МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ имени М. В. ЛОМОНОСОВА

МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ

Кафедра высшей алгебры

на правах рукописи
УДК 512.54

Клячко Антон Александрович

УРАВНЕНИЯ В ГРУППАХ И СМЕЖНЫЕ ВОПРОСЫ

1.1.5 — математическая логика, алгебра, теория чисел и дискретная математика
(01.01.06 — математическая логика, алгебра и теория чисел)

ДИССЕРТАЦИЯ
на соискание ученой степени
доктора физико-математических наук

МОСКВА 2022

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Краткое содержание работы

Диссертация посвящена следующим вопросам теории групп и смежных областей.

Пересечение подгрупп в группах, близким к свободным (главы 1 и 2)

Нам удалось, в частности, получить (короткое) доказательство следующего обобщения теоремы Минеева–Фридмана (ранее известной как гипотеза Ханны Нейман):

> *если A и B — нетривиальные свободные подгруппы почти свободной группы, содержащей свободную подгруппу индекса n, то*
>
> $$\operatorname{rank}(A \cap B) - 1 \leqslant n \cdot (\operatorname{rank}(A) - 1) \cdot (\operatorname{rank}(B) - 1)$$

(и эта оценка неулучшаема). Мы получаем также аналог этого утверждения для почти свободных произведений.

Факт, сформулированный выше, доказывается в главе 1; а в главе 2 читатели могут найти формулировку и доказательство «почти свободного аналога» утверждения, которое принято называть усиленной гипотезой Ханны Нейман.

Делимость в группах (главы 3–7)

Общий факт, который нам удалось получить, включает в себя естественным образом теорему Фробениуса (1895) о числе решений уравнения $x^n = 1$ в группе, теорему Соломона (1969) о числе решений в группе системы уравнений, в которой уравнений меньше, чем неизвестных, и теорему Ивасаки (1985) о корнях из подгрупп. Из этого общего факта вытекают и новые любопытные следствия о группах и кольцах. Если говорить чуть более подробно, то результаты этой части распределены по главам так:

- в главе 3 доказывается аналог теоремы Соломона для произвольных формул первого порядка в групповом языке (в том смысле, что системы уравнений в группах представляют собой простейшие такие формулы);
- в главе 4 доказывается общее утверждение о числе решений систем уравнений в группах, включающая в себя теоремы Соломона и Ивасаки;
- в главе 5 основной результат главы 4 (включающий в себя теоремы Соломона и Ивасаки) обобщается путём добавления «фробениусовости» и, таким образом, получается факт, включающий в себя все три классические теоремы о делимости в группах;
- в главе 7 этот результат ещё более обобщается;
- глава 6 стоит несколько особняком: в ней мы доказываем аналоги результатов глав 3–5 для алгебраических групп (то есть вместо количества решений уравнений, мы рассматриваем размерность множества решений).

Вербальная замкнутость (главы 8–10)

Наши исследования в этом направлении были вдохновлены следующей теоремой Мясникова и Романькова (2014):

> *подгруппа H конечно порождённой свободной группы G является ретрактом тогда и только тогда, когда каждое уравнение вида $w(x_1, \ldots, x_n) = h$ (где w — это произвольное слово в алфавите $\{x_1^{\pm 1}, \ldots, x_n^{\pm 1}\}$ и $h \in H$), имеющее решение в G, имеет решение и в H.*

Мы показываем, что то же самое верно для л ю б о й конечно порождённой группы G, если подгруппа H

- свободна (глава 8);
- или почти свободна и не имеет нетривиальных конечных нормальных (в H) подгрупп (глава 8, кроме одного исключительного случая, который рассмотрен в главе 9);
- или является свободным произведением нескольких (больше, чем одной) нетривиальных групп с тождествами (глава 9);

А в главе 10 показано, что фундаментальная группа бутылки Клейна этим свойством не обладает, в отличие от всех остальных групп поверхностей.*)

*) Факт про «все остальные группы поверхностей» — это результат Андрея Мажуги, ученика автора данной диссертации.

Цена симметрии (главы 11–14)

Хорошо известно и просто доказывается, что

> *если группа G содержит абелеву подгруппу конечного индекса, то G содержит характеристическую (то есть инвариантную относительно всех автоморфизмов) абелеву подгруппу конечного индекса.*

Этот простой факт много раз обобщался в разных направлениях (смотрите введение к главе 14). Утверждения такого сорта называют иногда *теоремами типа Макаренко–Хухро* в честь одного из таких нетривиальных обобщений. Наш вклад здесь состоит в следующем:

- в главе 11 приводится короткое (на порядок короче оригинального) доказательство собственно теоремы Макаренко–Хухро;
- в главе 12 эта теорема существенно обобщается;
- в главе 13 она ещё больше обобщается (так, что все, или почти все, известные результаты такого типа становятся частными случаями нашей обобщённой теоремы);
- а в главе 14 рассматривается применение общей теоремы из главы 13 к комбинаторным задачам; во многих случаях удаётся получить неулучшаемую оценку; простейшим частным случаем теоремы из главы 14 является, например, (неулучшаемый) ответ на следующий естественный вопрос.

> *Пусть известно, что в графе можно уничтожить все стоугольники, удалив 2021 ребро. Сколько рёбер заведомо достаточно удалить, если мы хотим уничтожить все стоугольники так, чтобы множество удаляемых рёбер было инвариантно относительно всех автоморфизмов исходного графа?*

Произведения коммутаторов в свободных произведениях (глава 15)

В свободной группе, как известно, никакой неединичный коммутатор не является истинной степенью. Мы доказываем одну общую теорему, из которой вытекает несколько любопытных фактов, например, следующее усиление упомянутого выше утверждения:

> *если в свободной группе неединичный коммутатор разложить в произведение нескольких сопряжённых между собой элементов, то все эти элементы обязательно окажутся попарно разными.*

Сбалансированные разложения на множители (главы 16 и 17)

Следующее простое, но не тривиальное, утверждение предлагалось в качестве задачи на олимпиаде для школьников:

> *всякое рациональное число можно разложить в произведение нескольких рациональных чисел, сумма которых равна нулю.*

А если здесь слово *нескольких* заменить на *четырёх*, то получится уже не школьная задача, которую, как выяснилось, решил ещё Эйлер. Мы занимались этим вопросом, не зная (к своему стыду) о результате Эйлера, но наше решение оказалось г о р а з д о проще и эйлерова, и вообще всех известных, смотрите главу 17. Мы решаем также аналогичные задачи в конечных полях и в некоторых других кольцах. Интересно, что в конечных полях приходится использовать нетривиальные факты об эллиптических кривых (смотрите главу 16).

Алгоритмически конечные группы (глава 18)

Мы строим конечно порождённую бесконечную рекурсивно представленную финитно аппроксимируемую алгоритмически конечную группу G, отвечая тем самым на вопрос Мясникова и Осина. При этом группа G «сильно бесконечна» и «сильно алгоритмически конечна», в том смысле, что G содержит бесконечную абелеву нормальную подгруппу, а все конечные декартовы степени группы G алгоритмически конечны (то есть ни для какого n не существует алгоритма, выписывающего бесконечное число попарно различных элементов группы G^n).

Тождества аддитивной двоичной арифметики (глава 19)

Мы показываем, что операции произвольной арности, выражающиеся через сложение по модулю 2^n и побитовое сложение по модулю 2, допускают простое описание. Тождества, связывающие эти два сложения, имеют конечный базис. Более того, универсальная алгебра $\mathbb{Z}/2^n\mathbb{Z}$ с этими двумя операциями рационально эквивалентна нильпотентному кольцу и, следовательно, порождает шпехтово многообразие. (Слово «бит» означает двоичный разряд, то есть *побитовое сложение* — это сложение в столбик в двоичной записи без переноса разрядов; сложение по модулю 2^n и побитовое сложение — это базовые операции, которые компьютерные процессоры способны выполнять быстро, смотрите введение к соответствующей главе.)

Экономное присоединение квадратных корней к группам (глава 20)

Насколько нужно увеличить группу, чтобы в получившейся группе все элементы исходной группы являлись квадратами? Мы даём довольно точный ответ на этот вопрос (наилучшая возможная оценка сверху отличается от полученной оценки не более, чем в два раза).

Относительные копредставления (главы 21–26)

Один старый, не вошедший в диссертацию, результат автора говорит, что

> *из нетривиальной группы без кручения нельзя сделать тривиальную путём добавления одного образующего и одного соотношения,*

то есть, если группа без кручения $G = \langle X \mid R \rangle$ нетривиальна, то и группа $\widehat{G} = \langle X \sqcup \{t\} \mid R \cup \{w\} \rangle$ тоже нетривиальна (для любого слова w в алфавите $X^{\pm 1} \sqcup \{t^{\pm 1}\}$).*) В этой работе мы доказываем аналогичные (в разных смыслах) факты:

- в главе 21 доказывается «многомерный аналог» этой теоремы;
- в главе 22 доказывается, что из непростой группы G нельзя получить неабелеву простую группу $\widehat{G}$;
- в главе 23 доказывается, что $\widehat{G}$ почти всегда содержит неабелеву свободную подгруппу;
- в главе 24 показано, что если добавить два образующих и одно соотношение, то всегда получится SQ-универсальная группа;
- в главе 25 показано, например, что если добавить два образующих и одно соотношение, то центр полученной группы $\widehat{G}$ будет тривиален (при некоторых естественных предположениях);
- в главе 26 показано, например, что если к к любой группе (возможно даже с кручением) добавить один образующий и одно соотношение, являющееся по крайней мере третьей степенью (в свободной группе), то полученная группа будет относительно гиперболична и SQ-универсальна.

Автоморфизмы групп и алгебр Шевалле (глава 27)

Мы показываем, что присоединённая группа Шевалле ранга большего единицы над $\mathbb{Q}$-алгеброй (или похожим кольцом), её элементарная подгруппа и соответствующее кольцо Ли имеют одинаковые группы автоморфизмов. Эти автоморфизмы явно описываются.

Число нерешений уравнений в группах и нетопологизируемые группы (глава 28)

Показано, что для любой пары кардиналов с бесконечной суммой найдётся такая группа и такое уравнение над этой группой, что первый кардинал является числом решений этого уравнения, а второй — числом нерешений этого уравнения. В частности,

> *существует такая бесконечная группа G, что все её элементы, кроме ровно одного, являются решениями некоторого уравнения $g_1 x^{n_1} \dots g_k x^{n_k} = 1$ (где $g_i \in G$ и $n_i \in \mathbb{Z}$).*

Из существования таких удивительных уравнений легко выводится, что существует бесконечная счётная нетопологизируемая группа без кручения.

---

*) А верно ли это без предположения об отсутствии кручения, никто не знает; это знаменитая гипотеза Кервера–Лауденбаха.

Актуальность темы и степень её разработанности

Вопросами о пересечениях подгрупп в свободных и близких к ним группах занимались такие известные люди, как, например, Дикс [D12], Антолин, Мартино и Шваброу [AMS14], Захаров [Za14], Араухо, Сильва и Сикотис [ASS15], Носков [Нос16], Хелфер и Вайс [HW16], Иванов [Iv17], Хайкин [JZ17] и, конечно же Ханна Нейман, которая в 1957 году показала, что

для любых нетривиальных подгрупп A и B свободной группы

$$\operatorname{rank}(A \cap B) - 1 \leqslant 2 \cdot (\operatorname{rank}(A) - 1) \cdot (\operatorname{rank}(B) - 1),$$

и задала вопрос, нельзя ли убрать двойку в этой оценке. Гипотеза оказалась верной, но доказать это удалось лишь в 2012 году Минееву [Mi12a] и Фридману [Fr14]. Альтернативные доказательства и обобщения этого результата можно найти, например, в работах, процитированных выше (а также в первых двух главах этой диссертации).

Делимостью числа решений уравнений в группах математики интересуются со времён Фробениуса, который в 1895 году показал, что

число решений уравнения $x^n = 1$ в конечной группе G делится на $\operatorname{НОД}(|G|, n)$ *для любого натурального n.*

Похожие (и не очень похожие) результаты о числе решений уравнений в группах можно найти в очень многих работах известных (и не очень известных) математиков, например, смотрите [Hall36b], [Kula38], [Sehg62], [BrTh88], [Yosh93], [AsTa01], [ACNT13] [Isaa70], [Стру95], [AmV11], [GRV12], [Iwa82] (а также соответствующие главы этой диссертации).

Вопросы о вербальной замкнутости в группах имеют не такую древнюю историю; пионерской работой здесь стала статья [MR14] 2014 года, в которой доказана теорема Мясникова–Романькова (смотрите начало этого введения). Работ по этой теме не так много пока, но смотрите, например, [Маж19], [PT19], [PX13], [Bog18], [Bog19], [Mazh17], [Mazh18] (а также работы автора этой диссертации, которые изложены в соответствующих главах, и работу [KMO21], результаты которой не вошли в диссертацию).

Теоремы о симметричности, то есть теоремы типа Макаренко–Хухро, стали известны, на самом деле, задолго до работы Макаренко и Хухро [KhM07a]; например, простой (но не тривиальный) факт об абелевых характеристических подгруппах, приведённый в первом параграфе этого введения, можно найти в классических учебниках по теории групп (в [KaM82], например). В общем виде эти теоремы выглядят так:

если где-то есть что-то большое и хорошее, то там можно найти также что-то большое, хорошее и симметричное.

Конкретных примеров таких утверждений в алгебре очень много; смотрите, например, [Вд00], [BrNa04], [ChD89], [dGT18a], [Fr18], [KhM07b], [MSh12], [PSz02] (а также соответствующие главы этой диссертации).

Изучение коммутаторов в свободных группах можно назвать классикой комбинаторной теории групп. Началась эта наука с наблюдения Шюценберже [Sch59], который ещё в 1959 году заметил, что

в свободной группе неединичные коммутаторы не являются истинными степенями,

и это не такой тривиальный факт, как может показаться на первый взгляд. Дело в том, что между коммутаторами и степенями есть неочевидные связи: например, Каллер [Cull81] обнаружил такое тождество, выполненное вообще для любых элементов любой группы: $[a,b]^3 = [a^{-1}ba, a^{-2}bab^{-1}][bab^{-1}, b^2]$, то есть куб любого коммутатора в любой группе можно разложить не только в произведение трёх коммутаторов (что очевидно), но и в произведение двух коммутаторов (что вряд ли кто-то осмелится назвать очевидным). В более общем виде *оценка Каллера* состоит в том, что $[a,b]^n$ *раскладывается в произведение k коммутаторов, если* $n \leqslant 2k-1$. То, что оценка Каллера точная в свободной группе, называют *гипотезой Комерфорда–Комерфорда–Эдмундса* [CCE91]:

в свободной группе равенство $[x_1, y_1] \dots [x_k, y_k] = z^n$, *где* $n \geqslant 2k$, *влечёт, что* $z = 1$.

Данкану и Хауи [DuH91] удалось доказать, что это действительно так. Позже выяснилось, что аналогичный факт верен и в любых свободных произведениях групп без кручения; этот результат был получен в совместной работе автора и Иванова [IK18], а также (одновременно, независимо и другими методами) в работе Чена [Ch18]. В свободных произведениях групп с кручением ситуация сложнее: что-то на эту тему доказано в [IK18] и [Ch18], а почти окончательный результат получен в совместной работе автора этого труда и Вадима Юрьевича Березнюка [BeK21] (не вошедшей в диссертацию). Обобщения наблюдения Шюценберже в других направлениях можно найти, например, в [CCE91] и в совместной работе автора и Елизаветы Владимировны Френкель [FK12] (тоже не вошедшей в диссертацию).

Уравновешенными разложениями на множители (при всей кажущейся несерьёзности этой задачи) занимались и Эйлер (смотрите первый параграф этого введения), и вполне современные математики [ZS18]. Явные формулы для таких разложений напоминают *теорему Райли* [Ra25] (опубликованную в 1825 году в журнале с интересным названием):

всякое рациональное число раскладывается в сумму трёх кубов рациональных чисел.

Доказательство этой теоремы удивительным образом состоит из одной строчки: $x = \left(\frac{\cdots}{\cdots}\right)^3 + \left(\frac{\cdots}{\cdots}\right)^3 + \left(\frac{\cdots}{\cdots}\right)^3$, где точки обозначают некоторые конкретные многочлены от x (которые мы поленились выписать) с целыми коэффициентами, остаётся только проверить, что это равенство действительно является тождеством...*)

В работе Мясникова и Осина [MO11] был построен первый пример конечно порождённой рекурсивно представленной бесконечной группы, которая является *алгоритмически конечной*, в том смысле, что не существует алгоритма, выписывающего бесконечное количество попарно различных элементов этой группы. Группы, обладающие этими свойствами (то есть конечно порождённые рекурсивно представленные бесконечные и алгоритмически конечные), авторы [MO11] предложили называть *монстрами Дэна* и поставили вопрос: *существуют ли финитно аппроксимируемые монстры Дэна?* Нам удалось получить положительный ответ. Впоследствии выяснилось, что задача была решена раньше [KhM14], однако наш пример обладает дополнительными удивительными свойствами (смотрите соответствующую главу).

Про проблему конечного базиса тождеств в различных алгебрах есть огромное число работ, смотрите, например, [БаОл88], [Нейм69], [Бело99], [ВаЗе89], [Гриш99], [Зайц78], [Кеме87], [Крас90], [Латы73], [Льво73], [О70], [О89], [Щиго99], [GuKr03], [Kras09], [Speht52]. Мы рассматриваем в каком-то смысле «прикладную» (универсальную) алгебру с двумя «компьютерными» операциями: сложение и побитовое сложение. Оказалось, что тождества такой «компьютерной» алгебры тоже конечно базируемы.

Исследованию разрешимости уравнений над группами посвящено множество работ (смотрите, например, [GR62], [Le62], [Ly80], [Б84], [EH91], [How91], [K93], [КП95], [FeR96], [K97], [CG00], [EdJu00], [Juhá03], [K06] и литературу там цитируемую).**) В этих статьях доказывается, что при тех или иных условиях уравнение $w(x) = 1$ с коэффициентами из группы G *разрешимо над* G, то есть найдётся группа H, содержащая G в качестве подгруппы, и элемент $h \in H$ такой, что $w(h) = 1$. Мы пытаемся исследовать количественный вопрос: *насколько большой должна быть такая группа* H*?* Даже для простых уравнений, разрешимость которых давно известна, этот вопрос оказывается весьма трудным, и мы ограничиваемся изучением самого простейшего нетривиального уравнения $x^2 = g$.

Вопросы об относительных копредставлениях тесно связаны с вопросом об уравнениях над группой: если есть уравнение $w(x) = 1$ с коэффициентами из какой-то группы G, то естественным образом возникает относительное копредставление $\widehat{G} = \langle G \sqcup \{x\} \mid w(x) = 1\rangle$, при этом естественное отображение $G \to \widehat{G}$ инъективно тогда и только тогда, когда уравнение разрешимо над G. Таким образом, все работы, упомянутые в предыдущем абзаце (и множество других работ), можно назвать работами об относительных копредставлениях. Смотрите также совместную работу автора и Андреаса Тома [KT17] (результаты которой не вошли в диссертацию).

Про группы Шевалле над кольцами есть очень много работ, например, [Wat80], [Пет82], [ГМи83], [HO'M89], [Абе93], [Che00], [Бун07]. Идея описания автоморфизмов линейных групп путём перехода к соответствующим алгебрам Ли была впервые предложена и применена Левчуком [Лев83] и Зельмановым [Зел85]. Мы используем ту же самую общую идею, но в остальном наш подход сильно отличается.

Как было упомянуто в конце предыдущего раздела этого введения, группа, в которой все элементы, кроме ровно одного, являются решениями некоторого уравнения $w(x) = 1$, заведомо *нетопологизируема*, то есть не допускает недискретных отделимых групповых топологий. Впервые пример бесконечной нетопологизируемой группы был построен Шелахом. Ольшанский [O80] (смотрите также [O89]) построил счётный пример. Вопрос о существовании счётной нетопологизируемой группы без кручения оставался открытым [НЗТА85, вопрос 1.4], пока мы его не решили (в совместной работе с учеником, Антоном Трофимовым). Другие интересные примеры нетопологизируемых групп были получены в совместной работе автора, Александра Юрьевича Ольшанского и Дениса Валентиновича Осина [KOO13] (но эти результаты не вошли в диссертацию).

---

*) Спасибо Виктору Сергеевичу Губе, который обратил внимание автора на теорему Райли.

**) В этой диссертации совсем не рассматриваются вопросы о поведении множества решений уравнений в конкретных интересных группах (в свободных группах, например). Смотрите по этому поводу, скажем, [KhV12] и литературу там цитируемую.

Цели и задачи диссертации

- обобщить теорему Минеева–Фридмана на почти свободные группы;
- получить общий факт, включающий в себя естественным образом теорему Фробениуса (1895) о числе решений уравнения $x^n = 1$ в группе, теорему Соломона (1969) о числе решений в группе системы уравнений, в которой уравнений меньше, чем неизвестных, и теорему Ивасаки (1985) о корнях из подгрупп;
- доказать или опровергнуть вербальную замкнутость свободных и других интересных групп;
- получить обобщение теоремы Макаренко–Хухро, включающее в себя все известные результаты на эту тему;
- доказать неулучшаемость оценки Каллера для свободных произведений групп без кручения;
- решить полностью задачу об уравновешенных разложениях на множители в конечных полях;
- построить финитно аппроксимируемый монстр Дэна;
- доказать шпехтовость аддитивной бинарной арифметики;
- получить теорему об экономном присоединении квадратных корней к группам;
- доказать, что из непростой группы без кручения нельзя получить неабелеву простую группу путём добавления одного образующего и одного соотношения;
- описать автоморфизмы присоединённой группы Шевалле ранга большего единицы над $\mathbb{Q}$-алгеброй;
- построить бесконечную счётную нетопологизируемую группу без кручения.

Объект и предмет исследования

В диссертации изучаются в основном группы (и конечные, и бесконечные), а также (в некоторой степени) кольца, конечные поля, некоторые универсальные алгебры и графы.

Теоретическая и практическая значимость работы

Диссертация носит теоретический характер. Результаты, полученные в работе, расширяют знания о группах, графах и других алгебраических и комбинаторных структурах. Результаты диссертации могут найти применение в теории групп, колец, тождеств, а также оказаться полезными при работе с графами. Результаты диссертации могут быть использованы для чтения спецкурсов по теории групп и графов.

Методы исследования

Используются как традиционные методы комбинаторной и структурной теории групп, так и разработанные автором, например, движения на картах.

Положения, выносимые на защиту

1. Аналог теоремы Минеева–Фридмана для почти свободных групп.
2. Единое обобщение теоремы Фробениуса о числе решений уравнения $x^n = 1$ в группе, Соломона о числе решений в группе системы уравнений и Ивасаки о корнях из подгрупп.
3. Доказательство вербальной замкнутости (почти) свободных и других интересных групп.
4. Обобщение теоремы Макаренко–Хухро.
5. Неулучшаемость оценки Каллера для свободных произведений групп без кручения.
6. Полное решение задачи об уравновешенных разложениях на множители в конечных полях.
7. Построение финитно аппроксимируемого монстра Дэна с другими интересными свойствами.
8. Доказательство шпехтовости аддитивной бинарной арифметики.
9. Теорема об экономном присоединении квадратных корней к группам.
10. Доказательство того, что из непростой группы без кручения нельзя получить неабелеву простую группу путём добавления одного образующего и одного соотношения.
11. Описание автоморфизмов присоединённой группы Шевалле ранга большего единицы над $\mathbb{Q}$-алгеброй.
12. Пример бесконечной счётной нетопологизируемой группы без кручения.

Степень достоверности и апробация результатов

Результаты диссертации обоснованы при помощи строгих математических доказательств, докладывались на конференциях и семинарах. Полные тексты всех работ, на основе которых написана диссертация, выложены в открытый доступ на известном сайте `arXiv.org` (и опубликованы в хороших журналах, 26 статей).

Структура и объём диссертации

Диссертация состоит из 28 глав. Каждая глава снабжена введением, и читать каждую главу можно независимо. Объём диссертации — 237 страниц.

Научная новизна

Все результаты являются новыми. В двух случаях аналогичные результаты были получены независимо другими авторами; об этом мы явно пишем (и выше, и во введениях к соответствующим главам). Часть результатов этой диссертации была получена в неразделимом соавторстве со следующими товарищами:

Дмитрий Владимирович Баранов:	глава 20,
Елена Константиновна Брусянская:	главы 5, 7,
Андрей Викторович Васильев (Новосибирск):	глава 5,
Антон Николаевич Васильев (Астана):	глава 16,
Александр Олегович Захаров:	глава 2,
Сергей Владимирович Иванов (Урбана-Шампань):	глава 15,
Наталья Михайловна Лунева:	глава 14,
Денис Евгеньевич Лурье:	глава 26,
Андрей Михайлович Мажуга:	главы 8, 9, 17,
Наталья Юрьевна Макаренко (Новосибирск):	глава 12,
Юлия Борисовна Мельникова:	главы 11, 12,
Екатерина Викторовна Меньшова:	глава 19,
Мария Владимировна Милентьева (Москва):	глава 13,
Вероника Юрьевна Мирошниченко:	глава 9,
Анна Ашотовна Мкртчян:	главы 3, 4,
Айрана Каадыр-ооловна Монгуш:	глава 18,
Анастасия Николаевна Понфиленко:	главы 1, 17,
Мария Андреевна Рябцева:	глава 6,
Антон Владимирович Трофимов:	глава 28,
Евгений Иванович Хухро (Новосибирск):	глава 12,

то есть результаты, изложенные в главах 10, 21–25 и 27, были получены автором самостоятельно (в работах [K21], [K06a], [K05], [K07], [K06б], [K09] и [K10]), а

результаты главы 1 получены в неразделимом соавторстве с Понфиленко	в [KP20],
результаты главы 2 получены в неразделимом соавторстве с Захаровым	в [KZ21],
результаты главы 3 получены в неразделимом соавторстве с Мкртчян	в [KM14],
результаты главы 4 получены в неразделимом соавторстве с Мкртчян	в [KM17],
результаты главы 5 получены в неразделимом соавторстве с Брусянской и **А.В.Васильевым**	в [BKV19],
результаты главы 6 получены в неразделимом соавторстве с Рябцевой	в [KR20],
результаты главы 7 получены в неразделимом соавторстве с Брусянской	в [БК21],
результаты главы 8 получены в неразделимом соавторстве с Мажугой	в [KM18],
результаты главы 9 получены в неразделимом соавторстве с Мажугой и Мирошниченко	в [KMM18],
результаты главы 11 получены в неразделимом соавторстве с Мельниковой	в [KM09],
результаты главы 12 получены в неразделимом соавторстве с **Макаренко**, Мельниковой и **Хухро**	в [KhKMM09],
результаты главы 13 получены в неразделимом соавторстве с **Милентьевой**	в [KMi15],
результаты главы 14 получены в неразделимом соавторстве с Луневой	в [KL21],
результаты главы 15 получены в неразделимом соавторстве с **Ивановым**	в [IK18],
результаты главы 16 получены в неразделимом соавторстве с **А.Н.Васильевым**	в [KV16],
результаты главы 17 получены в неразделимом соавторстве с Мажугой и Понфиленко	в [KMП17],
результаты главы 18 получены в неразделимом соавторстве с Монгуш	в [KMo15],
результаты главы 19 получены в неразделимом соавторстве с Меньшовой	в [KM12],
результаты главы 20 получены в неразделимом соавторстве с Барановым	в [БК12],
результаты главы 26 получены в неразделимом соавторстве с Лурье	в [KL12],
результаты главы 28 получены в неразделимом соавторстве с Трофимовым	в [KT05],

Все соавторы, кроме **выделенных**, являются учениками автора этой диссертации.

Автор благодарит

- всех своих учеников и соавторов за плодотворное и интересное сотрудничество,
- коллектив кафедры алгебры и участников семинара «Теория групп» МГУ за дружескую и творческую атмосферу,
- Ольгу Викторовну Сипачёву за всемерную поддержку.

Особых слов благодарности заслужил Александр Юрьевич Ольшанский: чем старше я становлюсь, тем лучше я понимаю, как много он делает для своих учеников и для науки в целом.

ГЛАВА 1.
ПЕРЕСЕЧЕНИЕ ПОДГРУПП В ПОЧТИ СВОБОДНЫХ ГРУППАХ И ПОЧТИ СВОБОДНЫХ ПРОИЗВЕДЕНИЯХ

1. Введение

Гипотеза Ханны Нейман (1957), доказанная Минеевым ([Mi12a], [Mi12b]) и Фридманом [Fr14], утверждает что

для любых нетривиальных подгрупп A и B свободной группы выполнено неравенство
$$\operatorname{rank}(A\cap B)-1\leqslant(\operatorname{rank}(A)-1)\cdot(\operatorname{rank}(B)-1).$$

Мы получаем следующее обобщение этого утверждения.

Теорема 1. *Для любых нетривиальных свободных подгрупп A, B и F любой группы G выполняется неравенство*
$$\operatorname{rank}(A\cap B)-1\leqslant|G{:}F|\cdot(\operatorname{rank}(A)-1)\cdot(\operatorname{rank}(B)-1). \tag{1}$$

Это неравенство можно понимать в смысле кардинальной арифметики, но очевидно, что нетривиальный случай возникает только тогда, когда все три величины в правой части: ранг подгруппы A, ранг подгруппы B и индекс подгруппы F — конечны.

Ранее были известны следующие неравенства:

$$\operatorname{rank}(A\cap B)-1\leqslant 6|G{:}F|(\operatorname{rank}(A)-1)(\operatorname{rank}(B)-1) \qquad \text{[Za14]};$$
$$\operatorname{rank}(A\cap B)-1\leqslant |G{:}F|^2(\operatorname{rank}(A)-1)(\operatorname{rank}(B)-1)+|G{:}F|-1 \qquad \text{[ASS15]}.$$

Оценка из [ASS15], разумеется, асимптотически хуже оценки из [Za14], но бывает лучше при маленьких значениях индекса. Теорема 1 улучшает оба эти неравенства, и дальнейшие улучшения уже невозможны:

для любых $k,l,n\in\mathbb{N}$ найдётся группа G, содержащая свободные подгруппы A, B и F такие, что $\operatorname{rank}(A)=k$, $\operatorname{rank}(B)=l$, $|G{:}F|=n$, *и неравенство* (1) *является равенством.*

Действительно, рассмотрим эпиморфизм $\varphi\colon x\mapsto\big(\alpha(x),\beta(x)\big)$ из свободной группы F ранга два на свободную абелеву группу $\mathbb{Z}\oplus\mathbb{Z}$ и положим

$$A=\alpha^{-1}\big((k-1)\mathbb{Z}\big),\quad B_0=\beta^{-1}\big((l-1)\mathbb{Z}\big),\quad G=F\times(\mathbb{Z}/n\mathbb{Z})\supset B=\Big\{\Big(b,\ \beta(b)/(l-1)\Big)\ \Big|\ b\in B_0\Big\}.$$

Таким образом,
$$B\cap F=\beta^{-1}\big(n(l-1)\mathbb{Z}\big)\quad\text{и}\quad B\cap A=\varphi^{-1}\big((k-1)\mathbb{Z}\times n(l-1)\mathbb{Z}\big).$$
Ясно, что $|G{:}F|=n$. Кроме того $|F{:}A|=k-1$, $|F{:}B_0|=l-1$ и $|F{:}B\cap A|=n(l-1)(k-1)$. Ранги этих подгрупп равны k, l и $n(l-1)(k-1)+1$, соответственно, по формуле Шрайера: $\operatorname{rank}(H)-1=|F{:}H|(\operatorname{rank}(F)-1)$ (справедливой для любой подгруппы H, имеющий конечный индекс в свободной группе F). Осталось заметить, что $\operatorname{rank}(B)=\operatorname{rank}(B_0)$, поскольку проекция $\Big(b,\ \beta(b)/(l-1)\Big)\mapsto b$ является изоморфизмом из B в B_0.

(Заметим в скобках, что из теоремы 1.8, сформулированной в [Mi12b] без доказательства, вытекала бы оценка (1) без множителя $|G{:}F|$; очевидно там какие-то опечатки...)

Следующую теорему можно рассматривать как обобщение теоремы 1. Напомним, что группа называется *левоупорядочиваемой*, если на ней существует линейный порядок, такой, что $x\leqslant y\Longrightarrow zx\leqslant zy$ для любых элементов x,y,z.

Теорема 2. *Пусть группа G обладает подгруппой F конечного индекса, раскладывающейся в свободное произведение левоупорядочиваемых групп: $F=\mathop{\ast}\limits_{i\in I}G_i$. Тогда для любых нетривиальных свободных подгрупп A и B в G, тривиально пересекающих все подгруппы, сопряжённые к G_i, выполняется неравенство*
$$\operatorname{rank}(A\cap B)-1\leqslant|G{:}F|(\operatorname{rank}(A)-1)(\operatorname{rank}(B)-1).$$

При $F=G$ это утверждение было доказано в [AMS14] (смотрите также [Iv17]).

2. Инструменты

Под *графом* мы всегда понимаем ориентированный граф, петли и кратные рёбра допускаются. *Путь* в графе и *связность* графа определяются естественным образом (при этом ориентация игнорируется). *Приведённым рангом* $\overline{\mathbf{r}}(D)$ конечного графа D мы называем следующую величину: $\overline{\mathbf{r}}(D) \stackrel{\text{опр}}{=} \sum\limits_K \max(0, -\chi(K))$, где сумма распространяется на все компоненты связности K графа D, а $\chi(K)$ — *эйлерова характеристика* графа K, то есть разность числа вершин и числа рёбер.

Назовём (некоторое) множество E рёбер графа D *максимальным существенным*, если $\overline{\mathbf{r}}(D \setminus E) = \overline{\mathbf{r}}(D) - |E| = 0$. Другими словами, множество E рёбер графа D максимально существенно, если $D \setminus E$ является максимальным по включению подграфом в D, каждая компонента которого гомотопна точке или окружности.

Мы говорим, что граф *упорядочен*, если на множестве его рёбер зафиксирован частичный порядок, ограничение которого на каждую компоненту связности является линейным порядком. Ребро e упорядоченного леса называют *существенным относительно порядка*, если через e проходит бесконечный в обе стороны путь без самопересечений, состоящий из рёбер, не превосходящих e.

Действие группы на графе называют

- *кокомпактным*, если число орбит вершин и число орбит рёбер конечны;
- *свободным*, если стабилизатор каждой вершины тривиален (и, следовательно, стабилизаторы рёбер тоже тривиальны);
- *свободным на рёбрах*, если стабилизатор каждого ребра тривиален.

Теорема Минеева о существенных рёбрах ([Mi12b], теорема 1.6). *Пусть группа G свободно и кокомпактно действует на упорядоченном лесе T, сохраняя порядок. Тогда множество орбит существенных относительно порядка ребер является максимальным существенным множеством в факторграфе T/G. В частности, приведённый ранг $\overline{\mathbf{r}}(T/G)$ этого факторграфа равен числу орбит существенных относительно порядка ребер.*

Лемма о ранге группы. *Пусть свободная конечно порожденная группа A свободно кокомпактно и сохраняя порядок действует на упорядоченном лесе L, состоящем из n деревьев. Тогда число орбит существенных относительно порядка рёбер равно $n \cdot \overline{\mathrm{rk}}(A)$.*

Здесь и далее $\overline{\mathrm{rk}}(A) \stackrel{\text{опр}}{=} \max(\mathrm{rank}(A) - 1, 0)$ — это *приведённый ранг* свободной группы A.

Доказательство. Пусть $\mathbf{NO}(G, \Gamma)$ обозначает число G-орбит существенных относительно порядка рёбер в упорядоченном графе Γ (на котором группа G действует, сохраняя порядок).

Случай 1: $n = 1$. В этом случае утверждение (как замечено в [Mi12b], лемма 1.1) немедленно вытекает из теоремы Минеева о существенных рёбрах, поскольку $\overline{\mathbf{r}}(T/A) = \overline{\mathrm{rk}}(A)$, если T — дерево.

Случай 2: действие группы A на множестве деревьев (компонент) леса L транзитивно. Пусть T — одно из деревьев леса L. Тогда $\mathbf{NO}(A, L) \stackrel{t}{=} \mathbf{NO}(\mathrm{St}(T), T) \stackrel{1}{=} \overline{\mathrm{rk}}(\mathrm{St}(T)) \stackrel{S}{=} |A : \mathrm{St}(T)| \cdot \overline{\mathrm{rk}}(A) = n \cdot \overline{\mathrm{rk}}(A)$, где равенство $\stackrel{t}{=}$ вытекает из транзитивности действия на множестве деревьев, равенство $\stackrel{1}{=}$ — это уже разобранный случай 1, равенство $\stackrel{S}{=}$ — это формула Шрайера, а последнее равенство вытекает из того, что длина орбиты равна, как известно, индексу стабилизатора.

Случай 3: общий случай. Пусть $L = P_1 \sqcup \ldots \sqcup P_k$ и на на каждом (инвариантном) лесе P_i, состоящем из l_i деревьев, действие транзитивно. Тогда

$$\mathbf{NO}(A, L) = \mathbf{NO}(A, P_1) + \ldots + \mathbf{NO}(A, P_k) \stackrel{2}{=} l_1 \cdot \overline{\mathrm{rk}}(A) + \ldots + l_k \cdot \overline{\mathrm{rk}}(A) = (l_1 + \ldots + l_k) \cdot \overline{\mathrm{rk}}(A) = n \cdot \overline{\mathrm{rk}}(A),$$

где равенство $\stackrel{2}{=}$ — это случай 2. Лемма доказана.

Следующую простую лемму можно найти, например, в [Za14] (лемма 2).

Лемма о пересечении орбит. *Пусть A и B — подгруппы группы G, свободно действующей на множестве X, содержащем A-инвариантное подмножество $Y \subseteq X$ и B-инвариантное подмножество $Z \subseteq X$. Тогда*

$$(\text{число } (A \cap B)\text{-орбит в } Y \cap Z) \leqslant (\text{число } A\text{-орбит в } Y) \cdot (\text{число } B\text{-орбит в } Z).$$

Лемма об индуцированном действии. *Пусть группа G обладает подгруппой F конечного индекса n, которая действует на некотором упорядоченном дереве T, сохраняя порядок. Тогда G способна сохраняя порядок действовать на упорядоченном лесе, состоящем из n деревьев, причём стабилизаторы вершин и рёбер при этом действии будут сопряжены стабилизаторам вершин и рёбер при исходном действии F на T.*

Доказательство. Пусть $S \ni 1$ — система представителей левых смежных классов G по F (то есть $|S| = n$). Таким образом, каждый элемент $g \in G$ однозначно раскладывается в произведение $g = \mathbf{s}(g)\mathbf{f}(g)$ элемента $\mathbf{s}(g) \in S$ и элемента $\mathbf{f}(g) \in F$.

Возьмём упорядоченный лес $L = \bigcup\limits_{s \in S} sT$, состоящий из n копий sT упорядоченного дерева T (считая, что рёбра из разных копий несравнимы) и рассмотрим обычное индуцированное действие группы G на лесе L: $g \circ st \stackrel{\text{опр}}{=} \mathbf{s}(gs)\Big(\mathbf{f}(gs) \circ t\Big)$. Ясно, что это действие удовлетворяет всем требованиям.

Лемма об инвариантном лесе. *Пусть конечно порождённая группа G действует на лесе L с конечным числом компонент связности. Тогда всякое конечное множество X вершин леса L содержится в некотором G-инвариантном подлесе $L_X \supseteq X$, пересечение которого с каждой компонентой леса L связно, а действие группы G на L_X кокомпактно.*

Доказательство. Для каждой компоненты T леса L выберем конечное множество порождающих S в стабилизаторе дерева T (этот стабилизатор конечно порождён, поскольку его индекс в конечно порождённой группе G конечен), после чего сделаем следующее:

– соединим все точки множества $X \cap T$ (кратчайшими) путями;

– соединим полученное дерево R путями с деревьями $s^{\pm 1}R$ для всех $s \in S$ и добавим эти пути к R.

После этого мы добавим к полученному конечному лесу $R' \supseteq X$ все его сдвиги gR', где $g \in G$. Понятно, что получится G-инвариантный лес $R'' = \bigcup\limits_{g \in G} gR'$, действие группы G на котором кокомпактно.

Проверим, что пересечение $R'' \cap T$ связно для каждой компоненты T леса L. Действительно, дерево $R' \cap T$ по построению соединено путём с деревом $s^{\pm 1}R' \cap T$, значит, дерево $gR' \cap T$ соединено путём с деревом $gs^{\pm 1}R' \cap T$ для всех $g \in \mathrm{St}(T)$ и $s \in S$; в частности, деревья $gR' \cap T$ и $g'R' \cap T$ лежат в одной компоненте леса $R'' \cap T$, где длина элемента $g' = gs^{\pm 1} \in \mathrm{St}(T)$ (в образующих S) меньше длины элемента g. Очевидная индукция завершает доказательство.

2. Доказательство теорем 1 и 2

Пусть F — подгруппа группы G, которая либо является свободной, либо, по крайней мере, раскладывается в свободное произведение левоупорядочиваемых групп. Как известно, свободная группа способна свободно действовать на некотором дереве T, а свободное произведение $F = \mathop{\ast}\limits_{i \in I} G_i$ способно действовать на некотором дереве T таким образом, что стабилизатор каждой вершины будет сопряжён одному из сомножителей G_i.

Дерево T можно упорядочить: порядок на рёбрах дерева T определяется левоинвариантным порядком на группе F (который, как известно, существует [Ви49], [DŠ14]). Таким образом, действие F на T сохраняет порядок и свободно на рёбрах (в обоих случаях).

По лемме об индуцированном действии группа G действует на некотором упорядоченном лесе L свободно на рёбрах. При этом действия групп A и B на L свободны. По лемме об инвариантном лесе выберем A-инвариантный подлес $\mathcal{A} \subseteq L$ и B-инвариантный подлес $\mathcal{B} \subseteq L$ таким образом, что

– действия групп A и B на этих лесах $\mathcal{A}$ и $\mathcal{B}$ кокомпактно (и, следовательно, действие группы $A \cap B$ на $\mathcal{A} \cap \mathcal{B}$ тоже кокомпактно по лемме о пересечении орбит);

– пересечение каждой компонентой леса L с каждым из лесов $\mathcal{A}$, $\mathcal{B}$ и $\mathcal{A} \cap \mathcal{B}$ непусто и связно.

Положив в лемме о пересечении орбит

$$X = \{\text{рёбра леса } L\}, \qquad Y = \{\text{рёбра леса } \mathcal{A}, \text{ существенные относительно порядка (в } \mathcal{A})\},$$
$$Z = \{\text{рёбра леса } \mathcal{B}, \text{ существенные относительно порядка (в } \mathcal{B})\}$$

и заметив, что каждое существенное относительно порядка ребро леса $\mathcal{A} \cap \mathcal{B}$ заведомо является существенным относительно порядка в лесах $\mathcal{A}$ и $\mathcal{B}$, мы получим $\mathbf{NO}(A \cap B, \mathcal{A} \cap \mathcal{B}) \leqslant \mathbf{NO}(A, \mathcal{A}) \cdot \mathbf{NO}(B, \mathcal{B})$. По лемме о ранге группы левая часть полученного неравенства равна $n \cdot \overline{\mathrm{rk}}(A \cap B)$, а правая часть равна $n^2 \cdot \overline{\mathrm{rk}}(A) \cdot \overline{\mathrm{rk}}(B)$. Сокращая на n, получаем то, что требовалось.

ГЛАВА 2.
АНАЛОГ УСИЛЕННОЙ ГИПОТЕЗЫ ХАННЫ НЕЙМАН В ПОЧТИ СВОБОДНЫХ ГРУППАХ И ПОЧТИ СВОБОДНЫХ ПРОИЗВЕДЕНИЯХ

0. Введение

Гипотеза Ханны Нейман (1957), доказанная независимо Минеевым и Фридманом представляет собой следующий факт.

Теорема Минеева–Фридмана [Mi12a], [Mi12b], [Fr14]. *Для любых нетривиальных подгрупп A и B свободной группы F*

$$\operatorname{rank}(A\cap B)-1\leqslant(\operatorname{rank}(A)-1)\cdot(\operatorname{rank}(B)-1);\qquad\text{(\textit{классическая гипотеза Ханны Нейман})}$$

более того, для любой системы представителей S двойных смежных смежных классов AsB в F

$$\sum_{s\in S}\overline{\operatorname{rank}}(A\cap sBs^{-1})\leqslant\overline{\operatorname{rank}}(A)\cdot\overline{\operatorname{rank}}(B),\qquad\text{(\textit{усиленная гипотеза Ханны Нейман})}$$

где $\overline{\operatorname{rank}}(H)\overset{\text{опр}}{=}\max(0,\,\operatorname{rank}(H)-1)$ *— это приведённый ранг свободной группы H.*

Альтернативные доказательства и обобщения этого результата можно найти, например, в [D12], [AMS14], [Za14], [ASS15], [Hoc16], [HW16], [Iv17], [JZ17] и [KP20]. В частности, в [KP20] был доказан следующий аналог классической гипотезы Ханны Нейман для свободных подгрупп почти свободной группы:

для любых свободных подгрупп A и B почти свободной группы G, содержащей свободную подгруппу F конечного индекса

$$\overline{\operatorname{rank}}(A\cap B)\leqslant|G{:}F|\cdot\overline{\operatorname{rank}}(A)\cdot\overline{\operatorname{rank}}(B).$$

Эта оценка усилила ранее известные неравенства [Za14], [ASS15] (и является уже неулучшаемой). Мы обобщаем этот факт в двух направлениях:

– во-первых, мы получаем аналог усиленной гипотезы Ханны Нейман;
– а во-вторых, наша оценка имеет смысл для произвольных подгрупп A и B почти свободной группы.

Теорема о пересечении подгрупп в почти свободных группах. *Для любых подгрупп A и B почти свободной группы G, содержащей свободную группу F в качестве подгруппы конечного индекса, и для любой системы представителей S двойных смежных смежных классов AsB в G*

$$\sum_{s\in S}\overline{\operatorname{rk}}(A\cap sBs^{-1})\leqslant|G{:}F|\cdot\overline{\operatorname{rk}}(A)\cdot\overline{\operatorname{rk}}(B).\quad\textit{В частности, }\overline{\operatorname{rk}}(A\cap B)\leqslant|G{:}F|\cdot\overline{\operatorname{rk}}(A)\cdot\overline{\operatorname{rk}}(B).$$

Здесь $\overline{\operatorname{rk}}(H)$ — это *виртуальный приведённый ранг* почти свободной группы: $\overline{\operatorname{rk}}(H)\overset{\text{опр}}{=}\frac{1}{|H:K|}\cdot\max\big(0,\operatorname{rank}(K)-1\big)$, где K — свободная подгруппа конечного индекса в H. Нетрудно убедиться, что это определение к корректно (то есть не зависит от выбора свободной подгруппы K); и $\overline{\operatorname{rk}}(H)=\overline{\operatorname{rank}}(H)$, если группа H свободна. Отметим ещё, что виртуальный приведённый ранг почти свободной группы совпадает с её *ранговым градиентом* [La05].

На самом деле, сформулированная выше теорема о пересечении подгрупп в почти свободных группах является частным случаем более общей *основной теоремы* этой работы (смотрите следующий параграф), в которой речь идёт о пересечении подгрупп в почти свободных произведениях. В частности, наша основная теорема обобщает следующий известный аналог усиленной гипотезы Ханны Нейман.

Теорема AMS [AMS14] (см. также [Iv17]). *Для любых подгрупп A и B свободного произведения $G=\mathop{\ast}\limits_{i\in I}G_i$ левоупорядочиваемых групп G_i и для любой системы представителей S двойных смежных смежных классов AsB в G*

$$\sum_{s\in S}\overline{\operatorname{rank}}_{\mathrm{K}}(A\cap sBs^{-1})\leqslant\overline{\operatorname{rank}}_{\mathrm{K}}(A)\cdot\overline{\operatorname{rank}}_{\mathrm{K}}(B).\quad\textit{В частности, }\overline{\operatorname{rank}}_{\mathrm{K}}(A\cap B)\leqslant\overline{\operatorname{rank}}_{\mathrm{K}}(A)\cdot\overline{\operatorname{rank}}_{\mathrm{K}}(B).$$

Здесь $\overline{\operatorname{rank}}_{\mathrm{K}}(H)$ — это *приведённый ранг Куроша* подгруппы $H\subseteq G=\mathop{\ast}\limits_{i\in I}G_i$, который определяется так: подгруппа H раскладывается (по теореме Куроша) в свободное произведение $H=\left(\mathop{\ast}\limits_{j\in J}H_j\right)\ast F$, где каждая

подгруппа H_j нетривиальна и сопряжена подгруппе одной из G_i, а подгруппа F свободна и тривиально пересекается со всеми сопряжёнными к подгруппам G_i; тогда $\overline{\mathrm{rank}}_{\mathrm{K}}(H) \stackrel{\text{опр}}{=} \max(0,\ |J| + \mathrm{rank}(F) - 1)$.

