УДК 512.543.72 + 512.542.68 + 512.544.33 MSC: 20F70, 20E10, 20D15, 20F18

КОНЕЧНЫЕ И НИЛЬПОТЕНТНЫЕ СИЛЬНО ВЕРБАЛЬНО ЗАМКНУТЫЕ ГРУППЫ

Антон А. Клячко[♭♮] Вероника Ю. Мирошниченко[♭] Александр Ю. Ольшанский[♯♭♮]

[♭] *Механико-математический факультет Московского государственного университета Москва 119991, Ленинские горы, МГУ.*

[♮] *Московский центр фундаментальной и прикладной математики.*

[♯] *Department of Mathematics, Vanderbilt University, Nashville 37240, U.S.A.*

klyachko@mech.math.msu.su werunik179@gmail.com alexander.olshanskiy@vanderbilt.edu

Мы показываем, в частности, что, если конечная группа H является ретрактом всякой конечной группы, содержащей H в качестве вербально замкнутой подгруппы, то центр группы H выделяется в ней прямым сомножителем.

1. Введение

Подгруппа H группы G называется *вербально замкнутой* [MR14], если всякое уравнение вида

$$w(x, y, \ldots) = h, \quad \text{где } w \text{ — это элемент свободной группы } F(x, y, \ldots) \text{ и } h \in H,$$

имеющее решение в G, имеет решение в H. Если же каждая конечная система уравнений с коэффициентами из H

$$\{w_1(x, y, \ldots) = 1, \ldots, w_m(x, y, \ldots) = 1\}, \quad \text{где } w_i \in H * F(x, y, \ldots) \text{ (а } * \text{ — это свободное произведение)},$$

имеющая решение в G, имеет решение в H, то подгруппу H называют *алгебраически замкнутой* в G.

Алгебраическая замкнутость — это более сильное свойство, чем вербальная замкнутость, но во многих случаях эти свойства оказываются эквивалентными (смотрите [Rom12], [PX13], [MR14], [Mazh17], [PXK17], [KM18], [KMM18], [Mazh18], [Bog18], [Bog19], [Маж19], [PT19], [PT20], [Тим21]). Группу H называют *сильно вербально замкнутой* [Mazh18], если она алгебраически замкнута во всякой группе, содержащей H в качестве вербально замкнутой подгруппы. Таким образом, вербальная замкнутость — это свойство подгруппы, а сильная вербальная замкнутость — это свойство абстрактной группы. Класс сильно вербально замкнутых групп довольно широк. Например, сильно вербально замкнутыми являются

– все абелевы группы [Mazh18],
– все свободные группы [KM18],
– все почти свободные группы, не содержащие неединичных конечных нормальных подгрупп [KM18], [KMM18],
– все группы, раскладывающиеся в свободное произведение нетривиальным образом [Маж19],
– фундаментальная группа любой связной поверхности, кроме, бутылки Клейна [Mazh18], [K21].

В [Bog18] и [Bog19] можно найти обобщения некоторых из приведённых выше результатов.

В частности, из этих результатов вытекает, что

бесконечная диэдральная группа сильно вербально замкнута.

Этот невинно выглядящий частный случай является одним из самых трудоёмких и его приходится рассматривать отдельно. Фактически именно это утверждение является основным результатом работы [KMM18] (который потом применяется в [Маж19], [Bog18] и [Bog19]). В параграфе 4 мы естественным образом дополняем этот факт и описываем все конечные диэдральные сильно вербально замкнутые группы.

Работа первого автора выполнена при поддержке Российского научного фонда, грант № 22-11-00075. Работа третьего автора выполнена при поддержке NSF, грант DMS-1901976.

Доказать сильную вербальную замкнутость бывает непросто, но доказать её отсутствие тоже непросто. В литературе встречаются только следующие примеры не сильно вербально замкнутых групп:

– уже упомянутая фундаментальная группа бутылки Клейна [K21]
– и две неабелевы группы порядка восемь [KM18], [PXK17].

Последний пример нам удалось сильно обобщить: в параграфе 3 мы доказываем, что

центр конечной сильно вербально замкнутой группы выделяется в ней прямым сомножителем

(и вообще, абелевы нормальные подгруппы конечных сильно вербально замкнутых групп очень специфически расположены, смотрите теорему о центрах в параграфе 3). В частности, это означает, что конечные нильпотентные неабелевы группы не бывают сильно вербально замкнутыми. Это приводит к такому естественному вопросу.

Вопрос 1. *Существуют ли конечно порождённые нильпотентные неабелевы сильно вербально замкнутые группы?*

Мы предполагаем, что ответ отрицательный, но пока нам удалось справиться (в параграфе 5) только с простейшей бесконечной нильпотентной неабелевой группой:

$$\text{группа Гейзенберга } \mathbf{UT}_3(\mathbb{Z}) = \begin{pmatrix} 1 & \mathbb{Z} & \mathbb{Z} \\ 0 & 1 & \mathbb{Z} \\ 0 & 0 & 1 \end{pmatrix} \text{ не сильно вербально замкнута.}$$

Алгебраическая замкнутость может быть охарактеризована на структурном языке, если группа H *нётерова по уравнениям* (то есть любая система уравнений над H от конечного числа неизвестных имеет те же решения, что некоторая её конечная подсистема), а именно, алгебраическая замкнутость в этом случае эквивалентна «локальной ретрактности» [KMM18]:

> *нётерова по уравнениям подгруппа H группы G алгебраически замкнута в G тогда и только тогда, когда H является ретрактом* (то есть образом эндоморфизма ρ такого, что $\rho\circ\rho = \rho$) *каждой конечно порождённой над H подгруппы группы G* (то есть подгруппы вида $\langle H \cup X\rangle$, где множество $X \subseteq G$ конечно).

Другой известный (и несложный) факт доказан в [PX13] (лемма 1.1):

> *если $V(G)$ — вербальная подгруппа группы G, а H — вербально замкнутая подгруппа группы G, то $H \cap V(G) = V(H)$ (то есть вербальная подгруппа группы H, соответствующая тому же многообразию) и образ $H/V(H) \subseteq G/V(G)$ подгруппы H при естественном гомоморфизме $G \to G/V(G)$ вербально замкнут в $G/V(G)$.*

Из этих двух фактов (и из того, что многообразие, порождённое конечной группой, состоит из локально конечных групп [Ней69], теорема 15.71) сразу же вытекает, что

> *конечная группа H сильно вербально замкнута тогда и только тогда, когда она является ретрактом всякой конечной группы G, содержащей H в качестве вербально замкнутой подгруппы и удовлетворяющей всем тождествам группы H.*

Следующий параграф содержит (короткое) доказательство того, что конечные группы с неабелевым монолитом (например, все конечные простые группы) не только сильно вербально замкнуты, но обладают даже более сильным свойством.

Теорема 1. *Конечные группы с неабелевым монолитом сильно вербально замкнуты. Более того, каждая такая группа H является ретрактом любой содержащей её конечной группы, в которой выполнены все тождества группы H.*
(То есть вербальную замкнутость можно не требовать — она имеет место автоматически в такой ситуации.)

Напомним, что *монолитом* группы называют пересечение всех неединичных нормальных подгрупп этой группы. Многие конечные группы с абелевыми монолитами оказываются тоже сильно вербально замкнутыми и даже ретрактами в группах из порожденных ими многообразий, (смотрите теорему 2 в следующем параграфе); в частности, этим свойством обладают полупрямые произведения, возникающие из точных неприводимых представлений конечных p'-групп над $\mathbb{Z}_p$.

Мы завершаем это краткое введение следующим простым наблюдением, которое, в частности, показывает необходимость оговорки о конечной порождённости в вопросе про нильпотентные группы, сформулированном выше.

Теорема о вложении. *Всякая группа H вкладывается в сильно вербально замкнутую группу мощности $|H| + \aleph_0$, удовлетворяющую всем тождества группы H.*

Доказательство. Если группа H алгебраически замкнута в в каком-то многообразии $\mathcal{M}$ (то есть алгебраически замкнута во всякой группе из $\mathcal{M}$, содержащей H), то H сильно вербально замкнута в силу упомянутой выше леммы из [РХ13]. Поэтому доказываемое утверждение вытекает из следующей теоремы Скотта [Sco51]:

любая группа H из любого многообразия $\mathcal{M}$ вкладывается в алгебраически замкнутую в $\mathcal{M}$ группу из $\mathcal{M}$ мощности $|H|+\aleph_0$.

