarrow F_M$, переводящее элемент $x \in M$ в класс однобуквенного слова $x \in F_M$, обладает следующим свойством: для любой группы G и любого отображения множеств $\varphi_M : M \rightarrow G$ существует единственный гомоморфизм групп $\varphi : F_M \rightarrow G$, такой что $\varphi_M = \varphi \circ i_M$. Для любого обладающего этим свойством отображения $i'_M : M \rightarrow F'$ множества M в группу F' имеется единственный изоморфизм групп $i' : F_M \simeq F'$, такой что $i'_M = i' \circ i_M$.

Доказательство. Гомоморфизм φ единствен, поскольку обязан переводить слово

$$w = x_1^{\varepsilon_1} x_2^{\varepsilon_2} \dots x_m^{\varepsilon_m} \in F_M \quad (x_v \in M, \quad \varepsilon_v = \pm 1)$$

в произведение $\varphi_M(x_1)^{\varepsilon_1} \varphi_M(x_2)^{\varepsilon_2} \dots \varphi_M(x_m)^{\varepsilon_m} \in G$. С другой стороны, это правило корректно задаёт гомоморфизм групп, что доказывает первое утверждение. Если отображение $i' : M \rightarrow F'$ множества M в группу F' обладает универсальным свойством из предл. 13.1, то существуют единственные гомоморфизмы $i' : F_M \rightarrow F'$ и $i : F' \rightarrow F_M$, встраивающиеся в коммутативные диаграммы



¹в начале, в конце, или же между произвольными двумя последовательными буквами слова
²т. 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 $\varphi = \text{Id}_{F_M}$, $\psi = \text{Id}_{F'}$. Поэтому $i' \circ i = \text{Id}_{F'}$, $i \circ i' = \text{Id}_{F_M}$. \square

13.1.1. Задание групп образующими и соотношениями. Если гомоморфизм групп

$$\varphi : F_M \twoheadrightarrow G, \quad (13-1)$$

заданный отображением $\varphi_M : M \rightarrow G$, $m \mapsto g_m$, 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 $\ker \varphi \triangleleft F_M$ 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 $\varphi : M \rightarrow G_2$ тогда и только тогда корректно задаёт гомоморфизм групп $G_1 \rightarrow G_2$ 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 $\varphi_M : M \rightarrow G_2$ биективно соответствуют гомоморфизмам групп $\varphi : F_M \rightarrow G_2$. Такой гомоморфизм φ факторизуется до гомоморфизма из группы $G_1 = F_M/N_R$, где $N_R \triangleleft F_M$ — наименьшая нормальная подгруппа, содержащая R , тогда и только тогда, когда $N_R \subset \ker \psi$. Так как $\ker \psi \triangleleft F_M$, для этого необходимо и достаточно включения $R \subset \ker \psi$. \square

¹в 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

$$x_1^2 = x_2^2 = (x_1x_2)^n = e. \quad (13-2)$$

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

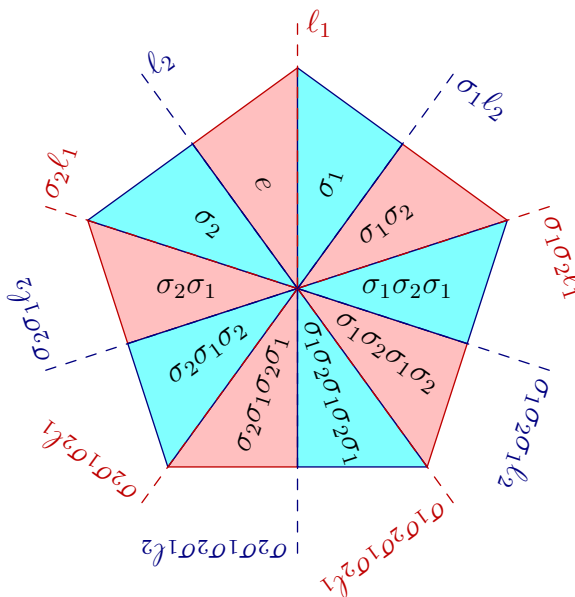


Рис. 13◊1. Группа диэдра порождается отражениями.