Доказательство основной теоремы основано на подходе Минеева [Mi12b], но наши определения слегка отличаются, поэтому мы доказываем всё «с нуля» и, стало быть, эта глава содержит также очередное альтернативное (и более простое) доказательство теоремы Минеева–Фридмана. Главные отличия нашего рассуждения состоят в том, что при рассмотрении действий групп на лесах мы

– нигде не рассматриваем в явном виде факторграф по этому действию
– и нигде не требуем кокомпактности действия.

Это позволяет нам сказать, что наша основная теорема и все её следствия, сформулированные выше (включая теорему Минеева–Фридмана) являются, в некотором смысле, частными случаями совсем элементарной леммы о действиях групп на множествах (смотрите параграф 2).

1. Основная теорема

Если группа G содержит свободное произведение $F = \mathop{*}\limits_{i\in I} G_i$ бесконечных групп G_i в качестве подгруппы конечного индекса, то для любой подгруппы $H \subseteq G$ определён *виртуальный приведённый ранг Куроша* $\overline{\mathrm{rk}}(H)$ относительно семейства подгрупп G_i:

$$\overline{\mathrm{rk}}(H) \stackrel{\text{опр}}{=} \frac{\overline{\mathrm{rank}}_{\mathrm{K}}(K)}{|H{:}K|},$$

где K — подгруппа конечного индекса в H, содержащаяся в F, а $\overline{\mathrm{rank}}_{\mathrm{K}}(K)$ — это (обычный) приведённый ранг Куроша подгруппы K группы $F = \mathop{*}\limits_{i\in I} G_i$. Эта величина определена корректно, то есть не зависит от выбора подгруппы K (так как для ранга Куроша верен аналог формулы Шрайера [Ku83]), но не очень хорошо себя ведёт, поскольку не инвариантна относительно сопряжения, то есть числа $\overline{\mathrm{rk}}(H)$ и $\overline{\mathrm{rk}}(gHg^{-1})$ не обязаны совпадать. Чтобы исправить эту неприятность, определим *тотальный виртуальный приведённый ранг Куроша* $\overline{\mathbf{r}}(H)$ (относительно семейства групп $\{G_i \mid i \in I\}$) так: $\overline{\mathbf{r}}(H) = \sum\limits_{j=1}^{n} \overline{\mathrm{rk}}(g_j H g_j^{-1})$, где $\overline{\mathrm{rk}}$ — это виртуальный приведённый ранг Куроша относительно данного семейства подгрупп, а $g_1, \ldots, g_n$ суть представители правых смежных классов группы G по подгруппе F. Нетрудно сообразить, что эта величина уже инвариантна относительно сопряжения и не зависит от выбора представителей g_j. Отметим, что $\overline{\mathbf{r}}(H) = 0$ для конечной группы H.

Основная теорема. *Пусть группа G является почти свободным произведением левоупорядочиваемых групп, то есть G содержит в качестве подгруппы конечного индекса свободное произведение $F = \mathop{*}\limits_{i\in I} G_i$, где все группы G_i левоупорядочиваемы. Пусть A и B — это подгруппы в G, и пусть S — это множество представителей двойных смежных классов вида AgB в группе G. Тогда $\sum\limits_{s\in S} \overline{\mathbf{r}}(A\cap sBs^{-1}) \leqslant \overline{\mathbf{r}}(A)\cdot\overline{\mathbf{r}}(B)$, где $\overline{\mathbf{r}}(H)$ — это тотальный виртуальный приведённый ранг Куроша подгруппы $H \subseteq G$ (относительно семейства групп $\{G_i \mid i \in I\}$).*
В частности, $\overline{\mathbf{r}}(A \cap B) \leqslant \overline{\mathbf{r}}(A) \cdot \overline{\mathbf{r}}(B)$.

Это обобщает ранее известные результаты:

– в случае, когда $F = G$, наша теорема превращается в теорему AMS [AMS14] (а если при этом все G_i являются бесконечными циклическими, то мы получаем теорему Минеева–Фридмана, ранее известную, как усиленная гипотеза Ханны Нейман);
– а в случае, когда A и B являются свободными группами, тривиально пересекающими подгруппы, сопряжённые к свободным сомножителям G_i, утверждение «В частности» превращается в основной результат работы [KP20].

Чтобы вывести из основной теоремы теорему о пересечении подгрупп в почти свободных группах (смотрите введение), достаточно заметить, что виртуальный приведённый ранг $\overline{\mathrm{rk}}(H)$ почти свободной подгруппы $H \subseteq G$ совпадает с виртуальным приведённым рангом Куроша относительно любого семейства бесконечных циклических подгрупп, свободное произведение которых есть F. Поэтому все слагаемые в определении тотального виртуального ранга $\overline{\mathbf{r}}(H)$ равны (а их количество есть индекс подгруппы F), то есть $\overline{\mathbf{r}}(H) = |G{:}F| \cdot \overline{\mathrm{rk}}(H)$ в данном случае.

2. Действия

Следующую простую лемму нам (как ни странно) не удалось найти в литературе.

Лемма о пересечении орбит. *Пусть A и B — подгруппы группы G, свободно действующей на некотором множестве X, и D — множество представителей двойных смежных классов AgB. Тогда*

$$\sum_{d\in D} (\text{число } (A^d\cap B)\text{-орбит}) \leqslant (\text{число } A\text{-орбит})\cdot(\text{число } B\text{-орбит}).$$

Более того, для любого A-инвариантного подмножества $Y\subseteq X$ и любого B-инвариантного подмножества $Z\subseteq X$

$$\sum_{d\in D}\Big(\text{число } (A^d\cap B)\text{-орбит в } (d^{-1}\circ Y)\cap Z\Big) \leqslant (\text{число } A\text{-орбит в } Y)\cdot(\text{число } B\text{-орбит в } Z).$$

Доказательство. Пусть $G\times X\xrightarrow{\circ} X$ — свободное действие, и X/H — это множество орбит действия подгруппы $H\subseteq G$. Рассмотрим отображение

$$\Phi\colon \Big\{(d,U)\mid d\in D,\ U\in \Big((d^{-1}\circ Y)\cap Z\Big)/(A^d\cap B)\Big\}\to Y/A\times Z/B,\quad \big(d,\ (A^d\cap B)\circ x\big)\mapsto (A\circ d\circ x,\ B\circ x).$$

Утверждение леммы немедленно вытекает из того, что это отображение

- корректно определено,
  то есть не зависит от выбора точки x в $(A^d\cap B)$-орбите (очевидно),
- и инъективно;
  действительно, $(A\circ d\circ x,\ B\circ x)=(A\circ d'\circ x',\ B\circ x')$ означает, что $d'\circ x'\in A\circ d\circ x$ и $x'\in B\circ x$, то есть $(d'B)\cap(Ad)\neq\varnothing$ (в силу свободности действия) и, значит, $d'=d$ (по определению множества D); а тогда, $x'\in(A^d\circ x)\cap(B\circ x)=(A^d\cap B)\circ x$, что и требовалось.

3. Действия на лесах

Все графы в этой главе считаются ориентированными. Пусть группа G действует на лесе Γ свободно на рёбрах (то есть стабилизатор каждого ребра тривиален). Множество E орбит рёбер графа Γ называется *максимальным существенным* если E является максимальным по включению множеством таким, что стабилизатор каждой компоненты леса $\Gamma\setminus\bigcup E$ (то есть каждая компонента леса, полученного из Γ удалением всех рёбер, лежащих во всех орбитах множества орбит E), не являющейся компонентой леса Γ, нетривиален. Отметим, что, на самом деле, стабилизатор компоненты леса Γ не может быть тривиальным, если число компонент конечно, а группа бесконечна (но мы не предполагаем, что эти условия выполнены по умолчанию).

Следующая лемма представляет собой простейший (и, вероятно, известный) факт о группах, действующих на деревьях

Лемма о ранге Куроша. *Группа G, действующая на дереве Γ свободно на рёбрах, раскладывается в свободное произведение: $G=F*\Big(\mathop{*}_{i\in I} G_i\Big)$, где F — свободная группа, действующая на Γ свободно, а $G_i\neq\{1\}$ суть стабилизаторы некоторых вершин; при этом, если ранг Куроша этого разложения конечен (то есть $\operatorname{rank}(F)+|I|<\infty$), то мощность каждого максимального существенного множества E равна приведённому рангу Куроша этого разложения: $|E|=\max(0,\ \operatorname{rank}(F)+|I|-1)$.*

Набросок доказательства. Первое утверждение хорошо известно. Чтобы доказать второе утверждение, для каждого ребра e рассмотрим компоненты связности X и Y леса $\Gamma\setminus(G\circ e)$, соединённые ребром e. Из леммы о пинг-понге сразу следует, что

$$G=\begin{cases}\operatorname{St}(X)*\langle g\rangle_\infty, & \text{если } g\circ X=Y \text{ для некоторого } g\in G \text{ (который обязан действовать свободно на } \Gamma);\\ \operatorname{St}(X)*\operatorname{St}(Y), & \text{если } g\circ X\neq Y \text{ ни для какого } g\in G.\end{cases}$$

Очевидная индукция завершает доказательство (так как ранг Куроша конечен). Эта лемма можно также вывести из [AMS14] (теорема 2.4, используя рассуждения из предложения 3.4).

Нас будет интересовать обобщение этой простой леммы на случай, когда граф Γ является лесом, состоящим из конечного числа деревьев: $\Gamma=T_1\sqcup\ldots\sqcup T_n$. В этом случае у группы G есть смысл рассматривать *виртуальный приведённый ранг Куроша*, который определяется естественным образом: выберем в группе G

подгруппу H конечного индекса, которая стабилизирует дерево T_j и, следовательно, раскладывается в свободное произведение $H = F * \left(\ast\limits_{i\in I} G_i \right)$, где F — свободная группа, действующая на T_j свободно, а $G_i \neq \{1\}$ суть стабилизаторы некоторых вершин дерева T_j; приведённый ранг Куроша этой подгруппы (относительно данного действия на T_j) тогда определяется как $\overline{\mathrm{rk}}(H) \overset{\text{опр}}{=} \max(0,\ \mathrm{rank}(F)+|I|-1)$, а виртуальный приведённый ранг Куроша группы G (относительно данного действия на Γ и данной компоненты T_j леса Γ) естественно определить так: $\overline{\mathrm{rk}}_j(G) \overset{\text{опр}}{=} \frac{1}{|G:H|} \cdot \overline{\mathrm{rk}}(H)$. Нетрудно сообразить, что эта величина не зависит от выбора подгруппы H (если нетривиальные стабилизаторы вершин бесконечны), но может зависеть от j. *Тотальным приведённым виртуальным рангом Куроша* этого действия мы назовём величину $\sum\limits_j \overline{\mathrm{rk}}_j(G)$.

Лемма о виртуальном ранге Куроша. *Пусть группа G действует свободно на рёбрах на лесе $\Gamma = T_1 \sqcup \ldots \sqcup T_n$, состоящем из деревьев T_j, и стабилизатор каждого дерева T_j имеет конечный ранг Куроша (относительно действия на T_j), а нетривиальные стабилизаторы вершин бесконечны. Тогда $|E| = \sum\limits_{j=1}^{n} \overline{\mathrm{rk}}_j(G)$ для каждого максимального существенного множества E.*

Доказательство. Пусть $\Gamma = \Gamma_1 \sqcup \ldots \sqcup \Gamma_k$ и на каждом G-инвариантном лесе Γ_i, действие группы G транзитивно на компонентах (то есть для любых компонент $T_l, T_m \subseteq \Gamma_i$ существует $g \in G$ такой, что $g \circ T_l = T_m$). Тогда $E = E_1 \sqcup \ldots \sqcup E_k$, где $E_i = \{G \circ e \in E \mid G \circ e \subseteq \Gamma_i\}$ — это максимальное существенное множество орбит рёбер леса Γ_i. Поэтому утверждение достаточно доказать для случая, когда действие группы G на лесе Γ транзитивно на деревьях этого леса.

А в этом случае все стабилизаторы $H_j = \mathrm{St}(T_j)$ деревьев T_j сопряжены, а значит, изоморфны и действуют на своих деревьях одинаково. В частности, $\overline{\mathrm{rk}}(H_j)$ не зависит от j. Кроме того, $|G{:}H_j| = n$ для всех j (так как длина орбиты равна индексу стабилизатора). Поэтому

$$\sum_{j=1}^{n} \overline{\mathrm{rk}}_j(G) = \sum_{j=1}^{n} \frac{1}{|G:H_j|} \cdot \overline{\mathrm{rk}}(H_j) = \sum_{j=1}^{n} \frac{1}{n} \cdot \overline{\mathrm{rk}}(H_1) = \overline{\mathrm{rk}}(H_1).$$

С другой стороны, множество H_1-орбит рёбер $E' = \{G \circ e \cap T_1 \mid G \circ e \in E\}$ является, очевидно, максимальным существенным относительно действия группы H_1 на T_1. Поэтому $|E| = |E'| = \overline{\mathrm{rk}}(H_1)$ (последнее равенство следует из леммы о ранге Куроша). Это завершает доказательство.

4. Действия на упорядоченных лесах

Мы говорим, что граф *упорядочен*, если на множестве его рёбер зафиксирован частичный порядок, ограничение которого на каждую компоненту связности является линейным порядком.

Лемма об индуцированном действии [KP20]. *Пусть группа G обладает подгруппой F конечного индекса n, которая действует на некотором упорядоченном дереве T, сохраняя порядок. Тогда G способна сохраняя порядок действовать на упорядоченном лесе, состоящем из n деревьев, причём стабилизаторы вершин и рёбер при этом действии будут сопряжены стабилизаторам вершин и рёбер при исходном действии F на T.*

Доказательство. Пусть $S \ni 1$ — система представителей левых смежных классов G по F (то есть $|S| = n$). Таким образом, каждый элемент $g \in G$ однозначно раскладывается в произведение $g = \mathbf{s}(g)\mathbf{f}(g)$ элемента $\mathbf{s}(g) \in S$ и элемента $\mathbf{f}(g) \in F$.

Возьмём упорядоченный лес $L = \bigcup\limits_{s\in S} sT$, состоящий из n копий sT упорядоченного дерева T (считая, что рёбра из разных копий несравнимы) и рассмотрим обычное индуцированное действие группы G на лесе L: $g \circ st \overset{\text{опр}}{=} \mathbf{s}(gs)\Big(\mathbf{f}(gs) \circ t\Big)$. Ясно, что это действие удовлетворяет всем требованиям, что и доказывает лемму.

Ребро e упорядоченного леса, на котором действует некоторая группа H, сохраняя порядок, мы называем *важным* (или *H-важным*), если оно является максимальным ребром на некоторой прямой $T(e)$, пересекающей лишь конечное число H-орбит рёбер. Отметим, что при $K \subseteq H$ любое K-важное ребро H-важно.

Лемма о важных рёбрах. *Пусть группа G действует на упорядоченном лесе T сохраняя порядок и свободно на рёбрах. Тогда*

- *множество $\mathcal{E}$ орбит важных рёбер содержит некоторое максимальное существенное множество;*
- *каждое конечное подмножество $\mathcal{E}' \subseteq \mathcal{E}$ содержится в некотором максимальном существенном множестве.*

В частности, тотальный приведённый виртуальный ранг Куроша этого действия

- *равен $|\mathcal{E}|$, если $|\mathcal{E}| < \infty$,*

– *бесконечен, если множество $\mathcal{E}$ бесконечно.*

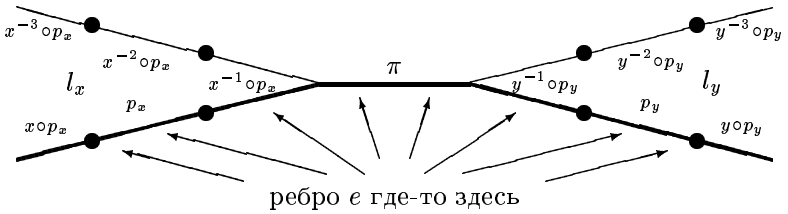
Доказательство. Утверждение «В частности» вытекает из основного утверждения по лемме о ранге Куроша. Остаётся доказать основное утверждение. Возьмём произвольное конечное подмножество $\mathcal{E}'$ множества $\mathcal{E}$ и положим $E = \bigcup \mathcal{E}$ и $E' = \bigcup \mathcal{E}'$ (то есть $e \in E$ тогда и только тогда, когда $G \circ e \in \mathcal{E}$; и аналогично $e \in E'$ тогда и только тогда, когда $G \circ e \in \mathcal{E}'$; таким образом, E и E' суть множества рёбер, а $\mathcal{E}$ и $\mathcal{E}'$ — множества орбит рёбер). Надо доказать две вещи:

1) стабилизатор $\mathrm{St}(K)$ каждой компоненты K леса $T \setminus E$ имеет в K либо неподвижную точку, либо инвариантную прямую;
2) но при этом стабилизатор каждой компоненты K леса $T \setminus E'$ нетривиален, если в T существует важное ребро $e \in E'$, инцидентное вершине из K.

И то, и другое доказывается легко.

1) Если свойство 1) не выполнено, то стабилизатор компоненты K графа $T \setminus E$ содержит свободную подгруппу ранга два $F(x, y) \subseteq \mathrm{St}(K)$, действующую свободно на K (поскольку каждая недиэдральная группа, нетривиальным образом раскладывающаяся в свободное произведение содержит свободную подгруппу, тривиально пересекающую свободные сомножители, а группа G из условия теоремы не может быть диэдральной, так как не может иметь кручения, если в T есть хоть одно ребро). Пусть l_x и l_y — инвариантные прямые в K для элементов x и y, соответственно. Пересечение этих прямых представляет собой конечный граф: либо отрезок, либо точку, либо пустое множество (оно не может быть лучом, как известно). Соединим прямые l_x и l_y путём π. Выберем конечные отрезки p_x и p_y такие, что $l_x = \bigcup\limits_{k \in \mathbb{Z}} x^k \circ p_x$ и $l_y = \bigcup\limits_{k \in \mathbb{Z}} y^k \circ p_x$ и возьмём максимальные рёбра e_x и e_y на отрезках p_x и p_y. Не ограничивая общности, мы будем считать, что
   - $x \circ e_x < e_x$ и $y \circ e_y < e_y$ (заменим x на x^{-1} и/или y на y^{-1}, если это не так);
   - и $\left(\bigcup\limits_{k=0}^{\infty} x^k \circ p_x\right) \cap (l_y \cup \pi) = \varnothing = \left(\bigcup\limits_{k=0}^{\infty} y^k \circ p_y\right) \cap (l_x \cup \pi)$ (заменим p_x на $x^n \circ p_x$ и/или p_y на $y^n \circ p_y$ с достаточно большим $n \in \mathbb{N}$, если это не так).

   Соединим теперь p_x и p_y путём $p \supset (p_x \cup p_y)$ и увидим, что максимальное ребро e пути p является максимальным ребром прямой $p \cup \left(\bigcup\limits_{k=0}^{\infty} x^k \circ p_x\right) \cup \left(\bigcup\limits_{k=0}^{\infty} y^k \circ p_y\right)$, то есть ребро e важно (рис. 1). Это противоречие завершает доказательство свойства 1).



Жирная линия — это прямая $T(e)$

Рис. 1

2) Пусть важное ребро $e \in E'$ кончается в вершине из K. Если ребро $g \circ e$ тоже кончается в какой-то вершине из K, то $g \in \mathrm{St}(K)$ и, следовательно, $\mathrm{St}(K) \neq \{1\}$, если $g \neq 1$. Поэтому достаточно рассмотреть случай, когда важных рёбер из E', инцидентных вершинам из K, лишь конечное число (не больше, чем $2|\mathcal{E}'|$). Пусть $e \in E'$ — минимальное ребро из E', инцидентное вершине из K. Тогда бесконечный луч прямой $T(e)$ (из определения важности) обязан содержаться в K (из-за минимальности ребра e). Поскольку этот луч может проходить лишь через конечное число орбит рёбер (по определению важности), мы получаем бесконечное множество рёбер из K, лежащих в одной орбите. Стало быть, $\mathrm{St}(K) \neq \{1\}$, что и требовалось.

5. Доказательство основной теоремы

Пусть $n = |G{:}F|$ и T — дерево (Басса–Серра) для разложения $F = \mathop{\ast}\limits_{i\in I} G_i$, то есть F действует на T свободно на ребрах и так, что стабилизатор каждой вершины сопряжён одному из сомножителей G_i. Дерево T можно упорядочить: порядок на рёбрах дерева T определяется левоинвариантным порядком на группе F (который, как известно, существует [Ви49], [DŠ20]). Таким образом, действие F на T сохраняет порядок и свободно на рёбрах. По лемме об индуцированном действии группа G транзитивно на компонентах действует на некотором упорядоченном лесе $\Gamma = T_1 \sqcup \ldots \sqcup T_n$, состоящем из n деревьев T_j, свободно на рёбрах и сохраняя порядок. При этом $\mathrm{St}(T_1) = F$ и $T_j = g_j T_1$, где $g_1 = 1, g_2, \ldots, g_n$ суть представители левых смежных классов группы G по подгруппе F.

Группы A и B действуют на том же лесе Γ свободно на ребрах и сохраняя порядок. Тогда

$$
\begin{aligned}
&\sum_{s\in S} \big(\text{число } (A^s\cap B)\text{-орбит } (A^s\cap B)\text{-важных рёбер}\big) \leqslant\\
\leqslant &\sum_{s\in S} \big(\text{число } (A^s\cap B)\text{-орбит рёбер, которые и } A^s\text{-важны, и } B\text{-важны}\big) = \\
= &\sum_{s\in S} \Big(\text{число } (A^s\cap B)\text{-орбит в множестве } \big(s^{-1}\circ\{A\text{-важные рёбра}\}\big)\cap\{B\text{-важные рёбра}\}\Big) \leqslant\\
\leqslant &\big(\text{число } A\text{-орбит } A\text{-важных рёбер}\big)\cdot\big(\text{число } B\text{-орбит } B\text{-важных рёбер}\big),
\end{aligned}
\qquad (*)
$$

где

- первое неравенство вытекает из того, что если ребро важно относительно какой-то группы, то оно важно относительно любой большей группы;
- равенсто вытекает из того, что ребро e является A-важным тогда и только тогда, когда ребро $s^{-1}\circ e$ является A^s-важным;
- последнее неравенство вытекает из леммы о пересечении орбит, применённой к

$$Y = \{A\text{-важные рёбра графа }\Gamma\} \subseteq X = \{\text{рёбра графа }\Gamma\} \supseteq Z = \{B\text{-важные рёбра графа }\Gamma\}.$$

По лемме о важных рёбрах множество орбит важных рёбер есть максимальное существенное множество (если максимальное существенное множество конечно). Таким образом, число C-орбит C-важных рёбер в неравенстве $(*)$ равно мощности максимального существенного множества для действия группы C на Γ (где C — это A, B или $A^s\cap B$). Значит, по лемме о виртуальном ранге Куроша мы имеем

$$\sum_{s\in S} \overline{\mathbf{r}}(A\cap sBs^{-1}) \leqslant \overline{\mathbf{r}}(A)\cdot\overline{\mathbf{r}}(B), \quad \text{где } \overline{\mathbf{r}}(H) = \sum_{j=1}^{n} \overline{\mathrm{rk}}_j(H),$$

а $\overline{\mathrm{rk}}_j(H)$ — это виртуальный приведённый ранг Куроша, относительно (соответствующего разложения) подгруппы $\mathrm{St}(T_j)$. Осталось заметить, что «соответствующее разложение» стабилизатора j-го дерева имеет вид $\mathrm{St}(T_j) = g_j F g_j^{-1} = \mathop{\ast}\limits_{i\in I} g_j G_i g_j^{-1}$. Это завершает доказательство.

ГЛАВА 3.
СКОЛЬКО НАБОРОВ ЭЛЕМЕНТОВ ГРУППЫ ОБЛАДАЕТ ДАННЫМ СВОЙСТВОМ?

0. Введение

Теорема Соломона [Solo69]. *В любой группе число решений системы уравнений без коэффициентов делится на порядок этой группы, если уравнений меньше, чем неизвестных.*

Эта тема развивалась в разных направлениях (см., например, [Стру95], [AmV11], [Isaa70] и литературу, там цитируемую), но наиболее простое и естественное обобщение теоремы Соломона было получено совсем недавно.

Теорема Гордона–Родригеса-Виллегаса [GRV12]. *В любой группе число решений системы уравнений без коэффициентов делится на порядок этой группы, если ранг матрицы, составленной из сумм показателей степеней при i-м неизвестном в j-м уравнении, меньше числа неизвестных.*

Например, к системе уравнений $x^2y^3[x,y]y^{-1} = 1 = (yx)^2$ теорема Соломона неприменима, но по теореме Гордона–Родригеса-Виллегаса число решений всё же делится на порядок группы, так как ранг соответствующей матрицы $\left(\begin{smallmatrix}2&2\\2&2\end{smallmatrix}\right)$ равен единице, а неизвестных два.

Напрашивается гипотеза, что если ранг матрицы сильно меньше числа неизвестных, то число решений должно делиться на высокую степень порядка группы. Однако ни эта гипотеза, ни её естественное ослабление не верны. В параграфе 2 мы приводим соответствующий пример.

Мы обобщаем теорему Гордона–Родригеса-Виллегаса в других направлениях. Мы изучаем уравнения с коэффициентами, причём не только системы уравнений, но и произвольные формулы первого порядка. Основная теорема позволяет заключить, что имеет место множество фактов, подобных тому, что упомянут в аннотации. В параграфе 1 читатель может найти формулировку основной теоремы, в параграфе 2 — несколько примеров, а в параграфе 3 — доказательство, которое для случая систем уравнений без коэффициентов превращается в доказательство теоремы Гордона–Родригеса-Виллегаса, немного более простое по сравнению с оригинальным, на наш взгляд, но основанное на тех же идеях. В параграфе 4 мы даём прямое доказательство забавного факта, сформулированного в аннотации. Нам не удалось найти этот факт в литературе,*) хотя он легко мог бы быть выведен из одной теоремы Ф. Холла (смотрите параграф 1), обобщающей известную теорему Фробениуса [Frob03] (смотрите также [Hall59]), которая утверждает, что *число решений уравнения $x^n = g$ делится на* НОД$(n, |C(g)|)$. Теорема Фробениуса обобщалась в разных направлениях (смотрите, например, [Hall36b], [Kula38], [Sehg62], [BrTh88], [AsTa01] и литературу там цитируемую).

Обозначения, которые мы используем, в целом стандартны. Отметим только, что если $k \in \mathbb{Z}$, а x и y — элементы некоторой группы, то x^y, x^{ky} и x^{-y} обозначают $y^{-1}xy$, $y^{-1}x^ky$ и $y^{-1}x^{-1}y$, соответственно. Коммутатор $[x,y]$ мы понимаем как $x^{-1}y^{-1}xy$. Если X — подмножество некоторой группы, то $|X|$, $\langle X\rangle$ и $C(X)$ означают, соответственно, мощность множества X, подгруппу, порождённую множеством X, и централизатор множества X. Буква $\mathbb{Z}$ обозначает множество целых чисел.

1. Основная теорема

Рассмотрим групповой язык L над группой G, в нём имеется два функциональных символа: $\cdot$ и $^{-1}$, кроме того, для каждого элемента группы G имеется константный символ g. Мы не предполагаем, что группа конечна (хотя это так в большинстве интересных случаев); результаты о делимости следует понимать в смысле кардинальной арифметики: любой бесконечный кардинал делится на любой не превосходящий его ненулевой кардинал (а ноль делится на любой кардинал).

Рассмотрим произвольную формулу φ первого порядка в языке L. Каждая атомарная подформула может быть записана в виде

$$u = 1,$$

где слова $u \in G * F$, а F — свободная группа, порождённая всеми (свободными и связанными) переменными формулы φ. Таким образом, слова u (возможно, разные для разных подформул) могут содержать свободные и связанные переменные и элементы группы G (называемые *коэффициентами* формулы φ).

Формуле φ мы сопоставляем ориентированный *граф* $\Gamma(\varphi)$ *формулы* φ следующим образом. Вершинами графа $\Gamma(\varphi)$ служат связанные переменные формулы φ. Каждая атомарная подформула, содержащая связанные переменные, имеет вид

$$v_1(y_1)w_1(x_1\ldots,x_n)\ldots v_r(y_r)w_r(x_1\ldots,x_n) = h,$$

где y_i — связанные переменные формулы φ (необязательно различные), $x_1\ldots,x_n$ — все (различные) свободные переменные формулы φ, слова $v_i(y_i)$ являются элементами свободного произведения $G * \langle y_i\rangle_\infty$ группы G

*) В 2017 году мы узнали, что этот факт был установлен в [Iwa82].

и бесконечной циклической группы, порождённой буквой y_i, слова $w_i(x_1 \ldots, x_n)$ являются элементами свободного произведения $G * F(x_1 \ldots, x_n)$ группы G и свободной группы с базисом $x_1 \ldots, x_n$, а $h \in G$. Соединим вершины y_i и y_{i+1} (индексы по модулю r) ориентированным ребром и пометим это ребро целочисленной строкой $(\alpha_1, \ldots, \alpha_n)$, где α_j — это сумма показателей степеней при переменной x_j в слове w_i; причём петли с нулевыми метками мы не проводим. Проделаем это с каждой атомарной подформулой, содержащей связанные переменные.

Например, если формула $\varphi(x_1, x_2)$ имеет вид *)

$$\forall y \exists z \ \left(\left([ygy, x_1 g x_2] x_1 z^{-1} a z x_2^{-3} x_1^3 h x_2^7 = 1 \right) \wedge \neg \left(z^{-1} b z (x_2 x_1)^2 = 1 \right) \vee \left((x_1^2 x_2^2)^5 = 1 \right) \right), \tag{1}$$

где $g, h, a, b \in G$ — фиксированные элементы (необязательно различные), то граф $\Gamma(\varphi)$ имеет выглядит так:

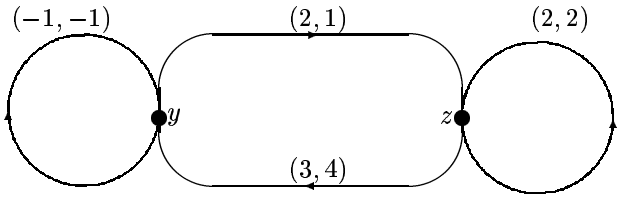


Рис. 1

Далее выберем в графе $\Gamma(\varphi)$ циклы $c_1, c_2, \ldots$, порождающие его первую группу гомологий (например, порождающие фундаментальных групп всех компонент), и составим *матрицу* $A(\varphi)$ *формулы* φ следующим образом: для каждого из порождающих циклов c_i напишем строку, являющуюся суммой меток рёбер этого цикла (взятых со знаком плюс или минус в зависимости от ориентации), после чего добавим ещё строки, состоящие из сумм показателей степеней в атомарных подформулах, не содержащих связанных переменных.

Эта матрица зависит от выбора порождающих циклов, но целочисленная линейная оболочка её строк определяется однозначно формулой φ. В приведённом выше примере матрица $A(\varphi)$ будет иметь вид

$$A(\varphi) = \begin{pmatrix} -1 & -1 \\ 5 & 5 \\ 2 & 2 \\ 10 & 10 \end{pmatrix} \quad \text{(при очевидном выборе трёх порождающих циклов).} \tag{2}$$

Связанную переменную t назовём *изолирующей*, если она входит в атомарные подформулы только в составе подслов вида $t^{-1} g_i t$, где $g_i \in G$. Соответствующие коэффициенты g_i мы будем называть *изолированными*. Более точно, элемент g группы G называется *изолированным*, если он встречается в формуле φ только в подсловах вида $t_i^{-1} g t_i$, где все t_i — изолирующие переменные. В рассматриваемом примере z является изолирующей переменной, а a и b — изолированными коэффициентами.

Основная теорема. *Если ранг матрицы $A(\varphi)$ формулы φ меньше числа свободных переменных в этой формуле, то число наборов элементов группы, удовлетворяющих формуле φ делится на порядок централизатора множества всех неизолированных коэффициентов формулы φ. В частности, это число делится на порядок группы, если все неизолированные коэффициенты равны единице.*

В приведённом выше примере ранг матрицы равен единице, а свободных переменных две, поэтому можно утверждать, что мощность множества

$$\left\{ (x_1, x_2) \in G^2 \ ; \ \forall y \exists z \ \left(\left([ygy, x_1 g x_2] x_1 z^{-1} a z x_2^{-3} x_1^3 h x_2^7 = 1 \right) \wedge \neg \left(z^{-1} b z (x_2 x_1)^2 = 1 \right) \vee \left((x_1^2 x_2^2)^5 = 1 \right) \right) \right\}$$

делится на $|C(g, h)|$ (даже если $g = a$, мы должны считать коэффициент g неизолированным). В следующем параграфе мы приведём более содержательные примеры.

Следствие 1. *Число решений системы уравнений в группе делится на порядок централизатора множества всех коэффициентов, если ранг матрицы этой системы меньше числа неизвестных.*

Это следствие превращается в теорему Гордона–Родригеса-Виллегаса в случае, когда все коэффициенты равны единице.

*) Мы не предполагаем, что в формуле всегда кванторы вынесены наружу, как в этом примере.

Теорема Гордона–Родригеса-Виллегаса о сопряжённости ([GRV12], следствие 3.5*)).
Пусть $\{w_j(x_1,\dots,x_n)\} \subset F(x_1,\dots,x_n)$ *— произвольное множество слов (элементов свободной группы) такое, что ранг матрицы, составленной из сумм показателей степеней при* x_i *в* w_j *меньше* n*. Тогда для любой группы* G *и любых элементов* $h_j \in G$ *число наборов, удовлетворяющих формуле*

$$\bigwedge_j \left(\exists q_j\ w_j(x_1,\dots,x_n) = q_j^{-1} h_j q_j\right),$$

делится на порядок группы G*.*

Это утверждение (обобщающее теорему о сопряжённости из работы [Solo69]) очевидно сильнее, чем теорема Гордона–Родригеса-Виллегаса, сформулированная во введении. Наша теорема даёт ещё более сильное утверждение: поточечная сопряжённость заменяется на сопряжённость одним элементом.

Следствие 2. *В условиях теоремы Гордона–Родригеса-Виллегаса о сопряжённости число наборов, удовлетворяющих формуле*

$$\exists q\ \left(\bigwedge_j \left(w_j(x_1,\dots,x_n) = q^{-1} h_j q\right)\right),$$

делится на порядок группы G*.*
(А если $w_j(x_1,\dots,x_n) \in G * F(x_1,\dots,x_n)$*, то число удовлетворяющих наборов делится на порядок централизатора множества всех коэффициентов слов* w_j*.)*

Доказательство. В этом случае граф имеет единственную вершину, соответствующую изолирующей переменной q, коэффициенты h_j изолированы и матрица формулы совпадает с матрицей из теоремы Гордона–Родригеса-Виллегаса о сопряжённости. Таким образом, это следствие немедленно вытекает из основной теоремы.

Следующее утверждение обобщает теорему Гордона–Родригеса-Виллегаса о сопряжённости в другом направлении.

Теорема об инвариантных множествах. *Пусть* U_j, V_j *— подмножества конечной группы* G*, инвариантные относительно сопряжённости (то есть объединения некоторых классов сопряжённости) и* $\{w_j(x_1,\dots,x_n)\} \subset F(x_1,\dots,x_n) * G$ *— произвольное множество слов такое, что ранг матрицы, составленной из сумм показателей степеней при* x_i *в* w_j *меньше* n*. Тогда число наборов элементов группы* G*, удовлетворяющих формуле*

$$\bigwedge_j (w_j U_j \subseteq V_j),$$

делится на порядок централизатора множества всех коэффициентов слов w_j*. В частности, это число делится на порядок группы* G*, если* $\{w_j(x_1,\dots,x_n)\} \subset F(x_1,\dots,x_n)$*.*

Доказательство. Рассмотрим одно из включений $wU \subseteq V$. Разложим множества U и V в объединения классов сопряжённости:

$$U = a_1^G \cup a_2^G \cup \dots, \quad V = b_1^G \cup b_2^G \cup \dots.$$

Тогда включение $wU \subseteq V$ эквивалентно следующей формуле первого порядка:

$$\forall y_1 \forall y_2 \dots \exists z_1 \exists z_2 \dots \bigwedge_k \bigvee_l w y_k^{-1} a_k y_k = z_l^{-1} b_l z_l.$$

Таким образом исходная конъюнкция включений превращается в формулу первого порядка, в которой все связанные переменные являются изолирующими, а все коэффициенты a_i и b_i — изолированными. Матрица этой формулы отличается от матрицы, составленной из сумм показателей степеней при x_i в w_j, только повторением строчек и утверждение вытекает теперь из основной теоремы.

Доказанное утверждение превращается в теорему Гордона–Родригеса-Виллегаса о сопряжённости, если $U_j = \{1\}$ и все $w_j \in F(x_1,\dots,x_n)$. Отметим, что теорема об инвариантных множествах останется верной, если конъюнкцию включений заменить на конъюнкцию произвольных (возможно различных) теоретико-множественных отношений, «логически выражающихся» через включения. Например, $\subseteq$ можно заменить на $\subset$, $\supseteq$, $\supset$, $=$, $\neq$, $\not\subset$, *«пересекается с»*,... Саму конъюнкцию тоже можно заменить на любую бесквантерную формулу

*) которое мы переформулировали на удобном для нас языке.

первого порядка. Например, *если* $A = a^G$ *и* $B = b^G$ *— какие-то классы сопряжённости в группе* G*, то число пар элементов* $(x, y) \in G^2$ *таких, что*

$$x^2y^3[x,y]y^{-1}AB = A \quad \textit{или} \quad (yx)^2A \textit{ не пересекается с } B,$$

делится на $|G|$. Это следует из основной теоремы. (Второе утверждение дизъюнкции эквивалентно формуле $\forall z \forall t\ (yx)^2z^{-1}az \neq t^{-1}bt$.)

Следующее утверждение является аналогом теоремы Соломона (и превращается в неё в случае, когда все коэффициенты равны единице, формула является бесквантором ной и имеет вид конъюнкции равенств).

Следствие 3. *Число наборов элементов группы, удовлетворяющих формуле* φ*, делится на порядок централизатора множества всех неизолированных коэффициентов формулы* φ *(в частности, это число делится на порядок группы при условии, что все неизолированные коэффициенты равны единице), если в формуле* φ

$$\begin{gathered}(\textit{число собственных вхождений связанных переменных})+\\ +(\textit{число компонент связности графа } \Gamma(\varphi))+ \qquad (*)\\ +(\textit{число атомарных подформул, не содержащих связанных переменных}) < (\textit{число всех переменных}).\end{gathered}$$

Под *вхождением переменной* y здесь понимается максимальное подслово в левой части уравнения, рассматриваемой как циклическое слово, содержащее переменную y и не содержащее других переменных; вхождение называем *собственным*, если оно не совпадает со всей левой частью равенства. В приведённом выше примере имеется два вхождения переменной y и два вхождения переменной z, всего четыре вхождения связанных переменных, все эти вхождения собственные. Число вхождений особой переменной q всегда равно числу неоднородных уравнений (из-за того, что мы рассматриваем левые части уравнений как циклические слова).

Доказательство. Ранг первой группы гомологий графа, как известно, равен числу рёбер минус число вершин плюс число компонент связности. Число вершин равно числу связанных переменных, а число рёбер равно числу вхождений связанных переменных, причём несобственные вхождения дадут петли с нулевой меткой. Поэтому ранг матрицы $A(\varphi)$ не больше чем величина, стоящая в левой части неравенства $(*)$, минус число связанных переменных. Остаётся сослаться на теорему.

Следствие 4. *Число элементов группы,* k*-е степени которых лежат в данной подгруппе, делится на порядок этой подгруппы.*[*)]

Доказательство. Пусть H — подгруппа группы G. Нас интересуют элементы x, для которых $x^k \in H$. Предположим сперва, что подгруппа H является централизатором некоторой подгруппы A. Тогда включение $x \in H$ равносильно системе уравнений $\{[x^k, a] = 1\ ;\ a \in A\}$, удовлетворяющей основной теореме (здесь связанных переменных нет и матрица нулевая). Поэтому число решений делится на порядок централизатора множества коэффициентов, то есть на $|H|$, что и требовалось.

Пусть теперь H — произвольная подгруппа. Можно применить следующий трюк. Вложим группу G в бóльшую группу $\widehat{G}$ так, что H станет централизатором некоторой подгруппы A группы $\widehat{G}$. Ещё надо позаботиться о том, чтобы все решения нашей системы уравнений над $\widehat{G}$ лежали в G. Для этого мы сделаем G централизатором некоторой другой подгруппы $B \subset \widehat{G}$ и рассмотрим систему уравнений

$$\left(\bigwedge_{a\in A}\left([x^k,a]=1\right)\right) \wedge \left(\bigwedge_{b\in B}\left([x,b]=1\right)\right).$$

Это докажет следствие 4 в общем случае.

В качестве $\widehat{G}$ можно взять свободное произведение с объединёнными подгруппами $\widehat{G} = (B \times G) \underset{H}{*} (H \times A)$, где A и B — произвольные нетривиальные группы с тривиальными центрами. Ясно, что $C(A) = H$ и $C(B) = G$, то есть решениями нашей системы уравнений являются в точности элементы группы G, k-е степени которых лежат в H. Согласно основной теореме число решений делится на $|C(A) \cap C(B)| = |H \cap G| = |H|$, что и требовалось.

Это доказательство следствия 4 использует лишь очень частный случай основной теоремы, когда формула φ представляет собой систему уравнений с одним неизвестным. В этом случае наша теорема немедленно вытекает из старого результата Ф. Холла (обобщающего теорему Фробениуса).

[*)] В 2017 году мы узнали, что этот факт был установлен в [Iwa82].

Теорема Холла ([Hall36], Теорема II). *В любой группе число решений системы уравнений с одним неизвестным делится на* НОД$(|C|, n_1, n_2, \ldots)$, *где C — это централизатор множества всех коэффициентов, а n_i — сумма показателей степеней при неизвестном в i-м уравнении.*

Трюк (но другой) с превращением произвольной подгруппы в централизатор также можно найти в [Hall36]. В параграфе 4 мы приведём прямое доказательство следствия 4, иллюстрирующее часть доказательства основной теоремы.

Аналогичным образом доказывается более общий факт.

Следствие 5. *Пусть H — подгруппа группы G и W — подгруппа (или подмножество) конечно порождённой группы F с бесконечным индексом коммутанта. Тогда число гомоморфизмов $f\colon F \to G$ таких, что $f(W) \subseteq H$, делится на $|H|$.*

Доказательство. Пусть группа F задаётся копредставлением $F = \langle X \mid R\rangle$. Тогда число интересующих нас гомоморфизмов равно числу решений системы уравнений

$$\left(\bigwedge_{r\in R}(r=1)\right) \wedge \left(\bigwedge_{a\in A,\ w\in W}([w,a]=1)\right) \wedge \left(\bigwedge_{b\in B\ x\in X}([x,b]=1)\right) \quad \text{с множеством неизвестных } X$$

в группе $\widehat{G} = (B\times G) \underset{H}{*} (H\times A)$, где A и B — произвольные нетривиальные группы с тривиальными центрами. Ранг матрицы этой системы совпадает с рангом матрицы системы $\{r = 1\,;\ r\in R\}$ (так как остальные уравнения коммутаторные) и меньше числа неизвестных X, поскольку индекс коммутанта группы $F = \langle X \mid R\rangle$ бесконечен. Согласно следствию 1 число решений делится на $|C(A)\cap C(B)| = |H\cap G| = |H|$, что и требовалось.

Отметим, что следствие 5 превращается в следствие 4 в случае $F = \mathbb{Z}$ и в теорему Гордона–Родригеса-Виллегаса в случае $H = G$.

2. Примеры

Начнём с любопытного примера применения теоремы Соломона.

Пример 1. Скажем, что два элемента группы принадлежат одному *племени*, если их квадраты равны. Ясно, что суммарная численность всех племён равна порядку группы. Менее очевидно, что

сумма 2022-х степеней численностей племён всегда делится на порядок группы.

Для доказательства этого факта достаточно рассмотреть систему уравнений $x_1^2 = \ldots = x_{2022}^2$. Число решений, очевидно, равно сумме 2022-х степеней численностей племён, а уравнений меньше чем неизвестных. Остаётся сослаться на теорему Соломона. Утверждение останется справедливым, если 2022 заменить на любое натуральное число; квадраты в определении племени тоже можно заменить на любые (одинаковые) натуральные степени.

Пример 2. *Число пар элементов группы, произведение квадратов которых является кубом, делится на порядок группы.* Это вытекает из следствия 3, поскольку в формуле $\exists z\ x^2y^2 = z^3$ одна связанная переменная, она входит один раз, равенств без связанных переменных нет, граф связный, свободных переменных две: $1+0+1 < 2+1$. Правда, этот факт легко вывести из теоремы Гордона–Родригеса-Виллегаса о сопряжённости. Действительно, эта теорема, в частности, означает, что на порядок группы делится число пар элементов группы, произведение квадратов которых сопряжено любому заданному элементу. По тем же причинам *на порядок группы делятся, например, следующие числа:*

- *число пар некоммутирующих элементов группы, произведение квадратов которых является кубом нецентрального элемента;*
- *число пар некоммутирующих элементов группы, произведение квадратов которых является кубом тогда и только тогда, когда куб их произведения лежит в центре;*
- *число пар элементов группы, у которых либо произведение квадратов является кубом, либо коммутатор не является квадратом;*
- $\ldots$

Пример 3. *На порядок группы делится число пар элементов этой группы, произведение квадратов которых является кубом коммутатора ($x_1^2x_2^2 = [z,t]^3$), а квадрат произведения — коммутатором кубов тех же элементов* ($(x_1x_2)^2 = [z^3,t^3]$). Этот факт уже затруднительно вывести из теоремы Гордона–Родригеса-Виллегаса о сопряжённости, но он немедленно вытекает из нашей основной теоремы. В силу следствие 2 верен более общий факт:

на порядок группы делится число пар элементов, квадрат произведения которых и произведение квадратов которых одновременным сопряжением могут быть превращены в любую фиксированную пару элементов.

Аналогия между теоремой Гордона–Родригеса-Виллегаса и всем известными свойствами решений систем линейных уравнений (скажем, над конечными полями) может навести на мысль, что если ранг матрицы намного меньше числа неизвестных, то число решений должно делиться на более высокую степень порядка группы. Более реалистичный вопрос следующий:

если конечно порождённая группа H допускает эпиморфизм на свободную группу ранга m, то верно ли, что число гомоморфизмов $H \to G$ делится на $|G|^m$?

Дело в том, что число решений системы уравнений $\{u(x_1,\dots,x_n) = v(x_1,\dots,x_n) = \dots = 1\}$ без коэффициентов равно числу гомоморфизмов из группы $H = \langle x_1,\dots,x_n \,|\, u(x_1,\dots,x_n) = v(x_1,\dots,x_n) = \dots = 1\rangle$ в группу G. Матрица системы имеет ранг не больше r тогда и только тогда, когда группа H обладает эпиморфизмом на свободную абелеву группу ранга $n - r$. Наличие эпиморфизма на абсолютно свободную группу такого ранга является гораздо более сильным свойством, но тем не менее гипотеза, о которой мы говорим, неверна при $m > 1$, как показывает следующий пример.

Пример 4. Группа $\langle x, y, z \,|\, z = z^x z^y\rangle$ обладает эпиморфизмом на свободную группу ранга два (посылающим z в единицу), но число решений уравнения $z = z^x z^y$ в симметрической группе S_3 не делится на $|S_3|^2 = 36$. Действительно, при $z = 1$ мы имеем 36 решений (x и y могут принимать любые значения). При $z = (123)$ мы имеем $3 \cdot 3 = 9$ решений (x и y — любые транспозиции). При $z = (321)$ аналогично имеем ещё 9 решений. А если z — транспозиция, то решений нет (по соображениям чётности). Всего получается $36 + 2 \cdot 9$ решений.

3. Доказательство основной теоремы

Лемма 1. *В условиях теоремы обратимой заменой свободных переменных можно добиться того, что первый столбец матрицы $A(\varphi)$ станет нулевым. В частности, в каждый цикл графа $\Gamma(\varphi)$ переменная x_1 будет входить в нулевой суммарной степени.*

Доказательство. Ранг матрицы $A(\varphi)$ меньше чем число её столбцов, поэтому, как известно, целочисленными (обратимыми) элементарными преобразованиями столбцов её можно превратить в матрицу с нулевым первым столбцом. Элементарные преобразования столбцов происходят при очевидных заменах переменных, например, замена $x_i \to x_i x_j^k$ даёт прибавление к j-му столбцу i-го столбца, умноженного на k. Лемма 1 доказана.