В [Sco51] (смотрите также [ЛШ80]) эта теорема сформулирована для многообразия всех групп, но нетрудно сообразить, что (простое) доказательство проходит без каких-либо изменений для любого многообразия (и даже для любого класса групп, замкнутого относительно объединений возрастающих цепочек).

Авторы благодарят Филиппа Денисова за ценные замечания.

2. Монолитические группы

Напомним некоторую терминологию (смотрите [Ней69]):
- *многообразие, порождённое классом групп $\mathcal{K}$* — это класс всех групп, в которых выполнены все тождества всех групп из $\mathcal{K}$;
- группа называется *критической*, если она не содержится в многообразии, порождённом классом, состоящим из всех её собственных подгрупп и всех её факторгрупп по нетривиальным нормальным подгруппам.

Доказательство теоремы о неабелевых монолитах. Пусть M — неабелев монолит подгруппы H конечной группы G, удовлетворяющей всем тождествам группы H. Надо показать, что H — ретракт группы G. Любая нетривиальная нормальная подгруппа в минимальном гипотетическом контрпримере G нетривиально пересекает H (или M, что равносильно). Отсюда следует, что в G есть лишь одна минимальная нормальная подгруппа, причем она содержит M. Обе группы H и G критические, ибо их монолиты неабелевы ([KoN66], смотрите также [Ней69], 53.44). Поскольку они порождают при этом одно и то же многообразие, они изоморфны ([Ней69], 53.33), то есть $G = H$. Это завершает доказательство.

Для групп с абелевыми монолитами ситуация сложнее.

Лемма 1. *Пусть $M \neq \{0\}$ — конечный модуль над групповым кольцом $\mathbb{Z}_{p^m}[G]$, где простое p не делит $|G|$. Тогда*
1) *если M имеет экспоненту p^k, а все собственные подмодули — меньшую экспоненту, то*
   а) *M однороден (то есть, является прямой суммой циклических групп экспоненты p^k),*
   б) *все его слои $p^iM/p^{i+1}M$, где $i \in \{0, \ldots, k-1\}$, суть изоморфные простые G-модули;*

    в) *элементы группы G, действующие тождественно на нижнем слое, действуют тождественно на всём модуле M;*
2) *если M не раскладывается в прямую сумму нетривиальным образом, то все его собственные подмодули имеют меньшую экспоненту.*

Доказательство.

1) Пусть $L = \{x \in M \mid p^{k-1}x = 0\}$. По теореме Машке $M/pM = L/pM \oplus N/pM$ для некоторого G-модуля N. Подмодуль N имеет экспоненту p^k, ибо L имеет меньшую экспоненту. Значит, $L = pM$ в силу условия минимальности 1). Это доказывает утверждение а).
   Модуль M/pM простой из-за того же условия минимальности — прообраз в M всякого ненулевого подмодуля модуля M/pM имеет экспоненту p^k. В силу однородности, отображение $M/pM \to M/p^{s+1}M$, $a + pM \mapsto p^s a + p^{s+1}M$ является корректно определённым изоморфизмом. Это доказывает утверждение б). Свойство в) вытекает из б): элемент, действующий тождественно на нижнем слое, действует тождественно на всех слоях; а автоморфизмы абелевой p-группы, действующие тождественно на слоях, образуют подгруппу, порядок которой есть степень числа p; поэтому в) следует из того, что $|G|$ не делится на p.
2) Выберем в M минимальный подмодуль N экспоненты p^k, равной экспоненте модуля M. Из-за однородности N имеет прямое дополнение в абелевой группе M. Тогда есть и прямое модульное дополнение (это простое обобщение теоремы Машке, смотрите, например, [Pas83], лемма 1.1). Поскольку M неразложим, мы получаем, что $N = M$.

Теорема 2. *Пусть конечная группа H содержит нормальную подгруппу C такую, что C совпадает со своим централизатором, не разлагается в прямое произведение нетривиальных нормальных в H подгрупп и* НОД$(|C|, |H/C|) = 1$. *Тогда H — ретракт любой конечной группы $G \supseteq H$, в которой выполнены все тождества группы H. В частности, группа H сильно вербально замкнута.*

Доказательство. Лемма 1 показывает, что группа H монолитическая, подгруппа C является централизатором монолита $M = \{c \in C \mid c^p = 1\}$ и раскладывается в прямое произведение циклических групп одинакового порядка p^k. Заметим ещё, что подгруппа C является силовской, поскольку её порядок взаимно прост с индексом.

Доказывая, что H — ретракт группы G, мы можем сразу предположить, что любая нетривиальная нормальная подгруппа группы G содержит M, и G монолитична с монолитом $L \supseteq M$ (поскольку это заведомо так для минимального гипотетического контрпримера G).

Заметим, что M содержится в абелевой группе $C = H^m$, где $m = |G : C|$. Поскольку $G \in \mathbf{var}\, H$, мы имеем $M \subseteq G^m = S$ — (нормальная) абелева силовская в G, а значит, и $L \subseteq S$. Абелева силовская подгруппа S выделяется прямым сомножителем в своём централизаторе по теореме Шура–Цассенхауза: $\mathrm{C}_G(S) = S \times U$. Подгруппа U характеристическая (и даже вербальная) в $\mathrm{C}_G(S)$, стало быть, $U \triangleleft G$. Но $U \cap M = \{1\}$, то есть $U = \{1\}$ из-за монолитичности группы G. Таким образом, силовская p-подгруппа S группы G совпадает со своим централизатором. Значит, по лемме 1 получаем, что S — однородная группа экспоненты l, причем $l = k$, ибо $G \in \mathbf{var}\, H$, и $S = \mathrm{C}_G(L)$ (по утверждению 1) в) леммы 1).

Чтобы доказать равенство $G = H$, осталось показать, что $|L| = |M|$ и $|G/\mathrm{C}_G(L)| = |H/\mathrm{C}_H(M)|$. Поскольку левые части этих равенств заведомо не больше правых (ибо H — подгруппа в G), равенства следуют из леммы 53.25 из книги [Ней69], которая говорит, в частности, что

> *монолит L всякой группы G из многообразия, порождённого конечной группой H, изоморфен монолиту N некоторого фактора F (то есть факторгруппы подгруппы) группы H, причём $G/\mathrm{C}_G(L) \simeq F/\mathrm{C}_F(N)$.*

Это означает, что в нашем случае $L = M$ и $G/\mathrm{C}_G(L) \simeq H/\mathrm{C}_H(M)$, и завершает доказательство.

Теоремы 1 и 2 подсказывают следующее определение. Группу H назовём *сильным ретрактом*, если она является ретрактом в каждой группе $G \supseteq H$ из многообразия $\mathbf{var}\, H$. Свойство быть сильным ретрактом — это свойство абстрактной группы H, более сильное, чем сильная вербальная замкнутость.

Утверждение. *Конечная подгруппа H группы G является ретрактом тогда и только тогда, когда она является ретрактом каждой конечно порождённой подгруппы группы G, содержащей H. В частности, сильными ретрактами являются*

- *все конечные группы с неабелевым монолитом*
- *и каждая конечная группа H, содержащая нормальную подгруппу C такую, что C совпадает со своим централизатором, не разлагается в прямое произведение нетривиальных нормальных в H подгрупп и* $\text{НОД}(|C|, |H/C|) = 1$.

Доказательство. Утверждение «В частности» немедленно вытекает из основного утверждения и теорем 1 и 2. А основное утверждение следует из локальной теоремы Мальцева (смотрите [KaM82], теорема 37.3.1):

> *если предметно-универсальная формула истинна на подсистемах локально покрывающих алгебраическую систему A, то она истинна на A.*

Достаточно применить эту теорему к формуле «существует ретракция $G \to H$» на алгебраической системе $(G, \cdot, {}^{-1}, h_1, \ldots, h_n)$, где $\{h_1, \ldots, h_n\} = H$, заметив, что каждой ретракции $\rho \colon G \to H$ соответствует двуместный предикат $P(x, y)$ (график этой ретракции), причём условие того, что двуместный предикат является графиком ретракции записывается в виде универсальной формулы (поскольку группа H конечна).