пометятся элементами $\sigma_2, \sigma_2\sigma_1, \sigma_2\sigma_1\sigma_2, \sigma_2\sigma_1\sigma_2\sigma_1, \dots$, а треугольники, получающиеся «перекатываниями» по ЧС — элементами $\sigma_1, \sigma_1\sigma_2, \sigma_1\sigma_2\sigma_1, \sigma_1\sigma_2\sigma_1\sigma_2, \dots$

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

$$\sigma_1^2 = \sigma_2^2 = (\sigma_1\sigma_2)^n = e. \quad (13-3)$$

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 $H \triangleleft F_2$, 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 $x_1x_2x_1 \dots$ или $x_2x_1x_2 \dots$ 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 равна¹ $2n$:

$$\varphi(\underbrace{x_1x_2x_1 \dots}_k) = \underbrace{\sigma_1\sigma_2\sigma_1 \dots}_k = g = \underbrace{\sigma_2\sigma_1\sigma_2 \dots}_{2n-k} = \varphi(\underbrace{x_2x_1x_2 \dots}_{2n-k}). \quad (13-4)$$

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

Таким образом, гомоморфизм $\varphi : F_2/H \twoheadrightarrow D_n$ биективен.

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

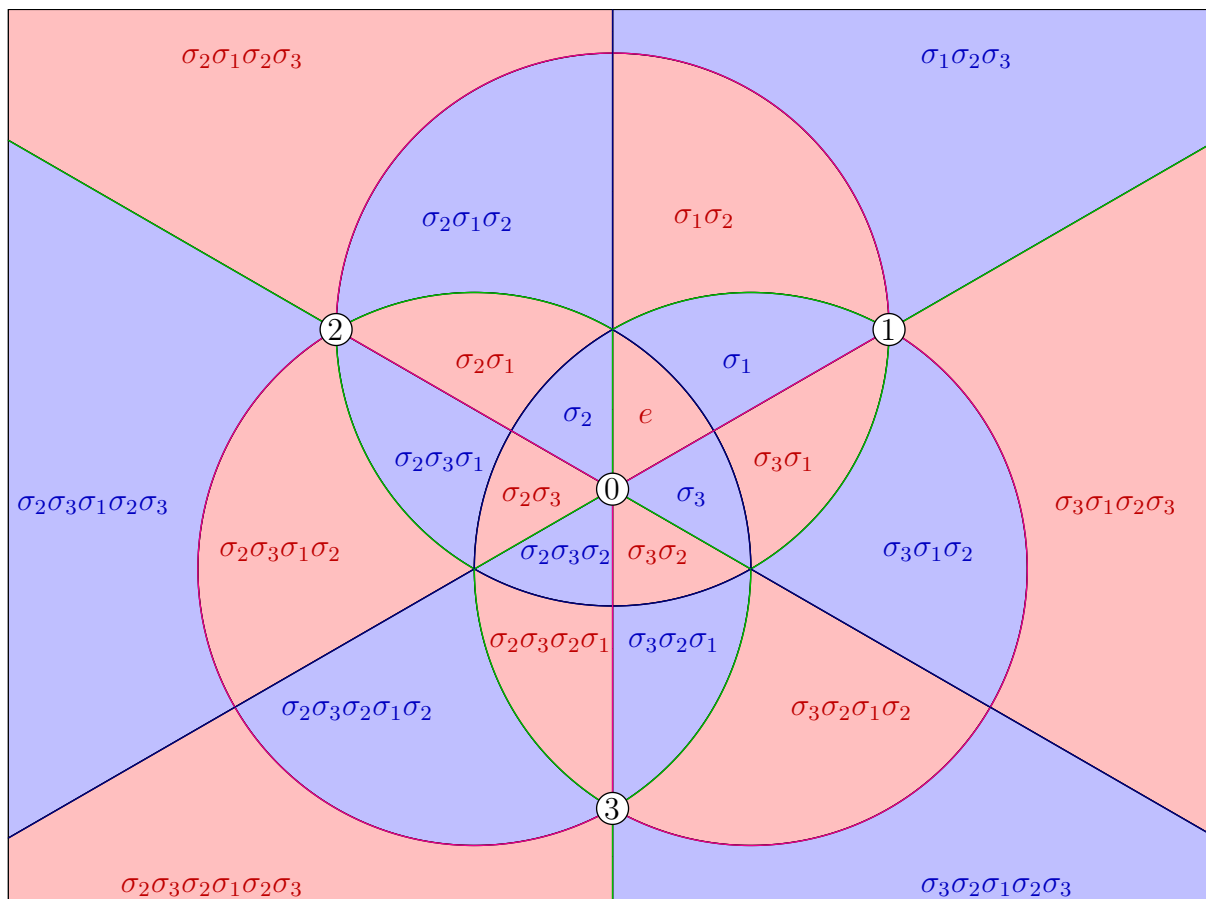


Рис. 13◊2. Триангуляция сферы плоскостями симметрии тетраэдра в стереографической проекции из диаметрально противоположной к вершине «0» точки на плоскость, параллельную грани «123».