Например, чтобы обнулить первый столбец матрицы (2) из параграфа 1, достаточно из первого столбца вычесть второй, то есть в формуле (1) надо сделать замену переменных $x_2 \to x_2 x_1^{-1}$. Формула (1) примет вид

$$\forall y \exists z \ \left(\left([ygy, x_1 g x_2 x_1^{-1}] x_1 a^z (x_2 x_1^{-1})^{-3} x_1^3 h (x_2 x_1^{-1})^7 = 1\right) \wedge \neg \left(b^z x_2^2 = 1\right) \vee \left(x_1^2 (x_2 x_1^{-1})^2)^5 = 1\right)\right), \qquad (3)$$

её граф изображён на рисунке 2

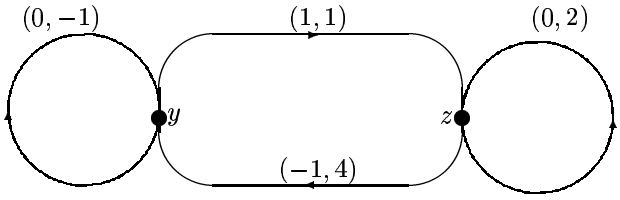


Рис. 2

и её матрица имеет вид

$$\begin{pmatrix} 0 & -1 \\ 0 & 5 \\ 0 & 2 \\ 0 & 10 \end{pmatrix}.$$

Далее считаем, что в каждый цикл графа $\Gamma(\varphi)$ переменная x_1 входит в нулевой суммарной степени.

Для каждой переменной t (свободной или связанной) введем новые символы $t^{(i)}$, где $i \in \mathbb{Z}$ (смысл их будет состоять в том, что $t^{(i)} = t^{x_1^i} = x_1^{-i} t x_1^i$, если переменная t неизолирующая, и $t^{(i)} = t x_1^i$, если переменная t изолирующая, но мы пока действуем чисто формально). Аналогично для каждого неизолированного коэффициента g введём новые символы $g^{(i)}$, где $i \in \mathbb{Z}$. Преобразуем формулу φ следующим образом:

1) заменим в атомарных подформулах каждый символ t на $t^{(0)}$, где t — переменная, отличная от x_1, или коэффициент;
2) каждое подслово вида $(t^{(i)})x_1^l$, где t — неизолирующая переменная или коэффициент, заменим на слово $x_1^l(t^{(i+l)})$; каждое подслово вида $(g^{t^{(i)}})x_1^l$, где t — изолирующая переменная и $g \in G$, заменим на слово $x_1^l(g^{t^{(i+l)}})$;
3) повторим шаг 2) до тех пор, пока это возможно.

После такого сдвига влево символов x_1 мы получим формулу, не содержащую x_1 (из того, что сумма степеней при x_1 равна нулю и в каждом цикле графа, и в каждой атомарной подформуле без связанных переменных следует, что сумма степеней при x_1 равна нулю во всех атомарных подформулах). Например, формула (3) после этих преобразований будет иметь следующие атомарные подформулы:

$$\begin{aligned}[y^{(0)}g^{(0)}y^{(0)}, g^{(-1)}x_2^{(-1)}]a^{z^{(-1)}}\left(x_2^{(-4)}x_2^{(-3)}x_2^{(-2)}\right)^{-1}h^{(-7)}x_2^{(-7)}x_2^{(-6)}x_2^{(-5)}x_2^{(-4)}x_2^{(-3)}x_2^{(-2)}x_2^{(-1)} &= 1,\\ b^{z^{(0)}}(x_2^{(0)})^2 &= 1,\\ (x_2^{(-2)}x_2^{(-1)})^5 &= 1.\end{aligned} \tag{4}$$

Теперь продолжим преобразование формулы:

4) В каждой атомарной подформуле α заменим все входящие в неё символы $t^{(i)}$ на $t^{(i+j_\alpha)}$, где целые числа j_α подберём таким образом, чтобы для каждой связанной переменной t символы $t^{(i)}$ встречались во всей формуле не более чем при одном значении i; это возможно из-за того, что сумма степеней при x_1 равна нулю в каждом цикле графа.

   В рассматриваемом примере (4) достаточно уменьшить на единицу верхние индексы во втором равенстве. В общем случае следует действовать так. В каждой компоненте связности K графа Γ выберем вершину (переменную) y_K. В каждой атомарной подформуле α, содержащем связанные переменные, выберем одну из таких переменных y_α. Соединим каждую вершину y_α путём p_α с вершиной y_K такой, что $y_\alpha \in K$. Сумма s_α первых координат меток рёбер пути p_α не зависит от выбора пути по условию. Положим $j_\alpha = -i_\alpha - s_\alpha$, где i_α — такое единственное число, что $y_\alpha^{(i_\alpha)}$ входит в уравнение α. То, что сумма первых координат меток рёбер в каждом цикле равна нулю, означает, что $s_\alpha = s_\beta$, если $y_\alpha = y_\beta$, величина j_α не зависит от выбора переменных y_α, входящих в уравнение α, и после замен $t^{(i)}$ на $t^{(i+j_\alpha)}$ в каждом уравнении α каждая связанная переменная t будет входить во всю формулу только с одним индексом (i), где i есть сумма первых координат меток рёбер пути, соединяющего y_K с t.
5) Заменим в каждой кванторной приставке $\forall y$ и $\exists y$ на $\forall y^{(p)}$ и $\exists y^{(p)}$, где $p \in \mathbb{Z}$ — такое единственное число, что $y^{(p)}$ встречается в атомарных подформулах;
6) добавим к полученной формуле $\widehat{\varphi}$ равенства, определяющие новые символы, то есть заменим $\widehat{\varphi}$ на бесконечную формулу

$$\varphi' = \widehat{\varphi} \wedge \underbrace{\left(\bigwedge_g \left(g^{(0)} = g\right)\right) \wedge \left(\bigwedge_{t,i} \left(t^{(i)} = x_1^{-1}t^{(i-1)}x_1\right)\right)}_{\delta}, \tag{**}$$

   где t пробегает все свободные переменные и все коэффициенты исходной формулы, i пробегает все целые числа, а g пробегает все коэффициенты. Символы $g^{(i)}$, где $g \in G$, мы тоже считаем свободными переменными формулы φ'.

Полученной формуле φ' удовлетворяет столько же наборов элементов группы, сколько удовлетворяет исходной формуле φ. Действительно, формуле $\varphi' = \widehat{\varphi} \wedge \delta$ удовлетворяет, очевидно, столько же наборов, сколько формуле $\overline{\varphi} = \widehat{\varphi}\big|_{t^{(i)}=t^{x_1^i}}$ (то есть формуле $\widehat{\varphi}$, в которую вместо каждого символа $t^{(i)}$, где t — свободная переменная исходной формулы или коэффициент, подставлено выражение $x_1^{-i}tx_1^i$). Формула $\overline{\varphi}$ эквивалентна формуле φ (то есть этим формулам удовлетворяют одни и те же наборы). Действительно, формула $\overline{\varphi}$ отличается от формулы φ двумя моментами:

а) в кванторных приставках вместо символов y стоят символы $y^{(p)}$;
б) в атомарных подформулах вместо связанных переменных y стоят выражения $(y^{(p)})x_1^{-p}$ или $(y^{(p)})^{x_1^{-p}}$, в зависимости от того, является ли переменная y изолирующей, где p одно и то же для всех вхождений переменной y.

Но формулы, отличающиеся только этим, очевидно эквивалентны: например, $(\forall y\, \alpha(y, z, \ldots)) \equiv (\forall t\, \alpha(t^{z^2}, z, \ldots))$, так как для любого $g \in G$ верно, что если y пробегает всё группу, то y^g пробегает всю группу.

Таким образом, нам достаточно показать, что число наборов, удовлетворяющих формуле φ' (такие наборы мы будем называть *решениями*), делится на $|C|$, где буквой C мы обозначили централизатор множества всех коэффициентов формулы φ (или φ', что то же самое).

Рассмотрим одно решение $X = \left(\widetilde{x}_1,\, \widetilde{x}_i^{(j)},\, \widetilde{g}^{(j)}\ i = 2, \ldots, n,\ j \in \mathbb{Z}\right)$. Набор $\left(\widetilde{x}_i^{(j)},\, \widetilde{g}^{(j)}\right)$, то есть всё, кроме $\widetilde{x}_1$, будем называть *хвостом* решения X. Буквой B_X мы обозначим централизатор хвоста решения X. Заметим, что $B_X \subseteq C$ (из-за уравнений $g^{(0)} = g$ в формуле $(**)$).

Будем говорить, что два решения *похожи*, если их хвосты сопряжены при помощи какого-то элемента из C. Ясно, что это отношение эквивалентности. Теорема очевидным образом вытекает из следующего утверждения.

Утверждение. *В каждом классе похожих решений содержится ровно $|C|$ решений.*

Найдем число решений, похожих на X. Число возможных хвостов таких решений равно $|C|/|B_X|$, так как на множестве хвостов решений, похожих на X, группа C действует сопряжением (так как набор, сопряжённый при помощи $c \in C$ к хвосту любого решения Y также является хвостом некоторого решения, например, Y^c) и B_X — это стабилизатор хвоста решения X.

Число решений с таким же хвостом, как у X, равно $|B_X|$, поскольку если набор с тем же хвостом и первой координатой $\widetilde{x}_1'$ тоже является решением, то частное $\widetilde{x}_1'(\widetilde{x}_1)^{-1}$ должно коммутировать с хвостом, как показывают уравнения δ в формуле $(**)$, то есть $\widetilde{x}_1' \in B_X\widetilde{x}_1$. С другой стороны, любой элемент $\widetilde{x}_1' \in B_X\widetilde{x}_1$ даёт решение с тем же хвостом, так как переменная x_1 входит в формулу φ' только в подформуле δ.

Если X' — решение, похожее на X, то число решений с таким же хвостом, как у X', равно $|B_{X'}| = |B_X|$ (раз хвосты сопряжены, то их централизаторы сопряжены и имеют одинаковые порядки).

В итоге получаем, что число решений, похожих на X, равно $(|C|/|B_X|) \cdot |B_X| = |C|$, что и доказывает утверждение, а вместе с ним и теорему.

4. Корни из подгрупп

В параграфе 1 следующее утверждение было выведено из основной теоремы.

Следствие 4. *Число элементов группы, k-е степени которых лежат в данной подгруппе, делится на порядок этой подгруппы.*

Здесь мы приведём прямое доказательство с целью продемонстрировать заключительную часть доказательства основной теоремы на простом примере.

Будем для простоты предполагать, что $k = 2$. Итак, есть группа G и её подгруппа H. Нас интересуют элементы $x \in G$ такие, что $x^2 \in H$, такие элементы мы называем *решениями*. Утверждение немедленно вытекает из следующей леммы.

Лемма. *В каждом двойном смежном классе HxH содержится либо 0, либо $|H|$ решений.*

Доказательство. Пусть x — решение, его *хвостом* мы назовём смежный класс Hx.

Группа H действует (справа) на множестве хвостов решений из двойного смежного класса HxH умножением справа:

$$Hy \circ h = Hyh\ (= \textit{хвост решения } y^h).$$

Стабилизатор хвоста Hx — это $B_x \stackrel{\text{опр}}{=} H \cap H^x$:

$$Hx = Hxh \iff h \in H^x.$$

Значит, *у всевозможных решений, лежащих в HxH, ровно $|H|/|B_x|$ различных хвостов.*

Сколько решений имеет такой же хвост, как x?

$$Hx = Hy \Longrightarrow yx^{-1} \in H,$$

но если при этом y тоже является решением, то

$$(Hx)x = Hx^2 = H = Hy^2 = (Hx)y,$$

то есть

$$yx^{-1} \in H^x.$$

Таким образом, каждое решение y с таким же хвостом, как у x, лежит в B_xx. С другой стороны, каждый элемент из этого смежного класса является решением:

$$(bx)^2 = bxbx = bb^{x^{-1}}x^2 \in H, \quad \text{так как } b,\ b^{x^{-1}} \text{ и } x^2 \text{ лежат в } H.$$

Получается, что *число решений с таким же хвостом, как у x, равно* $|B_x|$.

Так как $|B_x| = |B_y|$, если x и y лежат в одном двойном смежном классе по H (поскольку B_x и B_y сопряжены в этом случае), всего получается $|B_x| \cdot (|H|/|B_x|) = |H|$ решений, что и завершает доказательство.

Недавно И. М. Айзекс [Isaa12] получил получил доказательство этого следствия, опирающееся на теорию характеров.

В 2017 году мы узнали, что это следствие было получено в [Iwa82].

ГЛАВА 4.
СТРАННАЯ ДЕЛИМОСТЬ В ГРУППАХ И В КОЛЬЦАХ

0. Введение

Отправной точкой нашего исследования послужил следующий результат, обобщающий одну старую теорему Соломона [Solo69].

Теорема Гордона–Родригеса-Виллегаса [GRV12]. *Пусть F — конечно порождённая группа с бесконечным индексом коммутанта, а G — произвольная группа. Тогда число гомоморфизмов $F \to G$ делится на порядок группы G.*

Эта теорема говорит, по сути, о числе решений систем бескоэффициентных уравнений в группе. В работе [KM14] этот результат был обобщен на системы уравнений с коэффициентами и даже на произвольные формулы первого порядка в групповом языке (с константами).

Основная теорема настоящей работы претендует на звание «максимального» обобщения результата Гордона–Родригеса-Виллегаса (хотя такую максимальность доказать невозможно). Формулировку основной теоремы читатель может найти в первом параграфе, а её (вполне элементарное) доказательство — в последнем. Грубо говоря, основная теорема утверждает, что делимость сохранится, если рассматривать не все гомоморфизмы, а их подмножество, от которого требуется инвариантность относительно некоторых естественных операциях над гомоморфизмами. Одним из следствий основной теоремы является неожиданный факт, упомянутый в аннотации:

> *в любой группе G число порождающих наборов $(g_1, \dots, g_{2022}) \in G^{2022}$ (то есть таких наборов, что $G = \langle g_1, \dots, g_{2022} \rangle$) всегда делится на порядок коммутанта группы G.*

Это и иные теоретико-групповые следствия мы доказываем в параграфе 2. Удивительно, но этот результат кажется новым, хотя известно много близких фактов о делимости функции Мёбиуса (которая связана с числом порождающих наборов формулой Холла [Hall36a]), см., например, [Bro00], [HIÖ89], [KT84] и литературу там цитируемую). О других не очень широко известных, но красивых фактах о системах порождающих в группах мы советуем почитать в [Coll10].

Основная теорема является утверждением о группах, но (как это ни парадоксально) имеет нетривиальные теоретико-кольцевые следствия. В параграфе 3 мы выводим из основной теоремы теоретико-кольцевой аналог теоремы Гордона–Родригеса-Виллегаса (точнее говоря, аналог обобщения этой теоремы, полученного в [KM14] и говорящего об уравнениях с коэффициентами). Частным случаем этой теоремы об уравнениях над кольцами является факт, упомянутый в аннотации, или, например, следующее утверждение высшего порядка:

> *в любом ассоциативном кольце R с единицей число наборов обратимых элементов $(a, b, \dots, z) \in (R^*)^{26}$ таких, что $a^{2022} + b^{2022} + \dots + z^{2022} = 0$, делится на порядок мультипликативной группы этого кольца, то есть на $|R^*|$.*

Обозначения, которые мы используем, в целом стандартны. Отметим только, что если $k \in \mathbb{Z}$, а x и y — элементы некоторой группы, то x^y, x^{ky} и x^{-y} обозначают $y^{-1}xy$, $y^{-1}x^k y$ и $y^{-1}x^{-1}y$, соответственно. Коммутант группы G мы обозначаем G'. Если X — подмножество некоторой группы, то $|X|$, $\langle X \rangle$, $\langle\langle X \rangle\rangle$ и $C(X)$ означают, соответственно, мощность множества X, подгруппу, порождённую множеством X, нормальное замыкание множества X и централизатор множества X. Индекс подгруппы H группы G обозначается $|G : H|$. Символ $N(H)$ обозначает нормализатор подгруппы H (в группе G). Свободное произведение групп A и B мы обозначаем символом $A * B$, а свободную группу с базисом $x_1, \dots, x_n$ — символом $F(x_1, \dots, x_n)$. Если R — ассоциативное кольцо с единицей, то R^* обозначает группу обратимых элементов этого кольца.

Отметим ещё, что в почти всех утверждениях о делимости в данной работе (например, в вышеупомянутой теореме Гордона–Родригеса-Виллегаса) необязательно предполагать, что соответствующая группа конечна. Делимость можно понимать в смысле кардинальной арифметики: бесконечный кардинал делится на все ненулевые кардиналы, не превосходящие его. Единственное место, где нам действительно нужна конечность — это теорема о мономорфизмах и подгруппах в параграфе 2, смотрите замечание после этой теоремы.

1. Основная теорема

Группу F с фиксированным эпиморфизмом $F \to \mathbb{Z}$ мы называем *индексированной* группой. Этот эпиморфизм $F \to \mathbb{Z}$ мы называем *степенью* и обозначаем deg; таким образом, для любого элемента f индексированной группы F определено целое число $\deg f$, причём группа F содержит элементы всех целых степеней и $\deg(fg) = \deg f + \deg g$ для любых $f, g \in F$.

Пусть имеется гомоморфизм $\varphi\colon F \to G$ из индексированной группы F в какую-то группу G и подгруппа H группы G. Мы называем подгруппу

$$H_\varphi = \bigcap_{f \in F} H^{\varphi(f)} \cap C(\{\varphi(f) \mid \deg f = 0\})$$

φ-сердцевиной подгруппы H. Другими словами, φ-сердцевина H_φ подгруппы H состоит из таких её элементов h, что $h^{\varphi(f)} \in H$ для всех f, причём $h^{\varphi(f)} = h$, если $\deg f = 0$.

Основная теорема. *Пусть H — подгруппа некоторой группы G и Φ — некоторое множество гомоморфизмов из индексированной группы F в G, причём множество Φ обладает следующими двумя свойствами.*

I. *Φ инвариантно относительно сопряжения элементами из H:*

$$\text{если } h \in H \text{ и } \varphi \in \Phi, \text{ то гомоморфизм } \psi\colon f \mapsto \varphi(f)^h \text{ тоже лежит в } \Phi.$$

II. *Для любого $\varphi \in \Phi$ любого элемента h из φ-сердцевины H_φ подгруппы H гомоморфизм ψ, определённый правилом*

$$\psi(f) = \begin{cases} \varphi(f) & \text{для всех элементов } f \in F \text{ степени ноль;} \\ \varphi(f)h & \text{для некоторого элемента } f \in F \text{ степени один (а значит и для всех элементов степени один),} \end{cases}$$

также содержится в Φ.

Тогда $|\Phi|$ делится на $|H|$.

Отметим, что отображение ψ из условия I является гомоморфизмом при любом $h \in G$, а формула для ψ из условия II определяет гомоморфизм при любом $h \in C(\varphi(\ker\deg))$ (смотрите лемму 0). Смысл условий I и II состоит в том, что эти гомоморфизмы лежат в Φ (при некоторых дополнительных предположениях об h).

Лемма 0. *Пусть $\varphi\colon F \to G$ — это гомоморфизм из индексированной группы F в некоторую группу G, f_1 — элемент степени один группы F и $g \in G$. Тогда*

1) *гомоморфизм $\psi\colon F \to G$ такой, что $\psi(f) = \varphi(f)$ для всех f степени ноль и $\psi(f_1) = \varphi(f_1)g$, существует тогда и только тогда, когда $g \in C(\varphi(\ker\deg))$;*
2) *если такой гомоморфизм ψ существует и H — это подгруппа в G, то $\psi(f)H = \varphi(f)H$ для всех $f \in F$ тогда и только тогда, когда $g \in H_\varphi$.*

Доказательство. Заметим, что F раскладывается в полупрямое произведение $F = \langle f_1 \rangle_\infty \leftthreetimes \ker\deg$. Это означает, что отображение $\alpha\colon \ker\deg \cup \{f_1\} \to G$ продолжается до гомоморфизма тогда и только тогда, гкогда его ограничение на $\ker\deg$ является гомоморфизмом и $\alpha(f^{f_1}) = \alpha(f)^{\alpha(f_1)}$ для всех $f \in \ker\deg$. Таким образом, для всех $f \in \ker\deg$ мы имеем $\psi(f^{f_1}) = \varphi(f^{f_1}) = \varphi(f)^{\varphi(f_1)}$ и $\psi(f)^{\psi(f_1)} = \varphi(f)^{\varphi(f_1)g}$. Значит, $\psi(f^{f_1}) = \psi(f)^{\psi(f_1)}$ для всех $f \in \ker\deg$ тогда и только тогда, когда $\varphi(x)^g = \varphi(x)$ для всех $x \in \ker\deg$. Это доказывает первое утверждение.

Чтобы доказать 2), заметим, что каждый $f \in F$ имеет вид $f = f_1^k x$, где $x \in \ker\deg$ и $k \in \mathbb{Z}$. Таким образом,

$$\psi(f)H = \psi(f_1)^k\psi(x)H = \psi(f_1)^k\varphi(x)H = (\varphi(f_1)g)^k\varphi(x)H \mathrel{=\!=} \varphi(f_1)^k\varphi(x)H = \varphi(f_1^k x)H = \varphi(f)H$$

(где равенство $=\!=$ выполняется, поскольку $\varphi(F)$ нормализует H_φ и $g \in H_\varphi \subseteq H$). Это доказывает утверждение 2) в одну сторону. Доказательство в другую сторону мы оставляем читателям в качестве упражнения (поскольку мы не будем это использовать).

2. Применения. Группы

Прежде всего заметим, что условия основной теоремы очевидно выполняются, если в качестве Φ взять множество всех гомоморфизмов $F \to G$ (а в качестве H взять любую подгруппу группы G, например, всю группу G). Поэтому теорема Гордона–Родригеса-Виллегаса является простейшим частным случаем основной теоремы.

Теорема об уравнениях над группами [KM14]. *Число решений (в G) системы уравнений $\{v_i(x_1, \dots, x_n) = 1\}$ над группой G (где $v_i(x_1, \dots, x_n) \in G * F(x_1, \dots, x_n)$) делится на порядок централизатора множества всех коэффициентов, если ранг матрицы, состоящей из сумм показателей при i-м неизвестном в j-м уравнении, меньше числа неизвестных.*

Доказательство. Пусть $A \subseteq G$ — подгруппа, порождённая всеми коэффициентами всех уравнений. В качестве группы F мы возьмём факторгруппу $F = (A * F(x_1, \dots, x_n))/\langle\langle\{v_i\}\rangle\rangle$ свободного произведения $A * F(x_1, \dots, x_n)$ группы A и свободной группы по нормальной подгруппе $\langle\langle\{v_i\}\rangle\rangle$, порождённой левыми частями уравнений. В качестве множества Φ мы рассмотрим гомоморфизмы $F \to G$, тождественные на A. (Мы предполагаем, что A вкладывается в F посредством естественного отображения $A \to F$, поскольку если это отображение не инъективно, то решений нет и доказывать нечего.) Ясно, что решения системы уравнений находятся в естественном взаимно однозначном соответствии с элементами множества Φ.

Условие на ранг означает, что группа F обладает эпиморфизмом на $\mathbb{Z}$, ядро которого содержит A. Если теперь в качестве H взять централизатор подгруппы A в G, то условия основной теоремы окажутся очевидным образом выполненными. Действительно, I выполняется, поскольку h централизует $A \subseteq G$ и, следовательно, ψ совпадает с φ на $A \subset F$, а II выполнено, поскольку элементы из $A \subset F$ имеют степень ноль и, значит, опять ψ совпадает с φ на $A \subset F$.

Теорема о корне из подгруппы [KM14]. *Число элементов g произвольной группы G таких, что $g^n \in H$, делится на $|H|$ для любой подгруппы H группы G и любого целого n.*[*)]

Теорема о корне из подгруппы является простейшим частным случаем следующего факта.

Теорема о гомоморфизмах и подгруппах [KM14]. *Пусть H — подгруппа группы G, а W — подгруппа (или подмножество) конечно порождённой группы F и индекс коммутанта $|F : F'|$ бесконечен. Тогда число гомоморфизмов $\varphi\colon F \to G$ таких, что $\varphi(W) \subseteq H$, делится на $|H|$.*

Мы докажем ещё более общее утверждение.

Теорема о гомоморфизмах и двойных смежных классах. *Пусть H — подгруппа группы G, а W — подмножество конечно порождённой группы F и индекс коммутанта $|F : F'|$ бесконечен. Пусть $W \ni w \mapsto g_w \in G$ — произвольное отображение $W \to G$. Тогда число гомоморфизмов $\varphi\colon F \to G$ таких, что $\varphi(w) \in Hg_wH$ для всех $w \in W$, делится на $|H|$.*

Доказательство. Выберем какой-нибудь эпиморфизм $\deg\colon F \to \mathbb{Z}$ (который существует, поскольку F/F' является бесконечной конечно порождённой абелевой группой) и возьмём в основной теореме в качестве Φ множество всех гомоморфизмов $\varphi\colon F \to G$ таких, что $\varphi(w) \in Hg_wH$ для всех $w \in W$. Условия основной теоремы выполняются. Для условия I это совсем очевидно. А что касается условия II, то достаточно заметить, что из формулы для ψ вытекает равенство $\psi(f)H = \varphi(f)H$ для всех $f \in F$ по лемме 0.

Следующую теорему можно назвать «эпиморфным аналогом» теоремы Гордона–Родригеса-Виллегаса.

Теорема об эпиморфизмах. *Пусть F — конечно порождённая группа с бесконечным индексом коммутанта, а G — произвольная группа. Тогда число сюръективных гомоморфизмов $F \to G$ делится на порядок коммутанта группы G.*

Доказательство. Рассмотрим какой-нибудь эпиморфизм $\deg\colon F \to \mathbb{Z}$, возьмём качестве Φ множество всех эпиморфизмов $F \to G$ и положим $H = G'$. Проверим, что условия основной теоремы выполняются. Для условия I это очевидно.

Проверим условие II. Мы должны показать, что для любого эпиморфизма $\varphi\colon F \to G$ и любого элемента $h \in G'$, централизующего подгруппу $\varphi(\ker\deg)$, гомоморфизм ψ, определённый равенствами из условия II основной теоремы является сюръективным. По модулю G' гомоморфизм ψ сюръективен (то есть $\psi(F)G' = G$), поскольку он равен φ по модулю G'. Осталось показать, что каждый элемент $g \in G'$ лежит в образе гомоморфизма ψ. Пользуясь сюръективностью гомоморфизма φ, найдём $f \in F$ такой, что $\varphi(f) = g$; причём элемент f можно найти в коммутанте группы F (поскольку для эпиморфизма образ коммутанта равен коммутанту образа). Но тогда $f \in \ker\deg$ и, следовательно, $\psi(f) = \varphi(f) = g$, что и требовалось.

*) В 2017 году мы узнали, что этот факт был установлен в [Iwa82].

Замечание. Число сюръективных гомоморфизмов $F \to G$ делится на $|\operatorname{Aut} G|$, поскольку $\operatorname{Aut} G$ естественным образом точно действует на множестве эпиморфизмов $F \to G$. Однако теорема об эпиморфизмах не вытекает немедленно из этого наблюдения, поскольку, как нам любезно подсказал А. В. Васильев,

существует группа G такая, что $|\operatorname{Aut} G|$ не делится на $|G'|$.

Примерами таких групп могут служить группы $3 \cdot A_6$ и $3 \cdot A_7$ (см., например, [Wils09]) порядков $\frac{3}{2} \cdot 6! = 1080$ и $\frac{3}{2} \cdot 7! = 7560$, совпадающие с коммутантами и имеющие центры порядка три, факторгруппы по которым суть знакопеременные группы A_6 и A_7; при этом $|\operatorname{Aut}(3 \cdot A_6)| = 2 \cdot 6!$, а $\operatorname{Aut}(3 \cdot A_7)$ есть просто симметрическая группа порядка 7!. На самом деле, как показали Савелий Скресанов и Дмитрий Чуриков (с помощью GAPа), наименьшая группа G такая, что $|G'| \not| |\operatorname{Aut} G|$ имеет порядок 108.

Следствие о системах порождающих в группах. *Для каждой группы G и для каждого натурального числа n число наборов $(g_1, \ldots, g_n) \in G^n$ элементов группы G, порождающих группу G (то есть таких наборов, что $\langle g_1, \ldots, g_n \rangle = G$), всегда делится на $|G'|$.*

Доказательство. Порождающие наборы длины n находятся в естественном взаимно однозначном соответствии с эпиморфизмами из свободной группы ранга n в G. Поэтому утверждение немедленно вытекает из теоремы об эпиморфизмах.

Разумеется, ни в теореме об эпиморфизмах, ни в её следствии делимость на $|G'|$ нельзя усилить до делимости на $|G|$, как показывает пример группы простого порядка — число порождающих наборов длины n в такой группе очевидно равно $|G|^n - 1$.

Следующая теорема обобщает предыдущую и является аналогом теоремы о гомоморфизмах и подгруппах.

Теорема об эпиморфизмах и подгруппах. *Пусть A — подгруппа группы G и W — подгруппа конечно порождённой группы F и индекс коммутанта $|F : F'|$ бесконечен. Тогда число гомоморфизмов $\varphi\colon F \to G$ таких, что $\varphi(W) = A$, делится на $|A'|$.*

Доказательство. Рассмотрим какой-нибудь эпиморфизм $\deg\colon F \to \mathbb{Z}$ и положим

$$\Phi = \{\textit{гомоморфизмы } \varphi\colon F \to G \textit{ такие, что } \varphi(W) = A\} \quad \text{и} \quad H = A'.$$

Проверим, что условия основной теоремы выполняются. Для условия I это очевидно.

Проверим условие II. Мы должны показать, что для любого гомоморфизма $\varphi\colon F \to G$ такого, что $\varphi(W) = A$, и любого элемента $h \in A'$, централизующего подгруппу $\varphi(\ker \deg)$, гомоморфизм ψ, определённый равенствами из условия II, также удовлетворяет равенству $\psi(W) = A$. Включение $\psi(W) \subseteq A$, разумеется, выполняется. Для доказательства обратного включения сперва заметим, что ограничение гомоморфизма $\psi(W)A' = A$. Осталось показать, что каждый элемент $a \in A'$ лежит в $\psi(W)$. Воспользовавшись равенством $\varphi(W) = A$, найдём $w \in W$ такой, что $\varphi(w) = a$; ясно, что такой w можно найти в коммутанте группы W. Но тогда $w \in \ker \deg$ и, следовательно, $\psi(w) = \varphi(w) = a$, что и требовалось.

Аналогичная теорема об инъективных гомоморфизмах тоже верна (для конечных групп G), причём с гораздо более хорошей делимостью.

Теорема о мономорфизмах и подгруппах. *Пусть A — подгруппа группы G, а W — подгруппа конечно порождённой группы F и индекс $|F : F'W|$ бесконечен. Тогда $|N(A)|$ делит следующие числа:*

а) *число гомоморфизмов $\varphi\colon F \to G$ таких, что ограничение φ на W инъективно и $\varphi(W) \subseteq A$;*

б) *число гомоморфизмов $\varphi\colon F \to G$ таких, что ограничение φ на W инъективно и $\varphi(W) = A$;*

Доказательство. Докажем а) (доказательство для б) вполне аналогично). Рассмотрим какой-нибудь эпиморфизм $\deg\colon F \to \mathbb{Z}$ такой, что $W \subseteq \ker \deg$ и положим

$$\Phi = \{\textit{гомоморфизмы } \varphi\colon F \to G \textit{ такие, что } \varphi(W) \subseteq A \textit{ и } \varphi|_W \textit{ инъективно}\} \quad \text{и} \quad H = N(A).$$

Проверим, что условия основной теоремы выполняются. Для условия I это очевидно. Условие II также очевидно, поскольку W содержится в ядре гомоморфизма $\deg$ и, следовательно, ψ и φ (из условия II) одинаково действуют на элементы подгруппы W.

Замечание. Условие бесконечности индекса $|F : WF'|$ нельзя заменить в последней теореме на бесконечность индекса коммутанта (несмотря на то, что делимость мы понимаем в смысле кардинальной арифметики). Действительно,

а) если $F = W = A = \mathbb{Z}$ and $G = \mathbb{R}$, то число инъективных гомоморфизмов равно $\aleph_0$ и не делится на $|N(A)| = |\mathbb{R}| = 2^{\aleph_0}$;

б) если $F = W = G = A = \mathbb{Z}$, то число инъективных гомоморфизмов равно двум и не делится на $|N(A)| = |\mathbb{Z}| = \aleph_0$.

3. Применения. Кольца

Под *обобщённо однородным* уравнением над ассоциативным кольцом R с множеством неизвестных X мы понимаем конечную запись вида

$$\sum_i \prod_j c_{ij} x_{ij}^{k_{ij}} = 0, \quad \text{где } \textit{коэффициенты } c_{ij} \in R, \textit{ неизвестные } x_{ij} \in X \text{ и } \textit{показатели } k_{ij} \in \mathbb{Z},$$

такую, что для некоторого ненулевого отображения $\deg\colon X \to \mathbb{Z}$ величина $\sum\limits_j k_{ij} \deg(x_{ij})$ не зависит от i (то есть «многочлен» в левой части уравнения является однородным относительно некоторого ненулевого приписывания степеней переменным*)). Систему уравнений мы называем обобщённо однородной, если все уравнения этой системы являются обобщённо однородными (возможно разных степеней) относительно одной и той же функции $\deg\colon X \to \mathbb{Z}$.

Для проверки обобщённой однородности можно воспользоваться следующим простым алгоритмом.

АЛГОРИТМ ПРОВЕРКИ ОБОБЩЁННОЙ ОДНОРОДНОСТИ СИСТЕМЫ

1. Для каждого уравнения $v = 0$ системы составить матрицу A_v из целых чисел a_{ij}, представляющих собой степени i-го монома относительно j-го неизвестного (то есть a_{ij} есть сумма показателей в i-м мономе выражения v при j-м неизвестном).
2. Вычесть из всех строк матрицы A_v первую строку этой матрицы. Сделать это для всех матриц A_v.
3. Получившиеся матрицы A'_v (с нулевыми первыми строками) написать друг под другом: $A' = \begin{pmatrix} A'_v \\ A'_w \\ \vdots \end{pmatrix}$.
4. Система обобщённо однородна тогда и только тогда, когда $\operatorname{rank} A'$ меньше числа неизвестных.

Например, для системы уравнений $\begin{cases} (xdy)^2 - yx^2 + xy^2cy^{-100}x = 0 \\ xy - yx = 0 \end{cases}$ (где $c, d \in R$ — коэффициенты, а x и y — неизвестные) мы получаем:

$$A_u = \begin{pmatrix} 2 & 2 \\ 2 & 1 \\ 2 & -98 \end{pmatrix},\ A_v = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix},\quad A'_u = \begin{pmatrix} 0 & 0 \\ 0 & -1 \\ 0 & -100 \end{pmatrix},\ A'_v = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},\quad A' = \begin{pmatrix} 0 & 0 \\ 0 & -1 \\ 0 & -100 \\ 0 & 0 \\ 0 & 0 \end{pmatrix},$$

$\operatorname{rank} A' = 1$ и система является обобщённо однородной.

Утверждение. *Всякая система уравнений, в которой*

$$\sum_i \Big((\textit{число мономов в } i\textit{-м уравнении}) - 1 \Big) < (\textit{число неизвестных}),$$

является обобщённо однородной.

Доказательство. Утверждение немедленно вытекает из приведённого выше алгоритма, но доказательство корректности этого алгоритма мы оставляем читателю в качестве упражнения. (В дальнейшем мы не будем использовать ни это утверждение, ни этот алгоритм.)

Понятие *решения* системы уравнений определяется естественным образом (если среди показателей k_{ij} есть отрицательные числа, то соответствующие компоненты решения обязаны быть обратимыми элементами кольца).

Теорема об уравнениях над кольцами. *Пусть R — ассоциативное кольцо с единицей, и G — подгруппа мультипликативной группы этого кольца. Тогда для каждой обобщённо однородной системы уравнений над R от n неизвестных число её решений, лежащих в G^n, делится на порядок пересечения группы G с централизатором множества всех коэффициентов системы.*

Доказательство. Нужно применить основную теорему, взяв в качестве F свободную группу $F(x_1, \ldots, x_n)$ и продолжить отображение $\deg\colon \{x_1, \ldots, x_n\} \to \mathbb{Z}$ (из определения обобщённо однородной системы) до гомоморфизма $F \to \mathbb{Z}$, который можно считать сюръективным, поскольку он ненулевой. В качестве Φ следует взять множество всех гомоморфизмов $\varphi\colon F \to G$ таких, что набор $(\varphi(x_1), \ldots, \varphi(x_n))$ является решением нашей системы уравнений, а в качестве H следует взять пересечение группы G с централизатором множества всех коэффициентов системы.

*) Переменная может иметь степень ноль, но важно, что не все переменные имеют степень ноль.

Проверим, что условия основной теоремы выполнены. Условие I очевидно выполнено. Для проверки условия II выберем элемент $t \in F$ степени один и запишем каждую переменную x_i в виде $x_i = t^{\deg x_i} y_i$, где $y_i = t^{-\deg x_i} x_i$ имеет степень ноль.

Рассмотрим уравнение $w(x_1, \dots, x_n) = 0$ нашей системы. В новых обозначениях оно перепишется в виде $v(t, y_1, \dots, y_n) = 0$, причём в силу однородности каждое слагаемое в выражении $v(t, y_1, \dots, y_n)$ будет иметь одну и ту же степень k относительно переменной t.

Нам надо показать, что если $v(\varphi(t), \varphi(y_1), \dots, \varphi(y_n)) = 0$ и $h \in H_\varphi$, то $v(\varphi(t)h, \varphi(y_1), \dots, \varphi(y_n)) = 0$. Чтобы в этом убедиться достаточно заметить, что $v(\varphi(t)h, \varphi(y_1), \dots, \varphi(y_n))$ делится (справа) на $v(\varphi(t), \varphi(y_1), \dots, \varphi(y_n))$ в силу следующей леммы (которую следует применить к каждому моному выражения v).

Лемма 1. *Пусть M — моноид, $b_i, a, h \in M$, причём a и h обратимы, а элементы $a^{-s}ha^s$, где $s \in \mathbb{Z}$, коммутируют со всеми b_i. Тогда для выражения вида*

$$u(t) = b_0 t^{n_1} b_1 \dots t^{n_l} b_l, \quad \text{где } n_i \in \mathbb{Z},$$

имеет место равенство $u(ah) = \begin{cases} h^{a^{-1}} h^{a^{-2}} \dots h^{a^{-k}} u(a), & \text{если } k = \sum n_i > 0 \\ h^{-1} h^{-a} \dots h^{-a^{-1-k}} u(a), & \text{если } k = \sum n_i < 0 \\ u(a), & \text{если } k = \sum n_i = 0. \end{cases}$

Доказательство. Пользуясь правилами коммутирования $a^i h^{a^j} = h^{a^{j-i}} a^i$ и $b_i h^{a^j} = h^{a^j} b_i$, будем последовательно передвигать все буквы h (и h^{a^j}) в слове $u(ah)$ влево и получим то, что требуется. Это завершает доказательство леммы 1 и теоремы об уравнениях над кольцами.

Пример. *Число пифагоровых троек обратимых элементов ассоциативного кольца с единицей, то есть число обратимых решений уравнения*

$$x^2 + y^2 = z^2$$

всегда делится на порядок мультипликативной группы этого кольца.
Действительно, уравнение однородно, а в качестве G следует взять мультипликативную группу кольца R. Более того,
число обратимых решений уравнения

$$ax^k + by^l + cz^m + dt^n + \ldots = 0$$

делится на $|R^*|$ при любых фиксированных $a, b, c, d, \dots, k, l, m, \dots \in \mathbb{Z}$,
поскольку это уравнение является обобщённо однородным.

4. Доказательство основной теоремы

Наше доказательство в некотором смысле похоже на рассуждение, которое содержится в конце параграфа 3 работы [KM14]. Чтобы подчеркнуть эту аналогию, мы будем использовать те же термины, что в [KM14] (но означать они будут другие понятия, строго говоря).

Хвостом гомоморфизма $\varphi \in \Phi$ мы будем называть пару (φ_0, φ_H), где φ_0 — это ограничение гомоморфизма φ на подгруппу $\ker \deg \subset F$, а $\varphi_H \colon F \to \{gH \ ; \ g \in G\}$ — это отображение из F в множество левых смежных классов группы G по подгруппе H, которое переводит элемент $f \in F$ в класс $\varphi(f)H$.

Мы будем говорить, что два гомоморфизма $\varphi, \psi \in \Phi$ *похожи* и писать $\varphi \sim \psi$, если их хвосты сопряжены при помощи элемента из H, то есть

$$\varphi \sim \psi \iff \text{найдётся } h \in H \text{ такой, что } \begin{cases} \psi(f) = h\varphi(f)h^{-1} & \text{для всех } f \in F \text{ степени ноль и} \\ \psi(f)H = h\varphi(f)H & \text{для всех } f \in F. \end{cases}$$

Ясно, что похожесть — это отношение эквивалентности на Φ. Основная теорема немедленно вытекает из следующего утверждения.

Утверждение. *В каждом классе похожих гомоморфизмов из Φ содержится ровно $|H|$ элементов. Более точно, для каждого $\varphi \in \Phi$*

1) *число различных хвостов гомоморфизмов из Φ похожих на φ равно $|H : H_\varphi|$;*
2) *для каждого гомоморфизма ψ похожего на φ число гомоморфизмов из Φ с таким же хвостом как у ψ равно $|H_\varphi|$.*

Доказательство. Для доказательства утверждения 1) заметим, что на множестве хвостов гомоморфизмов из Φ группа H действует сопряжением. Действительно, если хвост гомоморфизма $\psi \in \Phi$ сопрячь при помощи элемента $h \in H$ то мы получим хвост гомоморфизма $f \mapsto \psi(f)^h$. Этот гомоморфизм лежит в Φ в силу условия I основной теоремы. Хвосты гомоморфизмов похожих на φ составляют орбиту хвоста гомоморфизма φ

при этом действии. Мощность орбиты равна, как известно, индексу стабилизатора. Осталось заметить, что подгруппа H_φ — это стабилизатор хвоста гомоморфизма φ.

Докажем второе утверждение. Выберем элемент $x \in F$ степени один. Гомоморфизм $\alpha\colon F \to G$ однозначно определяется своим хвостом и значением $\alpha(x)$. При этом для двух гомоморфизмов α и β с одинаковым хвостом частное $h = (\alpha(x))^{-1}\beta(x)$ должно коммутировать с этим хвостом, то есть лежать в H_α; действительно, для всех $f \in F$ степени ноль мы имеем

$$\alpha(f^x)^h = \alpha(f)^{\alpha(x)h} = \alpha(f)^{\beta(x)} = \beta(f)^{\beta(x)} = \beta(f^x) = \alpha(f^x), \quad \text{то есть } h \text{ централизует подгруппу } \alpha(\ker \deg);$$

а для любого элемента $f \in F$ мы имеем

$$\alpha(x)\alpha(f)H = \alpha(xf)H = \beta(xf)H = \beta(x)\beta(f)H = \alpha(x)h\beta(f)H = \alpha(x)h\alpha(f)H, \quad \text{то есть } h \in \alpha(f)H\alpha(f)^{-1}.$$

Таким образом, $h = (\alpha(x))^{-1}\beta(x) \in H_\alpha$.

С другой стороны, если h — произвольный элемент из H_α, то отображение $f \mapsto \begin{cases} \alpha(f), & \text{если } \deg f = 0 \\ \alpha(x)h, & \text{если } f = x \end{cases}$ очевидно продолжается до гомоморфизма с таким же хвостом, как у α (по лемме 0). Этот гомоморфизм лежит в Φ в силу условия II основной теоремы.

Мы показали, что для любого $\alpha \in \Phi$ множество Φ содержит ровно $|H_\alpha|$ гомоморфизмов с таким же хвостом как у α. Осталось заметить, что для похожих гомоморфизмов ψ и φ подгруппы H_φ и H_ψ имеют одинаковый порядок, поскольку эти подгруппы сопряжены. Это завершает доказательство утверждения 2), а вместе с ним и основной теоремы.

ГЛАВА 5.
ЧТО ОБЩЕГО МЕЖДУ ТЕОРЕМАМИ ФРОБЕНИУСА, СОЛОМОНА И ИВАСАКИ О ДЕЛИМОСТИ В ГРУППАХ?

0. Введение

Следующий результат доказан ещё в XIX веке.

Теорема Фробениуса [Frob95] (см. также [And16]). *Число решений уравнения $x^n = 1$ в конечной группе G делится на* $\text{НОД}(|G|, n)$ *для любого натурального n.*

Эта теорема много раз обобщалась в разных направлениях, смотрите, например, [Hall36b], [Kula38], [Sehg62], [BrTh88], [Yosh93], [AsTa01], [ACNT13] и литературу там цитируемую. Например, сам Фробениус в 1903 году [Frob03] доказал следующее обобщение:

> *для любого натурального n и любого элемента g любой конечной группы G число решений уравнения $x^n = g$ в G делится на наибольший общий делитель числа n и порядка централизатора элемента g;*

а Ф. Холл ([Hall36], теорема II) показал, что

> *в любой конечной группе число решений системы уравнений с одним неизвестным делится на* $\text{НОД}(|C|, n_1, n_2, \ldots)$, *где C — это централизатор множества всех коэффициентов, а n_i — сумма показателей степеней при неизвестном в i-м уравнении.*

Здесь, как обычно, под уравнением над группой G понимается формальная запись вида $v(x_1, \ldots, x_m) = 1$, где v является словом, в котором каждая буква — это либо неизвестный, либо обратный к неизвестному, либо элемент группы G (называемый *коэффициентом*). Другими словами, левая часть уравнения — это элемент свободного произведения $G * F(x_1, \ldots, x_m)$ группы G и свободной группы $F(x_1, \ldots, x_m)$ ранга m (где m — число неизвестных).

Теорема Соломона, о которой дальше пойдёт речь, тоже про уравнения в группах и тоже про делимость, но, на первый взгляд, не очень похожа на теорему Фробениуса и её обобщения.

Теорема Соломона [Solo69]. *В любой группе число решений системы уравнений без коэффициентов делится на порядок этой группы, если уравнений меньше, чем неизвестных.*

Эта теорема также обобщалась в разных направлениях, смотрите [Isaa70], [Стру95], [AmV11], [GRV12], [KM14], [KM17] и литературу, там цитируемую. Например, в [KM14] показано, что

> *в любой группе число решений системы уравнений с коэффициентами из этой группы делится на порядок пересечения централизаторов всех коэффициентов, если ранг матрицы, составленной из сумм показателей степеней при j-м неизвестном в i-м уравнении, меньше числа неизвестных.*

Сам Соломон написал в [Solo69]:

> *"There seems to be no connection between this theorem and the Frobenius theorem on solutions of $x^k = 1$."*

Тем не менее, связь между теоремами Фробениуса и Соломона есть.

Теорема 1*). *В любой (необязательно конечной) группе число решений (необязательно конечной) системы уравнений с m неизвестными делится на наибольший общий делитель централизатора множества всех коэффициентов и числа $\frac{\Delta_m}{\Delta_{m-1}}$, где Δ_i — это наибольший общий делитель всех миноров порядка i матрицы системы. При этом подразумеваются следующие соглашения: $\Delta_i = 0$, если i больше, чем число уравнений; $\Delta_0 = 1$; $\frac{0}{0} = 0$.*

Наибольшим общим делителем $\text{НОД}(G, n)$ группы G и целого числа n мы называем наименьшее общее кратное порядков подгрупп группы G, делящих n. Делимость всегда понимается в смысле кардинальной арифметики: каждый бесконечный кардинал делится на все меньшие ненулевые кардиналы (и, разумеется, ноль делится на все кардиналы, а на ноль делится только ноль). Это означает, что $\text{НОД}(G, 0) = |G|$ для любой группы G; а, например, $\text{НОД}(\mathbf{SL}_2(\mathbb{Z}), 2018) = 2$. Впрочем, читатель не очень много потеряет, если будет считать все группы в этой главе конечными, а в этом случае $\text{НОД}(G, n) = \text{НОД}(|G|, n)$ по теореме Силова (и поскольку конечная p-группа содержит подгруппы всех возможных порядков).

Под *матрицей системы уравнений над группой* понимается целочисленная матрица $A = (a_{ij})$, где a_{ij} — это сумма показателей степеней при j-м неизвестном в i-м уравнении. Например, матрица системы уравнений

$$\begin{cases} xay^2[x,y]^{2022}(xby)^3 = 1 \\ bx^3y[x,y]^{100}(xby)^4 = 1 \\ [x,y^5]x^{-2} = 1 \end{cases}$$

*) **Theorem 0** в журнальной версии.