Вопрос 2. *Как устроен произвольный конечный сильный ретракт?*

3. Центр конечной сильно вербально замкнутой группы

Лемма об аппроксимации. *Для любой конечной элементарной абелевой p-группы C (где число p простое) и любого натурального k найдётся такое $t \geqslant k$, что прямое произведение $P = \bigtimes_{i=1}^{t} C_i$ копий C_i группы C содержит подгруппу R, инвариантную относительно диагонального действия на P алгебры эндоморфизмов $\operatorname{End} C \simeq \mathrm{M}_d(\mathbb{Z}_p)$ (где $d = \log_p |C|$) группы C, со следующими свойствами:*

а) *R содержится в объединении ядер K_j естественных ретракций (проекций) $P \to C_j$,*

б) *но $R \cdot \bigtimes_{j \notin J} C_j = P$ для любого подмножества $J \subseteq \{1, \ldots, t\}$ мощности k;*

б$'$) *более того, каждое такое J содержится в множестве $J' \supseteq J$ таком, что $P = R \times \bigtimes_{j \notin J'} C_j$; причём существуют такие целые числа n_{ij}, что проекция $\pi \colon P \to \bigtimes_{j \notin J'} C_j$ с ядром R действует так: $C_i \ni c_i \mapsto \prod_j c_j^{n_{ij}}$, где $c_j \in C_j$ — элементы, соответствующие элементу c_i при изоморфизме $C_i \simeq C \simeq C_j$.*

Доказательство. Группу C (которую мы, разумеется, можем считать неединичной) реализуем, как аддитивную группу векторного пространства $\mathbb{Z}_p^d$, а группу P — как группу всех отображений из $X = V \setminus \{0\}$ в $\mathbb{Z}_p^d$, где V — конечное векторное пространство (размерности n, выбранной ниже) над $\mathbb{Z}_p$ (при этом C_i превратится в множество отображений, принимающих значение ноль во всех векторах из X, кроме одного, то есть $t = p^n - 1$). В качестве $R \subseteq P$ возьмём множество полиномиальных отображений, задаваемых многочленами степени не выше r без свободных членов:

$$R = R_r =$$
$$= \Big\{ (\widehat{x}_1, \ldots, \widehat{x}_n) \mapsto \big(f_1(\widehat{x}_1, \ldots, \widehat{x}_n), \ldots, f_d(\widehat{x}_1, \ldots, \widehat{x}_n)\big) \mid f_i \in \mathbb{Z}_p[x_1, \ldots, x_n],\ \deg f_i \leqslant r,\ f_i(0, \ldots, 0) = 0 \Big\}.$$

Здесь $(\widehat{x}_1, \ldots, \widehat{x}_n)$ — это координаты вектора $v \in V$ в некотором базисе; но нетрудно сообразить, что определение множества R не зависит от выбора базиса в V; а также не зависит от выбора базиса в $\mathbb{Z}_p^d$, что обеспечивает инвариантность подгруппы R относительно «диагонального» действия группы $\mathbf{GL}_d(\mathbb{Z}_p)$. По тем же причинам, имеет место $\mathrm{M}_d(\mathbb{Z}_p)$-инвариантность (вообще, для любого поля F

$\mathbf{GL}_d(F)$-инвариантность влечёт $\mathrm{M}_d(F)$-инвариантность, поскольку всякая матрица раскладывается в сумму невырожденных).

Теорема Шевалле ([Che35], смотрите также, например, [Лен68], глава 5, упражнение 6) говорит, что

многочлены $f_1, \ldots, f_d \in F[x_1, \ldots, x_n]$ без свободных членов над конечным полем F имеет общий ненулевой корень, если $n > \sum \deg f_j$.

Если выбрать пространство V (то есть число $t = p^{\dim V} - 1 = p^n - 1$) и число r так, что $n = \dim V > rd$, то свойство а) будет выполнено, поскольку любое отображение $f \in R$ отправляет в ноль некоторый вектор из X, то есть проекция элемента f на некоторый сомножитель C_i нулевая.

Чтобы выполнялось условие б) нам надо для произвольных векторов $v_1, \ldots, v_k \in X$ и $w_1, \ldots, w_k \in \mathbb{Z}_p^d$ найти такое отображение $f = f_{v_1, w_1, \ldots, v_k, w_k} \in R$, что $f(v_i) = w_i$ для всех i (так как тогда произвольное отображение $g \in P$ запишется в виде $g = f_{v_1, g(v_1), \ldots, v_k, g(v_k)} + h$, где $h(v_i) = 0$, что и требовалось).

Поскольку определение множества R не зависит от выбора базиса в V, мы можем считать, что у всех векторов v_i все координаты, кроме первых k, нулевые. Всякое отображение из k-мерного векторного пространства над $\mathbb{Z}_p$ в $\mathbb{Z}_p$ задаётся, как хорошо известно, многочленом, имеющим степень не выше $p-1$ по каждой переменной, то есть общая степень такого многочлена не выше $k(p-1)$. Значит, найдутся многочлены $f_1, \ldots, f_d \in \mathbb{Z}_p[x_1, \ldots, x_k]$ такие, что для всех $i \in \{1, \ldots, k\}$ и $j \in \{1, \ldots, d\}$

$$(\text{значение многочлена } f_j \text{ от первых } k \text{ координат вектора } v_i) = (j\text{-я координата вектора } w_i),$$
$$f_j(0, \ldots, 0) = 0, \quad \text{и} \quad \deg f_j \leqslant k(p-1).$$

Значит, если выбрать $r \geqslant k(p-1)$, то отображение $f \colon (\widehat{x}_1, \ldots, \widehat{x}_n) \mapsto \big(f_1(\widehat{x}_1, \ldots, \widehat{x}_k), \ldots, f_d(\widehat{x}_1, \ldots, \widehat{x}_k)\big)$ будет лежать в R и переводить v_i в w_i, что и завершает доказательство условия б).

Условие б$'$) вытекает из б), поскольку C_j — суть неприводимые подмодули полупростого $\mathrm{M}_d(\mathbb{Z}_p)$-модуля P, поэтому остаётся воспользоваться хорошо известным (и несложным) общим фактом о модулях:

если R — подмодуль полупростого модуля $P = R + \bigoplus\limits_{i \in I} C_i$, где модули C_i неприводимы, то $P = R \oplus \bigoplus\limits_{i \in I'} C_i$ для некоторого подмножества $I' \subseteq I$.

Чтобы понять, что проекция группы P на $\bigtimes\limits_{j \notin J'} C_j$ задаётся целочисленной матрицей, достаточно заметить, что эта проекция является эндоморфизмом $\mathrm{M}_t(\mathbb{Z}_p)$-модуля и воспользоваться хорошо известным общим фактом об эндоморфизмах полупростых модулей:

всякий эндоморфизм модуля $\bigoplus C_i$ над полупростой алгеброй A, где модули C_i неприводимы, задаётся матрицей с элементами из центра алгебры A,

то есть для всякого эндоморфизма φ найдётся матрица $M_\varphi = (m_{ij})$ с элементами из центра алгебры A такая, что для каждого $c_i \in C_i$ мы имеем $\varphi(c_i) = \sum\limits_{j \colon C_j \simeq C_i} m_{ij} c_j$, где $c_j \in C_j$ — элементы соответствующие элементу c_i при (фиксированном) изоморфизме $C_j \simeq C_i$. Это завершает доказательство леммы.

Аналогичный факт верен для произвольных конечных полей. Мы его сформулируем для будущего, но в этой работе он нам не понадобится. Доказательство легко получить из рассуждения выше очевидными изменениями.

Лемма об аппроксимации для конечных полей. *Для конечного векторного пространства C над конечным полем F и любого натурального k найдётся такое $t \geqslant k$, что прямая сумма $P = \bigoplus\limits_{i=1}^{t} C_i$ копий C_i пространства C содержит подпространство R, инвариантное относительно диагонального действия на P алгебры эндоморфизмов $\operatorname{End} C \simeq \mathrm{M}_d(F)$ (где $d = \dim C$) пространства C, со следующими свойствами:*

а) *R содержится в объединении ядер K_j естественных проекций $P \to C_j$,* б) *но* $R + \bigoplus_{j \notin J} C_j = P$ *для любого подмножества* $J \subseteq \{1, \dots, t\}$ *мощности* k;

б$'$) *более того, каждое такое* J *содержится в множестве* $J' \supseteq J$ *таком, что* $P = R \oplus \bigoplus_{j \notin J'} C_j$; *причём существуют такие* $n_{ij} \in F$, *что проекция* $\pi\colon P \to \bigoplus_{j \notin J'} C_j$ *с ядром* R *действует так:* $C_i \ni c_i \mapsto \sum_j n_{ij} c_j$, *где* $c_j \in C_j$ *— векторы, соответствующие вектору* c_i *при изоморфизме* $C_i \simeq C \simeq C_j$.