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 таковы¹:

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 углами² $\pi / m_1, \pi / m_2, \pi / m_3$

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

²они 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 триангуляции¹. Мы пометим каждый треугольник тем преобразованием $g \in O_M$, которое переводит в него треугольник e . Назовём плоскости, отсекающие 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:

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

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 $\varphi : F_3/H \rightarrow O_M$, где $H \triangleleft F_3$ — наименьшая нормальная подгруппа, содержащая 6 слов

$$x_i^2 \quad \text{и} \quad (x_i x_j)^{m_k}. \tag{13-6}$$

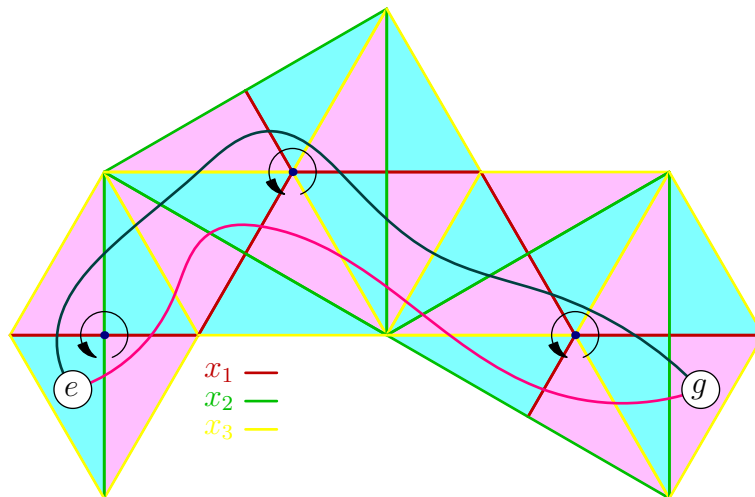


Рис. 13◊3. $x_1 x_2 x_3 x_2 x_3 x_1 x_3 x_1 x_2 x_3 x_2 x_1 x_3 x_1 x_2 = g = x_2 x_1 x_3 x_2 x_1 x_3 x_2 x_3 x_2 x_3 x_1 x_3 x_2$

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 $g \in O_M$, эквивалентны по модулю слов (13-6). Каждое слово $\sigma_{i_1} \sigma_{i_2} \dots \sigma_{i_m} = g$ задаёт последовательность треугольников $e = g_0, g_1, g_2, \dots, g_m = g$, в которой треугольник $g_{k+1} = g_k \sigma_{k+1}$ получается из треугольника g_k отражением относительно их общей стороны, отсекаемой на сфере плоскостью $g_k(\pi_{i_{k+1}})$ — образом плоскости $\pi_{i_{k+1}}$ при преобразовании g_k .

Упражнение 13.6. Удостоверьтесь, что

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

¹что 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 $x_1x_2x_1 \dots$ длины k заменится равным ему в F_3/H фрагментом вида $x_2x_1x_2 \dots$ «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

$$\begin{aligned} x_1x_2x_3x_2x_3x_1x_3x_1x_2x_3x_2x_1x_3x_1x_2 &\mapsto g \\ x_2x_1x_3x_2x_1x_3x_2x_3x_2x_3x_1x_3x_2 &\mapsto g, \end{aligned}$$

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:

- длина представляющего g слова, считанного с этой геодезической, не зависит от удовлетворяющего предыдущим условиям выбора точек a и b
- все считываемые с таких геодезических слова имеют наименьшую возможную длину, среди всех слов, представляющих g
- 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 симплекса² $\Delta = [0, 1, \dots, n] \subset \mathbb{R}^n$, 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 $\{1, 2, \dots, n\}$. 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 $\{0, 1, \dots, n\} \setminus \{i, j\}$. Отражение $\sigma_{ij} \in O_\Delta$ 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 $\{i, j\} \cap \{k, m\} = \emptyset$ ортогональны, а плоскости π_{ij} и π_{jk} с различными i, j, k пересекаются под углом 60° .