(где x и y — неизвестные, а a и b — коэффициенты, то есть фиксированные элементы группы) имеет вид

$$\begin{pmatrix} 4 & 5 \\ 7 & 5 \\ -2 & 0 \end{pmatrix}.$$

Под *минорами порядка i* мы понимаем, как обычно, определители подматриц, составленных из элементов стоящих на пересечении каких-то i строк и i столбцов. В описанном выше примере миноров порядка m три (с точностью до знаков):

$$\det\begin{pmatrix} 4 & 5 \\ 7 & 5 \end{pmatrix} = -15, \quad \det\begin{pmatrix} 4 & 5 \\ -2 & 0 \end{pmatrix} = 10, \quad \det\begin{pmatrix} 7 & 5 \\ -2 & 0 \end{pmatrix} = 10,$$

а миноров порядка $m-1$ — шесть: 4, 5, 7, 5, -2, 0. Таким образом, теорема утверждает, что в этом примере число решений делится на

$$\text{НОД}\left(\frac{\text{НОД}(-15,10,10)}{\text{НОД}(4,5,7,5,-2,0)}, |C(a)\cap C(b)|\right) = \text{НОД}(5, |C(a)\cap C(b)|).$$

Отметим, что соглашения по поводу пограничных случаев, указанные в теореме, вполне естественны. Действительно, мы всегда можем добавить фиктивные уравнения 1=1 и добиться того, что число уравнений станет больше чем m. Мы можем также добавить новую переменную z и уравнение $z=1$ (это не повлияет на число решений и сделает $m>1$). Что касается философского вопроса об интерпретации частного $\frac{0}{0}$, то его можно понимать как угодно, например, читатель вправе считать, что $\frac{0}{0}=2022$ — в любом случае наша теорема окажется верным утверждением (но более слабым, чем при нашей интерпретации).

Смысл величины $\frac{\Delta_m}{\Delta_{m-1}}$ состоит в следующем. Хорошо известно (смотрите, например, [Вин99]), что всякую целочисленную матрицу A обратимыми целочисленными элементарными преобразованиями строк и столбцов можно превратить в диагональную матрицу, причём диагональные элементы будут делить друг друга (каждый диагональный элемент будет делить следующий). Полученная диагональная матрица определяется однозначно с точностью до знаков диагональных элементов (и называется иногда *формой Смита* матрицы A); диагональные элементы формы Смита называют иногда *инвариантными множителями* матрицы A; они представляют собой частные $\frac{\Delta_i}{\Delta_{i-1}}$. Таким образом, в этой терминологии величина $\frac{\Delta_m}{\Delta_{m-1}}$ есть m-й инвариантный множитель матрицы системы уравнений. Можно ещё сказать так:

> *абсолютная величина частного $\frac{\Delta_m}{\Delta_{m-1}}$ есть период (экспонента) факторгруппы свободной абелевой группы $\mathbb{Z}^m$ по подгруппе, порождённой строками матрицы системы уравнений*

(с той оговоркой, что это частное равно нулю тогда и только тогда, когда период бесконечен).

В качестве частных случаев теоремы 1 мы немедленно получаем теоремы Фробениуса и Соломона, а также их усиления, сформулированные выше.

Следующая теорема, на первый взгляд, не похожа ни на теорему Фробениуса, ни на теорему Соломона.

Теорема Ивасаки [Iwa82]. *Для любого целого n число элементов конечной группы G, n-е степени которых лежат в данной подгруппе $H\subseteq G$, делится на $|H|$.*

Эта красивая теорема остаётся не очень широко известной (почему-то). В [SaAs07] было замечено, что делимость на $|H|$ имеет место и для числа решений «уравнения» $x^n\in HgH$, где HgH — любой двойной смежный класс по подгруппе H. Разумеется, в теореме Ивасаки и её обобщениях речь идёт уже не об уравнениях в обычном смысле. *Обобщённым уравнением* над группой G мы будем называть произвольную запись вида $w(x_1,\dots,x_n)\in HgH$, где H — подгруппа группы $G\ni g$, а $w(x_1,\dots,x_m)$ — элемент свободного произведения $G*F(x_1,\dots,x_m)$ группы G и свободной группы; другими словами, w представляет собой слово в алфавите $G\sqcup\{x_1^{\pm1},\dots,x_m^{\pm1}\}$. Элементы группы G, встречающиеся в этом слове, мы называем *коэффициентами* обобщённого уравнения. Система обобщённых уравнений и решение этой системы определяются естественным образом. Матрица системы обобщённых уравнений определяется аналогично.

В [KM17] было получено следующее обобщение теоремы Ивасаки:

> *число решений любой системы обобщённых уравнений без коэффициентов, в правой части которой стоят двойные смежные классы по одной и той же подгруппе H* (например, $\{x^{100}y^{2022}[x,y]^4\in Hg_1H,\quad [x^5,y^6]^7(xy)^8\in Hg_2H,\dots\}$) *делится на $|H|$.*

Теорема, которая включает в себя все сформулированные выше утверждения, звучит так.

Теорема 2 *). *Пусть S — (необязательно конечная) система обобщённых уравнений от конечного числа переменных $x_1, \dots, x_m$ над группой G а P — её подсистема:*

$$S = \{u_i(x_1, \dots, x_m) \in H_i g_i H_i \mid i \in I\} \supseteq P = \{u_j(x_1, \dots, x_m) \in H_j g_j H_j \mid j \in J\},$$

(где $J \subseteq I$, $u_i \in G * F(x_1, \dots, x_m)$, $g_i \in G$, а H_i — подгруппы группы G). Тогда число решений системы S в группе G делится на наибольший общий делитель подгруппы

$$\widetilde{H} = \left(\bigcap_{j\in J} N(H_j g_j H_j)\right) \cap \left(\bigcap_{i\in I\setminus J} H_i\right) \cap \big(\text{централизатор множества всех коэффициентов системы } S\big)$$

и числа $\frac{\Delta_m}{\Delta_{m-1}}$, где Δ_k — это наибольший общий делитель всех миноров порядка k матрицы подсистемы P. Здесь и далее $N(A) \stackrel{\text{опр}}{=} \{g \in G \mid g^{-1}Ag = A\}$ — это нормализатор подмножества A группы G.

Чтобы получить из теоремы 2 теорему 1, достаточно переписать систему уравнений в «обобщённом» виде, то есть положить $S = P = \Big\{u_1(x_1, \dots, x_m) \in \{1\}1\{1\}, \quad u_2(x_1, \dots, x_m) \in \{1\}1\{1\}, \dots\Big\}$ и заметить, что нормализатор тривиальной подгруппы — это вся группа.

С другой стороны, полагая

$$S = \Big\{u_1(x_1, \dots, x_m) \in Hg_1H, \quad u_2(x_1, \dots, x_m) \in Hg_2H, \dots\Big\} \quad \text{и} \quad P = \varnothing \quad (\text{где } u_i \in F(x_1, \dots, x_m)),$$

мы получаем упомянутое выше обобщение из [KM17] теоремы Ивасаки.

На самом деле, связь между теоремами Соломона и Ивасаки была установлена в [KM14] и [KM17], наше достижение состоит лишь в добавлении «фробениусовости». Основная теорема работы [KM17] говорит, что если имеется группа F с фиксированным эпиморфизмом на $\mathbb{Z}$ и некоторое множество гомоморфизмов из F в другую группу G, причём это множество инвариантно относительно некоторых естественных преобразований (зависящих от эпиморфизма $F \to \mathbb{Z}$ и подгруппы H группы G), то число рассматриваемых гомоморфизмов $F \to G$ делится на $|H|$. При подходящем выборе множества гомоморфизмов авторы [KM17] получают из своей основной теоремы и теорему Соломона, и теорему Ивасаки.

Наша основная теорема (смотрите параграф 1) представляет собой модулярный аналог основной теоремы из [KM17]: вместо фиксированного эпиморфизма $F \to \mathbb{Z}$ мы фиксируем эпиморфизм $F \to \mathbb{Z}/n\mathbb{Z}$. Можно сказать, что основная теорема этой главы относится к основной теореме из [KM17] так же, как теорема 1 относится к упомянутому в начале главы обобщению теоремы Соломона из [KM14]. Важную роль в доказательстве (а точнее, даже в корректности формулировки) основной теоремы играет одно элементарное, но не тривиальное, утверждение, принадлежащее Р. Брауэру [Bra69]. В последнем параграфе мы приводим доказательство леммы Брауэра, а в параграфе 5 доказываем основную теорему.

Одним из следствий нашей основной теоремы является теорема 2 (которую мы доказываем в параграфе 2). В качестве другого следствия мы получаем некоторую теорему об уравнениях в кольцах (теорема 3 в параграфе 3), из которой вытекает, например, следующий факт, который можно рассматривать как обобщение теоремы Фробениуса в несколько ином направлении:

для любого представления $\rho\colon G \to \mathbf{GL}(V)$ группы G и любых слов $u_i(x_1, \dots, x_m) \in F(x_1, \dots, x_m)$

$$\textit{число решений уравнения } \sum_{i=1}^{k} \Big(\rho\big(u_i(x_1, \dots, x_m)\big)\Big)^{l_i} = \mathrm{id} \quad \textit{делится на} \quad \begin{cases} \text{НОД}\big(G, \text{НОД}(\{l_i\})\big) & \textit{всегда;} \\ \text{НОД}\big(G, \text{НОК}(\{l_i\})\big), & \textit{если } k \leqslant m; \\ |G|, & \textit{если } k < m. \end{cases}$$

В параграфе 4 мы выводим из основной теоремы некоторый факт о числе скрещенных гомоморфизмов, усиливающий ранее известные результаты. В предпоследнем параграфе мы обсуждаем открытые вопросы.

Обозначения и соглашения, которые мы используем, в целом стандартны. Отметим только, что если $k \in \mathbb{Z}$, а x и y — элементы некоторой группы, то x^y, x^{ky} и x^{-y} обозначают $y^{-1}xy$, $y^{-1}x^ky$ и $y^{-1}x^{-1}y$, соответственно. Коммутант группы G мы обозначаем символом G' или $[G, G]$. Если X — подмножество некоторой группы, то $|X|$, $\langle X\rangle$, $\langle\langle X\rangle\rangle$, $C(X)$ и $N(X)$ означают, соответственно, мощность множества X, подгруппу, порождённую множеством X, нормальное замыкание множества X, централизатор множества X и нормализатор множества X. Индекс подгруппы H группы G обозначается $|G : H|$. Буква $\mathbb{Z}$ обозначает множество целых чисел. Если R — ассоциативное кольцо с единицей, то R^* обозначает группу обратимых элементов этого кольца. НОД и НОК — это наибольший общий делитель и наименьшее общее кратное. Символом $\exp(G)$ мы обозначаем период (экспоненту) группы G, если этот период конечен; и считаем $\exp(G) = 0$, если период бесконечен. Символ $\langle g\rangle_n$ обозначает циклическую группу порядка n, порождённую элементом g. Свободную группу ранга n мы обозначаем символом $F(x_1, \dots, x_n)$ или F_n. Символ $A * B$ обозначает свободное произведение групп A и B.

Кроме того, отметим ещё раз, что конечность групп нигде не предполагается по умолчанию, делимость всегда понимается в смысле кардинальной арифметики (бесконечный кардинал делится на все ненулевые кардиналы, не превосходящие его), а $\text{НОД}(G, n) \stackrel{\text{опр}}{=} \text{НОК}\left(\left\{|H| \;\middle|\; H \text{ — подгруппа в } G \text{ и } |H| \text{ делит } n\right\}\right)$.

*) **Theorem 1** в журнальной версии.

1. Основная теорема

Группу F с фиксированным эпиморфизмом $F \to \mathbb{Z}/n\mathbb{Z}$ (где $n \in \mathbb{Z}$) мы называем *n-индексированной* группой. Этот эпиморфизм $F \to \mathbb{Z}/n\mathbb{Z}$ мы называем *степенью* и обозначаем deg. Таким образом, для любого элемента f индексированной группы F определён элемент $\deg f \in \mathbb{Z}/n\mathbb{Z}$, причём группа F содержит элементы всех степеней и $\deg(fg) = \deg f + \deg g$ для любых $f, g \in F$.

Пусть имеется гомоморфизм $\varphi\colon F \to G$ из n-индексированной группы F в какую-то группу G и подгруппа H группы G. Подгруппу

$$H_\varphi = \bigcap_{f \in F} H^{\varphi(f)} \cap C(\varphi(\ker \deg))$$

называют *φ-сердцевиной* подгруппы H [KM17]. Другими словами, φ-сердцевина H_φ подгруппы H состоит из таких её элементов h, что $h^{\varphi(f)} \in H$ для всех f, причём $h^{\varphi(f)} = h$, если $\deg f = 0$.

Основная теорема. *Пусть целое число n делится на порядок подгруппы H некоторой группы G, и некоторое множество Φ гомоморфизмов из n-индексированной группы F в G удовлетворяет следующим условиям.*

I. *Φ инвариантно относительно сопряжения элементами из H:*

$$\text{если } h \in H \text{ и } \varphi \in \Phi, \text{ то гомоморфизм } \psi\colon f \mapsto \varphi(f)^h \text{ тоже лежит в } \Phi.$$

II. *Для любого $\varphi \in \Phi$ и любого элемента h из φ-сердцевины H_φ подгруппы H гомоморфизм ψ, определённый правилом*

$$\psi(f) = \begin{cases} \varphi(f) & \text{для всех элементов } f \in F \text{ степени ноль;} \\ \varphi(f)h & \text{для некоторого элемента } f \in F \text{ степени один (а, значит, и для всех элементов степени один),} \end{cases}$$

также содержится в Φ.

Тогда $|\Phi|$ делится на $|H|$.

Отметим, что отображение ψ из условия I является гомоморфизмом при любом $h \in G$. А формула для ψ из условия II определяет гомоморфизм при любых $h \in H_\varphi$ (как объясняется ниже). Смысл условий I и II состоит в том, что эти гомоморфизмы лежат в Φ.

Лемма 0[*]**.** *Пусть $\varphi\colon F \to G$ — гомоморфизм из n-индексированной группы F в группу G, $f_1 \in F$ — элемент степени один и $g \in G$. Тогда гомоморфизм $\psi\colon F \to G$ такой, что $\psi(f) = \varphi(f)$ для всех $f \in F$ степени ноль и $\psi(f_1) = \varphi(f_1)g$, существует тогда и только тогда, когда $g \in C(\varphi(\ker \deg))$ и $\big(\varphi(f_1)g\big)^n = \big(\varphi(f_1)\big)^n$.*

Доказательство. Группу F можно представить в виде

$$F \simeq \big(F_0 * \langle x \rangle_\infty\big) \big/ \left\langle\!\!\left\langle \{u^x u^{-f_1} \mid u \in F_0\} \cup \{x^n f_1^{-n}\} \right\rangle\!\!\right\rangle, \quad \text{где } F_0 = \ker \deg.$$

Значит, отображение $\psi\colon F_0 \cup \{x\} \to G$ продолжается до гомоморфизма тогда и только тогда, когда его ограничение на F_0 есть гомоморфизм, а соотношения $u^x = u^{f_1}$ (при $u \in F_0$) и $x^n = f_1^n$ превращаются в истинные равенства в группе G:

$$\psi(u)^{\psi(x)} = \psi(u^{f_1}) \quad \text{и} \quad \psi(x)^n = \psi(f_1^n). \tag{$*$}$$

Если ограничение ψ на F_0 совпадает с ограничением гомоморфизма φ на F_0, а $\psi(x) = \varphi(f_1)g$, то первое из равенств $(*)$ эквивалентно тому, что g коммутирует с $\varphi(u)$ (при всех $u \in F_0$), а второе из равенств $(*)$ принимает вид $\big(\varphi(f_1)g\big)^n = \big(\varphi(f_1)\big)^n$. Лемма доказана.

Напомним ещё следующий красивый (но не очень широко известный) факт.

Лемма Брауэра [Bra69]. *Если U — конечная нормальная подгруппа группы V, то для всех $v \in V$ и $u \in U$ элементы $v^{|U|}$ и $(vu)^{|U|}$ сопряжены при помощи элемента из U.*

Из этих двух лемм немедленно вытекает, что отображение ψ из условия II основной теоремы является гомоморфизмом при всех $h \in H_\varphi$, поскольку $(\varphi(f)h)^n = (\varphi(f))^n$ по лемме Брауэра, применённой к

$$U = H_\varphi \subset V = H_\varphi \cdot \langle \varphi(f_1) \rangle \ni \varphi(f_1) = v.$$

Действительно, мы получаем равенство $\big(\varphi(f_1)h\big)^{|H_\varphi|} = \big(\varphi(f_1)\big)^{|H_\varphi| u}$ при некотором $u \in H_\varphi$ и, следовательно, $\big(\varphi(f_1)h\big)^n = \big(\varphi(f_1)\big)^{nu} = \big(\varphi(f_1^n)\big)^u$ (поскольку $|H_\varphi|$ делит n). Остаётся заметить, что $u \in H_\varphi$ коммутирует с $\varphi(f_1^n)$, поскольку $\deg f_1^n = n = 0 \in \mathbb{Z}/n\mathbb{Z}$. Таким образом, мы получаем равенство $\big(\varphi(f_1)h\big)^n = \big(\varphi(f_1)\big)^n$ и остаётся сослаться на лемму 0.

Отметим, что в случае $n = 0$ основная теорема была доказана в [KM17], поэтому наша теорема представляет собой «модулярный аналог» основного результата работы [KM17]. С другой стороны, нашу основную теорему мы выводим (в параграфе 5) из этого частного случая $n = 0$.

---

[*] **Lemma 2** в журнальной версии.

Лемма 1)**. *В условии II основной теоремы* $\psi(f) \in \varphi(f)H_\varphi$ *при всех* $f \in F$.

Доказательство. Действительно, если $\deg f = d$, то $f = f_1^d f_0$, где f_1 — (фиксированный) элемент степени один (о котором идёт речь в условии II), а f_0 — некоторый элемент степени ноль. Тогда

$$\psi(f) = \psi(f_1)^d \psi(f_0) = (\varphi(f_1)h)^d \varphi(f_0) \mathrel{=\!=} \varphi(f_1)^d \varphi(f_0) h' = \varphi(f_1^d f_0)h' = \varphi(f)h',$$

где равенство $\mathrel{=\!=}$ имеет место для некоторого $h' \in H_\varphi$, поскольку $h \in H_\varphi$ и $\varphi(F)$ нормализует H_φ.

2. Доказательство теоремы 2

Пусть $L \subseteq G$ — подгруппа, порождённая всеми коэффициентами системы S. Возьмём в качестве H произвольную подгруппу группы $\widetilde{H}$, порядок которой делит $n \overset{\text{опр}}{=} \frac{\Delta_m}{\Delta_{m-1}}$, и положим

$$F = L * F(x_1, \ldots, x_m) \quad \text{и} \quad \Phi = \Big\{ \varphi\colon F \to G \;\Big|\; \varphi(f) = f \text{ при } f \in L \quad \text{и} \quad \varphi(u_i) \in H_i g_i H_i \text{ при } i \in I \Big\}.$$

В качестве индексации $\deg\colon F \to \mathbb{Z}/n\mathbb{Z}$ возьмём эпиморфизм, содержащий в своём ядре подгруппу L и все u_j, где $j \in J$. Такой эпиморфизм существует, поскольку число n есть период конечно порождённой абелевой группы $F/\big([F,F] \cdot L \cdot \langle\{u_j \mid j \in J\}\rangle\big)$.

Проверим, что условия основной теоремы выполнены. Условие I очевидно выполняется при всех $h \in H$ (и даже при всех $h \in \widetilde{H}$), поскольку подгруппа $\widetilde{H}$ по определению централизует подгруппу L и нормализует двойные смежные классы $H_i g_i H_i$.

Условие II тоже выполняется при всех $h \in H_\varphi$, так как

- на подгруппе L гомоморфизм ψ действует так же, как φ, поскольку L состоит из элементов степени ноль;
- $\psi(u_j) = \varphi(u_j)$ при $j \in J$, поскольку опять же $\deg u_j = 0$;
- а при $i \in I \setminus J$ мы имеем $\psi(u_i) \in \varphi(u_i)H_\varphi \subseteq \varphi(u_i)H_i$ (где включение $\in$ имеет место по лемме 1).

Таким образом, по основной теореме $|\Phi|$ делится на порядок любой подгруппы $H \subseteq \widetilde{H}$, порядок которой делит n, то есть $|\Phi|$ делится на НОД$(\widetilde{H}, n)$. Осталось заметить, что $|\Phi|$ есть число решений системы S.

3. Кольца и представления

Под *обобщённо однородным по модулю* n уравнением с множеством неизвестных X над ассоциативным кольцом R с единицей мы понимаем конечную запись вида

$$\sum_i \prod_j c_{ij} x_{ij}^{k_{ij}} = 0, \quad \text{где } \textit{коэффициенты } c_{ij} \in R, \textit{ неизвестные } x_{ij} \in X \text{ и } \textit{показатели } k_{ij} \in \mathbb{Z},$$

такую, что для некоторого отображения $\deg\colon X \to \mathbb{Z}/n\mathbb{Z}$ величина $\sum\limits_j k_{ij} \deg(x_{ij})$ (называемая *степенью уравнения*) не зависит от i (то есть «многочлен» в левой части уравнения является однородным относительно некоторого приписывания степеней переменным), причём $\langle\{\deg x \mid x \in X\}\rangle = \mathbb{Z}/n\mathbb{Z}$. Систему уравнений мы называем обобщённо однородной по модулю n, если все уравнения этой системы являются обобщённо однородными по модулю n (возможно разных степеней) относительно одной и той же функции $\deg\colon X \to \mathbb{Z}/n\mathbb{Z}$.

Ниже мы объясним, что множество $M = \{n \in \mathbb{Z} \mid$ данная система обобщённо однородна по модулю $n\}$ состоит из всевозможных делителей некоторого числа n_0, которое мы будем называть *модулем однородности* данной системы. Другими словами, модуль однородности представляет собой наибольшее число из M или ноль, если множество M бесконечно.

Для поиска модуля однородности составим систему линейных однородных уравнений, где неизвестными будут степени переменных, а также степени уравнений (взятые со знаком минус); уравнения говорят, что степень монома равна степени соответствующего уравнения. Матрица этой системы линейных уравнений (которую мы будем называть *матрицей однородности* исходной системы уравнений) устроена следующим образом. Пусть $X = \{x_1, \ldots, x_m\}$. *Матрица однородности* p*-го уравнения* — это целочисленная матрица $A_p = (a_{kl})$ размера

$$(\text{общее число мономов в системе}) \times \big(m + (\text{число уравнений})\big),$$

где при $l \leqslant m$ на (k,l)-м месте стоит сумма показателей степеней при l-м неизвестном в k-м мономе, $(m+p)$-й столбец состоит из единиц, а остальные столбцы нулевые при $l > m$. Тогда матрица однородности системы

) **Lemma 3 в журнальной версии.

уравнений будет составлена из таких матриц A_p, записанных друг под другом: $A = \begin{pmatrix} A_1 \\ A_2 \\ \vdots \end{pmatrix}$. Например, для системы уравнений

$$\left\{ax^3y^2 + y^7bx - 1 = 0, \quad xy^2x + y^7x^5 = 0\right\} \quad \text{(где } a, b \in R \text{ — коэффициенты, а } x \text{ и } y \text{ — неизвестные),}$$

получаем следующую матрицу однородности:

$$A = \begin{pmatrix} 3 & 2 & 1 & 0 \\ 1 & 7 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 2 & 2 & 0 & 1 \\ 5 & 7 & 0 & 1 \end{pmatrix}, \quad \text{составленную из матриц} \quad A_1 = \begin{pmatrix} 3 & 2 & 1 & 0 \\ 1 & 7 & 1 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \text{ и } A_2 = \begin{pmatrix} 2 & 2 & 0 & 1 \\ 5 & 7 & 0 & 1 \end{pmatrix}.$$

Лемма о модуле однородности. *Модуль однородности системы из s уравнений с m неизвестными над ассоциативным кольцом с единицей равен $\frac{\Delta_{m+s}}{\Delta_{m+s-1}}$, где Δ_i — это наибольший общий делитель всех миноров порядка i матрицы однородности данной системы уравнений. При этом подразумеваются следующие соглашения: $\Delta_i = 0$, если суммарное число мономов всех уравнений меньше, чем i; $\Delta_0 = 1$; $\frac{0}{0} = 0$.*

Доказательство. Пусть A — матрица однородности системы. Нас интересует максимальное число n такое, что система линейных однородных уравнений $AX = 0$ (от $m + s$ переменных) имеет решение в $\mathbb{Z}/n\mathbb{Z}$, компоненты которого порождают $\mathbb{Z}/n\mathbb{Z}$ как аддитивную группу (это эквивалентно тому, что первые m компонент решения порождают $\mathbb{Z}/n\mathbb{Z}$, поскольку последние s компонент решения выражаются через первые m компонент). Другими словами, n — это максимальный порядок циклической факторгруппы конечно порождённой абелевой группы $\mathbb{Z}^{m+s}/N$, где N — подгруппа, порождённая строками матрицы A. Как уже отмечалось, максимальный порядок n циклической факторгруппы группы $\mathbb{Z}^{m+s}/N$ равен $\frac{\Delta_{m+s}}{\Delta_{m+s-1}}$, что и требовалось.

Теорема 3*). *Пусть R — ассоциативное кольцо с единицей, а G — подгруппа мультипликативной группы этого кольца. Тогда для каждой системы уравнений над R от m неизвестных число её решений, лежащих в G^m, делится на наибольший общий делитель модуля однородности системы и пересечения группы G с централизатором множества всех коэффициентов системы.*

Доказательство. Пусть G_0 — пересечение группы G с централизатором множества всех коэффициентов системы и n — модуль однородности. Рассмотрим свободную группу $F(X)$ (где X — множество всех неизвестных нашей системы) и эпиморфизм $\deg\colon F(X) \to \mathbb{Z}/n\mathbb{Z}$.

Применим основную теорему, взяв в качестве Φ множество всех гомоморфизмов $\varphi\colon F(X) \to G$ таких, что набор $(\varphi(x_1), \ldots, \varphi(x_m))$ является решением нашей системы уравнений (и, таким образом, число решений данной системы уравнений равно $|\Phi|$). В качестве H возьмём произвольную подгруппу группы G_0, порядок которой делит n. Условие I основной теоремы очевидно выполнено. Для проверки условия II выберем элемент $t \in F$ степени один и запишем каждую переменную x_i в виде $x_i = t^{\deg x_i} y_i$, где $y_i = t^{-\deg x_i} x_i$ имеет степень ноль. В новых обозначениях каждое уравнение $w(x_1, \ldots, x_m) = 0$ нашей системы примет вид $v(t, y_1, \ldots, y_m) = 0$, при этом каждое слагаемое в этом уравнении будет иметь одну и ту же сумму (по модулю n) показателей степеней у переменной t. Далее заметим, что если $v(\varphi(t), \varphi(y_1), \ldots, \varphi(y_m)) = 0$ и $h \in H_\varphi$, то $v(\varphi(t)h, \varphi(y_1), \ldots, \varphi(y_m)) = 0$. Это вытекает из делимости $v(\varphi(t)h, \varphi(y_1), \ldots, \varphi(y_m))$ (справа) на $v(\varphi(t), \varphi(y_1), \ldots, \varphi(y_m))$ в силу следующего факта.

Факт ([KM17], лемма 1). *Пусть M — моноид, $b_i, a, h \in M$, причём a и h обратимы, а элементы $a^{-s}ha^s$, где $s \in \mathbb{Z}$, коммутируют со всеми b_i. Тогда для выражения вида $u(t) = b_0 t^{m_1} b_1 \ldots t^{m_l} b_l$, где $m_i \in \mathbb{Z}$, имеет место равенство* $u(ah) = \begin{cases} h^{a^{-1}} h^{a^{-2}} \ldots h^{a^{-k}} u(a), & \text{если } k = \sum m_i > 0; \\ h^{-1} h^{-a} \ldots h^{-a^{-1-k}} u(a), & \text{если } k = \sum m_i < 0; \\ u(a), & \text{если } k = \sum m_i = 0. \end{cases}$

Этот факт следует применить к каждому моному выражения v. При ненулевом n нужно дополнительно воспользоваться тем, что t^n — элемент степени ноль, и $(\varphi(t)h)^n = (\varphi(t))^n$ согласно лемме 0.

Таким, образом, по основной теореме $|\Phi|$ (то есть число решений нашей системы уравнений) делится на $|H|$, что и требовалось (поскольку H — произвольная подгруппа централизатора множества всех коэффициентов, порядок которой делит модуль однородности).

---

*) **Theorem 4** в журнальной версии.

Пример. *Если $\rho\colon G \to R^*$ — гомоморфизм из конечной группы G в мультипликативную группу ассоциативного кольца R с единицей* (например, $\rho\colon G \to \mathbf{GL}(V)$ — линейное представление группы G), *то для любых слов $u_i(x_1,\dots,x_m) \in F(x_1,\dots,x_m)$*

$$\textit{число решений уравнения } \sum_{i=1}^{k}\Big(\rho\big(u_i(x_1,\dots,x_m)\big)\Big)^{l_i} = 1 \quad \textit{делится на } \begin{cases} \text{НОД}\big(G, \text{НОД}(\{l_i\})\big) & \textit{всегда;} \\ \text{НОД}\big(G, \text{НОК}(\{l_i\})\big), & \textit{если } k \leqslant m; \\ |G|, & \textit{если } k < m. \end{cases}$$

Чтобы в этом убедиться, достаточно применить теорему 3 к подгруппе $\rho(G) \subseteq R^*$. Матрица однородности этого уравнения имеет вид $B = \begin{pmatrix} & & 1 \\ & A & \vdots \\ 0 & \dots & 0\ 1 \end{pmatrix}$, где последняя строка соответствует единице в правой части уравнения, а i-я строка матрицы A соответствует i-му слагаемому в левой части уравнения, и, стало быть, все элементы этой строки делятся на l_i. Осталось заметить, что j-й инвариантный множитель матрицы B совпадает с $(j-1)$-м инвариантным множителем матрицы A, и воспользоваться следующим фактом, который мы оставляем читателям в качестве несложного упражнения:

если i-я строка целочисленной матрицы $k \times m$ делится на l_i,

$$\textit{то } n\textit{-й инвариантный множитель этой матрицы} \begin{cases} \textit{делится на } \text{НОД}(\{l_i\}) & \textit{всегда;} \\ \textit{делится на } \text{НОК}(\{l_i\}) & \textit{при } k = m; \\ \textit{равен нулю} & \textit{при } k < m. \end{cases}$$

Отметим, что теорема 1 может быть получена, как следствие теоремы 3. Действительно, достаточно взять в качестве кольца R групповое кольцо $\mathbb{Z}G$ (которое очевидно содержит G в качестве подгруппы мультипликативной группы). Систему уравнений над G надо переписать в «кольцевом» виде: $\{w_i(x_1,\dots)-1=0\}$ и заметить, что величина $\frac{\Delta_m}{\Delta_{m-1}}$ из теоремы 1 превратится в точности в модуль однородности из леммы о модуле однородности.

4. Скрещенные гомоморфизмы

Пусть группа F действует (справа) на группе B автоморфизмами: $(f,b) \mapsto b^f$. Напомним, что *скрещенным гомоморфизмом* из F в B относительно этого действия называется отображение $\alpha\colon F \to B$ такое, что $\alpha(ff') = \alpha(f)^{f'}\alpha(f')$ для всех $f, f' \in F$. Савелий Скресанов заметил, что из основной теоремы легко выводится следующий факт, который был доказан в [ACNT13] (с использованием теории характеров) для случая, когда группы F и B конечны.

Теорема 4*). *Если группа F, допускающая эпиморфизм на $\mathbb{Z}/n\mathbb{Z}$, действует автоморфизмами на группе B, то число скрещенных гомоморфизмов $F \to B$ делится на* $\text{НОД}(B,n)$.

Доказательство. Интересующее нас множество скрещенных гомоморфизмов находится во взаимно однозначном соответствии с множеством Φ (обычных) гомоморфизмов из F в полупрямое произведение $G = F \leftthreetimes B$ (относительно данного действия) таких, что их композиция с проекцией $\pi\colon F \leftthreetimes B \to F$ есть тождественное отображение $F \to F$. Нам нужно показать, что $|\Phi|$ делится на $|H|$ для любой подгруппы $H \subseteq B$, порядок которой делит n (по определению числа $\text{НОД}(B,n)$).

Группа F по условию является n-индексированной. Поэтому доказываемое утверждение немедленно следует из основной теоремы. Условия основной теоремы выполнены по простым причинам: для условия I всё очевидно, поскольку $\pi(h^{-1}gh) = \pi(g)$; а условие II сразу вытекает из леммы 1, поскольку $\pi(gh) = \pi(g)$ (при $g \in G$ и $h \in H$).

5. Доказательство основной теоремы

Выберем элемент $f_1 \in F$ степени один, подгруппу $\ker\deg \subset F$ обозначим F_0 и рассмотрим полупрямое произведение $\widetilde{F} = \langle a\rangle_\infty \leftthreetimes F_0$, где a действует на F_0 так же, как $f_1\colon u^a = u^{f_1}$ при $u \in F_0$. Группа $\widetilde{F}$ обладает естественной индексацией (0-индексацией) $\deg\colon \widetilde{F} \to \mathbb{Z}$ (мы обозначаем её тем же символом deg). Ядро этого отображения есть F_0 и $\deg a = 1$. Кроме того, имеется естественный эпиморфизм $\alpha\colon \widetilde{F} \to F$, переводящий a в f_1, и тождественный на F_0. Проверим, что условия основной теоремы выполняются для множества $\widetilde{\Phi} = \{\varphi \circ \alpha \mid \varphi \in \Phi\}$ гомоморфизмов из $\widetilde{F}$ в G.

Условие I очевидно выполнено. Для проверки условия II выберем в качестве элемента степени один элемент $a \in \widetilde{F}$ и возьмём какой-то гомоморфизм $\widetilde{\varphi} = \varphi \circ \alpha \in \widetilde{\Phi}$ (где $\varphi \in \Phi$). Тогда гомоморфизм $\widetilde{\psi}$ из условия II имеет вид

$$\widetilde{\psi}(\widetilde{f}) = \begin{cases} \varphi(\widetilde{f}) & \text{для всех элементов } \widetilde{f} \in F_0; \\ \varphi(f_1)h & \text{при } \widetilde{f} = a; \end{cases} \qquad \text{где } \varphi \in \Phi \text{ и } h \in H_{\widetilde{\varphi}}. \tag{1}$$

---

*) **Theorem 5** в журнальной версии.

Нам надо показать, что гомоморфизм $\widetilde{\psi}$ содержится в $\widetilde{\Phi}$, то есть имеет вид $\widetilde{\psi} = \varphi' \circ \alpha$, где $\varphi' \in \Phi$. Заметим, что $H_{\widetilde{\varphi}} = H_\varphi$, поскольку образы гомоморфизмов $\widetilde{\varphi} = \varphi \circ \alpha$ и φ совпадают, и образы элементов степени ноль при этих гомоморфизмах совпадают: $\widetilde{\varphi}(\ker \deg) = \widetilde{\varphi}(F_0) = \varphi(F_0)$. Формула (1) приобретает вид

$$\widetilde{\psi}(\widetilde{f}) = \begin{cases} \varphi(\widetilde{f}) & \text{для всех элементов } \widetilde{f} \in F_0; \\ \varphi(f_1)h & \text{при } \widetilde{f} = a; \end{cases} \qquad \text{где } \varphi \in \Phi \text{ и } h \in H_\varphi.$$

Это означает, что $\widetilde{\psi} = \psi \circ \alpha$, где

$$\psi(f) = \begin{cases} \varphi(f) & \text{для всех элементов } f \in F_0; \\ \varphi(f_1)h & \text{при } f = f_1; \end{cases} \qquad \text{где } \varphi \in \Phi \text{ и } h \in H_\varphi.$$

Гомоморфизм $\psi\colon F \to G$ лежит в Φ по условию II доказываемой теоремы. Следовательно, $\widetilde{\psi} \in \widetilde{\Phi}$. Таким образом, условия основной теоремы выполнены для множества $\widetilde{\Phi}$ гомоморфизмов из 0-индексированной группы $\widetilde{F}$ в G и, стало быть, $|\widetilde{\Phi}|$ делится на $|H|$ в силу основной теоремы работы [KM17]. Осталось заметить, что $|\Phi| = |\widetilde{\Phi}|$ в силу сюръективности гомоморфизма α. Теорема доказана.

Отметим, что мы не проверяли здесь, что отображение ψ задаёт гомоморфизм; это хоть и неочевидно, но всегда верно, смотрите параграф 1.

6. Открытые вопросы

Теоремы 1,2,3,4 утверждают, что некоторые величины делятся на частные двух целых чисел. Это может показаться удивительным, но мы не знаем, *можно ли заменить эти частные на их числители.*

Вопросы 1 и 2*). *Можно ли в теоремах 1 и 2 заменить частное* Δ_m/Δ_{m-1} *на его числитель* Δ_m *?*

В случае системы уравнений без коэффициентов вопрос 1 превращается в следующий вопрос, который был впервые сформулирован в [AsYo93] (для конечных групп F и G):

верно ли, что число гомоморфизмов из конечно порождённой группы F в группу G всегда делится на НОД$(|F/F'|, G)$ *?*

Задача остаётся нерешённой даже для конечных групп (насколько мы знаем). Обзор некоторых результатов на эту тему можно найти в [AsTa01], например, известно, что ответ положительный, если группа F абелева [Yosh93].

Аналогичный вопрос возникает в связи с теоремой 3.

Вопрос 3).** *Можно ли в теореме 3 заменить модуль однородности на на его числитель* Δ_{m+s} (смотрите лемму о модуле однородности)?

Что касается теоремы 4, то здесь тоже возникает аналогичный вопрос. Действительно, теорема 4 означает, в частности, что *если конечно порождённая группа F действует автоморфизмами на группе B, то число скрещенных гомоморфизмов $F \to B$ делится на* НОД$(\exp(F/F'), B)$.

Вопрос 4*). *Можно ли в приведённом выше утверждении заменить период* $\exp(F/F')$ *факторгруппы по коммутанту на порядок этой факторгруппы?*

Этот вопрос был впервые сформулирован в [AsYo93] (для конечных групп F и B). Чтобы убедиться, что вопрос 4 аналогичен вопросу 1 достаточно вспомнить, что абсолютная величина частного Δ_m/Δ_{m-1} в вопросе 1 есть период факторгруппы свободной абелевой группы $\mathbb{Z}^m$ по подгруппе, порождённой строками матрицы системы уравнений, а абсолютная величина числителя Δ_m — это порядок этой факторгруппы.

---

*) **Questions 6 and 7** в журнальной версии.

) **Question 8 в журнальной версии.

*) **Question 9** в журнальной версии.

7. Доказательство леммы Брауэра

Мы следуем оригинальному доказательству из [Bra69], но переводим его на более удобный (на наш взгляд) язык.

Лемма Брауэра [Bra69]. *Если U — конечная нормальная подгруппа группы V, то для всех $v \in V$ и $u \in U$ элементы $v^{|U|}$ и $(vu)^{|U|}$ сопряжены при помощи элемента из U.*

Доказательство. Группа $\mathbb{Z}$ действует перестановками на подгруппе U по формуле

$$a \circ i = v^{-i} a (vu)^i, \quad (\text{где } i \in \mathbb{Z} \text{ и } a \in U).$$

Пусть m — минимальная длина орбиты. Другими словами m — это минимальная длина цикла в разложении перестановки $a \mapsto v^{-1}avu$ (на множестве U) на независимые циклы. Тогда множество $X = \{a \in U \mid a \circ m = a\}$ представляет собой объединение всех орбит длины m, поэтому $|X|$ делится на m. С другой стороны, (по определению нашего действия) $X = \{a \in U \mid v^{-m} a (vu)^m = a\} = \{a \in U \mid a^{-1} v^m a = (vu)^m\}$ и, стало быть, $|X|$ есть порядок централизатора элемента v^m в U (поскольку в любой группе непустое множество вида $\{x \mid x^{-1}yx = z\}$ является смежным классом по централизатору элемента y). Значит $|X|$ делит $|U|$ и, следовательно, m делит $|U|$. Таким образом, $a \circ |U| = a = a$ (если a лежит в орбите длины m), что и требовалось.

ГЛАВА 6.
РАЗМЕРНОСТЬ МНОЖЕСТВА РЕШЕНИЙ СИСТЕМЫ УРАВНЕНИЙ В АЛГЕБРАИЧЕСКОЙ ГРУППЕ

1. Введение

Теорема Соломона [Solo69]. *В любой группе число решений системы уравнений без коэффициентов делится на порядок этой группы, если уравнений меньше, чем неизвестных.*

Здесь, как обычно, под *уравнением над группой* G понимается формальная запись вида $v(x_1,\dots,x_m)=1$, где v является словом, в котором каждая буква — это либо неизвестный, либо обратный к неизвестному, либо элемент группы G, называемый *коэффициентом* (коэффициентов, впрочем, нет по условию теоремы Соломона). Другими словами, левая часть уравнения — это элемент свободного произведения $G * F(x_1,\dots,x_m)$ группы G и свободной группы $F(x_1,\dots,x_m)$ ранга m (где m — число неизвестных).

Теорема Соломона обобщалась в разных направлениях, смотрите [Isaa70], [Стру95], [AmV11], [GRV12], [KM14], [KM17], [BKV19] и литературу, там цитируемую. Например, в [KM14] доказано следующее обобщение.

Теорема KM [KM14]. *Число решений системы уравнений над группой делится на порядок централизатора множества всех коэффициентов, если ранг матрицы, составленной из сумм показателей степеней при j-м неизвестном в i-м уравнении, меньше числа неизвестных.*

Для случая уравнений без коэффициентов эта теорема была доказана ранее Гордоном и Родригесом-Виллегасом [GRV12] (и в этом случае имеет место делимость на порядок централизатора пустого множества, то есть на порядок всей группы). Например, число решений системы уравнений $\{x^{100}y^{100}[x,y]^{777}=1,\ (xy)^{2022}=1\}$ всегда делится на порядок группы, поскольку эта система, хотя и не удовлетворяет условиям теоремы Соломона, но удовлетворяет условиям теоремы Гордона–Родригеса-Виллегаса: матрица составленная из сумм показателей степеней (которую мы будем называть *матрицей системы уравнений*) имеет в данном случае вид $\left(\begin{smallmatrix}100 & 100\\ 2022 & 2022\end{smallmatrix}\right)$, и ранг её равен единице (а число неизвестных равно двойке).

Отметим, что в этих теоремах о делимости не предполагается, что группа конечная; делимость всегда понимается в смысле кардинальной арифметики: каждый бесконечный кардинал делится на все меньшие ненулевые кардиналы. Впрочем, наиболее интересные применения упомянутых теорем относятся всё же к конечным группам.

Цель нашей работы — получить аналоги упомянутых теорем для уравнений над алгебраическими группами. Аналогом числа решений системы уравнений является в этом случае размерность многообразия решений. Более точно (но всё равно грубо и «с философской точки зрения») можно сказать, что размерность есть логарифм числа решений. Отметим, что решения (конечной или бесконечной) системы уравнений от m неизвестных над аффинной алгебраической группой G всегда образуют аффинное алгебраическое подмногообразие в G^m. Аналогом теоремы Соломона является следующее простое наблюдение.

Теорема 0. *В любой аффинной алгебраической группе G размерность каждой неприводимой компоненты многообразия решений конечной системы уравнений (возможно с коэффициентами) не меньше, чем*

$$\Big((\textit{число неизвестных}) - (\textit{число уравнений})\Big)\cdot \dim G.$$

Доказательство. Левые части уравнений задают морфизм алгебраических многообразий $\gamma\colon G^m \to G^n$, где m — число неизвестных, а n — число уравнений. Многообразие решений представляет собой слой $\gamma^{-1}\big(1,\dots,1\big)$. Каждая неприводимая компонента M многообразия G^m изоморфна G_0^m как алгебраическое многообразие (где G_0 — неприводимая компонента единицы группы G) и, следовательно, $\dim M = m\cdot\dim G$. Сужение морфизма γ на M представляет собой доминантный морфизм неприводимых алгебраических многообразий $M\to N$, где N есть замыкание (в топологии Зарисского) множества $\gamma(M)$. Остаётся воспользоваться следующим общим фактом (смотрите, например, [Бо72]).

Лемма о слое. *Если $\gamma\colon M\to N$ — доминантный морфизм неприводимых алгебраических многообразий, то для любой точки $s\in f(M)$ размерность слоя $\gamma^{-1}(s)$ не меньше чем $\dim M-\dim N$; причём N содержит непустое открытое подмножество $U\subset f(X)$ такое, что $\dim\gamma^{-1}(u)=\dim M-\dim N$ для любой точки $u\in U$.*

Теорему 0 едва ли можно назвать новым результатом; для уравнений без коэффициентов этот факт был отмечен, например, в [LM11].

Теорема Соломона выглядит лучше теоремы 0 в том смысле, что в теореме Соломона утверждается делимость, а в теореме 0 — лишь неравенство; но здесь ничего нельзя поделать — ни о какой делимости размерностей не может быть речи. Во всех прочих отношениях теорема 0 выглядит лучше; но с этим тоже ничего нельзя сделать, как показывают следующие простые примеры.

Неверная теорема. *В любой группе G число решений совместной системы уравнений, в которой неизвестных больше чем уравнений,*

1) *не меньше порядка этой группы;*
2) *делится на $|G|^{(\text{число неизвестных})-(\text{число уравнений})}$, если коэффициентов нет.*

Доказательство.

1) Первое утверждение неверно по простой причине. В симметрической группе из шести элементов уравнение $x^3y^3 = (1\ 2\ 3)$ имеет ровно три решения, так как x и y должны иметь одинаковую чётность, причём чётными эти перестановки быть не могут, поскольку куб чётной перестановки равен единице; произведение двух различных транспозиций всегда равно тройному циклу, причём половина из этих шести произведений даёт один тройной цикл, а половина — другой. (Заметим в скобках, что число решений обязано делиться на три по теореме КМ.)
2) Второе утверждение тоже неверно, как показывает уравнение $x^2y^2z^2 = 1$ в той же симметрической группе из шести элементов. Квадраты перестановок чётные, поэтому эти квадраты должны быть либо одним и тем же тройным циклом, либо один из квадратов есть тождественная перестановка, а два других — разные тройные циклы, либо все три квадрата суть тождественные перестановки. При этом из тождественной перестановки четыре квадратных корня, из циклов по одному. Всего получается $2 + 3 \cdot 2 \cdot 4 + 4 \cdot 4 \cdot 4 = 90$ решений.

Аналогом теоремы КМ служит следующее утверждение.

Теорема 1. *Если ранг матрицы системы уравнений с конечным числом неизвестных над аффинной алгебраической группой меньше числа неизвестных, то размерность каждой компоненты многообразия решений этой системы не меньше, чем размерность централизатора множества всех коэффициентов.*

Пример уравнения $[x, y] = 1$ (с нулевой матрицей и двумя неизвестными) над связной неабелевой группой показывает, что оценку из теоремы 1 (даже при отсутствии коэффициентов) нельзя усилить до неравенства

$$\dim(\textit{многообразие решений}) \geqslant \Big((\textit{число неизвестных}) - (\textit{ранг матрицы системы})\Big) \cdot \dim G,$$

подобного тому, что написано в теоремы 0.

Вопрос (предложенный рецензентом). *Верно ли, что в условиях теоремы 1 класс многообразия решений делится на класс централизатора коэффициентов в кольце Гротендика (многообразий)?*

Если это верно, то это включало бы в себя и теорему 1, и теорему КМ (для конечных групп).

Следствие (а вернее сказать, переформулировка теоремы 1 для случая уравнений без коэффициентов). *Пусть G — аффинная алгебраическая группа, а F — конечно порождённая группа, коммутант которой имеет бесконечный индекс. Тогда размерность каждой неприводимой компоненты многообразия гомоморфизмов $F \to G$ не меньше размерности группы G.*

Многообразию представлений (или *Многообразию гомоморфизмов*) $\mathrm{Hom}(F, G)$ конечно порождённой группы F в алгебраической группе G посвящено очень много работ, смотрите, например, [RBCh96], [MO10], [LM11], [LL13], [LS05], [Ki18], [LT18] и литературу там цитируемую. В частности, исследовался вопрос, когда существуют инъективные или *топологически сюръективные* гомоморфизмы, то есть гомоморфизмы с всюду плотным (в топологии Зарисского) образом, и насколько много таких гомоморфизмов. Например, в [Ki18] показано, что топологически сюръективные гомоморфизмы из фундаментальной группы замкнутой ориентированной поверхности рода больше единицы в вещественную полупростую алгебраическую группу всегда существуют, причём их много в некотором смысле. А в работе [BGGT12] показано, что из свободной группы в почти любую полупростую алгебраическую группу существует гомоморфизм, ограничение которого на любую нециклическую подгруппу топологически сюръективно. Смотрите также недавний обзор [ГКП18].

Вообще говоря, ни инъективные, ни топологически сюръективные гомоморфизмы уже не образуют многообразия, но следующая теорема показывает, что в каком-то смысле все «компоненты» этих (и похожих) немногообразий имеют размерность не меньше, чем размерность коммутанта группы G. Мы рассматриваем следующие свойства гомоморфизма $\varphi\colon F \to G$ из конечно порождённой группы F, содержащей некоторую подгруппу W, в алгебраическую группу G, содержащую замкнутую подгруппу A.

$\mathbf{F}_{W,A}$ (точность): $\varphi(W) \subseteq A$ и ограничение гомоморфизма φ на подгруппу $W \subseteq F$ инъективно;
$\mathbf{S}_{W,A}$ (топологическая сюръективность): замыкание подгруппы $\varphi(W)$ равно A;
$\mathbf{C}_{W,A}$ (связность): $\varphi(W) \subseteq A$ и замыкание подгруппы $\varphi(W)$ неприводимо.