Теорема о центрах. *Центр любой конечной сильно вербально замкнутой группы выделяется в ней прямым сомножителем. Более того, для любой нормальной подгруппы* N *сильно вербально замкнутой группы* H *центр* $\mathrm{Z}\Big(\mathrm{C}\big(\mathrm{Z}(N)\big)\Big)$ *централизатора* $\mathrm{C}\big(\mathrm{Z}(N)\big)$ *центра* $\mathrm{Z}(N)$ *группы* N *выделяется в этом централизаторе прямым сомножителем, причём дополнение нормально в* H:

$$\underbrace{\mathrm{C}\big(\mathrm{Z}(N)\big)}_{\substack{\cup\!|\\ N}} = \underbrace{\mathrm{Z}\Big(\mathrm{C}\big(\mathrm{Z}(N)\big)\Big)}_{\substack{\cup\!|\\ \mathrm{Z}(N)}} \times D \quad \text{\textit{для некоторой подгруппы} } D \triangleleft H.$$

Доказательство. Вертикальные включения верны для любой подгруппы любой группы (мы их добавили в формулировку для наглядности).

Пусть $L = \mathrm{C}\big(\mathrm{Z}(N)\big)$. Достаточно для каждого простого p найти гомоморфизм $\psi_p\colon L \to \mathrm{Z}(L)$, коммутирующий с действием группы H на L сопряжениями и инъективный на p-компоненте $\mathrm{Z}_p(L)$ центра $\mathrm{Z}(L)$ группы L, поскольку тогда гомоморфизм $\psi\colon x \mapsto \prod_p \psi_p\big(\pi_p(x)\big)$ (где $\pi_p\colon \mathrm{Z}(L) \to \mathrm{Z}_p(L)$ — проекция на p-компоненту) будет инъективным на $\mathrm{Z}(L)$ и, следовательно, его ядро будет искомым дополнением D.

Предположим, что таких гомоморфизмов ψ_p нет для некоторого p, то есть всякий согласованный с действием группы H гомоморфизм $L \to \mathrm{Z}(L)$ не инъективен на $\mathrm{Z}_p(L)$, а значит, и на максимальной элементарной подгруппе $C \subseteq \mathrm{Z}_p(L)$. Надо показать, что группа H не сильно вербально замкнута.

Выберем t в соответствии с леммой об аппроксимации, применённой к C (для некоторого целого k, которое мы уточним позже), и рассмотрим расслоенное произведение

$$Q = \Big\{(h_1, \dots, h_t) \in H^t \;\Big|\; h_1 L = \ldots = h_t L\Big\} \quad t \text{ копий группы } H.$$

В качестве надгруппы $G \supset H$ возьмём факторгруппу $G = Q/R$, где подгруппа $R \subset C^t$ выбрана в соответствии с леммой об аппроксимации (R нормальна в Q, поскольку R инвариантна относительно диагонального действия группы $\mathrm{Aut}\, C$, а группа Q действует сопряжениями на P диагонально, так как L^t коммутирует с $P = C^t$).

Тогда H вкладывается в G диагональным образом: $h \mapsto (h, \dots, h)$. Этот гомоморфизм является вложением не только в Q, но и в G по свойству а) леммы об аппроксимации, поскольку все проекции нетривиального диагонального элемента группы Q нетривиальны.

Эта диагональная подгруппа $H \subset G$ вербально замкнута в G. Действительно, если уравнение

$$w(x_1, \dots, x_n) = h$$

разрешимо в G и $(\widetilde{x}_1, \dots, \widetilde{x}_n) \in H^t$ — (любой) прообраз (любого) решения, то

$$w(\widetilde{x}_1, \dots, \widetilde{x}_n) = (hc_1, \dots, hc_t),$$

где $(c_1, \dots, c_t) \in R$, а следовательно, по свойству а) $c_i = 1$ при некотором i, то есть i-е координаты набора $(\widetilde{x}_1, \dots, \widetilde{x}_n)$ являются решением уравнения $w(x_1, \dots, x_n) = h$ в H, что и требовалось.

Осталось показать, что диагональная подгруппа $H \subset G$ не является ретрактом. Пусть $\rho\colon G \to H$ — гипотетическая ретракция и $\widehat{\rho}\colon Q \to H$ — её композиция с естественным эпиморфизмом $Q \to Q/R = G$.

Во всех дальнейших построениях слова «подгруппы» и «централизаторы» по умолчанию относятся к расслоенному произведению Q (которое содержит диагонально вложенную подгруппу H); централизатор множества X в группе H мы обозначаем символом $\mathrm{C}_H(X)$, то есть $\mathrm{C}_H(X) = \mathrm{C}(X) \cap H$. Если U — подгруппа группы L, то символы U_i, где $i = 1, \dots, t$, обозначает соответствующие подгруппы $\{(1, \dots, 1, u, 1, \dots, 1) \mid u \in U\}$ группы Q.

Проверим, что

$$\widehat{\rho}(L_i) \subseteq \mathrm{C}_H\bigl(\mathrm{C}_H(L)\bigr) = L \quad \text{для каждого } i. \tag{$*$}$$

Действительно, если $h \in C_H(L)$, то h коммутирует с каждой компонентой каждого элемента из L, то есть h коммутирует с L_i. Применяя к этому соотношению ретракцию $\widehat{\rho}$, получаем, что $h = \widehat{\rho}(h)$ коммутирует с подгруппой $\widehat{\rho}(L_i)$, что и доказывает включение в формуле $(*)$. А равенство вытекает из того, что подгруппа L является централизатором (центра подгруппы N), а тройной централизатор любой подгруппы любой группы совпадает с одинарным всегда.
С другой стороны, взаимный коммутант $[L_i,\ L_j]$ при $i \neq j$ тривиален. Значит, $[\widehat{\rho}(L_i),\ \widehat{\rho}(L_j)] = \{1\}$. Стало быть, $\left[\widehat{\rho}(L_i),\ \prod\limits_{j \neq i} \widehat{\rho}(L_j)\right] = \{1\}$. Если же $\widehat{\rho}(L_i) = \widehat{\rho}(L_l)$ для каких-то различных i и l, то $\left[\widehat{\rho}(L_i),\ \prod\limits_{j} \widehat{\rho}(L_j)\right] = \{1\}$ и, следовательно, $[\widehat{\rho}(L_i),\ L] = \{1\}$ (поскольку $L = \widehat{\rho}(L) \subseteq \prod\limits_j \widehat{\rho}(L_j)$). Таким образом,

$$\widehat{\rho}(L_i) \subseteq \mathrm{C}_H(L), \quad \text{если } \widehat{\rho}(L_i) = \widehat{\rho}(L_l) \text{ для каких-то различных } i \text{ и } l. \tag{$**$}$$

Из $(*)$ и $(**)$ немедленно вытекает, что

если $\widehat{\rho}(L_i) = \widehat{\rho}(L_l)$ для каких-то различных i и l, то $\widehat{\rho}(L_i) \subseteq \mathrm{Z}(L)$.

Возьмём в лемме об аппроксимации в качестве k число всех подгрупп в H, а в качестве J — множество *уникальных* i, то есть таких, что $\widehat{\rho}(L_i) \neq \widehat{\rho}(L_l)$ ни для какого $l \neq i$. Тогда по пункту б$'$) имеет место разложение

$$\mathop{\times}_{i=1}^{t} C_i = R \times \mathop{\times}_{i \in I} C_i, \quad \text{где все } i \in I \text{ неуникальны,}$$

причём проектирование $\pi\colon \mathop{\times}\limits_{i=1}^{t} C_i \to \mathop{\times}\limits_{i \in I} C_i$ на второй сомножитель в этом разложении задаётся целочисленной матрицей (n_{ij}) (то есть $C_i \ni c_i \overset{\pi}{\mapsto} \prod\limits_j c_j^{n_{ij}}$, где $c_j \in C_j$ — элементы, соответствующие элементу c_i при изоморфизме $C_i \simeq C \simeq C_j$). Это означает, что ограничение $\widehat{\pi}\colon C \to \mathop{\times}\limits_{i \in I} C_i$ проектирования π на C задаётся формулой

$$\widehat{\pi}\colon c \overset{\pi}{\mapsto} \prod_{j \in I} c_j^{m_j}, \quad \text{где } m_j = \sum_i n_{ij} \text{ и } c_j \in L_j \text{ — элементы, соответствующие элементу } c \in C.$$

Стало быть, композиция

$$\Psi\colon C \to \mathrm{Z}(L), \quad \Psi\colon c \overset{\pi}{\mapsto} \prod_{j \in I} c_j^{m_j} \overset{\widehat{\rho}}{\mapsto} \prod_{j \in I} \widehat{\rho}\left(c_j^{m_j}\right)$$

продолжается до гомоморфизма $\Phi\colon L \to \mathrm{Z}(L)$, задающегося аналогичной формулой:

$$L \ni g \overset{\Phi}{\mapsto} \prod_{j \in I} \widehat{\rho}\left(g_j^{m_j}\right), \quad \text{где } g_j \in L_j \text{ — элементы, соответствующие элементу } g \in L.$$

(Это гомоморфизм, поскольку $\widehat{\rho}(L_j)$ при $j \in I$ содержится в абелевой группе $\mathrm{Z}(L)$.) Этот гомоморфизм Φ согласован с действием группы H и, следовательно, его ядро нетривиально пересекает C по условию. Таким образом, гомоморфизм Ψ, являющейся ограничением гомоморфизма Φ на C, имеет нетривиальное ядро. С другой стороны, Ψ — это просто тождественное отображение, как видно из его определения ($\widehat{\rho} \circ \pi = \widehat{\rho}$, поскольку $\widehat{\rho}(R) = \{1\}$). Полученное противоречие завершает доказательство.