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

²здесь 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 $0, 1, \dots, n$

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 точках¹

$$\langle g_0 \rangle, \langle g_0, g_1 \rangle, \langle g_0, g_1, g_2 \rangle, \dots, \langle g_0 g_1 \dots g_{n-1} \rangle, \langle g_0 g_1 \dots g_n \rangle. \quad (13-7)$$

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

$$\langle 0 \rangle, \langle 01 \rangle, \langle 012 \rangle, \dots, \langle 0, 1, \dots, n-1 \rangle, \langle 0, 1, \dots, n \rangle. \quad (13-8)$$

под действием ортогонального преобразования, задаваемого перестановкой g . Как и в предыдущем примере, напомним 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 $1 \leq i \leq n$. 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 соотношениям²

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

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

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

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

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 геодезическая³ не

¹т. 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

²соотношение $\sigma_i \sigma_{i+1} \sigma_i = \sigma_{i+1} \sigma_i \sigma_{i+1}$ 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 $\pi_i \cap \pi_{i+1}$

³кратчайшая 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 $x_1 x_2 \dots x_m$, где i_ν — это номер такой из плоскостей π_ν , что переход из ν -того встретившегося нам по дороге симплекса¹ 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 $g \in O_\Delta$, 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 $(x_i x_j)^2 = e$, отвечающего перпендикулярным плоскостям с $|i - j| \geq 2$, либо при помощи циклического соотношения $(x_i x_{i+1})^3$, 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 [н° 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 $2 \leq k \leq n$.

13.1.2. Порядок Брюа на S_{n+1} . Будем называть число инверсных пар в перестановке² $g = (g_0, g_1, \dots, g_n) \in S_{n+1}$ 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 :

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

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 длины m

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

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

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

²напомню, пара (i, j) , где $1 \leq i < j \leq n$ называется *инверсной парой* перестановки $g \in S_n$, если $g_i = g(i) > g(j) = g_j$, см. [н° 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 $g = \sigma_{i_1} \sigma_{i_2} \dots \sigma_{i_m}$. Начальные фрагменты минимального слова задают строго возрастающую в смысле порядка Брюа последовательность элементов $h_v = \sigma_{i_1} \sigma_{i_2} \dots \sigma_{i_v} \in S_{n+1}$. 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 считается с некоторой такой геодезической.

Предложение 13.3

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

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

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

Доказательство. Индукция по количеству букв в слове $w \in F_{n-1}$. Для $w = \emptyset$ утверждение очевидно. Пусть для всех слов из $\leq m$ букв предложение доказано. Достаточно для каждого m -буквенного слова w и каждой буквы x_v проверить предложение для слова $w x_v$. Если слово w не является минимальным словом элемента $g = \varphi(w)$, то по индукции оно эквивалентно более короткому минимальному слову. Тогда и $w x_v$ эквивалентно более короткому слову, и предложение справедливо по индукции. Поэтому мы будем далее считать, что слово w является минимальным словом элемента $g = \varphi(w) = (g_0, g_1, \dots, g_n)$. 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 $u x_v$, по предположению индукции эквивалентное слову w . Тогда $w x_v \sim u x_v x_v \sim u$ и элемент $\varphi(w x_v) = \varphi(u)$ является образом более короткого, чем w слова u , эквивалентного слову $w x_v$. По индукции, слово u эквивалентно минимальному слову элемента $\varphi(w x_v)$ и все такие слова эквивалентны друг другу. Поэтому то же верно и для эквивалентного u слова $w x_v$.

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

Пусть теперь $w' = u x_{v+1}$ — ситуация, когда $w' = u x_{v-1}$, полностью симметрична. Поскольку оба слова $w x_v$ и $u x_{v+1}$ минимальны для перестановки $h = \varphi(w x_v) = \varphi(u x_{v+1})$, 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 $g = (g_0, g_1, \dots, g_n) = \varphi(w)$ на этих же местах — числа $g_{v-1} < g_v > g_{v+1}$ с $g_{v-1} > g_{v+1}$. Поэтому у перестановки h имеется минимальное слово вида $s x_{v+1} x_v x_{v+1}$, а у перестановки g — минимальное слово вида $t x_v x_{v+1}$. Перестановка $h' = \varphi(s) = \varphi(t)$ отличается от h тем, что числа на местах с номерами $v - 1, v, v + 1$ в ней возрастают и равны $g_{v+1} < g_{v-1} < g_v$. 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 $t x_v x_{v+1}$.