Теорема 2. *Пусть A — подгруппа аффинной алгебраической группы G, а F — конечно порождённая группа, коммутант которой имеет бесконечный индекс. Тогда каждый гомоморфизм $F \to G$, обладающий какой-то (возможно бесконечной) комбинацией (конъюнкцией)*

$$\mathbf{P} = \left(\bigwedge_{W\in\mathcal{F}} \mathbf{F}_{W,A}\right) \wedge \left(\bigwedge_{W\in\mathcal{S}} \mathbf{S}_{W,A}\right) \wedge \left(\bigwedge_{W\in\mathcal{C}} \mathbf{C}_{W,A}\right), \quad \text{где } \mathcal{F},\mathcal{S},\mathcal{C} \text{ — некоторые семейства подгрупп группы } F,$$

перечисленных выше свойств содержится в $(\dim[A,A])$*-мерном неприводимом подмногообразии многообразия* $\mathrm{Hom}(F,G)$*, целиком состоящим гомоморфизмов обладающих той же комбинацией свойств* $\mathbf{P}$*, если индекс подгруппы* $[F,F]\cdot\prod\limits_{W\in\mathcal{F}\cup\mathcal{C}} W$ *в* F *бесконечен* (а на семейство $\mathcal{S}$ никаких условий не накладывается).

Заменить здесь размерность коммутанта на размерность всей группы нельзя, как показывает следующий простейший пример: из бесконечной циклической группы в тор $(\mathbb{C}^*)^{2022}$ есть топологически сюръективные гомоморфизмы, но они одиноки в том смысле, что всякое ненульмерное подмногообразие в $\mathrm{Hom}\left(\mathbb{Z},(\mathbb{C}^*)^{2022}\right)$ содержит не топологически сюръективный гомоморфизм (поскольку всякое бесконечное подмногообразие в $\mathbb{C}^*$ содержит элемент конечного порядка).

Убрать условия на семейства $\mathcal{F}$ и $\mathcal{C}$ тоже нельзя, как показывают простые примеры гомоморфизмов из $\mathbb{Z}$ в $\mathbf{SL}_n(\mathbb{C})$.

Например, теорема 2 говорит, что

> *если гомоморфизм из фундаментальной группы кренделя* $F=\langle x,y,z,t \mid [x,y]=[z,t]\rangle$ (или из любой другой группы, у которой образующих больше, чем соотношений) *в алгебраическую группу* G *инъективен на подгруппе* $\langle x,y,z\rangle$ *и переводит всякую неабелеву подгруппу во всюду плотную в* G *подгруппу, то он содержится в* $(\dim[G,G])$*-мерном подмногообразии многообразия* $\mathrm{Hom}(F,G)$*, состоящем из гомоморфизмов с теми же двумя свойствами.*

Частично теорема 2 также является аналогом известного факта [KM17]:

> *число сюръективных гомоморфизмов из конечно порождённой группы с бесконечным индексом коммутанта в* (конечную, если угодно) *группу* G *делится на порядок коммутанта группы* G. Например, *число пар элементов, порождающих* (2*-порождённую*) *группу всегда делится на порядок коммутанта этой группы.*

Но вообще говоря, в «алгебраической ситуации» возникают некоторые новые эффекты.

Теоремы 1 и 2 являются частными случаями более общей *основной теоремы*, которую мы формулируем в следующем параграфе. Наша основная теорема является прямым «алгебраическим» аналогом основной теоремы работы [KM17] (частными случаями которой являются все сформулированные выше теоремы о делимости и множество других любопытных фактов, смотрите [KM17] и [BKV19]).

Обозначения и соглашения, которые мы используем, в целом стандартны. Отметим только, что если $k\in\mathbb{Z}$, а x и y — элементы некоторой группы, то x^y, x^{ky} и x^{-y} обозначают $y^{-1}xy$, $y^{-1}x^ky$ и $y^{-1}x^{-1}y$, соответственно. Коммутант группы G мы обозначаем символом G' или $[G,G]$. Если X — подмножество некоторой группы, то $\langle X\rangle$, $\langle\langle X\rangle\rangle$ и $C(X)$ означают, соответственно, подгруппу, порождённую множеством X, нормальное замыкание множества X и централизатор множества X. Индекс подгруппы H группы G обозначается $|G:H|$. Буква $\mathbb{Z}$ обозначает множество целых чисел. Символом $\mathrm{Hom}(A,B)$ мы обозначаем множество гомоморфизмов из группы A в группу B. Свободную группу ранга n мы обозначаем символом $F(x_1,\ldots,x_n)$ или F_n. Символ $A*B$ обозначает свободное произведение групп A и B. Слово *многообразие* всегда означает (не обязательно неприводимое) квазипроективное алгебраическое многообразие над алгебраически замкнутым полем (произвольной характеристики), а слово *подмногообразие* означает локально замкнутое подмножество в многообразии. Все топологические термины относятся к топологии Зарисского.

2. Основная теорема

Группу F с фиксированным эпиморфизмом $F \to \mathbb{Z}$ мы называем *индексированной* группой. Этот эпиморфизм $F \to \mathbb{Z}$ мы называем *степенью* или *индексацией* и обозначаем deg; таким образом, для любого элемента f индексированной группы F определено целое число $\deg f$, причём группа F содержит элементы всех целых степеней и $\deg(fg) = \deg f + \deg g$ для любых $f, g \in F$.

Пусть имеется гомоморфизм $\varphi\colon F \to G$ из индексированной группы F в какую-то группу G и подгруппа H группы G. Мы называем подгруппу

$$H_\varphi = \bigcap_{f \in F} H^{\varphi(f)} \cap C(\{\varphi(f) \mid \deg f = 0\})$$

φ-сердцевиной подгруппы H. Другими словами, φ-сердцевина H_φ подгруппы H состоит из таких её элементов h, что $h^{\varphi(f)} \in H$ для всех f, причём $h^{\varphi(f)} = h$, если $\deg f = 0$.

Основная теорема. *Пусть H — аффинная алгебраическая подгруппа некоторой алгебраической группы G и Φ — некоторое подмногообразие многообразия гомоморфизмов из конечно порождённой индексированной группы F в G, причём множество Φ обладает следующими двумя свойствами.*

I. *Φ инвариантно относительно сопряжения элементами из H:*

$$\text{если } h \in H \text{ и } \varphi \in \Phi, \text{ то гомоморфизм } \psi\colon f \mapsto \varphi(f)^h \text{ тоже лежит в } \Phi.$$

II. *Для любого $\varphi \in \Phi$ любого элемента h из φ-сердцевины H_φ подгруппы H гомоморфизм ψ, определённый правилом*

$$\psi(f) = \begin{cases} \varphi(f) & \text{для всех элементов } f \in F \text{ степени ноль;} \\ \varphi(f)h & \text{для некоторого элемента } f \in F \text{ степени один} \text{ (а значит и для всех элементов степени один),} \end{cases}$$

также содержится в Φ.

Тогда размерность каждой неприводимой компоненты многообразия Φ не меньше, чем размерность группы H.

Отметим, что отображение ψ из условия I является гомоморфизмом при любом $h \in G$, а формула для ψ из условия II определяет гомоморфизм при любом $h \in C(\varphi(\ker \deg))$ ([KM17], лемма 0). Смысл условий I и II состоит в том, что эти гомоморфизмы лежат в Φ (при некоторых дополнительных предположениях об h).

Эта теорема является аналогом основной теоремы из [KM17], которая утверждает, что для любой (абстрактной) группы G и любой её подгруппы H мощность множества Φ гомоморфизмов из индексированной группы F в G делится на $|H|$ при выполнении условий I и II.

3. Доказательство теоремы 1

Пусть $A \subseteq G$ — подгруппа, порождённая всеми коэффициентами всех уравнений. В качестве группы F мы возьмём факторгруппу $F = (A * F(x_1, \dots, x_n))/\langle\langle\{v_i\}\rangle\rangle$ свободного произведения $A * F(x_1, \dots, x_n)$ группы A и свободной группы $F(x_1, \dots, x_n)$ по нормальной подгруппе $\langle\langle\{v_i\}\rangle\rangle$, порождённой левыми частями уравнений. В качестве множества Φ мы рассмотрим гомоморфизмы $F \to G$, тождественные на A (мы предполагаем, что A вкладывается в F посредством естественного отображения $A \to F$, поскольку если это отображение не инъективно, то решений нет и доказывать нечего). Ясно, что решения системы уравнений находятся в естественном взаимно однозначном соответствии с элементами множества Φ (которое, очевидно, является подмногообразием многообразия всех гомоморфизмов из F в G).

Условие на ранг означает, что группа F обладает эпиморфизмом на $\mathbb{Z}$, ядро которого содержит A. Если теперь в качестве H взять централизатор подгруппы A в G, то условия основной теоремы окажутся очевидным образом выполненными. Действительно, I выполняется, поскольку h централизует $A \subseteq G$ и, следовательно, ψ совпадает с φ на $A \subset F$, а II выполнено, поскольку элементы из $A \subset F$ имеют степень ноль и, значит, опять ψ совпадает с φ на $A \subset F$.

4. Доказательство теоремы 2

Если индекс коммутанта конечно порождённой группы бесконечен, то, как известно, существует эпиморфизм из этой группы на $\mathbb{Z}$. Поэтому из условий теоремы вытекает наличие индексации $\deg\colon F \to \mathbb{Z}$, ядро которой содержит все подгруппы из семейств $\mathcal{C}$ и $\mathcal{F}$ (и коммутант F' группы F, разумеется). Возьмём в качестве H коммутант A' группы A, а в качестве Φ — множество гомоморфизмов $F \to G$, совпадающих с данным гомоморфизмом $\alpha\colon F \to G$ по модулю H и совпадающих с α на элементах степени ноль:

$$\Phi = \{\varphi\colon F \to G \mid \quad \varphi(f)H = \alpha(f)H \text{ для всех } f \in F; \quad \varphi(f) = \alpha(f) \text{ для всех } f \in \ker\deg\}.$$

Ясно, что условия основной теоремы выполнены для этих F, $\deg$, Φ и H. Поэтому размерность каждой компоненты многообразия Φ не меньше, чем $\dim H = \dim A'$. Осталось проверить, что если гомоморфизм α обладает свойством $\mathbf{P}$, то все гомоморфизмы из Φ также обладают этим свойством. Пусть $\varphi \in \Phi$, то есть $\varphi(f) = \alpha(f)h_f$ для всех $f \in F$, где $h_f \in H = A'$.

Сперва заметим, что подгруппа $\varphi(W') = \alpha(W')$ плотна в коммутанте $H = A'$ группы A для всех $W \in \mathcal{S}$. Действительно, алгебраическая группа имеет конечную *коммутаторную ширину*, то есть морфизм $\varkappa\colon A^{2n} \to A'$, посылающий набор $(x_1, \ldots, x_n, y_1, \ldots, y_n)$ в произведение коммутаторов $\prod[x_i, y_i]$ сюръективен при достаточно большом n (смотрите, например, [BO88]). Образ всюду плотного множества при непрерывном сюръективном отображении всюду плотен (и D^{2n} плотно в A^{2n}, если множество D плотно в A). Так что в любом непустом открытом подмножестве коммутанта $A' = H$ группы A найдётся элемент из $\varkappa\left(\left(\alpha(W)\right)^{2n}\right) \subseteq \alpha(W') = \varphi(W')$, что и требовалось.

Пусть $U \subseteq A$ — непустое открытое множество. В силу плотности множества $\alpha(W)$ в A (где $W \in \mathcal{S}$) множество U содержит некоторый элемент $\alpha(w) = \varphi(w)h_w^{-1}$ где $w \in W$. Значит открытое множество $\varphi(w^{-1})U$ содержит $h_w^{-1} \in A' = H$. Следовательно, $\varphi(w^{-1})U \cap A'$ — непустое открытое подмножество в коммутанте $A' = H$ группы A. По доказанному оно содержит некоторый элемент $\varphi(w_1)$, где $w_1 \in W$. Следовательно, $U \ni \varphi(ww_1)$, и это завершает доказательство свойства $\mathbf{S}_{W,A}$ для гомоморфизма φ.

Свойства $\mathbf{F}_{W,A}$ (где $W \in \mathcal{F}$) и $\mathbf{C}_{W,A}$ (где $W \in \mathcal{C}$) выполняются по очевидной причине: все эти подгруппы W состоят из элементов степени ноль (по выбору индексации $\deg$), поэтому гомоморфизмы φ и α совпадают на таких подгруппах W.

5. Доказательство основной теоремы

Наше доказательство проводится по той же схеме, что доказательство основной теоремы работы [KM17]. Некоторая трудность состоит в том, что подгруппа $\ker\deg \subset F$ может оказаться не конечно порождённой, и поэтому множество гомоморфизмов $\ker\deg \to G$ не имеет, вообще говоря, естественной структуры алгебраического многообразия. Побороть эту неприятность позволяет следующее простое наблюдение:

> *существует такое конечное подмножество $K \subseteq \ker\deg \subset F$, что любые два гомоморфизма из F в G, совпадающие на K, совпадают на* $\ker\deg$.

Действительно, пусть $\ker\deg = \{d_1, d_2, \ldots\}$ и Π_i — это множество пар гомоморфизмов $F \to G$, совпадающих на $d_1, \ldots, d_i$. Ясно, что Π_i образуют убывающую цепочку подмногообразий в $\mathrm{Hom}(F, G) \times \mathrm{Hom}(F, G)$. Такая цепочка обязана стабилизироваться: $\Pi_n = \Pi_{n+1} = \ldots$ для некоторого n. Следовательно, можно положить $K = \{d_1, d_2, \ldots, d_n\}$.

Нам понадобится ещё аналогичный в некотором смысле факт:

> *существует такое конечное подмножество $A \subset F$, что если у двух гомоморфизмов α и β из F в G их композиции с естественной отображением $G \to G/H$ (где G/H — множество левых смежных классов G по H) совпадают на A, то они совпадают на всей группе F:*
>
> $$\forall \alpha, \beta \in \mathrm{Hom}(F, G) \qquad \Big(\forall a \in A \quad \alpha(a)H = \beta(a)H\Big) \Longrightarrow \Big(\forall f \in F \quad \alpha(f)H = \beta(f)H\Big).$$

Действительно, пусть теперь $F = \{d_1, d_2, \ldots\}$ и Π_i — это множество пар гомоморфизмов $\alpha, \beta\colon F \to G$ таких, что $\alpha(d_k)H = \beta(d_k)H$ при $k \leqslant i$. Ясно, что Π_i образуют убывающую цепочку многообразий. Такая цепочка обязана стабилизироваться: $\Pi_n = \Pi_{n+1} = \ldots$ для некоторого n. Следовательно, можно положить $A = \{d_1, d_2, \ldots, d_n\}$.

Рассмотрим теперь многообразие $X = G^K \times (G/H)^A$, состоящее из всех пар отображений $K \to G$ и $A \to G/H$ (где G/H — это многообразие левых смежных классов группы G по подгруппе H). На многообразии X действует группа H (сопряжениями): $h \circ (\alpha, \beta) = \big(f \mapsto h\alpha(f)h^{-1},\ a \mapsto h\beta(a)\big)$

Хвостом $\chi(\varphi)$ гомоморфизма $\varphi\colon F \to G$ мы будем называть пару (φ_0, φ_H), где φ_0 — это ограничение гомоморфизма φ на множество $K \subseteq \ker\deg \subset F$, а $\varphi_H\colon A \to \{gH\ ;\ g \in G\}$ — это отображение из A в G/H, которое

переводит элемент $a \in A$ в класс $\varphi(a)H$. Понятно, что отображение $\chi\colon \mathrm{Hom}(F,G) \to X$ является морфизмом алгебраических многообразий.

Мы будем говорить, что два гомоморфизма $\varphi, \psi \in \Phi$ *похожи*, и писать $\varphi \sim \psi$, если их хвосты лежат в одной орбите относительно описанного выше действия H на X. Отметим, что ни похожесть гомоморфизмов, ни совпадение их хвостов не зависят от выбора множеств A и K (они нам понадобились только для того, чтобы сопоставление гомоморфизму его хвоста оказалось морфизмом алгебраических многообразий, и действие группы H на хвостах оказалось действием алгебраической группы на алгебраическом многообразии):

$$\chi(\varphi) = \chi(\psi) \iff \begin{cases} \psi(f) = \varphi(f) & \text{для всех } f \in F \text{ степени ноль и} \\ \psi(f)H = \varphi(f)H & \text{для всех } f \in F. \end{cases} \qquad (*)$$

$$\varphi \sim \psi \iff \text{для некоторого } h \in H \begin{cases} \psi(f) = h\varphi(f)h^{-1} & \text{для всех } f \in F \text{ степени ноль и} \\ \psi(f)H = h\varphi(f)H & \text{для всех } f \in F. \end{cases}$$

Не ограничивая общности мы будем считать, что группа H неприводима (поскольку неприводимая компонента единицы группы H является группой той же размерности).

Каждый класс похожих гомоморфизмов является локально замкнутым подмногообразием в многообразии $\mathrm{Hom}(F,G)$, поскольку класс похожих — это прообраз орбиты при морфизме χ, а орбита действия алгебраической группы на алгебраическом многообразии всегда локально замкнута (смотрите, например, [BO88]). Основная теорема немедленно вытекает из следующего утверждения.

Утверждение. *Размерность каждой компоненты каждого класса похожих гомоморфизмов из* Φ *равна* $\dim H$. *Более точно, для каждого* $\varphi \in \Phi$

1) *размерность многообразия* X_φ *хвостов гомоморфизмов из* Φ, *похожих на* φ, *равна* $\dim H - \dim H_\varphi$;
2) *для каждого гомоморфизма* ψ, *похожего на* φ, *размерность каждой компоненты многообразия гомоморфизмов из* Φ *с таким же хвостом как у* ψ *равна* $\dim H_\varphi$.

Доказательство. Для доказательства утверждения 1) заметим, что множество $\chi(\Phi) \subseteq X$ инвариантно относительно действия H на X. Действительно, если на хвост гомоморфизма $\varphi \in \Phi$ подействовать элементом $h \in H$, то мы получим хвост гомоморфизма $f \mapsto h\varphi(f)h^{-1}$. Этот гомоморфизм лежит в Φ в силу условия I основной теоремы. Хвосты гомоморфизмов похожих на φ составляют орбиту хвоста гомоморфизма φ при этом действии. Размерность орбиты равна, как известно, коразмерности стабилизатора (это частный случай леммы о слое). Осталось заметить, что подгруппа H_φ есть стабилизатор хвоста гомоморфизма φ (по формуле $(*)$).

Докажем второе утверждение. Выберем элемент $x \in F$ степени один. Гомоморфизм $\alpha\colon F \to G$ однозначно определяется своим хвостом и значением $\alpha(x)$ (по формуле $(*)$). При этом для двух гомоморфизмов α и β с одинаковым хвостом частное $h = (\alpha(x))^{-1}\beta(x)$ должно стабилизировать этот хвост, то есть лежать в H_α. Действительно, для всех $f \in F$ степени ноль мы имеем

$$\alpha(f^x)^h = \alpha(f)^{\alpha(x)h} = \alpha(f)^{\beta(x)} \overset{*}{=} \beta(f)^{\beta(x)} = \beta(f^x) \overset{*}{=} \alpha(f^x), \quad \text{то есть } h \text{ централизует подгруппу } \alpha(\ker \deg)$$

(здесь и далее равенства $\overset{*}{=}$ имеют место в силу утверждения $(*)$); а для любого элемента $f \in F$ мы имеем

$$\alpha(x)\alpha(f)H = \alpha(xf)H \overset{*}{=} \beta(xf)H = \beta(x)\beta(f)H = \alpha(x)h\beta(f)H \overset{*}{=} \alpha(x)h\alpha(f)H, \quad \text{то есть } h \in \alpha(f)H\alpha(f)^{-1}.$$

Таким образом, $h = (\alpha(x))^{-1}\beta(x) \in H_\alpha$.

С другой стороны, если h — произвольный элемент из H_α, то отображение

$$f \mapsto \begin{cases} \alpha(f), & \text{если } \deg f = 0 \\ \alpha(x)h, & \text{если } f = x \end{cases} \qquad (**)$$

очевидно продолжается до гомоморфизма с таким же хвостом, как у α (смотрите замечание после формулировки основной теоремы в параграфе 2). Этот гомоморфизм лежит в Φ в силу условия II основной теоремы.

Мы показали, что для любого $\alpha \in \Phi$ отображение $H_\alpha \to \mathrm{Hom}(F,G)$, переводящее элемент $h \in H_\alpha$ в гомоморфизм $(**)$, является инъективным морфизмом алгебраических многообразий, образ которого представляет собой множество элементов из Φ с таким же хвостом как у α. Это означает, что $\dim \chi^{-1}(\chi(\alpha)) = \dim H_\alpha$.

Осталось заметить, что для похожих гомоморфизмов ψ и φ подгруппы H_φ и H_ψ изоморфны и даже сопряжены в H, поскольку они являются стабилизаторами точек $\chi(\varphi)$ и $\chi(\psi)$, лежащих в одной орбите при действии H на X. Это завершает доказательство утверждения 2).

Теперь заметим, что многообразие X_φ неприводимо (так как мы считаем группу H неприводимой), а каждая содержащая φ компонента Π_φ многообразия гомоморфизмов, похожих на φ, отображается на X_φ сюръективно, поскольку $\chi\bigl(f \mapsto h\varphi(f)h^{-1}\bigr) = h \circ \chi(\varphi)$, а многообразие $\{f \mapsto h\varphi(f)h^{-1} \mid h \in H\}$ неприводимо, так как является орбитой при действии связной группы H на $\mathrm{Hom}(F,G)$. Поэтому то, что размерность каждой компоненты каждого класса похожих гомоморфизмов из Φ равна $\dim H$, на самом деле вытекает из 1) и 2) в силу следующего общего факта.

Лемма. *Пусть γ — морфизм многообразия P в неприводимое многообразие N такой, что все компоненты всех слоёв $\gamma^{-1}(y)$ (где $y \in N$) имеют одинаковую размерность d, причём образ каждой компоненты многообразия P плотен в N. Тогда размерность каждой компоненты многообразия P равна* $\dim N + d$.

Доказательство. Пусть M — неприводимая компонента многообразия P. Выберем открытое непустое подмножество $U \subseteq \gamma(M) \subseteq N$, о котором идёт речь в лемме о слое. В силу неприводимости многообразия M в $\gamma^{-1}(U)$ найдётся точка x, не содержащаяся ни в какой другой компоненте многообразия P, кроме M. Тогда каждая компонента K слоя $\gamma^{-1}(\gamma(x))$, содержащая x, обязана целиком лежать в M и, следовательно, быть одной из компонент слоя ограничения морфизма γ на M. Понятно, что у остальных компонент этого слоя $M \cap \gamma^{-1}(\gamma(x))$ размерность не больше $d = \dim K$. По лемме о слое мы получаем $\dim M = \dim K + \dim N$, что и требовалось. Это завершает доказательство леммы, а вместе с ней и основной теоремы.

ГЛАВА 7.
О ЧИСЛЕ ЭПИ-, МОНО- И ГОМОМОРФИЗМОВ ГРУПП

0. Введение

Нас вдохновляли три классических результата про делимость в группах: теоремы Фробениуса (1895), Соломона (1969) и Ивасаки (1985).

Теорема Фробениуса [Frob95] (см. также [And16]). *Число решений уравнения $x^n = 1$ в конечной группе G делится на* $\text{НОД}(|G|, n)$ *для любого натурального n.*

Теорема Соломона [Solo69]. *В любой группе число решений конечной системы уравнений без коэффициентов делится на порядок этой группы, если уравнений меньше, чем неизвестных.*
Другими словами, *число гомоморфизмов $\langle x_1, \dots, x_m \mid w_1 = \dots = w_n = 1\rangle \to G$ делится на $|G|$, если $m > n$.*

Теорема Ивасаки [Iwa82]. *Для любого целого n число элементов конечной группы G, n-е степени которых лежат в данной подгруппе $A \subseteq G$, делится на $|A|$.*

Эти теоремы много раз обобщалась в разных направлениях, смотрите, например, [Frob03], [Hall36b], [Kula38], [Sehg62], [Isaa70], [BrTh88], [Yosh93], [Стру95], [AsTa01], [SaAs07], [AmV11], [GRV12], [ACNT13] [KM14], [KM17], [BKV19], [KR20] и литературу там цитируемую. Например, в [GRV12] доказано следующее обобщение теоремы Соломона.

Теорема Гордона–Родригеса-Виллегаса [GRV12]. *Число гомоморфизмов $F \to G$ делится на порядок группы G, если F — конечно порождённая группа, коммутант которой имеет бесконечный индекс.*

Позже выяснилось, что между тремя классическими результатами есть связь:
- в [KM17] доказан некоторый общий факт, который мы здесь называем *теоремой KM*, включающий в себя в качестве частных случаев теоремы Соломона и Ивасаки (и их обобщения);
- а в [BKV19] показано, что все три классических теоремы (и их обобщения, включая теорему KM) являются частными случаями одной очень общей теоремы, которую мы здесь называем *теоремой BKV* (смотрите следующий параграф).

Авторы [KM17] выводят из теоремы KM следующий факт о делимости числа гомоморфизмов, удовлетворяющих условиям типа инъективности или сюръективности. Пусть $F \supseteq W$ и $G \supseteq A$ — группы и

$$\text{Hom}(F, W; G, A) = \{\varphi\colon F \to G \mid \varphi(W) \subseteq A\}, \quad \text{Epi}(F, W; G, A) = \{\varphi\colon F \to G \mid \varphi(W) = A\},$$
$$\text{Mono}(F, W; G, A) = \{\varphi\colon F \to G \mid \varphi(W) \subseteq A \text{ и ограничение } \varphi \text{ на } W \text{ инъективно}\}.$$

Теорема об эпи- моно- и гомоморфизмах [KM17]. *Пусть W — подгруппа конечно порождённой группы F, коммутант F' которой имеет бесконечный индекс, а A — подгруппа группы G. Тогда*
а) *и $|\text{Hom}(F, W; G, A)|$, и $|\text{Epi}(F, W; G, A)|$, и $|\text{Mono}(F, W; G, A)|$ делятся на порядок нормализатора $N(A)$ подгруппы A, если индекс $|F : F'W|$ бесконечен*;
б) $|\text{Hom}(F, W; G, A)|$ *делится на* $|A|$;
в) $|\text{Epi}(F, W; G, A)|$ *делится на* $|A'|$.

Целью настоящей работы является добавление «фробениусовости» в эту теорему, то есть избавление от условий $|F : F'| = \infty$ и $|F : F'W| = \infty$. Ответ оказался ожидаемым для утверждений а) и б), гораздо менее очевидным в случае в), кроме того возникает новое утверждение г).

«Фробениусова» теорема об эпи- моно- и гомоморфизмах. *Пусть A — подгруппа группы G, а W — подгруппа конечно порождённой группы F. Тогда*
а) *и $|\text{Hom}(F, W; G, A)|$, и $|\text{Epi}(F, W; G, A)|$, и $|\text{Mono}(F, W; G, A)|$ делятся на* $\text{НОД}\Big(N(A), \exp\big(F/(F'W)\big)\Big)$;
б) $|\text{Hom}(F, W; G, A)|$ *делится на* $\text{НОД}\big(A, \exp(F/F')\big)$;
в) $|\text{Epi}(F, W; G, A)|$ *делится на* $\text{НОД}\big(A'A^{\exp(F/F')}, \exp(F/F')\big)$;
г) $|\text{Mono}(F, W; G, A)|$ *делится на* $\text{НОД}\Big(A, \exp\Big(F/\big(F'Z(W)\big)\Big)\Big)$.

Это сильно упрощённая формулировка теоремы 1, точнее её следствия, смотрите параграф 3. Всё, что здесь утверждается по поводу числа $|\text{Hom}(F, W; G, A)|$, не является новым — эти факты, установленные в [BKV19] (на немного другом языке), мы включили просто для полноты картины.

Отметим, что в этой теореме не предполагается, что группа G конечна. Мы придерживаемся обозначений из [BKV19]: *наибольшим общим делителем* $\text{НОД}(G, n)$ группы G и целого числа n мы называем наименьшее общее кратное порядков подгрупп группы G, делящих n; делимость всегда понимается в смысле кардинальной арифметики: каждый бесконечный кардинал делится на все меньшие ненулевые кардиналы (и, разумеется,

ноль делится на все кардиналы, а на ноль делится только ноль). Это означает, что $\text{НОД}(G,0)=|G|$ для любой группы G; а, например, $\text{НОД}(\mathbf{SL}_2(\mathbb{Z}),2020)=2$. Впрочем, читатель не очень много потеряет, если будет считать все группы в этой главе конечными, а в этом случае $\text{НОД}(G,n)=\text{НОД}(|G|,n)$ по теореме Силова (и поскольку конечная p-группа содержит подгруппы всех возможных порядков).

Пункт б) этой теоремы, разумеется, содержит классические теоремы

- Фробениуса (достаточно взять циклическую группу в качестве $F=W$ и положить $A=G$),
- Соломона, и даже Гордона–Родригеса-Виллегаса (достаточно взять в качестве $F=W$ конечно порождённую группу, коммутант которой имеет бесконечный индекс и положить $A=G$),
- и Ивасаки (достаточно положить $F=\mathbb{Z}\supseteq n\mathbb{Z}=W$).

А если, например, взять в пункте в) теоремы свободное произведение циклических групп в качестве $F=W$ и положить $A=G$, то мы получим следующий факт.

Следствие о системах порождающих. *Для любой группы G и любых $k_i\in\mathbb{Z}$ число наборов $(g_1,\dots,g_n)$ элементов группы G таких, что $\langle g_1,\dots,g_n\rangle=G$ и $g_i^{k_i}=1$, делится на* $\text{НОД}\left(G'\cdot G^{\text{НОК}(k_1,\dots,k_n)},\text{НОК}(k_1,\dots,k_n)\right)$.
(Здесь и далее $G^m\overset{\text{опр}}{=}\langle\{g^m\mid g\in G\}\rangle$.)

Читатель может догадаться, что ключом к нашему обобщению теоремы об эпи- моно- и гомоморфизмах является использование вместо теоремы KM её «фробениусова аналога», то есть теоремы BKV. Это верно, но на самом деле, мы обобщаем и саму теорему BKV, смотрите основную теорему в следующем параграфе и её доказательство в параграфе 2.

Обозначения и соглашения, которые мы используем, в целом стандартны. Отметим только, что если $k\in\mathbb{Z}$, а x и y — элементы некоторой группы, то x^y, x^{ky} и x^{-y} обозначают $y^{-1}xy$, $y^{-1}x^ky$ и $y^{-1}x^{-1}y$, соответственно. Коммутант группы G мы обозначаем символом G' или $[G,G]$, а центр группы G мы обозначаем символом $Z(G)$. Подгруппу группы G, порождённую n-ми степенями всех элементов мы обозначаем символом G^n. Мощность множества X мы обозначаем $|X|$. Если X — подмножество некоторой группы, то $\langle X\rangle$, $C(X)$ и $N(X)$ означают, соответственно, подгруппу, порождённую множеством X, централизатор множества X и нормализатор множества X. Индекс подгруппы H группы G обозначается $|G:H|$. Буква $\mathbb{Z}$ обозначает множество целых чисел. НОД и НОК — это наибольший общий делитель и наименьшее общее кратное. Символом $\exp(G)$ мы обозначаем период (экспоненту) группы G, если этот период конечен; и считаем $\exp(G)=0$, если период бесконечен. Кроме того, отметим ещё раз, что конечность групп нигде не предполагается по умолчанию, делимость всегда понимается в смысле кардинальной арифметики (бесконечный кардинал делится на все ненулевые кардиналы, не превосходящие его), а $\text{НОД}(G,n)\overset{\text{опр}}{=}\text{НОК}\left(\{|H|\ \mid\ H\text{ — подгруппа в }G\text{ и }|H|\text{ делит }n\}\right)$.

1. Основная теорема

Группу F с фиксированным эпиморфизмом $F\to\mathbb{Z}_n\overset{\text{опр}}{=}\mathbb{Z}/n\mathbb{Z}$ (где $n\in\mathbb{Z}$) мы называем *n-индексированной* группой [BKV19]. Этот эпиморфизм $F\to\mathbb{Z}_n$ мы называем *степенью* и обозначаем deg. Таким образом, для любого элемента f индексированной группы F определён элемент $\deg f\in\mathbb{Z}_n$, причём группа F содержит элементы всех степеней и $\deg(fg)=\deg f+\deg g$ для любых $f,g\in F$.

Пусть имеется гомоморфизм $\varphi\colon F\to G$ из n-индексированной группы F в какую-то группу G и подгруппа H группы G. Подгруппу $H_\varphi=\bigcap\limits_{f\in F}H^{\varphi(f)}\cap C\big(\varphi(\ker\deg)\big)$ называют *φ-сердцевиной* подгруппы H [KM17]. Другими словами, φ-сердцевина H_φ подгруппы H состоит из таких её элементов h, что $h^{\varphi(f)}\in H$ для всех f, причём $h^{\varphi(f)}=h$, если $\deg f=0$.

Теорема BKV [BKV19]**.** *Пусть целое число n делится на порядок подгруппы H некоторой группы G, и некоторое множество Φ гомоморфизмов из n-индексированной группы F в G удовлетворяет следующим условиям.*

I. *Φ инвариантно относительно сопряжения элементами из H: если $h\in H$ и $\varphi\in\Phi$, то гомоморфизм $\psi\colon f\mapsto\varphi(f)^h$ тоже лежит в Φ.*

II. *Для любого $\varphi\in\Phi$ и любого элемента h из φ-сердцевины H_φ подгруппы H гомоморфизм ψ, определённый правилом*

$$\psi(f)=\begin{cases}\varphi(f) & \text{для всех элементов } f\in F \text{ степени ноль;}\\ \varphi(f)h & \text{для некоторого элемента } f\in F \text{ степени один (а, значит, и для всех элементов степени один),}\end{cases}$$

также содержится в Φ.

Тогда $|\Phi|$ делится на $|H|$.

Отметим, что

- отображение ψ из условия I является гомоморфизмом при любом $h \in G$; а формула для ψ из условия II определяет гомоморфизм при любых $h \in H_\varphi$ (как объясняется в [BKV19]); смысл условий I и II состоит в том, что эти гомоморфизмы лежат в Φ;
- согласно (очень простой) лемме 3 из [BKV19] *в условии* II *теоремы BKV* $\psi(f) \in \varphi(f)H_\varphi$ *для всех* $f \in F$;
- условие «n делится на порядок подгруппы H» можно опустить, но тогда в заключении теоремы следует написать: «$|\Phi|$ делится на НОД(H, n)» (вместо «$|\Phi|$ делится на $|H|$»); это вытекает сразу из определения наибольшего общего делителя группы и числа (смотрите введение) и из того, что если условия I и II выполнены для H, то они выполнены и для любой подгруппы группы H;
- теорема KM (о которой мы говорили во введении) — это в точности теорема BKV при $n = 0$.

Основная теорема. *Пусть F — n-индексированная группа, H — подгруппа группы G, k — натуральное число, и Φ — некоторое множество гомоморфизмов из F в G, удовлетворяющее следующим условиям:*

(i) *для всех $\varphi \in \Phi$ и $h \in H$ гомоморфизм $\psi\colon f \mapsto \varphi(f)^h$ лежит в Φ;*

(ii) *для каждого $\varphi \in \Phi$, φ-сердцевина H_φ подгруппы H содержит подгруппу $H_{\varphi,k}$ такую, что*
   - $H_\varphi \supseteq H_{\varphi,k} \lhd \langle H_\varphi \cup \varphi(F)\rangle$;
   - $|H_\varphi / H_{\varphi,k}|$ *делит* k;
   - *если $\varphi \in \Phi$ и $\psi\colon F \to G$ — некоторый гомоморфизм, совпадающий с φ на элементах степени ноль и такой, что $\psi(w) \in \varphi(w)H_{\varphi,k}$ для всех элементов $w \in F$, степени которых делятся на k (то есть $\deg w \in k\mathbb{Z}_n$), то $\psi \in \Phi$.*

Тогда $|\Phi|$ делится на НОД(H, n).

Этот факт обобщает теорему BKV и по сути (то есть с учётом замечаний после теоремы BKV) превращается в неё, если положить $k = 1$ и $H_{\varphi,k} = H_\varphi$.

2. Доказательство основной теоремы

Можно предполагать, что $|H|$ делит n (по определению наибольшего общего делителя группы и числа и поскольку условия (i) и (ii) сохраняются при замене H на её подгруппу). Далее достаточно показать, что условия I и II теоремы BKV выполнены для этих F, G, H и Φ. Условие I очевидно выполнено в силу условия (i).

Проверим условие II. Пусть $\varphi \in \Phi$, элемент $f_1 \in F$ имеет степень один, $\varphi(f_1) = g$ и $h \in H_\varphi$. Надо показать, что гомоморфизм $\psi\colon F \to G$, совпадающий с φ на элементах степени ноль и переводящий f_1 в gh, лежит в Φ. Каждый элемент $w \in F$, степень которого делится на k, можно записать в виде $w = f_0 f_1^{ki}$ для некоторых $i \in \mathbb{Z}$ и $f_0 \in \ker\deg$. Тогда

$$\psi(w) = \psi(f_0 f_1^{ki}) = \psi(f_0)(gh)^{ki} = \varphi(f_0)(gh)^{ki} \quad \text{(поскольку } \varphi \text{ и } \psi \text{ совпадают на } \ker\deg\text{)}.$$

Подгруппа H_φ нормальна в $\langle H_\varphi, g\rangle$ по определению φ-сердцевины H_φ.

Лемма Брауэра [Bra69] (смотрите также [BKV19]). *Если U — конечная нормальная подгруппа группы V, то для всех $v \in V$ и $u \in U$ элементы $v^{|U|}$ и $(vu)^{|U|}$ сопряжены при помощи элемента из U.*

Применив лемму Брауэра к нормальной подгруппе $H_\varphi/H_{\varphi,k}$ группы $\langle g, H_\varphi\rangle / H_{\varphi,k}$, мы получим включение $(gh)^{ki} \in g^{kih'} H_{\varphi,k}$ для некоторого $h' \in H_\varphi$, который не зависит ни от i, ни от w, а определяется только гомоморфизмами φ и ψ. Поэтому

$$\psi(w) = \varphi(f_0)(gh)^{ki} \in \varphi(f_0)g^{kih'}H_{\varphi,k} \overset{(1)}{=} \left(\varphi(f_0)g^{ki}\right)^{h'} H_{\varphi,k} \overset{(2)}{=} \left(\varphi(f_0 f_1^{ki})\right)^{h'} H_{\varphi,k} \overset{(3)}{=} \left(\varphi(w)\right)^{h'} H_{\varphi,k}, \text{ где}$$

- равенство $\overset{(1)}{=}$ вытекает из того, что элемент $h' \in H_\varphi$ коммутирует с образом $\varphi(f_0)$ элемента f_0 степени ноль по определению φ-сердцевины H_φ;
- равенство $\overset{(2)}{=}$ вытекает из определения элемента g;
- равенство $\overset{(3)}{=}$ вытекает из определения элемента w.

Гомоморфизм $f \mapsto \left(\varphi(f)\right)^{h'}$ лежит в Φ по условию (i), и, следовательно, $\psi \in \Phi$ по условию (ii). Это завершает доказательство.

3. На что же делится число эпи- моно- и гомоморфизмов?

Пусть Φ — некоторое множество гомоморфизмов из n-индексированной группы F в группу G, а B и H — подгруппы в G. Подгруппу H назовём (B,k,Φ)-*гладкой*, если при всех $\varphi\in\Phi$ группа $H_\varphi\cap B$ содержит нормальную в $\langle H_\varphi,\varphi(F)\rangle$ подгруппу $\widehat{B}$ (зависящую от φ) такую, что $|H_\varphi/\widehat{B}|$ делит k.

Следующая лемма содержит вполне очевидные примеры гладких подгрупп.

Лемма о гладких подгруппах. *Следующие подгруппы группы G являются (B,k,Φ)-гладкими:*
1) *любая подгруппа, содержащаяся в B;*
2) *любая подгруппа, порядок которой делит k;*
3) *любая подгруппа H такая, что $|H:H\cap B|$ делит k, если $B\lhd G$.*

Доказательство. Достаточно взять в качестве $\widehat{B}$ следующие подгруппы: 1) H_φ; 2) $\{1\}$; 3) $H\cap B$.

Теорема 1. *Пусть A — подгруппа группы G, а W — подгруппа n-индексированной группы F, причём $\deg(W)=k\mathbb{Z}_n$. Пусть*

$$\mathrm{Hom}(F,W;G,A)=\{\varphi\colon F\to G\mid\varphi(W)\subseteq A\},\quad \mathrm{Epi}(F,W;G,A)=\{\varphi\colon F\to G\mid\varphi(W)=A\},$$
$$\mathrm{Mono}(F,W;G,A)=\{\varphi\colon F\to G\mid\varphi(W)\subseteq A\text{ и ограничение }\varphi\text{ на }W\text{ инъективно}\}.$$

Тогда $\mathrm{НОД}(H,n)$ *делит*
- а) $|\mathrm{Hom}(F,W;G,A)|$ *для любой* $\big(A,k,\mathrm{Hom}(F,W;G,A)\big)$*-гладкой подгруппы* $H\subseteq N(A)$ *группы* G;
- б) $|\mathrm{Epi}(F,W;G,A)|$ *для любой* $\big(A'A^n,k,\mathrm{Epi}(F,W;G,A)\big)$*-гладкой подгруппы* $H\subseteq N(A)$ *группы* G, *где* $A^n\overset{\text{опр}}{=}\langle\{a^n\mid a\in A\}\rangle$;
- в) $|\mathrm{Mono}(F,W;G,A)|$ *для любой* $\big(A,k,\mathrm{Mono}(F,W;G,A)\big)$*-гладкой подгруппы* $H\subseteq N(A)$ *группы* G, *если индексация группы F выбрана так, что* $\deg(w)=0$ *для каждого центрального (в W) элемента* $w\in W$ *такого, что* $w^n=1$.

(Заметим в скобках, что подгруппа $A'A^n$, о которой идёт речь в пункте б), и подгруппа $\{w\in Z(W)\mid w^n=1\}$, о которой говорится в пункте в), суть ни что иное, как вербальная подгруппа группы A и маргинальная подгруппа группы W, соответствующие многообразию абелевых групп экспоненты n.)

Доказательство. Достаточно проверить, что условия (i) и (ii) основной теоремы выполнены для данных F, G, H, k, Φ и $H_{\varphi,k}=\widehat{B}$ (где $\widehat{B}$ из определения гладкой подгруппы B, в качестве которой мы берём A в пунктах а) и в) и $A'A^n$ в пункте б)). Первые два пункта условия (ii) заведомо выполнены по определению гладкости, нуждается в проверке только последний пункт условия (ii).

а) $B=A$ и $\Phi=\mathrm{Hom}(F,W;G,A)$. Условие (i) очевидно выполнено, поскольку $H\subseteq N(A)$. Условие (ii) тоже выполнено, поскольку для всех $w\in W$ мы имеем $\psi(w)\in\varphi(w)\widehat{B}\subseteq\varphi(w)A=A$, то есть $\psi\in\Phi$, что и требовалось.

б) $B=A'A^n$ и $\Phi=\mathrm{Epi}(F,W;G,A)$. Условие (i) очевидно выполнено по той же причине: $H\subseteq N(A)$. Условие (ii) тоже выполнено: $A\overset{(1)}{=}\varphi(W)\overset{(2)}{\subseteq}\psi(W)A'A^n\overset{(3)}{=}\psi(W)\varphi(W'W^n)\overset{(4)}{=}\psi(W)\psi(W'W^n)=\psi(W)$, где
   - $\overset{(1)}{=}$ выполнено по определению $\Phi\ni\varphi$;
   - $\overset{(2)}{\subseteq}$ выполнено по определению ψ из условия (ii) при $B=A'A^n\supseteq\widehat{B}=H_{\varphi,k}$;
   - $\overset{(3)}{=}$ следует из $\overset{(1)}{=}$;
   - $\overset{(4)}{=}$ следует из того, что $\deg(W'W^n)=\{0\}$, а ψ и φ из условия (ii) совпадают на элементах степени нуль.

   В итоге мы получили, что $A=\psi(W)$, то есть $\psi\in\Phi$, что и требовалось.

в) $B=A$ и $\Phi=\mathrm{Mono}(F,W;G,A)$. Условие (i) очевидно выполнено по той же причине: $H\subseteq N(A)$. Покажем, что (ii) тоже выполнено. Во-первых, $\psi(W)\subseteq\varphi(W)A=A$. Осталось показать, что $\ker\psi\cap W=\{1\}$. Пусть $w\in\ker\psi\cap W$. Тогда
   - для каждого $w'\in W$ мы имеем $1=\psi([w,w'])=\varphi([w,w'])$ (так как коммутаторы имеют степень нуль, а на элементах степени нуль φ и ψ совпадают), следовательно, $[w,w']=1$ (так как гомоморфизм φ инъективен на W), то есть $w\in Z(W)$;
   - аналогично получаем $1=\psi(w^n)=\varphi(w^n)$ (так как $\deg(w^n)=n\deg(w)=0$, а на элементах степени нуль φ и ψ совпадают), следовательно, $w^n=1$ (так как гомоморфизм φ инъективен на W).

   Мы получили, что w — центральный элемент группы W и $w^n=1$, а такие элементы имеют степень нуль по условию. Значит, $\varphi(w)=\psi(w)=1$, то есть $w=1$ в силу того, что $\varphi\in\mathrm{Mono}(F,W:G,A)$. Стало быть, $\ker\psi\cap W=\{1\}$, что и требовалось.

Следствие. *В условиях теоремы 1 и* $|\mathrm{Hom}(F,W;G,A)|$, *и* $|\mathrm{Epi}(F,W;G,A)|$, *и* $|\mathrm{Mono}(F,W;G,A)|$ *делятся на* $\mathrm{НОД}\big(k,\ N(A)\big)$. *Кроме того,*

а) $|\mathrm{Hom}(F,W;G,A)|$ *делится*
- *на* $\mathrm{НОД}\big(n,\ A\big)$,
- *а также на* $\mathrm{НОД}\Big(n,\ |A|\cdot\mathrm{НОД}\big(k,\ |G/A|\big)\Big) = \mathrm{НОД}(n,\ |G|,\ k\cdot|A|)$, *если* $A\triangleleft G$ *и* G *конечна*;

б) $|\mathrm{Epi}(F,W;G,A)|$ *делится*
- *на* $\mathrm{НОД}\big(n,\ A'A^n\big)$ *и даже на* $\mathrm{НОД}\big(n,\ H\big)$, *где* H *— любая подгруппа в* $N(A)$ *такая, что* $|(C(A'A^n)\cap H : Z(A'A^n)\cap H|$ *делит* k,
- *а также на* $\mathrm{НОД}\Big(n,\ |A'A^n|\cdot\mathrm{НОД}\big(k,\ |G/(A'A^n)|\big)\Big) = \mathrm{НОД}(n,\ |G|,\ k\cdot|A'A^n|)$, *если* $A\triangleleft G$ *и* G *конечна*;

в) *если* $\deg\big(\{w\in Z(W)\mid w^n=1\}\big)=\{0\}$, *то* $|\mathrm{Mono}(F,W;G,A)|$ *делится*
- *на* $\mathrm{НОД}\big(n,\ A\big)$,
- *а также на* $\mathrm{НОД}\Big(n,\ |A|\cdot\mathrm{НОД}\big(k,\ |G/A|\big)\Big) = \mathrm{НОД}(n,\ |G|,\ k\cdot|A|)$, *если* $A\triangleleft G$ *и* G *конечна.*

Доказательство. Первое утверждение (о делимости на $\mathrm{НОД}\big(k,\ N(A)\big)$) вытекает немедленно из теоремы 1 и утверждения 2) леммы о гладких подгруппах.

Остальные утверждения этого следствия также вытекают из теоремы 1 и подходящего утверждения о гладких подгруппах.

а) Делимость на $\mathrm{НОД}\big(n,\ A\big)$ сразу вытекает из утверждения 1) леммы о гладких подгруппах. Делимость на $\mathrm{НОД}(n,\ |G|,\ k\cdot|A|)$ следует из утверждения 3) леммы о гладких подгруппах. Действительно, достаточно в теореме 1 взять в качестве H p-подгруппу группы G, порядок которой есть максимальная степень p^i числа p, делящая $\mathrm{НОД}(n,k|A|,|G|)$, причём выбрать H
- внутри A, если p^i делит $|A|$;
- содержащей силовскую p-подгруппу группы A в противном случае.

Эта подгруппа будет $\big(A,k,\mathrm{Hom}(F,W;G,A)\big)$-гладкой по лемме о гладких подгруппах. Значит, $|H|$ делит $\mathrm{Hom}(F,W;G,A)$ в силу теоремы 1. Проделав это для всех простых p, мы получим нужную делимость.