4. Диэдральные группы

Мы будем использовать (молча) следующие простые факты:

- *всякая группа G из многообразия, порождённого диэдральной группой конечного порядка $2n$ или $4n$, где n нечётно, раскладывается в полупрямое произведение $C \leftthreetimes Q$, где C — элементарная абелева 2-группа (силовская 2-подгруппа группы G), а Q — абелева группа периода n (холловская $2'$-подгруппа группы G или, если угодно, вербальная подгруппа, порождённая квадратами всех элементов группы G); таким образом, Q является C-модулем;*
- *всякий конечный модуль V нечётной мощности над любой элементарной абелевой 2-группой C раскладывается в прямую сумму $V = \bigoplus\limits_{\chi \in \mathrm{X}} V_\chi$, где X — множество всех гомоморфизмов (характеров) $C \to \{\pm 1\}$, а $V_\chi = \{v \in V \mid cv = \chi(c)v$ для всех $c \in C\}$.*

Лемма о полупрямых произведениях. *В полупрямом произведении $G = C \leftthreetimes Q$, где C — элементарная абелева 2-группа а Q — конечная абелева группа нечётного периода n', для любого делителя d числа $2n'$ такого, что либо $d = 2$, либо $d|n'$ и НОД$(d,\ n'/d) = 1$, выполнено равенство $\{g^{2n'/d} \mid g \in G\} = \{g \in G \mid g^d = 1\}$.*

Доказательство. Пусть $g = cq$, где $c \in C$ и $q \in Q$. Согласно сформулированным выше фактам мы получаем разложение $q = q_{c,+}q_{c,-}$, где $cqc^{-1} = q_{c,+}q_{c,-}^{-1}$, то есть $q_{c,+} \in \prod\limits_{\substack{\chi \\ \chi(c)=1}} Q_\chi$ и $q_{c,-} \in \prod\limits_{\substack{\chi \\ \chi(c)=-1}} Q_\chi$. Тогда

$$g^k = (cq)^k = (cq_{c,+}q_{c,-})^k = c^k q_{c,+}^k q_{c,-}^{\frac{1}{2}\left(1+(-1)^k\right)}.$$

Это означает, что при $d = 2$ множества, стоящие в обеих частях доказываемого равенства, состоят из всевозможных произведений $cq_{c,-}$. Если же d нечётно, то множества, равенство которых мы хотим проверить, превращаются в $\{q^{n'/d} \mid q \in Q\}$ и $\{q \in Q \mid q^d = 1\}$. В абелевой группе Q периода n' эти множества, конечно же, совпадают (если d и n'/d взаимно просты): оба этих множества являются прямым сомножителем в разложении $Q = \{q \in Q \mid q^d = 1\} \times \{q \in Q \mid q^{n'/d} = 1\}$. Это завершает доказательство.

Теорема о диэдральных группах. *Диэдральная группа D_n порядка $2n$ сильно вербально замкнута тогда и только тогда, когда n либо бесконечно, либо не делится на четыре.*
Более того, пусть $H = D_n = \langle b \rangle_2 \leftthreetimes \langle a \rangle_n$, где n не делится на четыре, это диэдральная подгруппа конечной группы G, содержащейся в многообразии, порождённом группой H. Тогда следующие условия равносильны:

1) *подгруппа H вербально замкнута в G;*
2) *подгруппа H алгебраически замкнута в G;*
3) *подгруппа H — ретракт группы G;*
4) *в терминах разложений, описанных в начале параграфа ($G = C \leftthreetimes Q$ и $Q = \bigtimes\limits_{\chi} Q_\chi$), порядок χ-компоненты $(a^2)_\chi$ элемента $a^2 \in H$ равен порядку элемента a^2 для некоторого характера $\chi\colon C \to \{\pm 1\}$.*

Доказательство. Сильная вербальная замкнутость бесконечной диэдральной группы доказана в [KMM18]. Отсутствие сильной вербальной замкнутости конечных диэдральных групп D_{4k} сразу же вытекает из теоремы о центрах.

Остаётся доказать равносильность условий 1) — 4) при конечных n, не делящихся на четыре. Для доказательства импликации 4) $\Longrightarrow$ 3) заметим, что циклическая (нормальная) подгруппа $\langle (a^2)_\chi \rangle$

выделяется прямым сомножителем в Q_χ (поскольку её порядок равен периоду абелевой группы Q_χ) и, следовательно, в Q, причём дополнение нормально в G (поскольку действие группы G на Q_χ «скалярно» и, стало быть, все подгруппы, содержащиеся в Q_χ, нормальны в G). Обозначив буквой π композицию $Q \to \langle (a^2)_\chi \rangle \xrightarrow{\simeq} \langle a^2 \rangle$, проверим, что отображение $\varphi\colon G = C \leftthreetimes Q \to H,\ c\cdot q \mapsto b^{\frac{1}{2}(1-\chi(c))}\cdot \pi(q)$ является гомоморфизмом. Гомоморфизмом является любое отображение из одного полупрямого произведения в другое $X \leftthreetimes Y \to Z \leftthreetimes T$ вида $xy \mapsto \alpha(x)\beta(y)$, где $\alpha\colon X \to Z$ и $\beta\colon Y \to T$ — гомоморфизмы такие, что $\beta(xyx^{-1}) = \alpha(x)\beta(y)\alpha(x)^{-1}$ для всех $x \in X$ и $y \in Y$. В данном случае это свойство выполнено:

$$\pi(cqc^{-1}) = \pi(cq_\chi c^{-1}) = \pi(q_\chi^{\chi(c)}) = \pi(q_\chi)^{\chi(c)} = b^{\frac{1}{2}(1-\chi(c))}\pi(q_\chi)b^{-\frac{1}{2}(1-\chi(c))} = \alpha(c)\pi(q_\chi)\alpha(c)^{-1}.$$

- Если n нечётно, то гомоморфизм φ инъективен на H, поскольку любая нетривиальная нормальная подгруппа в H нетривиально пересекает $\langle a \rangle = \langle a^2 \rangle$, а ограничение гомоморфизма φ на $\langle a^2 \rangle$ инъективно по условию 4).
- Если же n чётно, то возьмём произвольный гомоморфизм $\gamma\colon G \to G/Q \to \langle a^{\frac{n}{2}} \rangle$ такой, что $\gamma(a^{\frac{n}{2}}) = a^{\frac{n}{2}}$, и рассмотрим гомоморфизм $\varphi'\colon G \to H = \langle a^2, b \rangle \times \langle a^{\frac{n}{2}} \rangle$, $g \mapsto \varphi(g)\gamma(g)$, ограничение которого на H очевидно инъективно.

Таким образом, композиция гомоморфизма φ или φ' (в зависимости от чётности числа n) с подходящим автоморфизмом группы H есть искомая ретракция $G = C \leftthreetimes Q \to H$.

Импликации 3) $\Longrightarrow$ 2) $\Longrightarrow$ 1) — это общие факты, верные для любых групп (смотрите введение).

Осталось доказать импликацию 1) $\Longrightarrow$ 4). Для этого надо построить уравнение вида $w(x, y, \ldots) = h$, где w — элемент свободной группы $F(x, y, \ldots)$, а $h \in H$, обладающее следующими свойствам:

а) оно заведомо разрешимо в G;

б) а разрешимость этого уравнения в H влечёт условие 4).