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 перестановки¹ длины $m = \ell(h) - 1$. Таким образом, $wx_\nu \sim ux_{\nu+1}$.

Наконец, пусть $h = \varphi(wx_\nu) = \varphi(ux_\mu)$, где $|\mu - \nu| \geq 2$. 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 рассматриваемые 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. \square

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 $G \rightarrow G'$ либо является вложением, либо отображает всю группу G в единицу.

Определение 13.1 (композиционный ряд)

Конечная строго убывающая последовательность подгрупп

$$G = G_0 \supsetneq G_1 \supsetneq G_2 \supsetneq \dots \supsetneq G_{n-1} \supsetneq G_n = \{e\} \quad (13-12)$$

называется *композиционным рядом* или *рядом Жордана–Гельдера* 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–Гельдера*) 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

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

в котором $A_4 \triangleleft S_4$ — подгруппа чётных перестановок, $V_4 \triangleleft A_4$ — подгруппа Клейна, состоящая из тождественной перестановки и трёх перестановок циклового типа $\begin{smallmatrix} \square & \\ & \square \end{smallmatrix}$, а

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

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

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

¹она 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

$$G = P_0 \supseteq P_1 \supseteq P_2 \supseteq \dots \supseteq P_{n-1} \supseteq P_n = \{e\} \quad (13-13)$$

$$G = Q_0 \supseteq Q_1 \supseteq Q_2 \supseteq \dots \supseteq Q_{m-1} \supseteq Q_m = \{e\}. \quad (13-14)$$

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 $P_{i+1} \triangleleft P_i$ и подгруппам $Q_v \cap P_i \subset P_i$, мы для каждого i получаем цепочку

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

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

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

Упражнение 13.14. Убедитесь в этом, т. е. для любой четвёрки подгрупп A, B, C, D , таких что $A \triangleleft B$ и $C \triangleleft D$, 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

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

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 $Q_k \supseteq Q_{k+1}$ композиционного ряда (13-14) убывающую цепочку подгрупп

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

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

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

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} . \square

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 $n \geq 5$ и простые линейные алгебраические группы над конечными полями², такие как $\text{PSL}_n(\mathbb{F}_q)$, $\text{PSO}_n(\mathbb{F}_q)$, $\text{PSp}_n(\mathbb{F}_q)$ 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

$$\begin{array}{c} \square \square \square \square \square \\ \square \square \square \\ \square \square \square \\ \square \square \square \end{array} \quad \text{и} \quad \begin{array}{c} \square \\ \square \\ \square \\ \square \\ \square \end{array} \quad (13-20)$$

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

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

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

¹группа $A_3 \simeq \mathbb{Z}/(3)$ тоже проста

²описание 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 $\langle 1, 2, 3, 4, 5 \rangle$, и 12 циклов, сопряжённых $\langle 2, 1, 3, 4, 5 \rangle$. Поскольку любая нормальная подгруппа $H \triangleleft A_5$ 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 . \square

Теорема 13.2

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

Доказательство. Индукция по n . Стабилизатор $\text{Stab}_{A_n}(k)$ любого элемента $k \in \{1, 2, \dots, n\}$ изоморфен A_{n-1} . Если $N \triangleleft A_n$, то пересечение $N \cap \text{Stab}_{A_n}(k) \triangleleft \text{Stab}_{A_n}(k)$ по индукции либо совпадает со $\text{Stab}_{A_n}(k)$ 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. 13.10. Во втором случае если в N есть хоть одна перестановка, переводящая некое i в $j \neq i$, то в силу тривиальности $\text{Stab}_N(j)$ эта перестановка является *единственной* в N перестановкой, переводящей i в j . Но при $n \geq 6$ 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. \square