б) Второе утверждение пункта б) доказывается точно также, как второе утверждение пункта а). Чтобы доказать первое утверждение пункта б), по теореме 1 достаточно убедиться, что подгруппа H является $\big(A'A^n,k,\mathrm{Epi}(F,W;G,A)\big)$-гладкой, то есть при всех $\varphi\in\mathrm{Epi}(F,W;G,A)$ группа $H_\varphi\cap(A'A^n)$ содержит нормальную в $\langle H_\varphi,\varphi(F)\rangle$ подгруппу $\widehat{B}$ такую, что $|H_\varphi/\widehat{B}|$ делит k. В качестве такой подгруппы $\widehat{B}$ достаточно взять $Z(A'A^n)\cap H_\varphi$. Действительно,

$$H_\varphi \overset{(1)}{\subseteq} C\big(\varphi(\ker\deg)\big) \overset{(2)}{\subseteq} C\big(\varphi(W'W^n)\big) \overset{(3)}{=} C\big(A'A^n\big),\quad \text{где}$$

$\overset{(1)}{\subseteq}$ вытекает из определения φ-сердцевины H_φ, $\overset{(2)}{\subseteq}$ вытекает из того, что $\deg(W'W^n)=\{0\}$, а $\overset{(3)}{=}$ вытекает из равенства $\varphi(W)=A$.

Значит, по теореме Лагранжа $\big|H_\varphi/\big(Z(A'A^n)\cap H_\varphi\big)\big|$ делит $\big|\big(C(A'A^n)\cap H\big)/\big(Z(A'A^n)\cap H\big)\big|$, что делит k по условию.

в) Здесь всё полностью аналогично пункту а).

ГЛАВА 8.
ВЕРБАЛЬНО ЗАМКНУТЫЕ ПОЧТИ СВОБОДНЫЕ ПОДГРУППЫ

Введение

Подгруппа H группы G называется *вербально замкнутой* [MR14] (см. также [Rom12], [PX13], [Mazh17]), если всякое уравнение вида

$$w(x_1, x_2, \ldots) = h, \quad \text{где } w \text{ — это элемент свободной группы } F(x_1, x_2, \ldots) \text{ и } h \in H,$$

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

$$\{w_1(x_1, x_2, \ldots) = 1, \ldots, w_m(x_1, x_2, \ldots) = 1\}, \quad \text{где } w_i \in H * F(x_1, x_2, \ldots),$$

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

Ясно, что ретракт любой группы (то есть образ такого эндоморфизма ρ, что $\rho \circ \rho = \rho$) является алгебраически замкнутой подгруппой. Нетрудно показать [MR14], что для конечно порождённых подгрупп конечно определённых групп верно и обратное:

> *конечно порождённая подгруппа конечно определённой группы алгебраически замкнута тогда и только тогда, когда она является ретрактом.*

Для (более слабого) свойства вербальной замкнутости подобное структурное описание неизвестно. Однако в свободных группах ситуация простая: вербально замкнутые подгруппы, алгебраически замкнутые подгруппы и ретракты — это одно и то же.

Теорема Мясникова–Романькова. *Вербально замкнутые подгруппы конечно порождённых свободных групп являются ретрактами.*

Аналогичным образом дело обстоит в свободных нильпотентных группах [PX13].

Мы обобщаем теорему Мясникова–Романькова в двух направлениях: во-первых, мы рассматриваем подгруппы произвольных групп (а не только свободных); а во-вторых, мы рассматриваем не только свободные подгруппы, но и почти свободные подгруппы H, то есть обладающие свободной подгруппой конечного индекса (в H).

Основная теорема. *Пусть G — произвольная группа и H — её вербально замкнутая почти свободная бесконечная недиэдральная подгруппа, любая бесконечная абелева подгруппа которой является циклической. Тогда*

1) *H алгебраически замкнута в G;*
2) *если группа G конечно порождена над H* (то есть $G = \langle H, X\rangle$ для некоторого конечного подмножества $X \subseteq G$), *то H является ретрактом группы G;*
   в частности, группа H конечно порождена, если G конечно порождена.

(Для бесконечной группы *недиэдральная* означает неизоморфная свободному произведению двух групп порядка два.)

Отметим, что каждая нетривиальная свободная подгруппа H удовлетворяет всем условиям теоремы и, следовательно, является ретрактом в любой конечно порождённой группе, содержащей H в качестве вербально замкнутой подгруппы. Уже этот факт представляется нетривиальным. Следующее утверждение, немедленно вытекающее из основной теоремы, является усилением теоремы 1(1) из [Mazh17].

Следствие. *В свободном произведении конечного числа конечных групп всякая вербально замкнутая бесконечная недиэдральная подгруппа является ретрактом.*

Во втором параграфе мы обсудим примеры, показывающие, что основная теорема неулучшаема в некотором смысле (впрочем, там остаются открытые вопросы). Параграф 3 посвящён доказательству этой теоремы. Наше рассуждение чуть более хитрое, чем в [MR14], но также основано на использовании слов Ли [Lee02].

Зафиксируем некоторые обозначения. Если $k \in \mathbb{Z}$, а x и y — элементы некоторой группы, то x^y, x^{ky} и x^{-y} обозначают $y^{-1}xy$, $y^{-1}x^ky$ и $y^{-1}x^{-1}y$, соответственно. Коммутант группы G мы обозначаем G'. Если X — подмножество некоторой группы, то $|X|$, $\langle X\rangle$ и $C(X)$ означают, соответственно, мощность множества X, подгруппу, порождённую множеством X и централизатор множества X. Индекс подгруппы H группы G обозначается $|G{:}H|$. Свободное произведение групп A и B мы обозначаем символом $A * B$, а свободную группу с базисом $x_1, \ldots, x_n$ — символом $F(x_1, \ldots, x_n)$ или F_n.

Примеры

Посмотрим, нельзя ли отбросить какие-нибудь условия основной теоремы.

Подгруппа H бесконечная. Это условие не может быть отброшено. Рассмотрим в качестве G прямое произведение двух экземпляров группы кватернионов (порядка восемь) с объединёнными центрами. Ясно, что сомножители этого произведения не являются ретрактами (и, следовательно, не являются алгебраически замкнутыми, поскольку для конечно порождённых подгрупп конечно определённых групп это одно и то же). Действительно, ядро такой гипотетической ретракции обязано быть нетривиальной нормальной подгруппой. Поскольку группа G нильпотентна, эта нетривиальная нормальная подгруппа обязана нетривиально пересекать центр группы G (см., например, [KaM82]). Это немедленно приводит к противоречию, поскольку центр в данном случае содержится в каждом из сомножителей.

Покажем, что второй (например) сомножитель H такого произведения $G = Q_8 \underset{C}{\times} Q_8$ (где $C = \{\pm 1\}$) вербально замкнут в G. Пусть уравнение

$$w(x_1, \ldots, x_n) = (1, h'),$$

где $(1, h') \in H$ имеет решение $x_i = (h_i, h_i')$ в G. Покажем, что это уравнение имеет решение и в H. Пусть некоторая переменная x_i входит в $w(x_1, \ldots, x_n)$ в нечётной суммарной степени k. В этом случае уравнение $x^k = h'$ имеет решение q в Q_8 и подстановка $x_i = (1, q)$ и $x_j = (1, 1)$ при $j \neq i$ является решением исходного уравнения в H.

Пусть теперь все переменные входят в $w(x_1, \ldots, x_n)$ в четных суммарных степенях. В таком случае $h' = 1$ или $h' = -1$ (иначе уравнение не имеет решений в G). Если $h' = 1$, то подстановка $x_i = (1, 1)$ для всех i есть решение уравнения в H. Если же $h' = -1$, то ровно одна из подстановок: $x_i = (1, h_i)$ или $x_i' = (1, h_i')$ является решением рассматриваемого уравнения в H.

Подгруппа H недиэдральная. Мы не знаем, нужно ли это условие. Оставляем это в качестве открытого вопроса.

Любая бесконечная абелева подгруппа группы H является циклической. То, что это условие отбросить нельзя, показывает небольшая модификация рассмотренного выше примера центрального произведения $Q_8 \underset{C}{\times} Q_8$ (где $C = \{\pm 1\}$), в котором сомножители вербально замкнуты, но не являются ретрактами. Положим теперь $G = Q_8 \underset{C}{\times} Q_8 \times F$, где F — какая-нибудь нетривиальная свободная группа, а в качестве подгруппы H возьмём произведение второго и третьего сомножителя в этом произведении. Из доказанного выше вытекает, что H является вербально замкнутой подгруппой и не является ретрактом (поскольку ретракт ретракта — это ретракт, а второй сомножитель не является ретрактом в G и даже в $Q_8 \underset{C}{\times} Q_8$ по доказанному выше).

Подгруппа H почти свободная. Это условие не может быть отброшено. Известно (см., например, теоремы 1.5 и 3.3 в [Адян75]), что свободная бернсайдова группа $B(m, n)$ ранга $m \geqslant 2$ и нечётного периода $n \geqslant 665$ бесконечна, а любая ее абелева подгруппа конечна. Рассмотрим группу $G = Q_8 \underset{C}{\times} Q_8 \times B(2, 2017)$, а в качестве подгруппы H возьмём произведение второго и третьего сомножителя в этом произведении. Аналогично тому, как это было сделано выше, мы можем заключить, что H является вербально замкнутой подгруппой и не является ретрактом.

Группа G конечно порождена над H в пункте 2). Следующий пример показывает, что это условие нельзя отбросить. Возьмём подгруппу $H = \langle 1 \rangle$ целых чисел в аддитивной группе G целых p-адических чисел. Ясно, что она вербально замкнута (в абелевых группах вербально замкнутые подгруппы это то же самое, что алгебраически замкнутые подгруппы, и то же самое, что сервантные (чистые) подгруппы). С другой стороны, группа G не допускает вообще никаких нетривиальных разложений в прямую сумму (см., например, [Кур67]), то есть H не ретракт.

Доказательство основной теоремы

Заметим, что всякая почти свободная группа H является линейной (даже над $\mathbb{Z}$, если H счётна), поскольку свободная группа (любой мощности), как хорошо известно, линейна (над некоторым полем) (см., например, [KaM82]), а почти линейная группа всегда линейна. Следовательно, *H нётерова по уравнениям*, (как и всякая линейная (над полем) группа [BMRe99]), то есть всякая система уравнений с коэффициентами из H и конечным числом неизвестных эквивалентна своей конечной подсистеме.*) Это в свою очередь означает, что H является ретрактом любой конечно порождённой над H группы, содержащей H в качестве алгебраически замкнутой подгруппы [MR14]. Поэтому достаточно доказать пункт 1) теоремы.

*) Отметим ещё, что группа, содержащая нётерову по уравнениям подгруппу конечного индекса, сама нётерова по уравнениям [BMRo97].

Рассмотрим сперва случай циклической подгруппы H. Напомним, что всякую целочисленную матрицу целочисленными элементарными преобразованиями можно привести к диагональному виду. Это означает, что всякую конечную систему уравнений над H

$$\{w_1(x_1, x_2, \ldots) = 1,\ \ldots,\ w_m(x_1, x_2, \ldots) = 1\}, \quad \text{где } w_i \in H * F(x_1, x_2, \ldots),$$

заменами вида $w_i \to w_i w_j^{\pm 1}$ и $x_i \to x_i x_j^{\pm 1}$ можно преобразовать к виду

$$\{x_1^{n_1} u_1(x_1, x_2, \ldots) = h_1,\ \ldots,\ x_m^{n_m} u_m(x_1, x_2, \ldots) = h_m\}, \quad \text{где } u_i \in (H * F(x_1, x_2, \ldots))',\ n_i \in \mathbb{Z} \text{ и } h_i \in H.$$

При этом полученная система будет иметь столько же решений, сколько исходная (и в G, и в H). Предположим, что эта система имеет решение в G. Пусть каждое слово u_i представляется в виде произведения s коммутаторов в $H * F(x_1, x_2, \ldots)$. Тогда каждое отдельное уравнение $x_i^{n_i}[y_1, z_1] \ldots [y_s, z_s] = h_i$ (где y_j и z_j — новые переменные) имеет решение в G и, следовательно, имеет решение $\left(\widehat{x}_i, \widehat{y}_1^{(i)}, \widehat{z}_1^{(i)}, \ldots\right)$ в H (поскольку подгруппа H вербально замкнута). Но тогда, очевидно, $(\widehat{x}_1, \widehat{x}_2, \ldots)$ есть решение всей системы (так как коммутант подгруппы H тривиален).

Случай почти циклической подгруппы H легко сводится к случаю циклической группы в силу следующего простого наблюдения:

> *бесконечная почти циклическая группа, не содержащая бесконечных нециклических абелевых подгрупп, является либо циклической, либо диэдральной.*

Действительно, почти циклическая группа всегда содержит конечную нормальную подгруппу, факторгруппа по которой либо циклическая, либо диэдральная (см., например, [Sta71]). Эта конечная нормальная подгруппа обязана быть тривиальной, поскольку иначе мы найдём в её централизаторе (который имеет конечный индекс) элемент бесконечного порядка и получим бесконечную нециклическую абелеву подгруппу.

Рассмотрим теперь более трудный случай не почти циклической группы H.

Лемма 1. *В почти свободной группе, не являющаяся почти циклической, любой элемент раскладывается в произведение двух элементов бесконечного порядка.*

Доказательство. Понятно, что это утверждение достаточно доказать для конечно порождённых групп. Напомним, что конечно порождённая почти свободная группа допускает такое действие на (ориентированном) дереве, что стабилизаторы вершин конечны [KPS73]. Напомним также, что любой автоморфизм дерева, не имеющий неподвижных точек, имеет единственную инвариантную прямую [Ser77].

Рассмотрим такое действие группы H на дереве T. Пусть $h \in H$ — элемент, который мы хотим разложить, и $T_h \subseteq T$ — множество неподвижных точек для h. Если порядок элемента h бесконечен, то $h = h^2 h^{-1}$ — искомое разложение, поэтому мы будем считать, что порядок элемента h конечен и, следовательно, T_h непусто (и, стало быть, связно).

Возьмём какой-нибудь элемент $g \in H$ бесконечного порядка с инвариантной прямой l_g. Если элемент $g^{-1}h$ не имеет неподвижных точек, то его порядок бесконечен и $h = g \cdot (g^{-1}h)$ — искомое разложение. Пусть $a \in T$ — неподвижная точка для $g^{-1}h$. Тогда $h(a) = g(a) = b$.

Равенство $h(a) = b$ показывает, что отрезок, соединяющий точки a и b, обязан пересекать поддерево T_h по единственной точке, а именно, по по своей середине c. А равенство $g(a) = b$ показывает, что прямая l_g обязана проходить через точку c и пересекать отрезки $[a, c]$ и $[c, b]$ по отрезкам одинаковой ненулевой длины δ (в противном случае расстояния от l_g до a и до b не равны и, значит, $g(a) \neq b$). Элемент g обязан действовать сдвигом на 2δ на своей инвариантной прямой l_g, но нам пока важно только равенство $T_h \cap l_g = \{c\}$.

Возьмём теперь другой элемент $g' \in H$ бесконечного порядка с другой инвариантной прямой $l_{g'} \neq l_g$ (такой элемент существует, поскольку группа H не почти циклическая). Аналогичные рассуждения показывают, что либо $h = g' \cdot ((g')^{-1}h)$ — искомое разложение, либо $T_h \cap l_{g'} = \{c'\}$ для некоторой точки c'. В последнем случае рассмотрим элемент $g'' = g^k g' g^{-k}$. Его инвариантной прямой будет служить, очевидно, $g^k(l_{g'})$ и мы видим, что эта прямая не будет пересекать поддерево T_h, если число k выбрано достаточно большим положительным или отрицательным. Поэтому, в этом последнем случае $h = g'' \cdot ((g'')^{-1}h)$ — искомое разложение. (Более точно, если $c' \neq c$, то в качестве k можно взять единицу или любое другое ненулевое число; если же $c' = c$, то k нужно выбрать так, чтобы $|2k\delta|$ было больше чем расстояние от c до конца отрезка или луча $l_g \cap l_{g'}$.)

Лемма 2. *Если h_1 и h_2 — элементы бесконечного порядка почти свободной группы, любая бесконечная абелева подгруппа которой является циклической, и $h_1^k = h_2^k$ для некоторого ненулевого целого k, то $h_1 = h_2$.*

Доказательство. Корни из элемента лежат в его централизаторе, поэтому достаточно показать, что централизатор элемента бесконечного порядка h циклический. Этот централизатор $C(h)$ является почти свободной группой (как и любая подгруппа почти свободной группы) с бесконечным центром. Отсюда немедленно вытекает, что группа $C(h)$ почти циклическая. Осталось сослаться на упомянутый в начале параграфа факт: бесконечная почти циклическая группа без бесконечных абелевых нециклических подгрупп является либо циклической, либо диэдральной. При этом в рассматриваемом случае группа не может быть диэдральной, поскольку центр централизатора нетривиален.

Следующая лемма хорошо известна.

Лемма WA. *Если подгруппа H группы G такова, что любая конечная система уравнений вида*

$$\{w_1(x_1,\dots,x_n) = h_1,\ \dots,\ w_m(x_1,\dots,x_n) = h_m\}, \quad \text{где } w_i \in F(x_1,\dots,x_n) \text{ и } h_i \in H \tag{1}$$

имеющая решение в G, имеет решение в H, то H алгебраически замкнута.

Доказательство. Просто обозначим коэффициенты новыми буквами, которые будем считать неизвестными. Например, разрешимость уравнения

$$xyh_1[x^{2022}, h_2]y^{-1} = 1$$

эквивалентна разрешимости системы

$$\{xyz[x^{2022}, t]y^{-1} = 1,\ z = h_1,\ t = h_2\}.$$

Нам теперь понадобится один полезный инструмент. Напомним, что *словом Ли* для свободной группе ранга r от m переменных называют элемент $L(z_1,\dots,z_m)$ свободной группы ранга m такой, что

1) если $L(v_1,\dots,v_m) = L(v_1',\dots,v_m') \neq 1$ в F_r, то элементы $v_i' \in F_r$ получаются из элементов $v_i \in F_r$ одновременным сопряжением, то есть для некоторого $w \in F_r$ имеют место равенства $v_i' = v_i^w$ для всех $i = 1,\dots,m$;
2) $L(v_1,\dots,v_m) = 1$ тогда и только тогда, когда элементы $v_1,\dots,v_m$ группы F_r лежат в одной циклической подгруппе.

В работе [Lee02] такие слова были построены для всех целых $r, m \geqslant 2$. На самом деле, нетрудно сообразить, что это означает наличие *универсального слова Ли* от m переменных, то есть такого элемента $L(z_1,\dots,z_m) \in F_m$, что свойства 1) и 2) выполняются во всех свободных группах F_r и даже в F_∞.

Лемма о словах Ли. *Для любого положительного целого m существует такой элемент $L(z_1,\dots,z_m) \in F_m$, что свойства 1) и 2) выполняются во всех свободных группах F_r и даже в F_∞.*

Доказательство. Это утверждение немедленно вытекает из результата Ли и следующего простого факта:

свободная группа F_∞ вкладывается в F_2 в качестве мальнормальной подгруппы,

то есть такой подгруппы $S \subset F_2$, что $S^f \cap S = \{1\}$ для всех $f \in F_2 \setminus S$. Этот факт следует, например, из результата Вайза [Wise01]:

> *в свободной группе всякое множество, удовлетворяющее условию малого сокращения $C(5)$, свободно порождает мальнормальную подгруппу.*

Таким образом, слово Ли для свободной группе ранга два является универсальным, то есть годится и для группы F_∞.

Приступим к доказательству теоремы. Итак, мы считаем, что вербально замкнутая подгруппа H группы G почти свободна, не содержит бесконечных нециклических абелевых подгрупп и содержит нормальную (в H) неабелеву свободную подгруппу F индекса N (в H). Воспользовавшись леммой WA, мы можем считать, что система (1) имеет решение в G. Мы хотим показать, что эта система имеет решение в H.

Пусть $L(z_1,\dots,z_{2m+2})$ — это универсальное слово Ли от $2m+2$ переменных. Воспользовавшись леммой 1, для каждого элемента h_i выберем в H такой элемент f_i, что порядки элементов $h_i f_i$ и f_i бесконечны. Выберем ещё в F два некоммутирующих элемента u_1, u_2.

Уравнение

$$L\Big((w_1(x_1,\dots,x_n)y_1)^N,\dots,(w_m(x_1,\dots,x_n)y_m)^N, y_1^N,\dots,y_m^N, z_1^N, z_2^N\Big) = f,$$

где $f = L\Big((h_1 f_1)^N, \ldots, (h_m f_m)^N, f_1^N, \ldots, f_m^N, u_1^N, u_2^N\Big) \in F$, имеет решение в G по построению (его решением служит следующий набор: решение системы (1) в качестве x_i, элементы f_i в качестве y_i и u_i в качестве z_i).

Подгруппа H вербально замкнута в G и $f \in H$, значит последнее уравнение имеет некоторое решение $\widehat{x}_i, \widehat{y}_j, \widehat{z}_k$ в H.

В правой части уравнения стоит значение слова Ли на некоторых элементах свободной группы F (поскольку $h^N \in F$ для всех $h \in H$), причём элементы u_1^N и u_2^N не коммутируют (поскольку элементы свободной группы u_1 и u_2 выбраны не коммутирующими), значит, они не лежат в одной циклической подгруппе и поэтому из свойства 2) слов Ли следует, что $f \neq 1$. Согласно свойству 1) это влечёт равенства

$$(w_i(\widehat{x}_1, \ldots, \widehat{x}_n)\widehat{y}_i)^{Nw} = (h_i f_i)^N, \quad \widehat{y}_i^{Nw} = f_i^N \quad \text{и} \quad \widehat{z}_i^{Nw} = u_i^N \quad \text{для некоторого } w \in F.$$

Поскольку извлечение корня из элементов бесконечного порядка в H однозначно (по лемме 2), мы имеем равенства

$$(w_i(\widehat{x}_1, \ldots, \widehat{x}_n)\widehat{y}_i)^{w} = h_i f_i, \quad \widehat{y}_i^{w} = f_i, \quad \text{и} \quad \widehat{z}_i^{w} = u_i,$$

то есть $\widehat{x}_i^w$ — это решение системы (1) в H, что и требовалось.

ГЛАВА 9.
ПОЧТИ СВОБОДНЫЕ ГРУППЫ БЕЗ КОНЕЧНЫХ НОРМАЛЬНЫХ ПОДГРУПП СИЛЬНО ВЕРБАЛЬНО ЗАМКНУТЫ

0. Введение

Подгруппа H группы G называется *вербально замкнутой* [MR14] (см. также [Rom12], [PX13], [Mazh17], [KM18], [Mazh18]), если всякое уравнение вида

$$w(x_1, x_2, \ldots) = h, \quad \text{где } w \text{ — это элемент свободной группы } F(x_1, x_2, \ldots) \text{ и } h \in H,$$

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

$$\{w_1(x_1, x_2, \ldots) = 1, \ldots, w_m(x_1, x_2, \ldots) = 1\}, \quad \text{где } w_i \in H * F(x_1, x_2, \ldots),$$

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

Разумеется, алгебраическая замкнутость сильнее, чем вербальная замкнутость. Однако во многих случаях эти свойства оказываются эквивалентными. 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.) Например, сильно вербально замкнутыми являются

– все абелевы группы [Mazh18];
– все свободные группы [KM18];
– фундаментальные группы всех связных поверхностей, кроме, возможно, бутылки Клейна [Mazh18].

Основной результат этой главы можно сформулировать так.

Теорема 1. *Сильно вербально замкнутыми являются*

1) *все почти свободные группы, не имеющие неединичных нормальных конечных подгрупп;*
2) *все свободные произведения* $\ast\limits_{i\in I} H_i$, *где* I *— конечное или бесконечное множество,* $|I| > 1$ *и* H_i *— нетривиальные группы, удовлетворяющие нетривиальным тождествам (возможно, разным).*

Значительная часть теоремы 1 была известна ранее: в работе [Mazh18] доказано утверждение 2) для всех недиэдральных групп, при дополнительном предположении, что множество I конечно; а в работе [KM18] была доказана сильная вербальная замкнутость всех бесконечных почти свободных недиэдральных групп, не содержащих бесконечных абелевых нециклических подгрупп. В работе [KM18] можно найти также примеры почти свободных групп, не являющихся сильно вербально замкнутыми.

Фактически бóльшую часть данной главы занимает доказательство следующего частного случая (обоих утверждений) теоремы 1:

бесконечная диэдральная группа сильно вербально замкнута.

Для всех недиэдральных групп теорема 1 сравнительно легко выводится из известных фактов (в параграфе 1).

Проблема с бесконечной диэдральной группой состоит в том, что она, с одной стороны, «слишком абелева», чтобы к ней могли быть применены изощрённые инструменты, основанные на словах Ли [Lee02] (смотрите [MR14], [Mazh17], [KM18], [Mazh18]), а с другой стороны, «слишком неабелева», чтобы с ней работали простые соображения (смотрите [KM18], [Mazh18]). Разумеется, диэдральная группа метабелева, и это лежит в основе нашего подхода. В параграфе 3 мы приводим «явный» критерий вербальной (и алгебраической) замкнутости бесконечной диэдральной подгруппы, аналогичный (в некотором смысле) следующему простому утверждению об абелевых подгруппах, которое фактически доказано в [Mazh18]:

абелева подгруппа H вербально (и алгебраически) замкнута в группе G тогда и только тогда, когда она тривиально пересекается с коммутантом G' группы G, и образ H в факторгруппе G/G' является сервантной подгруппой.

Понятие алгебраической замкнутости может быть охарактеризовано на структурном языке, если группа H *нётерова по уравнениям* (любая система уравнений над H от конечного числа неизвестных эквивалентна своей конечной подсистеме), а именно, алгебраическая замкнутость в этом случае эквивалентна «локальной ретрактности» (смотрите параграф 1):

нётерова по уравнениям подгруппа H группы G алгебраически замкнута в G тогда и только тогда, когда она является ретрактом каждой конечно порождённой над H подгруппы группы G (то есть подгруппы вида $\langle H, X\rangle$, где множество $X \subseteq G$ конечно).

Все почти свободные группы (включая бесконечную диэдральную) нётеровы по уравнениям [KM18], поэтому теорема 1 означает, что

каждая почти свободная группа H, не содержащая неединичных конечных нормальных подгрупп, является ретрактом каждой конечно порождённой группы, содержащей H в качестве вербально замкнутой подгруппы.

В параграфе 1 мы доказываем некоторые вспомогательные факты общего характера, которые помогают свести доказательство основной теоремы к случаю, когда объемлющая группа G, содержащая вербально замкнутую диэдральную подгруппу H, является расширением абелевой группы Q при помощи элементарной абелевой 2-группы C, и, таким образом, подгруппа Q является C-модулем. Параграф 2 содержит необходимые сведения о таких модулях. В параграфе 3 мы формулируем и доказываем критерий алгебраической (и вербальной) замкнутости бесконечной диэдральной подгруппы.

В последнем параграфе мы разбираем основной этап доказательства на конкретном примере. По сути это простейший пример ситуации, когда отсутствие алгебраической замкнутости почти очевидно, а доказательство отсутствия вербальной замкнутости требует нетривиальных построений. Мы постарались сделать последний параграф независимым от всего остального, поэтому читатели могут ознакомиться с этим параграфом сначала, чтобы получить представление о том, что происходит. Предупреждаем, однако, что разобранный там пример иллюстрирует не все трудности, с которыми нам пришлось столкнуться.

Обозначения, которые мы используем, в целом стандартны. Отметим только, что если X — подмножество некоторой группы, то $|X|$, $\langle X\rangle$ и $C(X)$ означают, соответственно, мощность множества X, подгруппу, порождённую множеством X, и централизатор множества X. Буквы $\mathbb{Z}$ и $\mathbb{Q}$ обозначают множество целых и рациональных чисел. Циклическую группу порядка k, порождённую элементом x, мы обозначаем символом $\langle x\rangle_k$. Свободную группу с базисом $x_1,\dots,x_n$ мы обозначаем $F(x_1,\dots,x_n)$ (или F_n, если базис неважен).

1. Вспомогательные леммы

Утверждение 1. *Нётерова по уравнениям подгруппа H алгебраически замкнута в группе G тогда и только тогда, когда H является ретрактом каждой конечно порожденной над H подгруппы группы G.*

Доказательство. Пусть подгруппа H алгебраически замкнута в группе G. Тогда H алгебраически замкнута в любой подгруппе $\widetilde{G}$ группы G, содержащей H. Если подгруппа $\widetilde{G}$ конечно порождена над H, то H есть ретракт группы $\widetilde{G}$ в силу следующего факта [MR14]:

нётерова по уравнениям алгебраически замкнутая подгруппа H конечно порождённой над H группы является ретрактом.

Пусть H является ретрактом каждой конечно порожденной над H подгруппы группы G, и пусть система уравнений $S=\{w_1(x_1,\dots,x_n)=1,\dots,w_m(x_1,\dots,x_n)=1\}$, где $w_i\in F(x_1,\dots,x_n)*H$, имеет решение $g_1,\dots,g_n$ в G. По условию существует ретракция $\rho\colon\langle H,g_1,\dots,g_n\rangle\to H$. Значит $\rho(g_1),\dots,\rho(g_n)$ — это решение системы S в H, что и требовалось.

Утверждение 2. *Группа H, в которой каждое конечное подмножество содержится в сильно вербально замкнутой подгруппе, вербально замкнутой в H, сильно вербально замкнута.*

Доказательство. Предположим, что группа H вложена в некоторую бóльшую группу G в качестве вербально замкнутой подгруппы, и некоторая конечная система уравнений S с коэффициентами из H имеет решение в G. Множество коэффициентов этой системы содержится в некоторой подгруппе $H_1\subseteq H$, которая одновременно сильно вербально замкнута и вербально замкнута в H. Последнее означает, что H_1 вербально замкнута в G (поскольку вербальная замкнутость — это транзитивное свойство). Теперь сильная вербальная замкнутость подгруппы H_1 влечёт разрешимость системы S в группе $H_1\subseteq H$, что и требовалось.

Следствие. *Утверждение 2) теоремы 1 верно для всех групп, кроме, возможно, бесконечной диэдральной.*

Доказательство. Утверждения 2 позволяет свести доказательство к случаю, когда множество I конечно, поскольку подпроизведение $H_1=\mathop{*}\limits_{i\in J}H_i$ очевидным образом вербально замкнуто (и даже является ретрактом) в группе $H=\mathop{*}\limits_{i\in I}H_i$ для любого $J\subseteq I$. В случае же, когда множество I конечно, утверждение 2) теоремы 1 доказано для всех недиэдральных групп в [Mazh18].

Утверждение 3. *Утверждение* 1) *теоремы 1 верно для всех групп, кроме, возможно, бесконечной диэдральной.*

Доказательство. Если группа H является почти циклической, то в ней найдётся конечная нормальная подгруппа K, факторгруппа по которой либо тривиальная, либо бесконечная циклическая, либо бесконечная диэдральная [Sta71]. Конечная нормальная подгруппа K обязана быть тривиальной по условию. Все абелевы группы сильно вербально замкнуты [Mazh18], и всё доказано в этом случае.

Если же группа H не является почти циклической, то в ней найдётся неабелева свободная нормальная подгруппа F конечного индекса n. Это означает, что централизатор вербальной подгруппы $V = \langle\{h^n \mid h \in H\}\rangle \subseteq F$ нормален и конечен (поскольку централизатор любой неабелевой свободной подгруппы в почти свободной группе конечен). Значит $C(V) = \{1\}$ по условию. Стало быть, централизатор некоторой конечно порождённой подгруппы $V_1 \subseteq V$ тривиален (поскольку опять централизатор неабелевой свободной подгруппы почти свободной группы всегда конечен, и убывающая цепочка конечных групп стабилизируется). Остаётся воспользоваться следующим утверждением ([Mazh18], следствие 1):

> *если вербальная подгруппа V некоторой группы H свободная неабелева, и централизатор некоторой конечно порождённой подгруппы группы V тривиален, то группа H сильно вербально замкнута.*

Оставшаяся часть работы посвящена доказательству сильной вербальной замкнутости бесконечной диэдральной группы.

Лемма 1 ([PX13], лемма 1.1)**.** *Если $V(G)$ — вербальная подгруппа группы G, а H — вербально замкнутая подгруппа группы G, то образ подгруппы H при естественном гомоморфизме $G \to G/V(G)$ вербально замкнут.*

2. Коммутирующие инволюции на абелевых группах

Пусть конечная элементарная абелева 2-группа C (конечная прямая степень группы из двух элементов) действует автоморфизмами на конечно порождённой абелевой группе, то есть Q является C-модулем. Пусть X — множество всех гомоморфизмов (*характеров*) $\chi\colon C \to \{\pm 1\}$ и

$$Q_\chi = \{q \in Q \mid cq = \chi(c)q \text{ для всех } c \in C\}.$$

Имеется естественный гомоморфизм из группы Q в аддитивную группу векторного пространства (над полем рациональных чисел) $\mathbb{Q} \otimes Q$, посылающий $q \in Q$ в $1 \otimes q$ (тензорное произведение здесь и далее над $\mathbb{Z}$). Ядром этого гомоморфизма служит периодическая часть $T(Q)$ группы Q. Действие группы C на Q естественным образом продолжается до линейного представления $C \to \mathbf{GL}(\mathbb{Q} \otimes Q)$. Это представление вполне приводимо и неприводимые представления одномерны (это характеры группы C). Таким образом, $\mathbb{Q} \otimes Q = \bigoplus\limits_{\chi \in X} (\mathbb{Q} \otimes Q_\chi)$. Естественные проекции $\mathbb{Q} \otimes Q \to \mathbb{Q} \otimes Q_\chi$ мы обозначим p_χ. Векторы $p_\chi(v) \in \mathbb{Q} \otimes Q_\chi$ мы будем называть χ-*компонентами* вектора $v \in \mathbb{Q} \otimes Q$ и обозначать v_χ. Ясно, что $\bigoplus\limits_{\chi \in X} (1 \otimes Q_\chi) \subseteq 1 \otimes Q \subseteq \bigoplus\limits_{\chi \in X} p_\chi(1 \otimes Q)$, причём если одно из этих включений является равенством, то и другое является равенством; в этом случае мы будем говорить, что C-модуль $1 \otimes Q$ *разложим*. В общем случае C-модуль $\bigoplus\limits_{\chi \in X} p_\chi(1 \otimes Q)$ можно назвать *разложимым замыканием* модуля $1 \otimes Q$.

Нам понадобится следующая простая формула, справедливая для любого характера χ и любого $q \in Q$:

$$1 \otimes \left(\left(\prod_{c \in C}\Big(1 + \chi(c)c\Big)\right) \cdot q\right) = \Big(2^{|C|} \otimes q\Big)_\chi \quad \text{и} \quad |T(Q)| \cdot \prod_{c \in C}\Big(1 + \chi(c)c\Big) \cdot q = \Big(2^{|C|} \cdot |T(Q)| \cdot q\Big)_\chi, \tag{1}$$

(где $x_\chi \in Q_\chi$ в правой части второго равенства — это компоненты элемента $x \in \bigoplus Q_\chi \subseteq Q$). Второе равенство здесь следует из первого, поскольку ядром гомоморфизма $q \mapsto 1 \otimes q$ служит периодическая часть группы Q (и первое равенство показывает, что модуль $2^{|C|} \cdot |T(Q)| \cdot Q$ содержится в прямой сумме χ-компонент модуля Q). Для доказательства первого равенства заметим, что χ-компонента элемента $1 \otimes q$ 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 $\chi(c) = -\chi'(c)$. Из формулы (1) вытекает, что для всех $q \in Q$ имеет место равенство

$$1 \otimes \left(\sum_{\chi \in X}\left(\prod_{c \in C}\Big(1 + \chi(c)c\Big)\right) \cdot q\right) = 2^{|C|} \otimes q \quad \text{и} \quad |T(Q)| \cdot \sum_{\chi \in X}\left(\prod_{c \in C}\Big(1 + \chi(c)c\Big)\right) \cdot q = |T(Q)| \cdot 2^{|C|} \cdot q. \tag{2}$$

Отметим ещё следующее простое обобщение формулы (1): *Если* $\varphi\colon C \to \widehat{C}$ *— эпиморфизм из одной конечной элементарной абелевой 2-группы на другую и* $\widehat{q} \in \widehat{Q}$ *— элемент разложимого* $\widehat{C}$*-модуля* $\widehat{Q}$*, то для любого характера* χ *группы* C

$$1 \otimes \left(\left(\prod_{c \in C} \bigl(1 + \chi(c)\varphi(c)\bigr) \right) \cdot \widehat{q} \right) = \begin{cases} 2^{|C|} \otimes \widehat{q}_{\widehat{\chi}}, & \text{если } \chi = \widehat{\chi} \circ \varphi; \\ 0, & \text{если } \chi \neq \widehat{\chi} \circ \varphi \text{ ни для какого характера } \widehat{\chi}\colon \widehat{C} \to \{\pm 1\}. \end{cases} \qquad (*)$$

Назовём элемент $q \in Q$ *простым*, если χ-компонента $(1 \otimes q)_\chi = p_\chi(1 \otimes q)$ для некоторого характера χ является примитивным элементом свободной абелевой группы $p_\chi(1 \otimes Q)$, то есть $p_\chi(1 \otimes q) \notin k \cdot p_\chi(1 \otimes Q) = p_\chi(k \otimes Q)$ при $k \in \mathbb{Z} \setminus \{\pm 1\}$.

Лемма о простых элементах. *Элемент* $q \in Q$ *является простым тогда и только тогда, когда его порядок бесконечен, и группа* Q *раскладывается в прямую сумму* $Q = \langle q \rangle \oplus M$*, причём подгруппа* $M \subset Q$ *является* C*-подмодулем, то есть* $cm \in M$ *для всех* $c \in C$ *и* $m \in M$*.*

Доказательство. Пусть q — простой элемент, то есть $(1 \otimes q)_\chi$ является примитивным элементом группы $p_\chi(1 \otimes Q)$. Ясно, что это означает бесконечность порядка элемента q (иначе $1 \otimes q = 0$). Кроме того, $p_\chi(1 \otimes Q) = \langle (1 \otimes q)_\chi \rangle \oplus D$ для некоторой подгруппы D (поскольку примитивный элемент свободной абелевой группы может быть включён в некоторый базис). Это означает, что $1 \otimes Q = \langle 1 \otimes q \rangle \oplus \bigl(p_\chi^{-1}(D) \cap (1 \otimes Q)\bigr)$. При этом группа $A = p_\chi^{-1}(D)$ является C-подмодулем. Следовательно, $Q = \langle q \rangle \oplus \psi^{-1}(A)$, где $\psi\colon Q \to \mathbb{Q} \otimes Q$ — естественный гомоморфизм, посылающий x в $1 \otimes x$.

Доказательство в другую сторону мы оставляем читателям в качестве упражнения, поскольку мы не собираемся этим пользоваться.

Пример. Пусть группа $C = \langle c \rangle_2$ действует на $Q = \mathbb{Z} \oplus \mathbb{Z}$ перестановкой координат. Тогда имеется два характера: $X = \{\chi_+, \chi_-\}$, где $\chi_+(c) = 1$ и $\chi_-(c) = -1$. При этом $Q_{\chi_+} = \langle (1,1) \rangle$, а $Q_{\chi_-} = \langle (1,-1) \rangle$. Подгруппа $Q_{\chi_+} \oplus Q_{\chi_-}$ имеет индекс два в Q. Разложимое замыкание имеет вид

$$\overline{Q} = \left\langle \left(\frac{1}{2}, \frac{1}{2} \right) \right\rangle \oplus \left\langle \left(\frac{1}{2}, -\frac{1}{2} \right) \right\rangle = \{(x,y) \in \mathbb{Q}^2 \mid x + y \in \mathbb{Z} \ni x - y\}.$$

Проекции $p_{\chi_\pm}\colon \overline{Q} \to \bigl(\overline{Q}\bigr)_{\chi_\pm}$ имеют вид $p_{\chi_+}(x,y) \mapsto \left(\frac{x+y}{2}, \frac{x+y}{2}\right)$ и $p_{\chi_-}(x,y) \mapsto \left(\frac{x-y}{2}, \frac{y-x}{2}\right)$. Элемент $(2,5)$ не является простым, поскольку $(2,5) = 7 \cdot \left(\frac{1}{2}, \frac{1}{2}\right) - 3 \cdot \left(\frac{1}{2}, -\frac{1}{2}\right)$. Вообще, нетрудно убедиться, что в этом примере элемент $(x,y) \in Q$ является простым тогда и только тогда, когда $x \pm y = \pm 1$ при каком-то выборе знаков.

3. Алгебраически замкнутые бесконечные диэдральные подгруппы

Мы будем иметь дело с конечно порождённой группой G, у которой подгруппа $Q = \bigl\langle \{g^2 \mid g \in G\} \bigr\rangle$, порождённая квадратами всех элементов, абелева. Группа Q в этой ситуации представляет собой конечно порождённую абелеву группу, на которой действует автоморфизмами конечная элементарная 2-абелева группа $C = G/Q$ по правилу

$$(gQ) \circ q \overset{\text{опр}}{=} gqg^{-1} \quad \text{(эта формула корректна, так как } Q \text{ абелева).}$$

Таким образом, группа Q превращается в C-модуль, и мы можем применять результаты предыдущего параграфа. Отметим только, что теперь мы придерживаемся мультипликативных обозначений, то есть пишем, например, $cq_1c^{-1}q_2^2$ вместо $cq_1 + 2q_2$. Для упрощения обозначений мы положим $\widetilde{q} \overset{\text{опр}}{=} q^{|T(Q)|}$. Формула (1) приобретает вид

$$w_\chi(\widetilde{q}) \overset{\text{опр}}{=} f_\chi(c_1, f_\chi(c_2, \ldots, f_\chi(c_{|C|}, \widetilde{q}) \ldots)) = \left((\widetilde{q})^{2^{|C|}} \right)_\chi, \quad \text{где } \{c_1, \ldots, c_{|C|}\} = C, \qquad (1')$$

а $f_\chi(gQ, x) \overset{\text{опр}}{=} xgx^{\chi(gQ)}g^{-1}$ — «косой коммутатор» (который определён корректно, то есть не зависит от выбора представителя g в смежном классе $c = gQ$).

Аналог формулы (2) приобретает вид

$$\prod_{\chi \in X} w_\chi(\widetilde{q}) = (\widetilde{q})^{2^{|C|}} \quad \text{для всех } q \in Q. \qquad (2')$$

Сильная вербальная замкнутость бесконечной диэдральной группы очевидным образом вытекает из утверждения 1 и следующей теоремы.

Теорема 2. *Пусть $H = \langle b\rangle_2 \leftthreetimes \langle a\rangle_\infty$ — бесконечная диэдральная подгруппа конечно порождённой группы G. Тогда следующие условия равносильны:*

1) *подгруппа H вербально замкнута в G;*
2) *подгруппа H алгебраически замкнута в G;*
3) *подгруппа H — ретракт группы G* (то есть образ эндоморфизма ρ такого, что $\rho\circ\rho = \rho$);
4) *a^2Q' является простым элементом G/Q-модуля Q/Q', где $Q = \big\langle\{g^2 \mid g\in G\}\big\rangle$.*

Доказательство. Для доказательства импликации 4) $\Longrightarrow$ 3) сперва заметим, что $H\cap Q' = \{1\}$ (иначе бы элемент a^2Q' имел бы конечный порядок в Q/Q' и не был бы простым).

Теперь по лемме о простых элементах мы получаем нормальную в G/Q' подгруппу $M\subset Q/Q'$ такую, что $Q/Q' = \big\langle a^2Q'\big\rangle \times M$. Тогда композиция естественных гомоморфизмов $G\to G/Q'\to (G/Q')/M = G_1$ действует инъективно на H, а получившаяся группа G_1 является почти циклической группой (подгруппа, порождённая квадратами всех её элементов, порождается образом элемента a^2). Как известно, почти циклическая группа всегда содержит конечную нормальную подгруппу N, факторгруппа по которой либо циклическая, либо диэдральная (см., например, [Sta71]). Следовательно, композиция гомоморфизмов $G\to G/Q'\to (G/Q')/M = G_1\to G_1/N$ есть искомая ретракция на H (здесь мы воспользовались тем, что в бесконечной диэдральной группе нет конечных нормальных подгрупп и тем, что в группе G_1 подгруппа, порождённая квадратами всех её элементов, порождается образом элемента a^2).

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

Осталось доказать импликацию 1) $\Longrightarrow$ 4). По лемме 1 мы можем считать, что группа G удовлетворяет тождеству $[x^2, y^2] = 1$, то есть подгруппа Q, порождённая квадратами всех элементов группы G, абелева (и конечно порождённая, поскольку это подгруппа имеет конечный индекс в конечно порождённой группе G). Действительно, при факторизации группы G по коммутанту подгруппы, порождённой квадратами всех элементов, не пострадает ни подгруппа H, ни условие 1) (по лемме 1), ни условие 4).

Допустим, что элемент a^2 не простой. Это означает, что

$$\widetilde{(a^2)} \overset{\text{опр}}{=} a^{2|T(Q)|} = \prod_{\chi\in X} \widetilde{q(\chi)}_\chi^{k_\chi}, \quad \text{для некоторых } k_\chi\in\mathbb{Z}\setminus\{\pm1\} \text{ и } q(\chi)\in Q$$

(где x_χ — компоненты элемента $x\in |T(Q)|Q\subseteq \mathbb{Q}\otimes Q = \bigoplus\limits_\chi(\mathbb{Q}\otimes Q_\chi)$). Из формулы $(2')$ получаем

$$\prod_{\chi\in X} w_\chi\Big((\widetilde{q(\chi)})^{k_\chi}\Big) = \widetilde{(a^2)}^{2^{|C|}}. \tag{3}$$

Теперь разложим конечную элементарную абелеву 2-группу G/Q в прямое произведение групп порядка два: $G/Q = \langle d_1Q\rangle_2\times\ldots\times\langle d_mQ\rangle_2$ и рассмотрим слова $v_\chi(x_1,\ldots,x_m,y)\in F(x_1,\ldots,x_m,y)$ в свободной группе, полученные из слов w_χ (смотрите формулу $(1')$) подстановкой вместо c_i их выражений через образующие $d_1,\ldots,d_m$ и подстановкой буквы y вместо q:

$$v_\chi(d_1,\ldots,d_m,q) = w_\chi(\widetilde{q}).$$

Формула (3) показывает, что уравнение

$$\prod_{\chi\in X}\left(v_\chi\left(x_1,\ldots,x_m,\prod_{i=1}^n y_{\chi,i}^{2|T(Q)|}\right)\right)^{k_\chi} = \big(a^2\big)^{2^{|C|}\cdot|T(Q)|}, \tag{4}$$

где n — такое число, что каждый элемент из Q является произведением n квадратов (например, $n = \mathrm{rk}Q+1$), имеет решение в группе G:

$$x_j = d_j, \quad y_{\chi,i} = g_{\chi,i}, \quad \text{где } g_{\chi,i}\in G \text{ таковы, что } \prod_i g_{\chi,i}^2 = q(\chi).$$

Осталось показать, что уравнение (4) не имеет решений в диэдральной группе $H = \langle b\rangle_2\leftthreetimes\langle a\rangle_\infty$.

Подстановка $x_j = b^{\varepsilon_j}a^{k_j}$ определяет гомоморфизм $\varphi\colon C\to H/\big\langle a^2\big\rangle$ и характер $\chi'\colon C\to\{\pm1\}$ естественным образом:

$$\chi'(d_jQ) = (-1)^{\varepsilon_j}, \quad \text{то есть } \chi' = \widehat{\chi}\circ\varphi, \text{ где } \widehat{\chi}\colon H/\big\langle a^2\big\rangle\to\{\pm1\} \text{ — характер действия } H/\big\langle a^2\big\rangle \text{ на } \big\langle a^2\big\rangle.$$

Подставим теперь вместо переменных $y_{\chi,i}$ элементы $h_{\chi,i} \in H$ и заметим, что

$$\prod_{i=1}^{n} y_{\chi,i}^2 = \prod_{i=1}^{n} h_{\chi,i}^2 = a^{2l_\chi} \quad \text{для некоторых } l_\chi \in \mathbb{Z}.$$

Тогда по мультипликативному аналогу формулы (*) мы имеем

$$v_\chi\left(x_1,\dots,x_m,\prod_{i=1}^{n} y_{\chi,i}^{2|T(Q)|}\right) = v_\chi\left(x_1,\dots,x_m,a^{2l_\chi\cdot|T(Q)|}\right) = \begin{cases} \left(a^{2l_{\chi'}}\right)^{2^{|C|}\cdot|T(Q)|}, & \text{если } \chi=\chi';\\ 1, & \text{если } \chi\neq\chi'. \end{cases}$$

Следовательно, левая часть уравнения (4) после такой подстановки превратится в

$$a^{2l_{\chi'}\cdot 2^{|C|}\cdot|T(Q)|\cdot k_\chi} \neq a^{2\cdot 2^{|C|}\cdot|T(Q)|}, \quad \text{поскольку } k_\chi \neq \pm 1,$$

и уравнение (4) не имеет решений в H, что и требовалось.