В явном виде такое уравнение выглядит довольно страшно. Для упрощения описания мы сделаем три вещи:

- во-первых, зафиксируем какой-то элемент $a' \in \langle a \rangle_n$, порядок которого есть произведение всех нечётных простых делителей числа n;
- во-вторых, мы будем строить *многосортное уравнение* (или *уравнение с типизированными переменными*), то есть уравнение, в котором каждой переменной $x^{[d]}$ приписан тип $[d]$,
  где $d \in \{2\} \cup \{$*натуральные делители d числа n, взаимно простые с n/d*$\}$; при этом под решением такого многосортного уравнения в некоторой группе мы понимаем подстановку вместо переменных элементов этой группы, превращающую уравнение в верное равенство, причём вместо переменных типа $[d]$ разрешается подставлять лишь элементы порядка, делящего d; проверим, что наличие многосортного уравнения со свойствами а) и б) влечёт наличие обычного уравнения с этими свойствами; действительно, если в многосортном уравнении заменить каждую типизированную переменную $x^{[d]}$ на $x^{2n'/d}$, где $n' = n$, если n нечётно, и $n' = n/2$, если n чётно, то мы получим обычное уравнение, разрешимость которого (в G или в H) равносильна разрешимости исходного многосортного уравнения в той же группе, поскольку $\{g^{2n'/d} \mid g \in G\} = \{g \in G \mid g^d = 1\}$ по лемме о полупрямых произведениях;
- в-третьих, мы будем писать уравнение на модульном языке, то есть умножение элементов из Q мы будем обозначать символом $+$ (и тем же символом мы обозначаем сложение в групповом кольце группы C), а символ $\cdot$ будет означать сопряжение элементов из Q элементами из C (а также умножение в групповом кольце группы C);

Например, при $n = 15$ многосортное уравнение $(x^{[2]} + 2y^{[2]}x^{[2]}) \cdot (3z^{[15]} + 4t^{[5]}) = a'$ переводится на обычный язык так: $x^{15}(z^6t^{24})x^{-15}(yx)^{15}(z^6t^{24})^2(yx)^{-15} = a$. Разумеется, в обратную сторону такой перевод не всегда возможен. Но нам это и не нужно — единственное многосортное уравнение, которое нам понадобится, мы напишем на модульном языке и его вид будет такой же, как в примере выше: сумма целочисленных многочленов от переменных типа $[2]$, умноженных на переменные нечётных типов, равна элементу из $Q \cap H$ (а именно, некоторой степени элемента a').

Нам понадобится следующее простое тождество (по сути скопированное из [KMM18]):

$$\left(\prod_{c\in C}\Bigl(1+\chi(c)c\Bigr)\right)\cdot q = 2^{|C|}q_\chi \quad \text{для любого характера } \chi \text{ и любого } q\in Q. \tag{1}$$

Для доказательства заметим, что χ-компонента элемента q в левой части равенства умножится на два $|C|$ раз. Что касается всех остальных компонент, то они обнулятся, поскольку для каждого характера $\chi'\neq\chi$ найдётся такой $c\in C$, что $\chi(c)=-\chi'(c)$.

Разложим теперь элементарную абелеву группу C в прямое произведение циклических

$$C=\langle c_1\rangle_2\times\ldots\times\langle c_m\rangle_2\,,$$

для каждого $c=\prod c_i^{\varepsilon_i}\in C$ (где $\varepsilon_i\in\{0,1\}$) положим $f_c(x_1^{[2]},\ldots,x_m^{[2]})=\prod\left(x_i^{[2]}\right)^{\varepsilon_i}$ и рассмотрим многосортное уравнение

$$\sum_{\chi\in X}\left(\prod_{c\in C}\Bigl(1+\chi(c)f_c(x_1^{[2]},\ldots,x_m^{[2]})\Bigr)\right)\cdot y_\chi^{\left[l\left|\left\langle a'_\chi\right\rangle\right|\right]}=2^{|C|}a', \tag{2}$$

где l — минимальное натуральное число такое, что $l\left|\left\langle a'_\chi\right\rangle\right|$ взаимно просто с $n/(l\left|\left\langle a'_\chi\right\rangle\right|)$. Это уравнение разрешимо в G: достаточно положить $x_i^{[2]}=c_i$ и $y_\chi^{\left[l\left|\left\langle a'_\chi\right\rangle\right|\right]}=a'_\chi$ и уравнение (2) превратится в сумму по всем характерам χ тождеств (1), в которые подставлены $q=a'_\chi$. Таким образом, свойство а) доказано.

Осталось понять, что происходит в диэдральной группе H. Подстановка $x_i^{[2]}\to h_i\in H$ определяет гомоморфизм $\varphi\colon C\to H/\langle a\rangle$, $c\mapsto f_c(h_1,\ldots,h_m)\langle a\rangle$ и некоторый характер $\chi\colon C\xrightarrow{\varphi}H/\langle a\rangle\xrightarrow{\simeq}\{\pm1\}$. Слагаемое в левой части уравнения (2), отвечающее любому другому характеру $\chi'\neq\chi$, обнулится, поскольку найдётся такой $c\in C$, что $\chi'(c)\neq\chi(c)$ и, стало быть, элемент

$$1+\chi'(c)f_c(h_1,\ldots,h_m)=1+\chi'(c)\varphi(c)\in\mathbb{Z}[H/\langle a\rangle]$$

будет обнулять $(H/\langle a\rangle)$-модуль $\langle a\rangle$. Значит, при такой подстановке уравнения (2) превратится в

$$ky_\chi^{\left[l\left|\left\langle a'_\chi\right\rangle\right|\right]}=2^{|C|}a' \quad (\text{где } k=2^{|C|}, \text{ как нетрудно сообразить}).$$

Если $\left|\left\langle a'_\chi\right\rangle\right|<|\langle a'\rangle|$, то

- некоторый нечётный простой делитель p числа n не делит $\left|\left\langle a'_\chi\right\rangle\right|$ (по определению элемента a');
- значит, p не делит $l\left|\left\langle a'_\chi\right\rangle\right|$ (по определению числа l),
- стало быть, вместо $y_\chi^{\left[l\left|\left\langle a'_\chi\right\rangle\right|\right]}$ нельзя подставлять элементы порядков, делящихся на p (по определению разрешимости многосортного уравнения);
- следовательно, уравнение не разрешимо в диэдральной группе (так как порядок элемента в правой части делится на p).

Значит, если уравнение (2) разрешимо в диэдральной группе, то $\left|\left\langle a'_\chi\right\rangle\right|=|\langle a'\rangle|$. Но $\langle a'\rangle$ есть цоколь (то есть произведение всех минимальных нормальных подгрупп) группы $\left\langle a^2\right\rangle$, то есть из инъективности ограничения гомоморфизма $a^2\mapsto(a^2)_\chi$ на $\langle a'\rangle$ следует инъективность этого гомоморфизма на всей группе $\left\langle a^2\right\rangle$. Таким образом, из разрешимости уравнения (2) в диэдральной группе вытекает равенство $\left|\left\langle (a^2)_\chi\right\rangle\right|=\left|\left\langle a^2\right\rangle\right|$, что и требовалось.

Проиллюстрируем на простейшем нетривиальном примере, что происходило при доказательстве импликации 1) $\Longrightarrow$ 4).

Пример. Пусть $G = D_3 \times D_5 = \big(\langle b_3\rangle_2 \leftthreetimes \langle a_3\rangle_3\big) \times \big(\langle b_5\rangle_2 \leftthreetimes \langle a_5\rangle_5\big)$ и группа $H = D_{15} = \langle b\rangle_2 \leftthreetimes \langle a\rangle_{15}$ вложена в G диагонально: $b = b_3b_5$ и $a = a_3a_5$. Подгруппа H, конечно же, не ретракт группы G, так что должно найтись уравнение, разрешимое в G, но не в H. Наше рассуждение позволяет в явном виде построить такое уравнение. Посмотрим, что получается.

В рассматриваемом случае C — это четверная группа Клейна: $C = \{1, b_3, b_5, b_3b_5\}$, а

$$Q = \langle a\rangle_{15} = \langle a_3\rangle_3 \times \langle a_5\rangle_5$$

и $a' = a$. Имеется четыре характера $C \to \{\pm 1\}$:
- два «важных»: τ и π: $\tau(b_3) = -1 = -\tau(b_5) = \pi(b_5) = -\pi(b_3)$,
- и два «неважных» (в этом примере): тривиальный характер ε и характер $\delta = \tau\pi$:

$$\delta(b_3) = -1 = \delta(b_5).$$

Далее, $Q_\tau = \langle a_3\rangle$, $Q_\pi = \langle a_5\rangle$, $a_\tau = a_3$ и $a_\pi = a_5$ (а $Q_\varepsilon = Q_\delta = \{1\}$). Имеется
- две переменных типа [2]: $x_3^{[2]}$ и $x_5^{[2]}$, которые в переводе с типизированного языка на обычный превращаются в x_3^{15} и x_5^{15},
- и две переменных нечётных типов: $y_3^{[3]}$ и $y_5^{[5]}$, которые в переводе с типизированного языка на обычный превращаются в y_3^{10} и y_5^{6}.