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

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

Отображение множеств $N \times H \rightarrow NH$, $(x, h) \mapsto xh$, биективно тогда и только тогда, когда $N \cap H = \{e\}$. В самом деле, при $x_1 h_1 = x_2 h_2$ элемент $x_2^{-1} x_1 = h_2 h_1^{-1} \in N \cap H$, 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 $N \triangleleft G$ при этом нормальна, то композиция элементов $g_1 = x_1 h_1$ и $g_2 = x_2 h_2$ может быть выражена в терминах пар $(x_1, h_1), (x_2, h_2) \in N \times H$. А именно, т. к.

$$g_1 g_2 = x_1 h_1 x_2 h_2 = x_1 (h_1 x_2 h_1^{-1}) \cdot h_1 h_2$$

и $h_1 x_2 h_1^{-1} \in N$, мы можем *описать* группу G как множество $N \times H$ с операцией композиции, заданной правилом

$$(x_1, h_1) \cdot (x_2, h_2) = (x_1 \text{Ad}_{h_1}(x_2), h_1 h_2), \quad (13-21)$$

где через $\text{Ad}_h : N \simeq N$, $x \mapsto h x h^{-1}$, обозначено присоединённое действие элемента h на нормальной подгруппе N . В этой ситуации говорят, что группа G является *полупрямым произведением* нормальной подгруппы $N \triangleleft G$ 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 $xh = hx$ 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 ($D_n = \mathbb{Z}/(n) \rtimes \mathbb{Z}/(2)$)

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

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

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

$$\psi : H \rightarrow \text{Aut } N, \quad h \mapsto \psi_h : N \simeq N, \quad (13-22)$$

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

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

Упражнение 13.17. Проверьте, что формула (13-23) задаёт на $N \times H$ структуру группы с единицей (e, e) и обращением $(x, h)^{-1} = (\psi_h^{-1}(x^{-1}), h^{-1})$, где $\psi_h^{-1} = \psi_{h^{-1}}$ — автоморфизм, обратный к $\psi_h : N \simeq N$.

Полученная таким образом группа называется *полупрямым произведением* групп N и H по действию $\psi : H \rightarrow \text{Aut } N$ и обозначается $N \rtimes_{\psi} H$. Подчеркнём, что результат зависит от выбора действия ψ . Если действие тривиально, т. е. $\psi_h = \text{Id}_N$ 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 $G = N \rtimes_{\psi} H$ 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. \square

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. \square

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

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

Теорема 13.3 (теорема Силова)

Для любого простого p , делящего $|G|$, силоские p -подгруппы в G существуют. Все они сопряжены друг другу, и любая p -подгруппа в G содержится в некоторой силоской 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:

$$\text{Stab}(F) = \{g \in G \mid gF \subset F\}.$$

Так как $g_1 x \neq g_2 x$ при $g_1 \neq g_2$ в группе G , группа $\text{Stab}(F)$ свободно действует на множестве F и все орбиты этого действия состоят из $|\text{Stab}(F)|$ точек. Поэтому $|F| = p^n$ делится на $|\text{Stab}(F)|$ 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 $|\text{Stab}(F)| = p^n$, т. е. подгруппа $\text{Stab}(F) \subset G$ силоская. Во втором случае согласно [предл. 13.4](#) каждая p -подгруппа $H \subset G$ (в частности, каждая силоская подгруппа), имеет на G -орбите элемента F неподвижную точку gF , а значит, содержится в силоской подгруппе $\text{Stab}(gF) = g \text{Stab}(F) g^{-1}$, сопряжённой к $\text{Stab}(F)$ (и совпадает с ней, если H силоская). 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. \square

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 $(1+x)^{p^n m} = \left(1+x^{p^n}\right)^m = 1+mx^{p^n} + \text{старшие степени}$. \square

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 $|\mathcal{S}| = |G|/|\text{Stab}(P)|$, где $P \in \mathcal{S}$ — произвольно взятая силовская p -подгруппа. Поскольку $P \subset \text{Stab}(P)$, порядок $|\text{Stab}(P)|$ 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 $P \subset \text{Stab}(H) = \{g \in G \mid gHg^{-1} \subset H\}$. Поскольку $H \subset \text{Stab}(H) \subset G$, порядок $|\text{Stab}(H)| = p^n m'$, где $m' \mid m$ и взаимно просто с p . Таким образом, и P , и H являются силовскими p -подгруппами в $\text{Stab}(H)$, причём H нормальна в $\text{Stab}(H)$. Так как все силовские подгруппы сопряжены, мы заключаем, что $H = P$, что и требовалось. \square

Пример 13.6 (группы порядка pq с простыми $p > q$ и $\text{нод}(p-1, q) = 1$)

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 $H_q \simeq \mathbb{Z}/(q)$. Поскольку H_p и H_q просты, $H_p \cap H_q = e$ и $G = H_p H_q$. Согласно н° 13.3 $G = H_p \rtimes_{\psi} H_q$ для некоторого гомоморфизма $\psi : H_q \rightarrow \text{Aut } H_p$.