4. Пример

Рассмотрим доказательство импликации из 1) в 4) на примере:

$$G = D_\infty \times D_\infty = \Big(\langle b_1\rangle_2 \leftthreetimes \langle a_1\rangle_\infty\Big) \times \Big(\langle b_2\rangle_2 \leftthreetimes \langle a_2\rangle_\infty\Big) \quad \text{и} \quad G \supset H = \langle b\rangle_2 \leftthreetimes \langle a\rangle_\infty \simeq D_\infty, \quad \text{где} \quad b = b_1b_2 \text{ и } a = a_1^3a_2^5.$$

В этом случае $Q = \big\langle\{g^2 \mid g\in G\}\big\rangle = \langle a_1^2\rangle_\infty \times \langle a_2^2\rangle_\infty \simeq \mathbb{Z}\oplus\mathbb{Z}$ и $C = G/Q = \langle a_1Q\rangle_2 \times \langle b_1Q\rangle_2 \times \langle a_2Q\rangle_2 \times \langle b_2Q\rangle_2$. Итак, у нас имеется $2^4 = 16$ различных характеров $C \to \{\pm 1\}$. При этом только для двух из них, α и β, подгруппы Q_χ нетривиальны:

$$\alpha : b_1 \mapsto -1,\ a_1,a_2,b_2 \mapsto 1, \qquad \beta : b_2 \mapsto -1,\ a_1,b_1,a_2 \mapsto 1.$$

Ясно, что элемент a^2 не является простым, и мы должны доказать, что подгруппа H не является вербально замкнутой.

Длинное слово $v_\chi(x_1,x_2,x_3,x_4,y)$ есть композиция (в произвольном порядке) следующих шестнадцати слов (как функций от y):

$$\begin{gathered} f_\chi(1,y),\ f_\chi(x_1,y),\ f_\chi(x_1x_2,y),\ f_\chi(x_1x_2x_3,y),\ f_\chi(x_1x_2x_3x_4,y),\ f_\chi(x_1x_2x_4,y),\ f_\chi(x_1x_3,y),\ f_\chi(x_1x_3x_4,y),\\ f_\chi(x_1x_4,y),\ f_\chi(x_2,y),\ f_\chi(x_2x_3,y),\ f_\chi(x_2x_3x_4,y),\ f_\chi(x_2x_4,y),\ f_\chi(x_3,y),\ f_\chi(x_3x_4,y),\ f_\chi(x_4,y). \end{gathered} \qquad (**)$$

Здесь в качестве первого аргумента выступают всевозможные выражения вида $x_1^{\varepsilon_1}x_2^{\varepsilon_2}x_3^{\varepsilon_3}x_4^{\varepsilon_4}$, где $\varepsilon_i \in \{0,1\}$, а

$$f_\chi(x_1^{\varepsilon_1}x_2^{\varepsilon_2}x_3^{\varepsilon_3}x_4^{\varepsilon_4},y) = y\cdot x_1^{\varepsilon_1}x_2^{\varepsilon_2}x_3^{\varepsilon_3}x_4^{\varepsilon_4}\cdot y^{\chi(a_1^{\varepsilon_1}b_1^{\varepsilon_2}a_2^{\varepsilon_3}b_2^{\varepsilon_4})}\cdot(x_1^{\varepsilon_1}x_2^{\varepsilon_2}x_3^{\varepsilon_3}x_4^{\varepsilon_4})^{-1}.$$

Например, $f_\alpha(x_1^{\varepsilon_1}x_2^{\varepsilon_2}x_3^{\varepsilon_3}x_4^{\varepsilon_4},y) = y\cdot x_1^{\varepsilon_1}x_2^{\varepsilon_2}x_3^{\varepsilon_3}x_4^{\varepsilon_4}\cdot y^{(-1)^{\varepsilon_2}}\cdot(x_1^{\varepsilon_1}x_2^{\varepsilon_2}x_3^{\varepsilon_3}x_4^{\varepsilon_4})^{-1}$. Мы видим, что в диэдральной группе

$$f_\alpha\Big(\left(a^{k_1}b^{\delta_1}\right)^{\varepsilon_1}\left(a^{k_2}b^{\delta_2}\right)^{\varepsilon_2}\left(a^{k_3}b^{\delta_3}\right)^{\varepsilon_3}\left(a^{k_4}b^{\delta_4}\right)^{\varepsilon_4},a^{2k}\Big) = \begin{cases} a^{4k}, & \text{если } \varepsilon_2+\sum\limits_{i=1}^{4}\delta_i\varepsilon_i \text{ чётно};\\ 1, & \text{если } \varepsilon_2+\sum\limits_{i=1}^{4}\delta_i\varepsilon_i \text{ нечётно}; \end{cases} \quad \text{где } k_i\in\mathbb{Z} \text{ и } \delta_i,\varepsilon_i\in\{0,1\}.$$

Таким образом, если взять $\delta_2 = 1$, а $\delta_1 = \delta_3 = \delta_4 = 0$, то $f_\alpha\Big(\left(a^{k_1}b^{\delta_1}\right)^{\varepsilon_1}\left(a^{k_2}b^{\delta_2}\right)^{\varepsilon_2}\left(a^{k_3}b^{\delta_3}\right)^{\varepsilon_3}\left(a^{k_4}b^{\delta_4}\right)^{\varepsilon_4},a^{2k}\Big)$ окажется равным a^{4k} при любом выборе ε_i; если же взять любой другой набор $\delta_i \in \{0,1\}$, то хотя бы одно из шестнадцати выражений (**) станет равным единице после подстановки $x_i \to a^{k_i}b^{\delta_i}$ и $y \to a^{2k}$. Это означает, что для композиции v_α выражений (**) мы имеем

$$v_\alpha\Big(\left(a^{k_1}b^{\delta_1}\right)^{\varepsilon_1},\left(a^{k_2}b^{\delta_2}\right)^{\varepsilon_2},\left(a^{k_3}b^{\delta_3}\right)^{\varepsilon_3},\left(a^{k_4}b^{\delta_4}\right)^{\varepsilon_4},a^{2k}\Big) = \begin{cases} a^{2^{17}k}, & \text{если } (\delta_1,\delta_2,\delta_3,\delta_4) = (0,1,0,0);\\ 1, & \text{в противном случае.} \end{cases}$$

Аналогичным образом ведут себя все остальные характеры. Например,

$$v_{\alpha\beta}\Big(\left(a^{k_1}b^{\delta_1}\right)^{\varepsilon_1},\left(a^{k_2}b^{\delta_2}\right)^{\varepsilon_2},\left(a^{k_3}b^{\delta_3}\right)^{\varepsilon_3},\left(a^{k_4}b^{\delta_4}\right)^{\varepsilon_4},a^{2k}\Big) = \begin{cases} a^{2^{17}k}, & \text{если } (\delta_1,\delta_2,\delta_3,\delta_4) = (0,1,0,1);\\ 1, & \text{в противном случае.} \end{cases}$$

Уравнения (4) в данном случае имеет вид

$$\left(v_\alpha\left(x_1,x_2,x_3,x_4,y_{\alpha,1}^2\right)\right)^3\cdot\left(v_\beta\left(x_1,x_2,x_3,x_4,y_{\beta,1}^2\right)\right)^5\cdot\prod_{\chi\neq\alpha,\beta}\left(v_\chi\left(x_1,x_2,x_3,x_4,y_{\chi,1}^2\right)\right)^{2022}=a^{2^{17}}.$$

(Мы написали в показателе 2022, чтобы подчеркнуть, что здесь можно писать любое число, кроме ±1; разумеется, проще всего заменить 2022 на 0.)

Сказанное означает, что при любой подстановке $x_i\to a^{k_i}b^{\delta_i}$ левая часть этого уравнения примет значение из

$$\left\langle a^{2^{17}\cdot3}\right\rangle,\text{ если }(\delta_1,\delta_2,\delta_3,\delta_4)=(0,1,0,0);$$
$$\left\langle a^{2^{17}\cdot5}\right\rangle,\text{ если }(\delta_1,\delta_2,\delta_3,\delta_4)=(0,0,0,1);$$
$$\left\langle a^{2^{17}\cdot2022}\right\rangle\text{ во всех остальных случаях.}$$

Это означает, что уравнение (4) не имеет решений в диэдральной группе. С другой стороны, в группе G решение есть: $x_1=a_1$, $x_2=b_1$, $x_3=a_2$, $x_4=b_2$, $y_{\alpha,1}=a_1$, $y_{\beta,1}=a_2$, $y_{\chi,1}=1$ при $\chi\notin\{\alpha,\beta\}$.

ГЛАВА 10.
ФУНДАМЕНТАЛЬНАЯ ГРУППА БУТЫЛКИ КЛЕЙНА НЕ СИЛЬНО ВЕРБАЛЬНО ЗАМКНУТА, НО ОЧЕНЬ БЛИЗКА К ЭТОМУ ЗВАНИЮ

0. Введение

Подгруппа H группы G называется *вербально замкнутой* [MR14] (смотрите также [Rom12], [PX13], [Mazh17], [KM18], [KMM18], [Mazh18], [Bog18], [Bog19], [Маж19], [PT19]), 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. 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, смотрите упомянутые выше статьи. Например, в [Mazh18] доказывается, что

сильно вербально замкнуты фундаментальные группы всех связных поверхностей, кроме, быть может, бутылки Клейна.

Это интригующее единственное возможное исключение возникло так:

- почти все фундаментальные группы поверхностей «похожи на свободные группы», и для таких групп работает «индустриальный» метод доказательства сильной вербальной замкнутости, берущий своё начало в самой первой статье [MR14] на эту тему и основанный на использовании слов Ли [Lee02] или каких-то их аналогов;
- оставшиеся несколько групп

  либо абелевы, а все абелевы группы сильно вербально замкнуты (по очень простой причине [Mazh18]), либо это злополучная фундаментальная группа $K=\langle a,b \mid a^b=a^{-1}\rangle$ бутылки Клейна, которая и на свободную непохожа, и неабелева, и непонятно, что с ней делать.

В этой работе доказывается естественное дополнение теоремы Мажуги:

фундаментальная группа бутылки Клейна не сильно вербально замкнута.

Похожая ситуация сложилась в своё время с почти свободными группами: в работе [KM18] была доказана общая теорема с единственным возможным исключением:

сильно вербально замкнуты все недиэдральные почти свободные группы, не содержащие неединичных конечных нормальных подгрупп

(и условие отсутствия конечных нормальных подгрупп здесь нельзя убрать); а позже выяснилось [KMM18], что

бесконечная диэдральная группа тоже сильно вербально замкнута,

и это скромный результат оказался более трудным, чем упомянутая выше общая теорема, полученная в [KM18] «индустриальным» методом. Вообще, если читатель возьмёт какую-нибудь конкретную свою любимую неабелеву группу, далёкую от свободных (конечную, например), то выяснить, является ли она сильно вербально замкнутой, окажется непросто (скорее всего): и доказать сильную вербальную замкнутость трудно, и опровергнуть трудно (на самом деле, даже просто привести пример не сильно вербально замкнутой группы не очень просто [KM18]).

Фундаментальная группа $K=\langle a,b \mid a^b=a^{-1}\rangle$ бутылки Клейна, конечно же, очень похожа на бесконечную диэдральную группу $D_\infty=\langle a,b \mid a^b=a^{-1},\ b^2=1\rangle$. Нам удаётся этим воспользоваться и, оперевшись на результаты работы [KMM18], показать, что группа K, хоть и не является сильно вербально замкнутой, обладает очень близким свойством.

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 эквивалентна

своей конечной подсистеме), 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).

Фундаментальные группы всех поверхностей линейны [New85], а все линейные группы нётеровы по уравнениям [BMRe99].

Таким образом, наш основной (и единственный) результат можно сформулировать следующим образом.

Теорема. *Фундаментальная группа K бутылки Клейна* (в отличие от всех остальных групп поверхностей) *может быть вложена в некоторую конечно порождённую группу G в качестве вербально замкнутой подгруппы, не являющейся ретрактом. Однако всякая такая группа G обязана иметь подгруппу индекса два, содержащую K в качестве своего ретракта.*

В следующем параграфе мы приводим пример, доказывающий первую часть теоремы (то есть отсутствие сильной вербальной замкнутости группы K). Параграф 2 содержит вспомогательные леммы. А в последнем параграфе мы доказываем второе утверждение теоремы (то есть обещанное в названии главы «но...»).

Обозначения, которые мы используем, в целом стандартны. Отметим только, что если x и y — элементы некоторой группы, то x^y обозначает $y^{-1}xy$, Коммутатор $[x,y]$ мы понимаем как $x^{-1}y^{-1}xy$. Если X — подмножество некоторой группы, то $\langle X\rangle$, $\langle\langle X\rangle\rangle$ и $C_H(X)$ означают, соответственно, подгруппу, порождённую множеством X, нормальное замыкание множества X и централизатор множества X в H (где H — некоторая подгруппа). Циклическую группу порядка k, порождённую элементом x, мы обозначаем символом $\langle x\rangle_k$. Свободную группу с базисом $x_1,\dots,x_n$ мы обозначаем $F(x_1,\dots,x_n)$.

1. Пример

Пусть $V_4=\{1,d_1,d_2,d_3\}$ — четверная группа Клейна (то есть нециклическая группа порядка четыре). Рассмотрим полупрямое произведение

$$G=\Big(V_4\times\langle b\rangle_\infty\Big)\leftthreetimes\Big(\langle a_1\rangle_\infty\times\langle a_2\rangle_\infty\times\langle a_3\rangle_\infty\Big),\quad\text{где действие такое: } a_i^b=a_i^{-1},\ a_i^{d_i}=a_i,\ a_i^{d_j}=a_i^{-1}\text{ при всех } i\neq j.$$

Утверждение. *Подгруппа $K=\langle a,b\rangle\subset G$, где $a=a_1a_2a_3$, (изоморфная фундаментальной группе бутылки Клейна) вербально замкнута в G, но не является ретрактом.*

Доказательство. Подгруппа K не ретракт, поскольку при гипотетической ретракции $G\to K$ элементы d_i, будучи элементами конечного порядка, обязаны перейти в единицу (поскольку в K нет кручения); а тогда соотношения $a_i^{d_j}=a_i^{-1}$ покажут, что образы элементов a_i тоже имеют конечный порядок, и, следовательно, равны единице; стало быть, образ элемента $a=a_1a_2a_3\in K$ тоже равен единице, что противоречит неподвижности элементов подгруппы K при ретракции.

Осталось показать, что подгруппа K вербально замкнута в G, то есть произвольное уравнение вида

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

разрешимое в G, разрешимо в K. Любое такое уравнение можно, как известно, путём замены переменных преобразовать к виду

$$x^m u(x,y,\dots)=h,\quad\text{где } h\in K\text{ и } u(x,y,\dots)\text{ — элемент коммутанта свободной группы } F(x,y,\dots).\tag{1}$$

Предположим, что уравнение (1) имеет некоторое решение $(\widetilde{x},\widetilde{y},\dots)$ в группе G. Поскольку все d_i равноправны, можно считать, что

$$\widetilde{x}=d_1^{\varepsilon}b^l a_1^{k_1}a_2^{k_2}a_3^{k_3},\quad\text{где } \varepsilon,l,k_i\in\mathbb{Z}.\tag{2}$$

У нас есть гомоморфизм *взятие первой координаты*:

$$f\colon G\to D_\infty=\langle b'\rangle_2\leftthreetimes\langle a'\rangle_\infty,\quad\text{где } f(a_1)=a',\quad f(a_2)=f(a_3)=f(d_1)=1,\quad f(b)=f(d_2)=f(d_3)=b',$$

и естественный гомоморфизм *степень*:

$$\deg\colon G\to\mathbb{Z},\quad\text{где } \deg(a_i)=\deg(d_i)=0,\quad \deg(b)=1,$$

Применив эти гомоморфизмы к имеющемуся у нас равенству $\widetilde{x}^m u(\widetilde{x},\widetilde{y},\ldots)=h$, мы получим

$$f\Big(\widetilde{x}^m u(\widetilde{x},\widetilde{y},\ldots)\Big)=f(\widetilde{x})^m u(f(\widetilde{x}),f(\widetilde{y}),\ldots)=f(h),\quad \text{и}\quad \deg\Big(\widetilde{x}^m u(\widetilde{x},\widetilde{y},\ldots)\Big)=m\cdot\deg(\widetilde{x})=\deg(h). \tag{3}$$

Теперь рассмотрим элементы $\widehat{x},\widehat{y},\ldots\in K$, получающиеся из элементов $\widetilde{x},\widetilde{y},\ldots\in G$ заменами

$$\begin{gathered}a_1\mapsto a=a_1a_2a_3,\quad a_2\mapsto 1,\quad a_3\mapsto 1,\quad d_1\mapsto 1,\quad d_2\mapsto b,\quad d_3\mapsto b\quad (\text{и } b\mapsto b),\\ \textit{которые сохраняют первую координату любого элемента.}\end{gathered} \tag{4}$$

Например, элемент $\widetilde{x}$, заданный выражением (2), превратится в

$$\widehat{x}=b^l a^{k_1}=b^l a_1^{k_1}a_2^{k_1}a_3^{k_1}. \tag{5}$$

Утверждается, что набор $(\widehat{x},\widehat{y},\ldots)$ есть решение уравнения (1) в K. Действительно,

- с первой координатой всё хорошо: $f\Big(\widehat{x}^m u(\widehat{x},\widehat{y},\ldots)\Big)=f(\widehat{x})^m u(f(\widehat{x}),f(\widehat{y}),\ldots)\overset{(4)}{=}f(\widetilde{x})^m u(f(\widetilde{x}),f(\widetilde{y}),\ldots)\overset{(3)}{=}f(h)$ (где из (4) и (3) вытекают соответствующие равенства);
- и со степенью всё хорошо: $\deg\Big(\widehat{x}^m u(\widehat{x},\widehat{y},\ldots)\Big)=m\cdot\deg(\widehat{x})\overset{(5)}{=}ml\overset{(2)}{=}m\cdot\deg(\widetilde{x})\overset{(3)}{=}\deg(h)$,

Остаётся заметить, что элемент группы $K\subset G$ однозначно определяется своей первой координатой и степенью. Таким образом, $\widehat{x}^m u(\widehat{x},\widehat{y},\ldots)=h$, мы нашли решение уравнения (1) в K, и это завершает доказательство.

2. Две леммы о факторизации

Лемма о факторизации по вербальным подгруппам ([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 $G/V(G)$.*

Лемма о диэдральной факторгруппе. *Если фундаментальная группа $K=\langle a,b\,|\,a^b=a^{-1}\rangle$ бутылки Клейна содержится в некоторой группе G в качестве вербально замкнутой подгруппы, то*

1) *$\langle\langle b^2\rangle\rangle\cap K=\langle b^2\rangle$, где $\langle\langle b^2\rangle\rangle$ — это нормальное замыкание элемента b^2 в G;*
2) *подгруппа $D_\infty=K/\langle b^2\rangle\subseteq G/\langle\langle b^2\rangle\rangle$ вербально замкнута в $G/\langle\langle b^2\rangle\rangle$.*

Доказательство. Можно считать, что группа G удовлетворяет тождеству $[x^2,y^2]=1$, (поскольку это тождество выполнено в K, и, следовательно, по лемме о факторизации по вербальным подгруппам можно факторизовать G по соответствующей вербальной подгруппе).

А для групп с таким тождеством, как и для всех метабелевых групп, утверждение 1) — это общий факт:

> *если A — нормальная абелева подгруппа группы G, и факторгруппа G/A тоже абелева, то пересечение $C_A(X)$ подгруппы A с централизатором любого подмножества $X\subseteq G$ нормально в G.*

Действительно, $\big(C_A(X)\big)^g=C_A(X^g)\supseteq C_A(XA)=C_A(X)$.

Чтобы вывести отсюда утверждение 1), достаточно положить $A=\big\langle\{g^2\mid g\in G\}\big\rangle$ и $X=K$; при этом мы получаем даже больше, чем 1):

$$\textit{подгруппы } \langle\langle b^2\rangle\rangle \textit{ и } K \textit{ коммутируют в } G\ .$$

Теперь докажем 2). Пусть уравнение

$$w(x,y,\ldots)=h\,\langle\langle b^2\rangle\rangle,\quad \text{где } h\in K \text{ и } w(x,y,\ldots)\in F(x,y,\ldots), \tag{$*$}$$

разрешимо в $G/\langle\langle b^2\rangle\rangle$. Мы хотим показать, что оно разрешимо в $D_\infty=K/\langle b^2\rangle\subseteq G/\langle\langle b^2\rangle\rangle$.
Случай 1: $h=1$. В этом случае уравнение $(*)$ имеет тривиальное решение $(1,1,\ldots)$ в D_∞.
Случай 2: $h=b$. В этом случае один из неизвестных (скажем, x) должен входить в w в нечётной степени (суммарно), поскольку иначе из разрешимости в $G/\langle\langle b^2\rangle\rangle$ уравнения $(*)$ мы получим, что элемент b является произведением квадратов в группе G, что противоречит вербальной замкнутости подгруппы K (так как в K элемент b не раскладывается в произведение квадратов, очевидно, даже по модулю $\langle a\rangle$). А уравнение с нечётной степенью вхождения переменной x имеет в D_∞ очевидное решение: $x=b,\ y=1,\ z=1,\ldots$.
Случай 3: $h=ba^k$. Этот случай немедленно сводится к предыдущему, поскольку у диэдральной группы есть автоморфизм, переводящий ba^k в b.

Случай 4 (последний случай по модулю $\langle b^2\rangle$)**:** $h = a^k$, где $k \neq 0$. Пусть $(\widetilde{x}\langle\langle b^2\rangle\rangle, \widetilde{y}\langle\langle b^2\rangle\rangle, \ldots)$ — решение уравнения $(*)$ в $G/\langle\langle b^2\rangle\rangle$. Тогда уравнение

$$[t, \big(w(x, y, \ldots)\big)^2] = [b, h^2] = a^{4k} \quad \text{(где } t \text{ — новый неизвестный)}$$

имеет в G решение $(\widetilde{t} = b, \widetilde{x}, \widetilde{y}, \ldots)$, поскольку $\langle\langle b^2\rangle\rangle$ коммутирует с K, как выше было замечено. В силу вербальной замкнутости K в G последнее уравнение имеет в K некоторое решение, то есть

$$[\widehat{t}, \big(w(\widehat{x}, \widehat{y}, \ldots)\big)^2] = a^{4k} \quad \text{для некоторых } \widehat{t}, \widehat{x}, \widehat{y}, \ldots \in K. \qquad (**)$$

Из этого равенства немедленно вытекает, что

а) $\widehat{t} \in b\langle a, b^2\rangle$ (поскольку все остальные элементы группы K коммутируют с квадратами); мы можем считать, что $\widehat{t} = b$, так как и a, и b^2 коммутируют со всеми квадратами и не влияют на коммутатор $(**)$;

б) $\big(w(\widehat{x}, \widehat{y}, \ldots)\big)^2 \in \langle b^2\rangle \cup \langle a^2, b^4\rangle$, поскольку только такие элементы являются квадратами в K;

в) $\big(w(\widehat{x}, \widehat{y}, \ldots)\big)^2 \in a^{2k}\langle b^4\rangle$, поскольку только у таких элементов из $\langle b^2\rangle \cup \langle a^2, b^4\rangle$ коммутатор с $\widehat{t} = b$ даёт a^{4k};

г) $w(\widehat{x}, \widehat{y}, \ldots) \in a^k\langle b^2\rangle$, поскольку из элементов смежного класса $a^{2k}\langle b^4\rangle$ квадратный корень извлекается однозначно в группе K.

Мы нашли решение $(\widehat{x}\langle b^2\rangle, \widehat{y}\langle b^2\rangle, \ldots)$ уравнения $(*)$ в $D_\infty = K/\langle b^2\rangle$, и это завершает доказательство.

3. Доказательство второго утверждения теоремы

Предположим, что фундаментальная группа K бутылки Клейна является вербально замкнутой подгруппой некоторой конечно порождённой группы G. Мы должны построить ретракцию на K из подгруппы индекса не больше двух (в G), содержащей K.

В группе G есть две нормальные подгруппы:

$$N_1 = G' \text{ — коммутант и } N_2 = \langle\langle b^2\rangle\rangle \text{ — нормальное замыкание элемента } b^2.$$

При факторизации по ним подгруппа K превращается в

$$K/K' = \langle a\rangle_2 \times \langle b\rangle_\infty \subseteq G/N_1 \text{ и } K/\langle b^2\rangle = D_\infty \subseteq G/N_2$$

(по лемме о факторизации по вербальным подгруппам и по лемме о диэдральной факторгруппе), причём эти образы группы K в G/N_i остаются вербально замкнутыми в G/N_i (по тем же леммам). Следовательно, K/K' и $K/\langle b^2\rangle$ являются ретрактами групп G/N_i, поскольку и всякая абелева группа [Mazh18], и бесконечная диэдральная группа [KMM18] сильно вербально замкнуты.

Таким образом, мы получаем эпиморфизмы

$$\deg\colon G \to G/G' \to K/K' = \langle a\rangle_2 \times \langle b\rangle_\infty \to \langle b\rangle_\infty \xrightarrow{\simeq} \mathbb{Z} \quad \text{и} \quad f\colon G \to G/\langle\langle b^2\rangle\rangle \to K/\langle b^2\rangle = D_\infty$$

такие, что $\deg(b) = 1$, $f(b) = b\langle b^2\rangle$, $f(a) = a\langle b^2\rangle$. Из этих двух «псевдоретракций» мы строим гомоморфизм

$$\Phi\colon G \to \mathbb{Z} \times D_\infty, \quad g \mapsto \big(\deg(g),\ f(g)\big).$$

Ограничение φ гомоморфизма Φ на подгруппу K инъективно, а образ этого ограничения — это так называемое *расслоенное произведение*:

$$\varphi(K) = \Phi(K) = \left\{ \Big(i,\ b^j a^k \langle b^2\rangle\Big) \;\middle|\; i \equiv j \pmod 2 \right\} \text{ — подгруппа индекса два в } \mathbb{Z} \times D_\infty\ .$$

Поэтому подгруппа $\Phi^{-1}(\Phi(K)) \subseteq G$ имеет индекс не больше двух в G и обладает ретракцией на K:

$$G \supseteq \Phi^{-1}(\Phi(K)) \xrightarrow{\Phi} \Phi(K) \xrightarrow{\varphi^{-1}} K.$$

ГЛАВА 11.
КОРОТКОЕ ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ МАКАРЕНКО–ХУХРО О БОЛЬШИХ ХАРАКТЕРИСТИЧЕСКИХ ПОДГРУППАХ С ТОЖДЕСТВОМ

Пусть G — группа и H — её подгруппа конечного индекса. В учебниках по теории групп (см., например, [KaM82]) можно обнаружить несколько простых фактов, позволяющих в этой ситуации найти в G подгруппу конечного индекса, которая похожа на H, но лучше неё. В частности,

– внутри H найдётся нормальная в G подгруппа конечного индекса (делящего $|G:H|!$);
– если группа G конечно порождена, то внутри H найдётся вполне характеристическая (и даже вербальная) в G подгруппа конечного индекса;
– если подгруппа H абелева, то в G найдётся характеристическая абелева подгруппа конечного индекса.

Последние утверждение было недавно существенно обобщено.

Теорема Макаренко–Хухро ([KhM07a], см. также [MaX07]). *Если в группе G есть подгруппа конечного индекса, удовлетворяющая внешнему (полилинейному, в авторской терминологии) коммутаторному тождеству, то в группе G найдётся также характеристическая подгруппа конечного индекса, удовлетворяющая этому тождеству.*

Примерами внешних коммутаторных тождеств могут служить нильпотентность или разрешимость данной ступени. Общее определение выглядит так. Пусть $F(x_1, x_2, \ldots)$ — свободная группа счётного ранга. *Внешними коммутаторами веса 1* называют образующие x_i. *Внешним коммутатором веса $t > 1$* называют каждое слово вида $w(x_1, \ldots, x_t) = [u(x_1, \ldots, x_r), v(x_{r+1}, \ldots, x_t)]$, где u и v — внешние коммутаторы веса r и $t-r$ соответственно. Говоря неформально, внешний коммутатор веса t представляет собой выражение $[x_1, x_2, \ldots, x_t]$, в котором каким-то осмысленным образом расставлены квадратные скобки. *Внешним коммутаторным тождеством веса t* называют тождество $w(x_1, \ldots, x_t) = 1$, левая часть которого является внешним коммутатором веса t.

Приводимое ниже доказательство теоремы Макаренко–Хухро значительно проще и короче оригинального.

Пусть $H_1, \ldots, H_t$ — нормальные подгруппы группы G и $w(x_1, \ldots, x_t)$ — внешний коммутатор. Тогда

1) подгруппа $w(H_1, \ldots, H_t) \stackrel{\text{опр}}{=} \langle w(h_1, \ldots, h_t) \ ; \ h_i \in H_i \rangle$ нормальна в группе G;
2) $w(G, \ldots, G) = 1$ тогда и только тогда, когда группа G удовлетворяет тождеству $w(x_1, \ldots, x_t) = 1$;
3) $w(H_1, \ldots, H_t) = [u(H_1, \ldots, H_r), v(H_{r+1}, \ldots, H_t)]$, если $w(x_1, \ldots, x_t) = [u(x_1, \ldots, x_r), v(x_{r+1}, \ldots, x_t)]$;
4) $w(H_1, \ldots, H_{i-1}, \prod\limits_{N \in \mathcal{N}} N, H_{i+1}, \ldots, H_t) = \prod\limits_{N \in \mathcal{N}} w(H_1, \ldots, H_{i-1}, N, H_{i+1}, \ldots, H_t)$
для произвольного семейства $\mathcal{N}$ нормальных подгрупп группы G.

Эти свойства почти очевидны и легко могут быть проверены по индукции.

Лемма. *Пусть $w(x_1, \ldots, x_t)$ — внешний коммутатор, m — натуральное число, G — группа и $\mathcal{N}$ — некоторое семейство её нормальных подгрупп таких, что*

$$w(\underbrace{N, N, \ldots, N}_{m \text{ раз}}, G, G, \ldots, G) = 1 \quad \textit{для всех } N \in \mathcal{N}.$$

Тогда

$$w(\underbrace{\widehat{N}, \widehat{N}, \ldots, \widehat{N}}_{m-1 \text{ раз}}, \widehat{G}, \widehat{G}, \ldots, \widehat{G}) = 1, \quad \textit{где } \widehat{N} = \bigcap_{N \in \mathcal{N}} N \textit{ и } \widehat{G} = \prod_{N \in \mathcal{N}} N.$$

Доказательство.

$$w(\underbrace{\widehat{N}, \widehat{N}, \ldots, \widehat{N}}_{m-1 \text{ раз}}, \widehat{G}, \widehat{G}, \ldots, \widehat{G}) = w(\underbrace{\widehat{N}, \widehat{N}, \ldots, \widehat{N}}_{m-1 \text{ раз}}, \prod_{N \in \mathcal{N}} N, \widehat{G}, \ldots, \widehat{G}) = \prod_{N \in \mathcal{N}} w(\underbrace{\widehat{N}, \widehat{N}, \ldots, \widehat{N}}_{m-1 \text{ раз}}, N, \widehat{G}, \ldots, \widehat{G}).$$

Но $\widehat{N} \subseteq N$ и $\widehat{G} \subseteq G$, поэтому каждый сомножитель последнего произведения содержится в группе

$$w(\underbrace{N, N, \ldots, N}_{m \text{ раз}}, G, G, \ldots, G), \quad \text{которая тривиальна по условию.}$$

В качестве следствия мы получаем усиленную версию теоремы Макаренко–Хухро с явной оценкой на индекс.

Теорема. *Если группа G содержит подгруппу N конечного индекса, удовлетворяющую внешнему коммутаторному тождеству $w(x_1,\dots,x_t)=1$, то G содержит характеристическую, и даже инвариантную относительно всех сюръективных эндоморфизмов, подгруппу H, удовлетворяющую тому же тождеству. Причём*

$$\log_2|G:H| \leqslant f^{t-1}(\log_2|G:N|), \quad \text{если подгруппа } N \text{ нормальна,} \tag{1}$$

и, следовательно, $\log_2|G:H| \leqslant f^{t-1}(\log_2|G:N|!)$ в общем случае, где $f^k(x)$ означает k-ю итерацию функции $f(x)=x(x+1)$.

Доказательство. Для простоты мы будем строить характеристическую подгруппу. Построение подгруппы, инвариантной относительно сюръективных эндоморфизмов, повторяет приводимые ниже рассуждения дословно, с заменой всех используемых автоморфизмов на сюръективные эндоморфизмы.

Рассмотрим подгруппу $G_1 = \prod\limits_{\varphi\in\operatorname{Aut}G} \varphi(N)$. Эта подгруппа характеристична и $|G:G_1| \leqslant |G:N|$. Ясно также, что G_1 является произведением не более чем $\log_2|G:N|+1$ автоморфных образов группы N (поскольку в цепочке $N \subseteq N\varphi_1(N) \subseteq N\varphi_1(N)\varphi_2(N) \subseteq \dots$ не может быть больше $\log_2|G:N|+1$ различных подгрупп). Таким образом,

$$G_1 = \prod_{k=0}^{p_1} \varphi'_k(N), \quad \text{где } \varphi'_k \in \operatorname{Aut}G \text{ и } p_1 \leqslant l_0 \stackrel{\text{опр}}{=} \log_2|G:N|.$$

Теперь рассмотрим подгруппу $N_1 = \bigcap\limits_{k=0}^{p_1} \varphi'_k(N)$. Индекс пересечения подгрупп не превосходит произведения их индексов (см., например, [KaM82]), следовательно,

$$l_1 \stackrel{\text{опр}}{=} \log_2|G:N_1| \leqslant \log_2(|G:N|^{p_1+1}) = (p_1+1)l_0 \leqslant (l_0+1)l_0 = f(l_0).$$

Согласно лемме

$$w(N_1,\dots,N_1,G_1)=1.$$

Аналогичным образом построим подгруппы

$$G_2 = \prod_{\varphi\in\operatorname{Aut}G_1} \varphi(N_1) = \prod_{k=0}^{p_2} \varphi''_k(N_1) \quad \text{и} \quad N_2 = \bigcap_{k=0}^{p_2} \varphi''_k(N_1), \quad \text{где } \varphi''_k \in \operatorname{Aut}G_1 \text{ и } p_2 \leqslant \log_2|G:N_1| = l_1 \leqslant f(l_0).$$

Ясно, что подгруппа G_2 характеристична в G (и даже в G_1). Причём,

$$\log_2|G:G_2| \leqslant \log_2|G:N_1| = l_1 \leqslant f(l_0) \text{ и } l_2 \stackrel{\text{опр}}{=} \log_2|G:N_2| \leqslant \log_2(|G:N_1|^{p_2+1}) = (p_2+1)l_1 \leqslant f(l_1) \leqslant f(f(l_0)).$$

Согласно лемме

$$w(N_2,\dots,N_2,G_2,G_2)=1.$$

Продолжая действовать в том же духе, на t-ом шаге мы получим характеристическую в G подгруппу

$$G_t = \prod_{\varphi\in\operatorname{Aut}G_{t-1}} \varphi(N_{t-1}) = \prod_{k=0}^{p_t} \varphi_k^{(t)}(N_{t-1}), \quad \text{где } \varphi_k^{(t)} \in \operatorname{Aut}G_{t-1}.$$

Причём,

$$w(G_t,\dots,G_t)=1 \quad \text{и} \quad \log_2|G:G_t| \leqslant \log_2|G:N_{t-1}| = l_{t-1} \leqslant f(l_{t-2}) \leqslant f(f(l_{t-3})) \leqslant \dots \leqslant f^{t-1}(l_0).$$

Таким образом, подгруппа $H=G_t$ является искомой и теорема доказана.

Замечание. В работах [KhM07a] и [MaX07] явная оценка не приводится, но отмечается, что она может быть получена из доказательства. По нашим подсчётам, оценка (1) лучше.

ГЛАВА 12.
ИНВАРИАНТНОСТЬ ОТНОСИТЕЛЬНО АВТОМОРФИЗМОВ И ТОЖДЕСТВА

0. Введение

В работе [KhM07a] показано, что каждая группа, почти удовлетворяющая внешнему коммутаторному тождеству, содержит характеристическую подгруппу конечного индекса, удовлетворяющую этому тождеству. Аналогичный результат был получен в [KhM08] для идеалов в произвольных алгебрах (роль индекса в этом случае играет коразмерность). Ещё один похожий результат можно найти в [KhM07b]: если конечная p-группа G содержит нормальную нильпотентную ступени t подгруппу N, то она содержит также характеристическую нильпотентную той же ступени подгруппу H, коранг которой ограничен некоторой функцией от коранга подгруппы N и числа t. В работе [KM09] было найдено новое, гораздо более короткое доказательство теоремы об индексе и получена более хорошая оценка индекса характеристической подгруппы.

В этой главе мы обобщаем рассуждение из [KM09] на широкий класс алгебраических систем, заменяя свойство конечности индекса некоторым абстрактным свойством «малости», индекс при этом заменяется на некоторую абстрактную «коразмерность». Общая теорема, которую мы доказываем в параграфе 3, включает в себя все результаты, перечисленные выше, как частные случаи. Более того, имеется много новых приложений. Например, полученная теорема охватывает случай конечных p-групп с нормальной подгруппой ограниченного коранга, удовлетворяющей произвольному внешнему коммутаторному тождеству (а не только тождеству нильпотентности, как в [KhM07b]).

С другой стороны, мы показываем, что оригинальные рассуждения из работ [KhM07a], [KhM07b] и [KhM08] дают несколько больше. А именно, в любой группе число подгрупп конечного индекса, являющихся максимальными (по включению) среди всех нормальных подгрупп, удовлетворяющих данному внешнему коммутаторному тождеству, конечно. Это означает, в частности, что характеристическую подгруппу конечного индекса можно найти внутри любой подгруппы конечного индекса, максимальной среди всех нормальных подгрупп с данным тождеством. Аналогичные более сильные результаты справедливы для алгебр над полями.

Для полноты картины мы приведём более ранние известные нам результаты на эту тему. Пусть G — группа и N — её подгруппа конечного индекса. Тогда

- внутри N найдётся нормальная в G подгруппа конечного индекса (делящего $|G:N|!$);
- если группа G конечно порождена, то внутри N найдётся вполне характеристическая (и даже вербальная) в G подгруппа конечного индекса;
- если подгруппа N абелева, то в G найдётся характеристическая абелева подгруппа конечного индекса.

Эти факты хорошо известны и их можно найти в учебниках по теории групп (см., например, [KaM82]). Отметим ещё, что в работе [БеК03] было доказано, что из наличия t-ступенно разрешимой подгруппы конечного индекса следует наличие характеристической разрешимой подгруппы конечного индекса ступени разрешимости не больше t^2. В работе [BrNa04] было показано, что всякая почти нильпотентная группа содержит характеристическую нильпотентную подгруппу конечного индекса.

В качестве приложения полученных результатов в пятом параграфе мы получаем неулучшаемую оценку на ступень почти разрешимости расширения почти разрешимой группы при помощи почти разрешимой, отвечая тем самым на вопрос Дж. Баттона.

Шестой параграф посвящён тождеству периодичности $x^p = 1$. Мы показываем, что для такого тождества аналог теоремы о характеристической подгруппе конечного индекса неверен (при больших простых p).

1. Формулировка результатов

Теорема 1 [KhM07a], [KM09]. *Если группа G содержит нормальную подгруппу N конечного индекса, удовлетворяющую внешнему коммутаторному тождеству $w(x_1,\dots,x_t) = 1$, то G содержит характеристическую, и даже инвариантную относительно всех сюръективных эндоморфизмов, подгруппу H, удовлетворяющую тому же тождеству, такую, что $\log_2 |G:H| \leqslant f^{t-1}(\log_2 |G:N|)$.*

Здесь и далее $f^k(x)$ означает k-ю итерацию функции $f(x) = x(x+1)$. Под *внешним* (или *полилинёйным*) *коммутаторным тождеством* понимается тождество вида $[\dots[x_1,\dots,x_t]\dots] = 1$, в котором каким-то осмысленным образом расставлены квадратные скобки, а все встречающиеся буквы $x_1,\dots,x_t$ различны. Примерами таких тождеств могут служить разрешимость, нильпотентность, центральная метабелевость и т.п. Формальное определение выглядит так. Пусть $F(x_1,x_2,\dots)$ — свободная группа счётного ранга. *Внешними коммутаторами веса 1* называют образующие x_i. *Внешним коммутатором веса $t > 1$* называют каждое слово вида $w(x_1,\dots,x_t) = [u(x_1,\dots,x_r), v(x_{r+1},\dots,x_t)]$, где u и v — внешние коммутаторы веса r и $t-r$ соответственно. *Внешним коммутаторным тождеством* понимается тождество вида $w = 1$, где w — внешний коммутатор.

Замечание 1. Условие нормальности подгруппы N в теореме 1 не является существенным. Хорошо известно, что любая подгруппа N конечного индекса содержит нормальную подгруппу $\widetilde{N}$ конечного индекса, причём $|G:\widetilde{N}|$ не превосходит (и даже делит) $|G:N|!$ (см., например, [KaM82]). Поэтому утверждение теоремы 1 остаётся справедливым и без предположения о нормальности подгруппы N, но с худшей оценкой: $\log_2|G:H| \leqslant f^{t-1}(\log_2|G:N|!)$.

Замечание 2. Из теоремы $1'$ (см. ниже) следует, что в условиях теоремы 1 характеристическая (и даже инвариантная относительно всех сюръективных эндоморфизмов) подгруппа конечного индекса найдётся внутри любой подгруппы конечного индекса, максимальной по включению среди всех нормальных подгрупп, удовлетворяющих данному внешнему коммутаторному тождеству.

Замечание 3. Из теоремы 4 (см. ниже), частным случаем которой является теорема 1, следует, что группа G/H лежит в многообразии, порождённом группой G/N (и даже в формации, порождённой этой группой).

Теорема 2 (сравните [KhM08]). *Пусть G — алгебра над полем (возможно, неассоциативная). Если G содержит подпространство N конечной коразмерности, на котором выполнено полилинейное тождество $w(x_1,\dots,x_t)=0$, то G содержит инвариантное относительно всех сюръективных эндоморфизмов подпространство H, удовлетворяющее тому же тождеству, такое, что $\operatorname{codim} H \leqslant f^{t-1}(\operatorname{codim} N)$. Это подпространство H будет левым, правым или двусторонним идеалом, если подпространство N было левым, правым или двусторонним идеалом, соответственно.*

Замечание. Из теоремы $2'$ (см. ниже) следует, что в условиях теоремы 2 подпространство конечной коразмерности, инвариантное относительно всех сюръективных эндоморфизмов, найдётся внутри любого подпространства конечной коразмерности, максимального по включению среди всех подпространств, удовлетворяющих данному полилинейному тождеству. Аналогичный факт верен и для идеалов (левых, правых и двусторонних).

Теорема 3 (сравните [KhM07b]). *Если конечная p-группа G содержит нормальную подгруппу N, удовлетворяющую внешнему коммутаторному тождеству $w(x_1,\dots,x_t)=1$, то G содержит характеристическую подгруппу H, удовлетворяющую тому же тождеству, такую, что $\operatorname{rank} G/H \leqslant f^{t-1}(\operatorname{rank} G/N)$.*

Здесь $\operatorname{rank} G$ — это наименьшее натуральное число n такое, что всякая конечно порождённая подгруппа группы G порождается не более чем n элементами.

Теорема 4. *Если группа G содержит нормальную подгруппу N, удовлетворяющую внешнему коммутаторному тождеству $w(x_1,\dots,x_t)=1$, и такую, что G/N обладает свойством малости $\mathcal{P}$, то G содержит характеристическую, и даже инвариантную относительно всех сюръективных эндоморфизмов, подгруппу H, удовлетворяющую тому же тождеству, такую, что G/H обладает свойством $\mathcal{P}$.*

Под *свойством малости* в теореме 4 понимается любое абстрактное свойство групп $\mathcal{P}$, удовлетворяющее следующим условиям:

1) факторгруппа группы со свойством $\mathcal{P}$ также обладает этим свойством;
2) подпрямое произведение двух групп со свойством $\mathcal{P}$ также обладает этим свойством;
3) каждая группа со свойством $\mathcal{P}$ удовлетворяет условию максимальности для нормальных подгрупп.

Примерами таких свойств могут служить: условие максимальности, условие максимальности для нормальных подгрупп, полицикличность, конечность и т. п.

Теорема 1 была впервые доказана в статье [KhM07a], но с худшей оценкой для индекса. Более простое доказательство и приведённая выше оценка получены в [KM09]. Теорема 2 доказана в [KhM08] с худшей оценкой для коразмерности. Важный частный случай теоремы 3, соответствующий тождеству нильпотентности, доказан в [KhM07b]. Теорема 4 является новой. Все эти утверждения оказываются частными случаями одного общего факта о группах с мультиоператорами.

Методы работ [KhM07a], [KhM07b] и [KhM08] позволяют доказать, на самом деле, утверждения, более сильные, чем теоремы 1 и 2, но с худшими оценками.

Теорема $1'$. *Пусть $w(x_1,\dots,x_t)$ — внешний коммутатор. Тогда в любой группе число подгрупп конечного индекса, являющихся максимальными (по включению) среди всех нормальных подгрупп, удовлетворяющих тождеству $w(x_1,\dots,x_t)=1$, конечно. Кроме того, число таких подгрупп индекса не больше n не превосходит*

$$2^{F^{t-1}(n)}, \quad \text{где } F^k(x) \text{ — это } k\text{-я итерация функции } F(x)=xn^{2^x}.$$

Замечание. Эта теорема содержит два не следующих друг из друга утверждения. С одной стороны, число максимальных среди нормальных подгрупп с тождеством $w(x_1,\dots,x_t)=1$ индекса не больше n ограниченно некоторой явной функцией от n и t. Эта функция очень быстро растёт, но с другой стороны, общее число

подгрупп конечного индекса, являющихся максимальными среди всех нормальных подгрупп с данным тождеством, конечно. Следующая теорема показывает, что аналогичная ситуация имеет место для подпространств (или идеалов) в алгебрах.

Теорема 2′. *Пусть $w(x_1, \dots, x_t)$ — полилинейный элемент свободной (неассоциативной) алгебры над полем F. Тогда в любой алгебре над F пересечение всех идеалов конечной коразмерности, являющихся максимальными (по включению) среди всех идеалов, на которых выполнено тождество $w(x_1, \dots, x_t) = 0$, имеет конечную коразмерность. Кроме того, пересечение таких идеалов коразмерности не больше n имеет коразмерность не больше, чем некоторая величина, зависящая только от n и t. Под словом идеал здесь можно понимать левый, правый, двусторонний идеал, либо просто подпространство (нуль-сторонний идеал).*

Теорема 1 позволяет дать максимально точный ответ на вопрос Дж. О. Баттона ([But08], проблема 3) о расширениях почти разрешимых групп при помощи почти разрешимых.

Теорема 5. *Расширение почти разрешимой ступени s группы при помощи почти разрешимой ступени t группы является почти разрешимой группой ступени не больше $t + s + 1$.*

В параграфе 5 мы докажем эту теорему, а также приведём простой пример, показывающий, что полученную оценку нельзя улучшить.

Следующее утверждение показывает, что ни теорема 1, ни другие варианты теоремы 4 не могут быть распространены на произвольные тождества.

Теорема 6. *Для любого достаточно большого простого числа p существует группа G периода p^2, содержащая подгруппу конечного индекса периода p, но не содержащая характеристических подгрупп конечного индекса периода p. Более того, никакая факторгруппа группы G по характеристической подгруппе периода p не удовлетворяет ни условию максимальности для нормальных подгрупп, ни условию минимальности для нормальных подгрупп и, следовательно, не обладает никаким свойством малости.*

2. Группы с мультиоператорами

Напомним, что согласно [Кур62], Ω-*группой* называют группу $(G, +)$ (необязательно коммутативную) с заданной на ней системой операций Ω. Каждая операция $f \in \Omega$ представляет собой отображение $f : G^{n_f} \to G$ из конечной декартовой степени группы G в G, удовлетворяющее условию $f(0, \dots, 0) = 0$.

Примеры:

1. Группы представляют собой Ω-группы с пустым набором операций Ω.
2. Кольца представляют собой Ω-группы с коммутативным сложением и набором операций Ω, состоящим из одной бинарной операции (умножения), удовлетворяющей условию дистрибутивности.
3. Алгебры над фиксированным полем F можно рассматривать, как Ω-группы с коммутативным сложением и набором операций Ω, состоящим из одной бинарной операции (умножения) и $|F|$ унарных операций (умножения на скаляры), удовлетворяющих известным условиям.

Пусть $\mathcal{V}$ — некоторое многообразие Ω-групп, $w(x_1, \dots, x_t)$ элемент свободной (в многообразии $\mathcal{V}$) алгебры $F_{\mathcal{V}}(x_1, \dots, x_t)$. Для нормальных подгрупп (по сложению) $A_1, \dots, A_t$ Ω-группы $G \in \mathcal{V}$ определим $w(A_1, \dots, A_t)$ как нормальную подгруппу, порождённую всеми элементами вида $w(a_1, \dots, a_t)$, где $a_i \in A_i$.