Слова f_c (где $c \in C$) здесь такие: $f_1 = 1$, $f_{b_3} = x_3^{15}$, $f_{b_5} = x_5^{15}$ и $f_{b_3b_5} = x_3^{15}x_5^{15}$. Выражения $\big(1 + \chi(c)f_c\big) \cdot q$ из (2) (где q — это выражение от переменных, принимающее значение в Q) переводятся с модульного языка на групповой так:

$$qf_cq^{\chi(c)}f_c^{-1} = \begin{cases} (qf_c)^2, & \text{если } \chi(c) = +1 \text{ (поскольку } f_c^2 = 1 \text{ всегда);} \\ [q, f_c], & \text{если } \chi(c) = -1. \end{cases}$$

Таким образом, уравнение (2) принимает вид

$$\left[\left[\left((y_3^{10})^2x_5^{15}\right)^2, x_3^{15}\right], x_3^{15}x_5^{15}\right] \cdot \left[\left[\left((y_5^{6})^2x_3^{15}\right)^2, x_5^{15}\right], x_3^{15}x_5^{15}\right] = a^{16} = a,$$

где сомножители в левой части отвечают характерам τ и π (а множители, отвечающие неважным характерам, мы не пишем, так как они тождественно равны единице). Воспользовавшись дистрибутивностью, мы можем это уравнение немного упростить:

$$[[(y_3^{20}x_5^{15})^2, x_3^{15}] \cdot [y_5^{12}(x_3^{15})^2, x_5^{15}],\ x_3^{15}x_5^{15}] = a.$$

В группе G имеется решение $x_3 = c_3$, $x_5 = c_5$, $y_3 = a_3^2$, $y_5 = a_5$ (то есть $y_3^{[3]} = a_3$ и $y_5^{[5]} = a_5$). А в диэдральной группе H решений нет, поскольку
- если $x_3^{15} \in \langle a\rangle \not\ni x_5^{15}$, то первый внутренний коммутатор $[(\ldots)^2, x_3^{15}]$ превратится в единицу, а второй внутренний коммутатор $[(x_3^{15}y_5^{6})^2, x_5^{15}]$ попадёт в $\langle a^3\rangle$ (при любых y_i); то есть левая часть уравнения попадёт в $\langle a^3\rangle$ и не сможет быть равна правой;
- если $x_3^{15} \notin \langle a\rangle \ni x_5^{15}$, то левая часть уравнения попадёт в $\langle a^5\rangle$ (по аналогичным причинам) и опять не сможет быть равна правой;
- если $x_3^{15} \in \langle a\rangle \ni x_5^{15}$, то левая часть уравнения вообще превратится в единицу и не сможет быть равна правой, тем более.
- если же $x_3^{15} \notin \langle a\rangle \not\ni x_5^{15}$, то $x_3^{15}x_5^{15} \in \langle a\rangle$ и левая часть уравнения превратится в единицу за счёт внешнего коммутатора.

5. Группа Гейзенберга

Лемма об аффинно-билинейных функциях. *Пусть $U \supseteq U'$ и V — конечно порождённые свободные абелевы группы, $f: U \times V \to \mathbb{Z}$ — билинейная функция, ранг ограничение которой на $U' \times V$ больше единицы. Тогда для любого $u \in U$ подмножество $f(u+U', V) \subseteq \mathbb{Z}$ является подгруппой, содержащей подгруппу $f(U', V)$.*

Доказательство. Поскольку базисы в U' и V мы можем выбрать, как хотим, и независимо друг от друга, можно считать, что матрица функции f диагональна, причём каждое число на диагонали делит следующее, так как любая целочисленная матрица приводится к такому виду (*нормальная форма Смита*) целочисленными обратимыми элементарными преобразованиями строк и столбцов, смотрите, например, [Вин99]). Таким образом, мы можем считать, что в координатах интересующая нас функция $(u', v) \mapsto f(u+u', v)$ записывается в виде $(u', v) \mapsto \sum n_i x'_i y_i + \sum m_i y_i$ (где x'_i и y_i — координаты векторов u' и v, соответственно, и $m_i, n_i \in \mathbb{Z}$, причём $n_1 | n_2 | \ldots$, а m_i линейно зависят от вектора u). При $n_i \neq 0$ арифметическая прогрессия $\{n_i x'_i + m_i \mid x'_i \in \mathbb{Z}\}$ содержит по теореме Дирихле число вида $p_i \cdot \text{НОД}(n_i, m_i)$, где p_i — сколь угодно большое простое число. Значит, простые числа p_i мы можем выбрать разными Стало быть, (в силу того, что $n_2 \neq 0$, поскольку ранг формы больше единицы) при подходящих x'_i мы имеем

$$\text{НОД}(n_1 x'_1 + m_1,\ n_2 x'_2 + m_2, \ldots) = \text{НОД}(n_1,\ m_1,\ m_2, \ldots) \quad \text{(мы воспользовались тем, что } n_1 | n_2 | \ldots\text{).}$$

Следовательно, выбрав теперь надлежащим образом y_i, мы получим

$$(n_1 x'_1 + m_1) y_1 + (n_2 x'_2 + m_2) y_2 + \ldots = \text{НОД}(n_1,\ m_1,\ m_2, \ldots).$$

Это показывает, что $f(u+U', V) = \text{НОД}(n_1,\ m_1,\ m_2, \ldots) \cdot \mathbb{Z} \supseteq n_1 \cdot \mathbb{Z} = f(U', V)$, что и требовалось.

Теорема о группе Гейзенберга. *Группа Гейзенберга $\mathbf{UT}_3(\mathbb{Z})$ не сильно вербально замкнута.*

Доказательство. *Вербальным отображением* в группе H называют отображение $H^s \to H$ вида

$$(h_1, \ldots, h_s) \mapsto w(h_1, \ldots, h_s),$$

где $w(t_1, \ldots, t_s)$ — какой-то элемент свободной группы $F_s = F(t_1, \ldots, t_s)$.

Проверим, что

в группе Гейзенберга $H = \mathbf{UT}_3(\mathbb{Z})$ пересечение образа каждого вербального отображения с центром является подгруппой; а сам этот образ является объединением некоторого количества смежных классов по этой подгруппе. (3)

Рассмотрим вербальное отображение $\varphi: (h_1, \ldots, h_s) \mapsto w(h_1, \ldots, h_s)$ и положим

$$h_i = T(x_i, y_i, z_i) \overset{\text{опр}}{=} \begin{pmatrix} 1 & x_i & z_i \\ 0 & 1 & y_i \\ 0 & 0 & 1 \end{pmatrix}.$$

Тогда $\varphi(h_1, \ldots, h_s) = T\big(l(x_1, \ldots, x_s),\ l(y_1, \ldots, y_s),\ f(x_1, \ldots, x_s; y_1, \ldots, y_s) + l(z_1, \ldots, z_s)\big)$, где $l: \mathbb{Z}^s \to \mathbb{Z}$ — линейная функция, а $f: \mathbb{Z}^s \times \mathbb{Z}^s \to \mathbb{Z}$ — билинейная функция. Автоморфизмом свободной группы каждое слово w можно привести к *нормальному виду* $w(t_1, \ldots, t_s) = t_1^m w'(t_1, \ldots, t_s)$, где слово w' содержится в коммутанте свободной группы. В нормальном виде линейная функция l приобретает простой вид: $l(x_1, \ldots, x_s) = m x_1$, а ограничение функции f на $U' \times V$ кососимметрично, то есть $f(u', u') = 0$ для всех $u' \in U'$. Действительно, если $u' = (a_1, \ldots a_s)$ (и, стало быть, $a_1 = 0$ или $m = 0$), то величина $f(u', u')$ определена равенством

$$w\big(T(a_1, a_1, 0), \ldots, T(a_s, a_s, 0)\big) = w'\big(T(a_1, a_1, 0), \ldots, T(a_s, a_s, 0)\big) = T\big(0, 0, f(u', u')\big)$$

и, следовательно, равна нулю, поскольку матрицы вида $T(a,a,0)$ коммутируют между собой, а слово w' коммутаторное.

Чтобы доказать (3), нам надо показать, что

а) $\varphi(H^s)\cap \mathrm{Z}(H)$ является подгруппой

б) и для каждого элемента $h=T(a,b,c)=\varphi(\widehat{h}_1,\dots \widehat{h}_s)\in\varphi(H^s)$ смежный класс $h\cdot\big(\varphi(H^s)\cap \mathrm{Z}(H)\big)$ целиком содержится в $\varphi(H^s)$.