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

Аддитивный гомоморфизм $\psi : \mathbb{Z}/(q) \rightarrow \mathbb{Z}/(p-1)$ однозначно задаётся своим значением на образующей $[1]_q$ $\mathbb{Z}/(q)$ -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 $\text{нод}(p-1, q) = 1$ в \mathbb{Z} -модуле $\mathbb{Z}/(p-1)$ этот оператор обратим, откуда $\psi = 0$, т. е. в мультипликативной записи гомоморфизм $\psi : H_q \rightarrow \text{Aut } H_p$ 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 $\text{нод}(p-1, q) = 1$.

Пример 13.7 (группы порядка $2p$)

Пусть $|G| = 2p$, где $p > 2$ простое. Рассуждая как в предыдущем примере, заключаем, что $G = \mathbb{Z}/(p) \rtimes_{\psi} \mathbb{Z}/(2)$ для некоторого действия $\psi : \mathbb{Z}/(2) \rightarrow \text{Aut}(\mathbb{Z}/(p)) \simeq \mathbb{F}_p^*$, 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 $G \simeq \mathbb{Z}/(p) \oplus \mathbb{Z}/(2)$. 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 обратно¹ 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 $x^n u x^n \in F_2$ 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 $(n_{ij}, v_k - (v_i + v_j)/2) = (v_i, v_k) - (v_j, v_k) + (v_i, v_i)/2 - (v_j, v_j)/2 = 0$, 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 $\{i, j\} \cap \{k, m\} = \emptyset$ 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.

¹обратите 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 $(A \cap D)C \triangleleft D$, поскольку $C \triangleleft D$. 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 $|H| \geq 16$, 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 $|H| \geq 25$, 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 $g(k) = t \notin \{i, j, k\}$. При $n \geq 6$ найдётся чётная перестановка h , оставляющая на месте i, j, k и переводящая t в $\ell \neq t$. Тогда ghg^{-1} переводит i в j , а k — в $\ell \neq t$.

Упр. 13.17. Проверка ассоциативности:

$$\begin{aligned} ((x_1, h_1) \cdot (x_2, h_2)) \cdot (x_3, h_3) &= (x_1 \psi_{h_1}(x_2), h_1 h_2) \cdot (x_3, h_3) = (x_1 \psi_{h_1}(x_2) \psi_{h_1 h_2}(x_3), h_1 h_2 h_3) \\ (x_1, h_1) \cdot ((x_2, h_2) \cdot (x_3, h_3)) &= (x_1, h_1) \cdot (x_2 \psi_{h_2}(x_3), h_2 h_3) = (x_1 \psi_{h_1}(x_2 \psi_{h_2}(x_3)), h_1 h_2 h_3). \end{aligned}$$

Но $\psi_{h_1}(x_2 \psi_{h_2}(x_3)) = \psi_{h_1}(x_2) \psi_{h_1} \circ \psi_{h_2}(x_3) = \psi_{h_1}(x_2) \psi_{h_1 h_2}(x_3)$. 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: $(\psi_h^{-1}(x^{-1}), h^{-1}) \cdot (x, h) = (\psi_h^{-1}(x^{-1}) \psi_h^{-1}(x^{-1}), h^{-1} h) = (e, e)$.

Упр. 13.18. Так как $\psi : H \rightarrow \text{Aut } N$ — гомоморфизм, $\psi_e = \text{Id}_N$ и

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

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

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

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

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

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 $b^k a^m$. 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 $\text{GL}_1(\mathbb{F}_p) \simeq \mathbb{F}_p^*$ ненулевых элементов поля \mathbb{F}_p по умножению. Как и всякая конечная мультипликативная подгруппа поля, она циклическая.