Оба факта вытекают из леммы об аффинно-билинейных функциях, применённой к свободным абелевым группам $U=\mathbb{Z}^s\supseteq U'=V=\{u\in\mathbb{Z}^s \mid l(u)=0\}$. Условие $\mathrm{rk} f|_{U'\times V}\geqslant 2$ выполнено, поскольку ранг кососимметрической билинейной функции всегда чётный (при ранге ноль доказывать нечего).

Проверим а). Мы имеем $\varphi(H^s)\cap\mathrm{Z}(H)=\Big\{T\big(0,\ 0,\ f(u,v)+l(r)\big)\ \Big|\ u,v,r\in\mathbb{Z}^s,\ l(u)=l(v)=0\Big\}$. По лемме $f(U',V)$ является подгруппой в $\mathbb{Z}$. А значит и $f(U',V)+l(\mathbb{Z}^s)$ является подгруппой (поскольку $l(\mathbb{Z}^s)$ очевидно является подгруппой).

Проверим теперь б). Мы можем считать, что $b=0$, поскольку всякий элемент $h=T(a,b,c)$ приводится к такому виду некоторым автоморфизмом группы H (так как группа H свободна в многообразии нильпотентных групп ступени два, и свободным базисом служит любая пара матриц $\{T(a_1,b_1,c_1),\ T(a_2,b_2,c_2)\}$ такая, что $a_1b_2-a_2b_1=\pm1$). А тогда мы получаем факт б) следующим образом. Если $\widehat{h}_i=T(\widehat{x}_i,\widehat{y}_i,\widehat{z}_i)$, $u=(\widehat{x}_1,\dots,\widehat{x}_s)$ и $v=(\widehat{y}_1,\dots,\widehat{y}_s)$, то

$$h\cdot\big(\varphi(H^s)\cap\mathrm{Z}(H)\big)=T\big(l(u),\ 0,\ f(u,v)+f(U',V)+l(\mathbb{Z}^s)\big)\subseteq T\big(l(u),\ 0,\ f(u+U',V)+l(\mathbb{Z}^s)\big)$$

(где включение вытекает из леммы). А для матриц $\widetilde{h}_i=T(\widehat{x}_i+u'_i,v'_i,z'_i)$ мы имеем

$$\varphi(\widetilde{h}_1,\dots,\widetilde{h}_s)=T\big(l(u),\ 0,\ f(u+u',v')+l(q')\big),$$

где $u'=(u'_1,\dots,u'_s)\in U'=V$, $v'=(v'_1,\dots,v'_s)\in U'=V$ и $q'=(z'_1,\dots,z'_s)\in U$ — векторы, которые мы можем подбирать, как хотим. Таким образом,

$$\varphi(H^s)\supseteq T\big(l(u),\ 0,\ f(u+U',V)+l(\mathbb{Z}^s)\big)\supseteq h\cdot\big(\varphi(H^s)\cap\mathrm{Z}(H)\big).$$

Это завершает доказательство факта (3).

Возьмём теперь центральное произведение

$$G=H\underset{\mathrm{Z}(H)=\mathrm{Z}(\widetilde{H})}{\times}\widetilde{H}=(H\times\widetilde{H})/\{c\widetilde{c}^{-1}\mid c\in\mathrm{Z}(H)\}$$

группы H и её копии $\widetilde{H}$. Вербальная замкнутость H в G вытекает немедленно из (3): если

$$w\big((h_1,h'_1),\dots,(h_s,h'_s)\big)=(h,1)$$

в G, то $w(h_1,\dots,h_s)=hc^{-1}$ и $w(h'_1,\dots,h'_s)=c\in\mathrm{Z}(H)$ для некоторого $c\in\mathrm{Z}(H)$; и тогда согласно (3) h тоже лежит в образе соответствующего вербального отображения. Таким образом, вербальная замкнутость доказана.

Группа H нётерова по уравнениям, как и всякая линейная группа [BMR99], поэтому если бы H была сильно вербально замкнутой, то она была бы ретрактом группы G (смотрите введение). А ретракции $G\to H$ быть не может, поскольку $\widetilde{H}$ коммутирует с H, следовательно, может отобразится только в центр при гипотетической ретракции, но тогда $\mathrm{Z}(\widetilde{H})=\mathrm{Z}(H)$ отобразился бы в единицу. Это противоречие завершает доказательство.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

[Вин99] Э. Б. Винберг, Курс алгебры, Факториал, М., 1999.

[КаМ82] М. И. Каргаполов, Ю. И. Мерзляков, Основы теории групп, Наука, М., 1982.

[КМ18] А. А. Клячко, А. М. Мажуга, Вербально замкнутые почти свободные подгруппы, Мат. сборник, 209:6 (2018), 75-82. См. также arXiv:1702.07761 .

[Лен68] С. Ленг, Алгебра, Мир, М., 1968.

[ЛШ80] Р. Линдон, П. Шупп, Комбинаторная теория групп, Мир, М., 1980.

[Ней69] Х. Нейман, Многообразия групп, Мир, М., 1969.

[Маж19] А. М. Мажуга, Свободные произведения групп сильно вербально замкнуты, Мат. сборник, 210:10 (2019), 122-160. См. также arXiv:1803.10634 .

[РТ19] В. А. Романьков, Е. И. Тимошенко, О вербально замкнутых подгруппах свободных разрешимых групп, Вестник Омского университета, 24:1 (2019), 9-16.

[РТ20] В. А. Романьков, Е. И. Тимошенко, О вербально замкнутых подгруппах свободных разрешимых групп, Алгебра и логика, 59:3 (2020), 367-384. См. также arXiv:1906.11689 .

[РХ13] В. А. Романьков, Н. Г. Хисамиев, Вербально и экзистенциально замкнутые подгруппы свободных нильпотентных групп, Алгебра и логика, 52:4 (2013), 502-525.

[РХК17] В. А. Романьков, Н. Г. Хисамиев, А. А. Конырханова, Алгебраически и вербально замкнутые подгруппы и ретракты конечно порожденных нильпотентных групп, Сиб. матем. журн., 58:3 (2017), 686-699.

[Тим21] Е. И. Тимошенко, Ретракты и вербально замкнутые подгруппы относительно свободных разрешимых групп, Сиб. матем. журн., 62:3 (2021), 659-667.

[BMR99] G. Baumslag, A. Myasnikov, V. Remeslennikov, Algebraic geometry over groups I. Algebraic sets and ideal theory, J. Algebra, 219:1 (1999), 16-79.

[Bog18] O. Bogopolski, Equations in acylindrically hyperbolic groups and verbal closedness, Groups, Geometry, and Dynamics (в печати). См. также arXiv:1805.08071 .

[Bog19] O. Bogopolski, On finite systems of equations in acylindrically hyperbolic groups, arXiv:1903.10906.

[Che35] C. Chevalley, Démonstration d'une hypothèse de M. Artin, Abh. Math. Semin. Univ. Hambg., 11 (1935), 73-75.

[K21] A. A. Klyachko, The Klein bottle group is not strongly verbally closed, though awfully close to being so, Canadian Mathematical Bulletin, 64:2 (2021), 491-497. См. также arXiv:2006.15523 .

[KMM18] A. A. Klyachko, A. M. Mazhuga, V. Yu. Miroshnichenko, Virtually free finite-normal-subgroup-free groups are strongly verbally closed, J. Algebra, 510 (2018), 319-330. См. также arXiv:1712.03406 .

[KoN66] L. G. Kovács, M. F. Newman, On critical groups, J. Austral. Math. Soc., 6:2 (1966), 237-250.

[Mazh17] A. M. Mazhuga, On free decompositions of verbally closed subgroups of free products of finite groups, J. Group Theory, 20:5 (2017), 971-986. См. также arXiv:1605.01766 .

[Mazh18] A. M. Mazhuga, Strongly verbally closed groups, J. Algebra, 493 (2018), 171-184. См. также arXiv:1707.02464 .

[MR14] A. Myasnikov, V. Roman'kov, Verbally closed subgroups of free groups, J. Group Theory, 17:1 (2014), 29-40. См. также arXiv:1201.0497 .

[Pas83] D. S. Passman, It's essentially Maschke's theorem, The Rocky Mountain Journal of Mathematics, 13:1 (1983), 37-54.

[Rom12] V. A. Roman'kov, Equations over groups, Groups - Complexity - Cryptology, 4:2 (2012), 191-239.

[Sco51] W. R. Scott, Algebraically closed groups, Proc. Amer. Math. Soc., 2:1 (1951), 118-121.