Элемент $w(x_1, \dots, x_t) \in F_{\mathcal{V}}(x_1, \dots, x_t)$ назовём *полилинейным*, если

$$w(A_1, \dots, A_i + A_i', \dots, A_t) = w(A_1, \dots, A_i, \dots, A_t) + w(A_1, \dots, A_i', \dots, A_t)$$

для всех $i = 1, \dots, t$ и любых нормальных подгрупп $A_1, \dots, A_i, A_i', \dots, A_t$ любой Ω-группы многообразия $\mathcal{V}$.

Полилинейными элементами свободной группы являются внешние коммутаторы, а полилинейными элементами свободной алгебры над полем являются полилинейные (в обычном смысле) выражения.

Пусть $\mathcal{C}$ — некоторый класс нормальных подгрупп Ω-группы G, обладающий следующими свойствами:

1) $\mathcal{C}$ замкнут относительно образов при сюръективных эндоморфизмах Ω-группы G, конечных сумм и конечных пересечений;
2) в любом подсемействе $\mathcal{N} \subseteq \mathcal{C}$ класса $\mathcal{C}$ найдётся такое конечное подсемейство $\mathcal{F} \subseteq \mathcal{N}$, что

$$\sum_{N \in \mathcal{N}} N = \sum_{N \in \mathcal{F}} N.$$

В этом случае мы будем говорить, что $\mathcal{C}$ является *классом больших нормальных подгрупп*. Функцию $\overline{\operatorname{codim}} : \mathcal{C} \to \mathbb{R}$ назовём (*обобщённой*) *коразмерностью*, если она обладает следующими свойствами:

0) $\overline{\operatorname{codim}} N_1 \leqslant \overline{\operatorname{codim}} N_2$, если $N_1 \supseteq N_2$;
1) $\overline{\operatorname{codim}} \varphi(N) \leqslant \overline{\operatorname{codim}} N$ для каждой подгруппы $N \in \mathcal{C}$ и каждого сюръективного эндоморфизма Ω-группы G;

2) $\overline{\operatorname{codim}}\,(N_1 \cap N_2) \leqslant \overline{\operatorname{codim}}\,N_1 + \overline{\operatorname{codim}}\,N_2$ для всех подгрупп $N_1, N_2 \in \mathcal{C}$;
3) в любом семействе $\mathcal{N}$ подгрупп из класса $\mathcal{C}$ найдётся $r \leqslant \max\limits_{N\in\mathcal{N}} \overline{\operatorname{codim}}\,N + 1$ подгрупп $N_1, \ldots, N_r$ таких, что

$$\sum_{N\in\mathcal{N}} N = \sum_{i=1}^{r} N_i.$$

Если G — алгебра над полем, а класс $\mathcal{C}$ состоит из всех подпространств или всех идеалов (односторонних или двусторонних) конечной коразмерности, то в качестве обобщённой коразмерности можно взять обычную коразмерность.

Если G — группа, а класс $\mathcal{C}$ состоит из всех нормальных подгрупп конечного индекса, то в качестве коразмерности можно взять двоичный логарифм индекса. Если же класс $\mathcal{C}$ состоит из всех нормальных подгрупп, индекс которых есть степень фиксированного простого числа p, то в качестве коразмерности подгруппы N можно взять ранг факторгруппы G/N (свойство 3 при этом будет выполнено в силу теоремы Бернсайда о базисе).

Класс всех нормальных подгрупп, факторгруппа по которым обладает каким-то фиксированным свойством малости $\mathcal{P}$, также является классом больших подгрупп. Но коразмерность в этом случае, вообще говоря, не определена.

3. Основная теорема

В доказательстве основной теоремы мы следуем рассуждению из работы [KM09], обобщая его на случай групп с мультиоператорами.

Лемма 1. *Пусть $w(x_1, \ldots, x_t)$ — полилинейный элемент свободной Ω-группы в некотором многообразии $\mathcal{V}$, m — натуральное число, $G \in \mathcal{V}$ — Ω-группа и $\mathcal{N}$ — некоторое конечное семейство её нормальных подгрупп таких, что*

$$w(\underbrace{N, N, \ldots, N}_{m \text{ раз}}, G, G, \ldots, G) = 0 \quad \text{для всех } N \in \mathcal{N}.$$

Тогда

$$w(\underbrace{\widehat{N}, \widehat{N}, \ldots, \widehat{N}}_{m-1 \text{ раз}}, \widehat{G}, \widehat{G}, \ldots, \widehat{G}) = 0, \quad \text{где } \widehat{N} = \bigcap_{N\in\mathcal{N}} N \text{ и } \widehat{G} = \sum_{N\in\mathcal{N}} N.$$

Доказательство.

$$w(\underbrace{\widehat{N}, \widehat{N}, \ldots, \widehat{N}}_{m-1 \text{ раз}}, \widehat{G}, \widehat{G}, \ldots, \widehat{G}) = w(\underbrace{\widehat{N}, \widehat{N}, \ldots, \widehat{N}}_{m-1 \text{ раз}}, \sum_{N\in\mathcal{N}} N, \widehat{G}, \ldots, \widehat{G}) = \sum_{N\in\mathcal{N}} w(\underbrace{\widehat{N}, \widehat{N}, \ldots, \widehat{N}}_{m-1 \text{ раз}}, N, \widehat{G}, \ldots, \widehat{G}).$$

Но $\widehat{N} \subseteq N$ и $\widehat{G} \subseteq G$, поэтому каждое слагаемое последней суммы содержится в нормальной подгруппе

$$w(\underbrace{N, N, \ldots, N}_{m \text{ раз}}, G, G, \ldots, G), \quad \text{которая тривиальна по условию.}$$

В качестве следствия мы получаем нашу основную теорему.

Основная теорема. *Пусть G — Ω-группа, лежащая в многообразии $\mathcal{V}$, $\mathcal{C}$ — некоторый класс её больших нормальных подгрупп, $w(x_1, \ldots, x_t) \in F_{\mathcal{V}}(x_1, \ldots, x_t)$ — полилинейный элемент, $N \in \mathcal{C}$ и $w(N, \ldots, N) = 0$. Тогда в G найдётся инвариантная относительно всех сюръективных эндоморфизмов нормальная подгруппа $H \in \mathcal{C}$, удовлетворяющая тому же тождеству $w(H, \ldots, H) = 0$. При этом, если $\overline{\operatorname{codim}}\colon \mathcal{C} \to \mathbb{R}$ — обобщённая коразмерность, то*

$$\overline{\operatorname{codim}}\,H \leqslant f^{t-1}(\overline{\operatorname{codim}}\,N),$$

где $f^k(x)$ означает k-ю итерацию функции $f(x) = x(x+1)$.

Доказательство. Пусть $\operatorname{End}^{\mathrm{s}} G$ — полугруппа всех сюръективных эндоморфизмов Ω-группы G. Рассмотрим нормальную подгруппу $G_1 = \sum\limits_{\varphi\in\operatorname{End}^{\mathrm{s}} G} \varphi(N)$. Эта подгруппа инвариантна относительно сюръективных эндоморфизмов, является большой (то есть содержится в $\mathcal{C}$) и $\overline{\operatorname{codim}}\,G_1 \leqslant \overline{\operatorname{codim}}\,N$ (если $\overline{\operatorname{codim}}$ определена). Ясно также, что G_1 является суммой конечного числа образов подгруппы N (поскольку N большая), причём, это конечное число не превосходит $\overline{\operatorname{codim}}\,N + 1$ (по определению коразмерности). Таким образом,

$$G_1 = \sum_{k=0}^{p_1} \varphi'_k(N), \quad \text{где } \varphi'_k \in \operatorname{End}^{\mathrm{s}} G \text{ и } p_1 \leqslant l_0 \overset{\text{опр}}{=} \overline{\operatorname{codim}}\,N.$$

Теперь рассмотрим нормальную подгруппу $N_1 = \bigcap\limits_{k=0}^{p_1} \varphi'_k(N)$. Ясно, что эта подгруппа также большая. По свойствам 1) и 2) коразмерности $\overline{\operatorname{codim}}$ имеем

$$l_1 \overset{\text{опр}}{=} \overline{\operatorname{codim}}\, N_1 \leqslant (p_1+1)\overline{\operatorname{codim}}\, N = (p_1+1)l_0 \leqslant (l_0+1)l_0 = f(l_0).$$

Согласно лемме 1

$$w(N_1, \ldots, N_1, G_1) = 0.$$

Аналогичным образом построим большие нормальные подгруппы

$$G_2 = \sum_{\varphi \in \operatorname{End} G} \varphi(N_1) = \sum_{k=0}^{p_2} \varphi''_k(N_1) \quad \text{и} \quad N_2 = \bigcap_{k=0}^{p_2} \varphi''_k(N_1), \quad \text{где } \varphi''_k \in \operatorname{End} G \text{ и } p_2 \leqslant \overline{\operatorname{codim}}\, N_1 = l_1 \leqslant f(l_0).$$

Ясно, что подгруппа G_2 инвариантна относительно всех сюръективных эндоморфизмов Ω-группы G. При этом

$$\overline{\operatorname{codim}}\, G_2 \leqslant \overline{\operatorname{codim}}\, N_1 = l_1 \leqslant f(l_0) \text{ и } l_2 \overset{\text{опр}}{=} \overline{\operatorname{codim}}\, N_2 \leqslant (p_2+1)\overline{\operatorname{codim}}\, N_1 = (p_2+1)l_1 \leqslant f(l_1) \leqslant f(f(l_0)).$$

Согласно лемме 1

$$w(N_2, \ldots, N_2, G_2, G_2) = 0.$$

Продолжая действовать в том же духе, на t-ом шаге мы получим в G инвариантную относительно сюръективных эндоморфизмов большую нормальную подгруппу

$$G_t = \sum_{\varphi \in \operatorname{End} G} \varphi(N_{t-1}) = \sum_{k=0}^{p_t} \varphi_k^{(t)}(N_{t-1}), \quad \text{где } \varphi_k^{(t)} \in \operatorname{End} G.$$

При этом

$$w(G_t, \ldots, G_t) = 0 \quad \text{и} \quad \overline{\operatorname{codim}}\, G_t \leqslant \overline{\operatorname{codim}}\, N_{t-1} = l_{t-1} \leqslant f(l_{t-2}) \leqslant f(f(l_{t-3})) \leqslant \ldots \leqslant f^{t-1}(l_0).$$

Таким образом, подгруппа $H = G_t$ является искомой и теорема доказана.

Теоремы 1 – 4 являются частными случаями основной теоремы:

Теорема 1:	$\mathcal{V} = \{\text{группы}\}$,	$\mathcal{C} = \{\text{нормальные подгруппы конечного индекса}\}$,	$\overline{\operatorname{codim}}\, N = \log_2 \lvert G : N \rvert$;
Теорема 2:	$\mathcal{V} = \{\text{алгебры}\}$,	$\mathcal{C} = \left\{\begin{matrix}\text{подпространства или идеалы} \\ \text{конечной коразмерности}\end{matrix}\right\}$,	$\overline{\operatorname{codim}} = \operatorname{codim}$;
Теорема 3:	$\mathcal{V} = \{\text{группы}\}$,	$\mathcal{C} = \{N \lhd G \ ; \ G/N$ — p-группа$\}$,	$\overline{\operatorname{codim}}\, N = \operatorname{rank} G/N$;
Теорема 4:	$\mathcal{V} = \{\text{группы}\}$,	$\mathcal{C} = \{N \lhd G \ ; \ G/N$ обладает свойством $\mathcal{P}\}$,	$\overline{\operatorname{codim}}$ не определена.

4. Доказательство теорем 1′ и 2′

Теорема 1′ немедленно вытекает из следующего утверждения.*)

Утверждение 1. *Предположим, что группа G содержит достаточно много нормальных подгрупп $N_1, \dots, N_m$ индекса n, удовлетворяющих внешнему коммутаторному тождеству $w(x_1, \dots, x_t) = 1$ (где m — достаточно большое число, зависящее только от n и t). Если*

$$\bigcap N_j \neq \bigcap_{j \neq k} N_j \quad \text{для всех } k = 1, \dots, m,$$

то в группе G найдётся нормальная подгруппа X, удовлетворяющая тому же тождеству и строго содержащая одну из подгрупп N_j (и, следовательно, имеющая индекс строго меньший n).

Доказательство. Это утверждение фактически было доказано в [KhM07a]. Подгруппа X, построенная при доказательстве утверждения 1 статьи [KhM07a] на самом деле содержит одну из подгрупп N_j.

Теорема 2′ аналогичным образом немедленно вытекает из следующего утверждения, доказанного в работе [KhM08].*)

Утверждение 2 ([KhM08], утверждение 3). *Пусть $N_1, \dots, N_m$ — идеалы алгебры A над полем K и $f(x_1, \dots, x_c) \in K\langle x_1, \dots, x_c\rangle$ — полилинейный многочлен. Предположим, что*
(a) *каждый идеал N_i удовлетворяет тождеству $f = 0$ и $\dim A/N_i \leqslant r$;*
(b) $\bigcap N_j \neq \bigcap_{j \neq k} N_j$ *для всех $k = 1, \dots, m$.*
Если $m \geqslant s(r, c)$ для некоторого (r, c)-ограниченного числа $s(r, c)$, то существует $k \in \{1, \dots, m\}$ такое, что идеал $N_k + \bigcap_{j \neq k} N_j$ удовлетворяет тождеству $f = 0$.

Для удобства читателей мы приведём здесь независимое и более простое доказательство теоремы 1′.

Доказательство теоремы 1′. Пусть $\mathcal{N}$ — некоторое множество подгрупп конечного индекса группы G, являющихся максимальными по включению среди всех нормальных подгрупп, удовлетворяющих внешнему коммутаторному тождеству $w(x_1, \dots, x_t) = 1$. Будем доказывать, что множество $\mathcal{N}$ конечно.

Если семейство $\mathcal{N}$ пусто, то доказывать нечего, в противном случае рассмотрим подгруппу $G_0 \in \mathcal{N}$. Эта подгруппа удовлетворяет тождеству

$$w_\sigma(G_0, \dots, G_0) = 1 \quad \text{для всех } \sigma \in S_t. \tag{0}$$

Здесь и далее под $w_\sigma(x_1, \dots, x_t)$, где σ — перестановка степени t, понимается $w(x_{\sigma(1)}, \dots, x_{\sigma(t)})$.

Подгруппа G_0 имеет конечный индекс. Следовательно, семейство подгрупп $\{NG_0 \mid N \in \mathcal{N}\}$ конечно и совпадает с семейством $\{NG_0 \mid N \in \mathcal{N}_1\}$, где $\mathcal{N}_1$ — некоторое конечное подсемейство семейства $\mathcal{N}$. Подгруппа

$$G_1 = G_0 \cap \bigcap_{N \in \mathcal{N}_1} N$$

имеет конечный индекс и удовлетворяет равенству

$$w_\sigma(G_1, \dots, G_1, NG_0) = 1 \quad \text{для всех } \sigma \in S_t \quad \text{и всех } N \in \mathcal{N}. \tag{1}$$

В самом деле, по выбору семейства $\mathcal{N}_1$ всякое произведение NG_0, где $N \in \mathcal{N}$, совпадает с произведением N_1G_0 для некоторой группы $N_1 \in \mathcal{N}_1$ и $N_1 \supseteq G_1 \subseteq G_0$. Следовательно,

$$\begin{aligned} w_\sigma(G_1, \dots, G_1, NG_0) = w_\sigma(G_1, \dots, G_1, N_1G_0) = & w_\sigma(G_1, \dots, G_1, N_1) w_\sigma(G_1, \dots, G_1, G_0) \subseteq \\ \subseteq & w_\sigma(N_1, \dots, N_1, N_1) w_\sigma(G_0, \dots, G_0, G_0) = 1. \end{aligned}$$

Подгруппа G_1 имеет конечный индекс. Следовательно, семейство подгрупп $\{NG_1 \mid N \in \mathcal{N}\}$ конечно и совпадает с семейством $\{NG_1 \mid N \in \mathcal{N}_2\}$, где $\mathcal{N}_2$ — некоторое конечное подсемейство семейства $\mathcal{N}$. Подгруппа

$$G_2 = G_1 \cap \bigcap_{N \in \mathcal{N}_2} N$$

*) Точнее, из утверждения 1 вытекает утверждение теоремы 1′, относящееся к подгруппам ограниченного индекса. Конечность общего числа максимальных нормальных подгрупп конечного индекса с данным тождеством следует из доказательства этого утверждения. Аналогичная ситуация имеет место с утверждением 2 и теоремой 2′.

имеет конечный индекс и удовлетворяет равенству

$$w_\sigma(G_2,\dots,G_2,NG_1,NG_1)=1 \quad \text{для всех } \sigma\in S_t \quad \text{и всех } N\in\mathcal{N}. \tag{2}$$

В самом деле, по выбору семейства $\mathcal{N}_2$ всякое произведение NG_1, где $N\in\mathcal{N}$, совпадает с произведением N_2G_1 для некоторой группы $N_2\in\mathcal{N}_2$ и $N_2\supseteq G_2\subseteq G_1\subseteq G_0$. Следовательно,

$$\begin{aligned}&w_\sigma(G_2,\dots,G_2,NG_1,NG_1)=w_\sigma(G_2,\dots,G_2,N_2G_1,N_2G_1)=\\ =&w_\sigma(G_2,\dots,G_2,N_2,N_2)w_\sigma(G_2,\dots,G_2,N_2,G_1)w_\sigma(G_2,\dots,G_2,G_1,N_2)w_\sigma(G_2,\dots,G_2,G_1,G_1)\subseteq\\ \subseteq&w_\sigma(N_2,\dots,N_2,N_2,N_2)w_\sigma(G_1,\dots,G_1,N_2,G_1)w_\sigma(G_1,\dots,G_1,G_1,N_2)w_\sigma(G_0,\dots,G_0,G_0,G_0).\end{aligned}$$

Первый сомножитель полученного произведения тривиален в силу того, что в группе N_2 выполнено тождество $w=1$. Второй и третий сомножители тривиальны в силу равенства (1). Четвёртый сомножитель тривиален в силу равенства (0).

Продолжая в том же духе, в конце концов мы получим такую подгруппу конечного индекса G_{t-1}, что

$$w_\sigma(NG_{t-1},\dots,NG_{t-1})=1 \quad \text{для всех } \sigma\in S_t \quad \text{и всех } N\in\mathcal{N}. \tag{t}$$

В силу максимальности всех подгрупп N, это означает, что $G_{t-1}\subseteq N$ для всех $N\in\mathcal{N}$, то есть $G_{t-1}\subseteq\bigcap\limits_{N\in\mathcal{N}}N$ и, следовательно, это пересечение имеет конечный индекс. Конечность индекса такого пересечения влечёт, в свою очередь, конечность семейства $\mathcal{N}$, что и требовалось доказать.

Чтобы получить оценки, достаточно заметить, что если все подгруппы семейства $\mathcal{N}$ имеют индекс не больше n, то

$$|G:G_k|\leqslant|G:G_{k-1}|n^{|\mathcal{N}_k|},\quad \text{а}\quad |\mathcal{N}_k|\leqslant 2^{|G:G_{k-1}|}\ \text{(это очень грубая оценка).}$$

Значит,

$$|G:G_k|\leqslant|G:G_{k-1}|\cdot n^{2^{|G:G_{k-1}|}},\quad \text{то есть}\quad |G:G_{t-1}|\leqslant F^{t-1}(n)\quad\text{и}\quad |\mathcal{N}|\leqslant 2^{F^{t-1}(n)},$$

где $F^k(x)$ — это k-я итерация функции $F(x)=xn^{2^x}$.

5. Расширения почти разрешимых групп при помощи почти разрешимых

В этом параграфе мы докажем теорему 5, то есть получим оценку на ступень почти разрешимости группы G, которая содержит нормальную почти разрешимою ступени s подгруппу A такую, что факторгруппа G/A почти разрешима ступени t. От второго «почти» легко избавиться. Действительно, заменяя группу G на её подгруппу конечного индекса (прообраз разрешимой подгруппы конечного индекса в факторгруппе G/A), мы можем считать, что факторгруппа G/A разрешима ступени t.

Далее, по теореме 1 разрешимую ступени s подгруппу N конечного индекса в группе A можно считать характеристической в A и, следовательно, нормальной в G. Для доказательства теоремы осталось показать, что факторгруппа $H=G/N$ содержит разрешимую ступени не выше $t+1$ подгруппу конечного индекса. Но группа H представляет собой расширение конечной группы $K=A/N$ при помощи разрешимой ступени t группы G/A.

У конечной группы K имеется лишь конечное число автоморфизмов, следовательно, централизатор этой группы в H имеет в ней конечный индекс. Такими образом, переходя к подгруппе конечного индекса, мы можем считать, что K содержится в центре группы H. Но тогда факторгруппа H по её центру имеет ступень разрешимости t и, следовательно, сама H разрешима ступени не больше $t+1$, что и требовалось доказать.

Нетрудно сообразить, что оценка в теореме 5 не может быть улучшена. Действительно, рассмотрим, например, центральное произведение G (то есть прямое произведение со склеенными центрами) бесконечного числа копий группы кватернионов. Эта группа G является расширением своей конечной (центральной) подгруппы (порядка 2) при помощи элементарной абелевой 2-группы бесконечного ранга. Нетрудно проверить, что эта группа не имеет абелевых подгрупп конечного индекса. (Чтобы в этом убедиться, можно снова воспользоваться теоремой 1: если есть какая-то абелева подгруппа конечного индекса, то есть и характеристическая абелева подгруппа конечного индекса).

Таким образом, расширение конечной группы (то есть почти тривиальной группы, или почти разрешимой ступени ноль группы) при помощи абелевой группы не обязано быть почти абелевой группой. Этот пример можно слегка усовершенствовать и построить расширение почти абелевой группы при помощи абелевой группы, не являющееся почти метабелевой группой. Действительно, возьмём какое-нибудь точное комплексное представление $\varphi\colon G\to\mathbf{GL}(V)$ описанной выше группы G. В качестве φ можно взять, например, регулярное представление. Соответствующее полупрямое произведение $G_1=V\leftthreetimes G$ является расширением почти абелевой группы $A=V\leftthreetimes\{\pm1\}$ при помощи (элементарной) абелевой группы $G_1/A\simeq G/\{\pm1\}$. Пусть H — подгруппа

конечного индекса в G_1. Покажем, что H не может быть метабелевой. Действительно, подгруппа H обязана содержать V (поскольку V, будучи комплексным векторным пространством, не имеет никаких собственных подгрупп конечного индекса). Факторгруппа $G_1/V \simeq G$ содержит подгруппу конечного индекса H/V. Следовательно, H/V — неабелева группа (как мы уже говорили, в G нет абелевых подгрупп конечного индекса). Значит, её коммутант $(H/V)'$ содержит нетривиальный элемент g порядка 2 и, стало быть, коммутант H' группы H содержит элемент $x = ug$ (для некоторого $u \in V$) и все элементы вида

$$[x, v] = xvx^{-1}(-v) = \varphi(g)v - v, \quad \text{где } v \in V.$$

Поскольку представление φ точное, пространство V содержит вектор v, не лежащий в ядре оператора $\varphi(g) - \mathrm{id}$, и, значит, H' содержит ненулевой вектор $w = \varphi(g)v - v$ такой, что $\varphi(g)w = v - \varphi(g)v = -w$. Тогда, $[x, w] = -2w \neq 0$, то есть группа H' неабелева, а группа H неметабелева, что и требовалось.

Аналогичным образом можно строить примеры высших ступеней.

6. Тождество Бернсайда

В этом параграфе мы докажем теорему 6, то есть построим группу, почти удовлетворяющую тождеству $x^p = 1$, но не имеющую больших характеристических подгрупп периода p. Чтобы построить группу G с нужным свойством, мы воспользуемся известной техникой работы с периодическими соотношениями, следуя книге [О89]. Аналогичные построения могут быть проведены и на основе книги [Адян75].

Рассмотрим бесконечный алфавит $X = \{a, x_1, x_2, \ldots\}$ и свободную группу $G(0) = F(X)$ с базисом X. Группы $G(i) = \langle X \mid R_i \rangle$, где $i \geqslant 1$, определяются по индукции следующим образом. Выберем множество P_i слов длины i в группе $F(X)$, обладающее следующими свойствами:

1) слова из множества P_i не сопряжены в группе $G(i-1)$ степеням слов меньшей длины;
2) различные слова из множества P_i не сопряжены в группе $G(i-1)$ друг другу и обратным друг к другу;
3) множество P_i максимально (по включению) среди всех множеств, удовлетворяющих условиям 1) и 2).

Слова из множества P_i называют *периодами ранга* i. Определим группу $G(i) = \langle X \mid R_i \rangle$, положив

$$R_0 = \varnothing \quad \text{и} \quad R_i = R_{i-1} \cup \{u^{n_u} = 1 \mid u \in P_i\} \text{ при } i \geqslant 1,$$

где n_u — некоторые натуральные числа (зависящие от u).

Ясно, что в группе

$$G = G(\infty) = \left\langle X \,\middle|\, \bigcup_{i=1}^{\infty} R_i \right\rangle$$

каждый неединичный элемент сопряжён со степенью некоторого периода (некоторого ранга). Известно, что если все числа n_u достаточно велики и нечётны, то порядок каждого периода u в группе $G(\infty)$ в точности равен n_u (см., например, [О89], теорема 26.4).

Выберем достаточно большое простое число p и положим

$$n_u = \begin{cases} p, & \text{если } \varphi(u) \notin \langle a \rangle \setminus \{1\}; \\ p^2, & \text{если } \varphi(u) \in \langle a \rangle \setminus \{1\}, \end{cases}$$

где $\varphi\colon F(X) \to \langle a \rangle_p \times \langle x_1 \rangle_p \times \langle x_2 \rangle_p \times \ldots$ — естественный гомоморфизм свободной группы на элементарную абелеву p-группу. При этом в группе $G = G(\infty)$ порядок каждого периода u будет p или p^2 в зависимости от значения $\varphi(u)$.

Лемма 2. *Если простое число p достаточно велико, то*

1) *группа G является периодической группой периода p^2;*
2) *гомоморфизм φ индуцирует гомоморфизм* (обозначаемый в дальнейшем той же буквой) *группы G на элементарную абелеву p-группу;*
3) *элемент g группы G имеет порядок p^2 тогда и только тогда, когда $\varphi(g) \in \langle a \rangle \setminus \{1\}$ (порядки остальных неединичных элементов равны p);*
4) *для каждого натурального i и каждого целого k отображение $f_{i,k}\colon X \to G$, переводящее букву x_i в $a^k x_i$ и оставляющее на месте остальные буквы алфавита X, продолжается до автоморфизма группы G.*

Доказательство. Первое утверждение немедленно вытекает из того, что (как мы уже говорили) каждый элемент сопряжён со степенью периода, а периоды имеют порядки p и p^2. Второе утверждение очевидным образом следует из того, что все определяющие соотношения имеют вид $u^p = 1$.

Чтобы доказать третье утверждение, рассмотрим произвольный элемент g группы G. Этот элемент сопряжён степени периода: $g = t^{-1}u^k t$. Если k делится на p, то из равенства $u^{p^2} = 1$ (верного для любого периода u) следует, что порядок элемента g либо p, либо 1. В то же время $\varphi(g) = \varphi(u^k) = 1$, то есть в данном случае

доказываемое утверждение верно. Если же k не делится на p, то порядок элемента g совпадает с порядком периода u. С другой стороны, включение $\varphi(g) \in \langle a \rangle \setminus \{1\}$ равносильно включению $\varphi(u) \in \langle a \rangle \setminus \{1\}$ и утверждение следует из сделанного выше замечания о порядках периодов.

Докажем четвёртое утверждение. Заметим, что достаточно показать, что указанные отображения продолжаются до эндоморфизмов, поскольку если это так, то эндоморфизмы $f_{i,k}$ и $f_{i,-k}$ будут взаимно обратными.

Чтобы проверить, что отображение $f_{i,k}$ продолжается до эндоморфизма, достаточно показать, что определяющие соотношения при таком отображении букв перейдут в верные равенства в группе G. Рассмотрим произвольное определяющее соотношение $u^l = 1$, где l равно либо p, либо p^2 в зависимости от значения $\varphi(u)$. Но отображение $f_{i,k}$ индуцирует автоморфизм элементарной абелевой p-группы, оставляющий на месте каждый элемент подгруппы $\langle a \rangle$. Поэтому $\varphi(f_{i,k}(u)) \in \langle a \rangle \setminus \{1\}$ тогда и только тогда, когда $\varphi(u) \in \langle a \rangle \setminus \{1\}$. Следовательно, по пункту 3, элемент $f_{i,k}(u)$ имеет в группе G такой же порядок l, как и период u. Стало быть, отображения $f_{i,k}$, действительно, превращают определяющие соотношения в верные равенства и лемма доказана.

Доказательство теоремы 6. Построенная выше группа G содержит подгруппу $N = \langle x_1, x_2, \ldots \rangle \ker \varphi$ индекса p. Согласно утверждению 3 леммы 2, эта подгруппа удовлетворяет тождеству $x^p = 1$.

Рассмотрим теперь произвольную характеристическую подгруппу H группы G. Она остаётся инвариантной, в частности, при действии автоморфизмов $f_{i,k}$. Но автоморфизмы $f_{i,k}$ индуцируют автоморфизмы элементарной абелевой p-группы $E = \langle a \rangle_p \times \langle x_1 \rangle_p \times \langle x_2 \rangle_p \times \ldots$. Следовательно образ $\varphi(H)$ подгруппы H будет подгруппой группы E, инвариантной относительно всех автоморфизмов $f_{i,k}$. Однако всякая такая инвариантная подгруппа группы E, как нетрудно убедиться, либо тривиальна, либо содержит a. Значит, либо H содержится в $\ker \varphi$ (и, следовательно, факторгруппа G/H бесконечна и даже обладает бесконечными в обе стороны цепочками нормальных подгрупп), либо H содержит элемент порядка p^2 (по утверждению 3 леммы 2) и, следовательно, не удовлетворяет тождеству $x^p = 1$. Это завершает доказательство теоремы.

ГЛАВА 13.
БОЛЬШОЕ И СИММЕТРИЧНОЕ:
ТЕОРЕМА МАКАРЕНКО–ХУХРО О ТОЖДЕСТВАХ — БЕЗ ТОЖДЕСТВ

0. Введение

Следующая короткая теорема обобщила и усилила различные результаты, разбросанные по литературе (см, например, [БеК03], [BrNa04] и раздел 21.1.4 книги [KaM82]).

Теорема Макаренко–Хухро [KhM07a]. *Если в группе G есть подгруппа конечного индекса, удовлетворяющая внешнему коммутаторному тождеству, то в группе G найдётся также характеристическая подгруппа конечного индекса, удовлетворяющая этому тождеству.*

Под *внешним* (или *полилинейным*) *коммутаторным тождеством* понимается тождество вида $[\dots[x_1,\dots,x_t]\dots]=1$, в котором каким-то осмысленным образом расставлены квадратные скобки, а все встречающиеся буквы $x_1,\dots,x_t$ различны. Примерами таких тождеств могут служить разрешимость, нильпотентность, центральная метабелевость и т.п. Формальное определение выглядит так. Пусть $F(x_1,x_2,\dots)$ — свободная группа счётного ранга. *Внешними коммутаторами веса 1* называют образующие x_i. *Внешним коммутатором веса* $t>1$ называют каждое слово вида $w(x_1,\dots,x_t)=[u(x_1,\dots,x_r),v(x_{r+1},\dots,x_t)]$, где u и v — внешние коммутаторы веса r и $t-r$ соответственно. *Внешним коммутаторным тождеством* понимается тождество вида $w=1$, где w — внешний коммутатор.

Теорема Макаренко–Хухро имеет различные приложения (см., например, [KhM07b], [KhKMM09], [AST13] и литературу, там цитируемую), она обобщалась и усиливалась в разных направлениях. В [KM09] было получено значительно более простое доказательство (по сравнению с оригинальным) и более хорошая оценка индекса характеристической подгруппы через индекс исходной подгруппы и степень тождества. В то же время, в работах [KhM07b] и [KhM08] были установлены некоторые факты (о группах и об алгебрах), похожие на теорему Макаренко–Хухро, но не вытекающие из неё.

В [KhKMM09] была предпринята попытка навести порядок, там было доказано очень общее утверждение о группах с операторами (в смысле [Higg56], см также [Кур62]), включающая в себя все известные результаты типа теоремы Макаренко–Хухро и несколько новых результатов такого вида. Однако позже были замечены некоторые факты, весьма похожие на теорему Макаренко–Хухро, но не вписывающиеся в общее утверждение из [KhKMM09]. Некоторые из этих фактов весьма изысканные [MSh12], а некоторые совсем простые (нетерпеливый читатель может заглянуть в последний параграф настоящей работы). В общем виде теоремы типа Макаренко–Хухро выглядят следующим образом.

«Теорема». *Если где-то есть что-то* (в классическом случае: в группе подгруппа) *большое* (конечного индекса) *и хорошее* (удовлетворяющая полилинейному тождеству), *то там есть и что-то большое, хорошее и симметричное* (инвариантное относительно всех автоморфизмов).

В этой главе мы делаем очередную попытку охватить всё. В параграфе 1 мы доказываем основную теорему, содержащую в качестве частных случаев все известные и несколько новых результатов, похожих на теорему Макаренко–Хухро (о группах, алгебрах, графах и других объектах). Основная идея состоит в том, что вместо полилинейных тождеств следует рассматривать «полилинейные свойства».

Один из новых результатов (параграф 2) показывает, что в теореме Макаренко–Хухро тождество, то есть тривиальность вербальной подгруппы, можно заменить на что-нибудь, похожее на тривиальность этой подгруппы. Например, верно, что *группа, содержащая подгруппу конечного индекса с аменабельным (или периодическим, или локально конечным...) 2022-м коммутантом, содержит характеристическую подгруппу конечного индекса с тем же свойством.*

Другой результат (параграф 3) можно назвать теоремой, двойственной к теореме Макаренко–Хухро. Он показывает, например, что *для любой конечной нормальной подгруппы N произвольной группы G ограниченного периода найдётся характеристическая конечная подгруппа $H\lhd G$ такая, что спектр* (то есть множество всех порядков элементов) *факторгруппы G/H содержится в спектре факторгруппы G/N.*

Параграф 4 содержит аналогичные результаты для алгебр.

Ещё одно утверждение из параграфа 2 даёт утвердительный ответ на вопрос Макаренко и Шумяцкого о возможности усиления основной теоремы работы [MSh12].

В параграфе 5 мы показываем, что некоторые свойства графов ведут себя аналогично полилинейным коммутаторным тождествам из теоремы Макаренко–Хухро. Например, верно, что *если какой-то граф можно сделать планарным путём выбрасывания конечного числа рёбер, то это конечное множество рёбер можно выбрать инвариантным относительно всех автоморфизмов исходного графа.*

В последнем параграфе, в качестве награды добравшимся до конца читателям, мы приводим две элементарные (но нетривиальные) задачки для школьников на тему, которой посвящена эта глава.

1. Основная теорема

Напомним, что *полурешёткой* называют частично упорядоченное множество $\mathcal{L}$, в котором каждое конечное подмножество $\mathcal{N} \subseteq \mathcal{L}$ имеет точную верхнюю грань $\sup \mathcal{N} \in \mathcal{L}$. *Направленной полурешёткой* мы будем называть полурешётку, которая является направленным вниз частично упорядоченным множеством; это означает, что для любого конечного множества $\mathcal{N} \subseteq \mathcal{L}$ найдётся элемент $\inf \mathcal{N} \in \mathcal{L}$ такой, что $\inf \mathcal{N} \leqslant N$ для любого $N \in \mathcal{N}$. Обращаем внимание, что в наших обозначениях sup — это точная верхняя грань, а inf — это к а к а я - т о нижняя грань; мы надеемся, что это не приведёт к путанице (смотрите ещё замечание после определения коразмерности, ниже). Полурешётку $\mathcal{L}$ называют *нётеровой*, если в ней все возрастающие цепочки обрываются, то есть не существует бесконечных цепочек вида $N_1 < N_2 < \ldots$, где $N_i \in \mathcal{L}$. Полурешётка $\mathcal{L}$ называется *решёткой*, если каждое конечное подмножество $\mathcal{N} \subseteq \mathcal{L}$ имеет точную нижнюю грань, которую мы будем обозначать $\inf \mathcal{N}$ в этом случае.

Будем называть t-арное свойство (предикат) $\mathcal{P}$ на полурешётке $\mathcal{L}$ *(поли)монотонным*, если из справедливости свойства $\mathcal{P}(N_1, \ldots, N_t)$, где $N_i \in \mathcal{L}$, следует, что верно и $\mathcal{P}(N'_1, \ldots, N'_t)$ для любых $N'_i \leqslant N_i$. Назовём свойство $\mathcal{P}$ *полилинейным*, если для любого i из справедливости свойств
$\mathcal{P}(N_1, \ldots, N_{i-1}, N'_i, N_{i+1}, \ldots, N_t)$ и $\mathcal{P}(N_1, \ldots, N_{i-1}, N''_i, N_{i+1}, \ldots, N_t)$
следует свойство $\mathcal{P}(N_1, \ldots, N_{i-1}, \sup(N'_i, N''_i), N_{i+1}, \ldots, N_t)$.

Нам понадобятся также двойственные понятия. Предикат $\mathcal{P}$ на полурешётке $\mathcal{L}$ назовём *комонотонным*, если из справедливости свойства $\mathcal{P}(N_1, \ldots, N_t)$, где $N_i \in \mathcal{L}$, следует, что верно и $\mathcal{P}(N'_1, \ldots, N'_t)$ для любых $N'_i \geqslant N_i$. Назовём предикат $\mathcal{P}$ *кополилинейным*, если для любого i из справедливости свойств
$\mathcal{P}(N_1, \ldots, N_{i-1}, N'_i, N_{i+1}, \ldots, N_t)$ и $\mathcal{P}(N_1, \ldots, N_{i-1}, N''_i, N_{i+1}, \ldots, N_t)$
следует свойство $\mathcal{P}(N_1, \ldots, N_{i-1}, \inf(N'_i, N''_i), N_{i+1}, \ldots, N_t)$ для некоторой нижней грани $\inf(N'_i, N''_i)$ (мы будем использовать слово *колинейный*, если $t = 1$).

Будем говорить, что полугруппа эндоморфизмов $\Phi \subseteq \operatorname{End} \mathcal{L}$ полурешётки $\mathcal{L}$ *сохраняет свойство* $\mathcal{P}$ (или свойство $\mathcal{P}$ Φ-*инвариантно*), если из $\mathcal{P}(N_1, \ldots, N_t)$ следует $\mathcal{P}(\varphi(N_1), \ldots, \varphi(N_t))$ для любых $N_i \in \mathcal{L}$ и $\varphi \in \Phi$. Например, свойство $\mathcal{R}(X, Y, Z) = \Big(X = \sup(Y, Z)\Big)$ является $(\operatorname{End} \mathcal{L})$-инвариантным по определению *эндоморфизмов полурешётки*. Элемент N полурешётки назовём Φ-*инвариантным*, если $\varphi(N) \leqslant N$ для всех $\varphi \in \Phi$ (это, в частности, означает, что $\varphi(N) = N$ для всех $\varphi \in \Phi$, если полугруппа Φ является подгруппой в $\operatorname{Aut} \mathcal{L}$).

Следующее утверждение представляет собой естественное обобщение леммы из работы [KM09] (в которой речь идёт о решётке нормальных подгрупп в группе, а в качестве свойства фигурирует полилинейное коммутаторное тождество) и леммы 1 из [KhKMM09] (в которой речь идёт о решётке подгрупп в мультиоператорных группах).

Лемма 1. *Пусть $\mathcal{M}$ — направленная полурешётка с наибольшим элементом* $\sup \mathcal{M}$, *$\mathcal{P}$ — монотонное полилинейное t-арное свойство на $\mathcal{M}$, m — натуральное число и $\mathcal{N} \subseteq \mathcal{M}$ — некоторое конечное подмножество в $\mathcal{M}$ такое, что*

$$\mathcal{P}(\underbrace{N, N, \ldots, N}_{m \text{ раз}}, \sup \mathcal{M}, \sup \mathcal{M}, \ldots, \sup \mathcal{M}) \quad \textit{верно для всех } N \in \mathcal{N}.$$

Тогда верно и

$$\mathcal{P}(\underbrace{\widehat{N}, \widehat{N}, \ldots, \widehat{N}}_{m-1 \text{ раз}}, \widehat{G}, \widehat{G}, \ldots, \widehat{G}), \quad \textit{где } \widehat{N} = \inf \mathcal{N} \textit{ и } \widehat{G} = \sup \mathcal{N}.$$

Доказательство. Так как $\mathcal{P}$ монотонно, а $\widehat{G} \leqslant \sup \mathcal{M}$ и $\widehat{N} \leqslant N$ для всех $N \in \mathcal{N}$, мы имеем

$$\mathcal{P}(\underbrace{\widehat{N}, \widehat{N}, \ldots, \widehat{N}}_{m-1 \text{ раз}}, N, \widehat{G}, \ldots, \widehat{G}) \quad \text{верно для всех } N \in \mathcal{N}.$$

Теперь из полилинейности (точнее, из линейности по m-му аргументу) следует доказываемое утверждение.

Пусть $\mathcal{L}$ — нётерова направленная полурешётка и $\Phi \subseteq \operatorname{End} \mathcal{L}$ — некоторая полугруппа её эндоморфизмов. Функцию $\operatorname{codim}\colon \mathcal{L} \to \mathbb{R}$ назовем *(обобщённой)* Φ-*коразмерностью*, если она обладает следующими свойствами:

1) $\operatorname{codim} N_1 \leqslant \operatorname{codim} N_2$, если $N_1 \geqslant N_2$;
2) $\operatorname{codim} \varphi(N) \leqslant \operatorname{codim} N$ для любых $N \in \mathcal{L}$ и $\varphi \in \Phi$;
3) $\operatorname{codim} \inf(N_1, N_2) \leqslant \operatorname{codim} N_1 + \operatorname{codim} N_2$ для любых $N_1, N_2 \in \mathcal{L}$ и некоторой нижней грани $\inf(N_1, N_2)$;
4) в любом семействе $\mathcal{N} \subseteq \mathcal{L}$ найдется $r \leqslant \max\limits_{N \in \mathcal{N}} \operatorname{codim} N + 1$ элементов $N_1, \ldots, N_r$ таких, что

$$\sup \mathcal{N} = \sup(N_1, \ldots, N_r).$$

Это определение коразмерности является естественным обобщением соответствующего понятия из работы [KhKMM09] (в которой речь идёт о решётке нормальных подгрупп в мультиоператорной группе). Если на некоторой полурешётке определена коразмерность, то символом inf мы всегда будем обозначать нижнюю грань, удовлетворяющую условию 3).

Основная теорема. *Пусть $\mathcal{L}$ — нётерова направленная полурешётка, $\Phi \subseteq \operatorname{End}\mathcal{L}$ — некоторая полугруппа её эндоморфизмов и $\mathcal{P}$ — полимонотонный полилинейный t-арный Φ-инвариантный предикат на $\mathcal{L}$. Тогда, если существует элемент $N \in \mathcal{L}$ со свойством $\mathcal{P}(N,\dots,N)$, то существует элемент $H \in \mathcal{L}$ такой, что*

1) *элемент H обладает тем же свойством: $\mathcal{P}(H,\dots,H)$;*
2) *элемент H Φ-инвариантен;*
3) *если $\varphi(N) \leqslant J$ для любого $\varphi \in \Phi$ и некоторого $J \in \mathcal{L}$, то $H \leqslant J$;*
4) *если $\mathcal{L}$ — решётка (то есть каждое конечное множество имеет точную нижнюю грань) и Φ состоит из эндоморфизмов решётки (то есть из отображений, коммутирующих с операциями взятия точной нижней грани конечных множеств), то H содержится в подрешётке, порождённой множеством $\{\varphi(N)\,;\,\varphi\in\Phi\}$;*
5) *если $\operatorname{codim}\colon \mathcal{L} \to \mathbb{R}$ — обобщенная Φ-коразмерность, то $\operatorname{codim} H \leqslant f^{t-1}(\operatorname{codim} N)$, где $f^k(x)$ означает k-ю итерацию функции $f(x) = x(x+1)$.*

Доказательство. В силу нётеровости полурешётка $\mathcal{L}$ содержит элемент $G_1 = \sup\limits_{\varphi\in\Phi}\varphi(N)$, причём

$$G_1 = \sup(\varphi'_0(N),\dots,\varphi'_{p_1}(N)) \quad \text{для некоторых эндоморфизмов } \varphi'_i \in \Phi.$$

Элемент G_1 Φ-инвариантен: $\varphi(G_1) = \sup(\varphi\varphi'_0(N),\dots,\varphi\varphi'_{p_1}(N)) \leqslant \sup\limits_{\varphi\in\Phi}\varphi(N) = G_1$. При этом $G_1 \leqslant J$ (если J такой, как в пункте 3) теоремы), а если на $\mathcal{L}$ задана коразмерность, то

$$p_1 \leqslant l_0 \overset{\text{опр}}{=} \operatorname{codim} N \quad \text{по свойству 4) коразмерности.}$$

Положим теперь $N_1 = \inf(\varphi'_0(N),\dots,\varphi'_{p_1}(N))$. По свойствам 2) и 3) коразмерности codim мы имеем

$$l_1 \overset{\text{опр}}{=} \operatorname{codim} N_1 \leqslant (p_1+1)\operatorname{codim} N = (p_1+1)l_0 \leqslant (l_0+1)l_0 = f(l_0).$$

Согласно лемме 1 (применённой к полурешётке $\mathcal{M} = \mathcal{L}$) выполняется свойство

$$\mathcal{P}(N_1,\dots,N_1,G_1).$$

Аналогичным образом выберем элементы

$$G_2 = \sup_{\varphi\in\Phi}\varphi(N_1) = \sup(\varphi''_0(N_1),\dots,\varphi''_{p_2}(N_1)) \;\text{ и }\; N_2 = \inf(\varphi''_0(N_1),\dots,\varphi''_{p_2}(N_1)), \quad \text{где } \varphi''_i \in \Phi.$$

При этом

$G_2 \leqslant G_1 \leqslant J$ (так как $N_1 \leqslant \varphi'_0(N)$, значит, $G_2 = \sup\limits_{\varphi\in\Phi}\varphi(N_1) \leqslant \sup\limits_{\varphi\in\Phi}\varphi\varphi'_0(N) \leqslant \sup\limits_{\varphi\in\Phi}\varphi(N) = G_1$) и

$p_2 \leqslant \operatorname{codim} N_1 = l_1 \leqslant f(l_0)$ (по свойствам 2) и 4) коразмерности codim).

Понятно, что элемент G_2 Φ-инвариантен (по тем же причинам, что G_1) и справедливы оценки

$$\operatorname{codim} G_2 \leqslant \operatorname{codim}\varphi''_0 N_1 \leqslant \operatorname{codim} N_1 = l_1 \leqslant f(l_0) \quad \text{и} \quad l_2 \overset{\text{опр}}{=} \operatorname{codim} N_2 \leqslant (p_2{+}1)\operatorname{codim} N_1 = (p_2{+}1)l_1 \leqslant f(l_1) \leqslant f(f(l_0)).$$

Снова по лемме 1 (применённой к полурешётке $\mathcal{M} = \{X \in \mathcal{L} \mid X \leqslant G_1\}$) получаем

$$\mathcal{P}(N_2,\dots,N_2,G_2,G_2).$$

Продолжая в том же духе, на t-ом шаге получим Φ-инвариантный элемент

$$G_t = \sup_{\varphi\in\Phi}\varphi(N_{t-1}) = \sup(\varphi_0^{(t)}(N_{t-1}),\dots,\varphi_{p_t}^{(t)}(N_{t-1})) \text{ и элемент } N_t = \inf(\varphi_0^{(t)}(N_{t-1}),\dots,\varphi_{p_t}^{(t)}(N_{t-1})), \text{ где } \varphi_i^{(t)} \in \Phi.$$

При этом выполняются свойство $\mathcal{P}(G_t,\dots,G_t)$ и неравенства

$$G_t \leqslant J, \qquad \operatorname{codim} G_t \leqslant \operatorname{codim} N_{t-1} = l_{t-1} \leqslant f(l_{t-2}) \leqslant f(f(l_{t-3})) \leqslant \dots \leqslant f^{t-1}(l_0).$$

Таким образом, элемент $H = G_t$ является искомым и теорема доказана. (Утверждение 4 очевидно из построения).

Следующее утверждение позволяет строить новые полилинейные свойства из известных полилинейных свойств.

Лемма о композиции. *Пусть на некоторой решётке имеется полилинейный монотонный предикат* $\mathcal{Q}(M_1,\dots,M_k)$ *и набор предикатов* $\mathcal{R}=\left\{\mathcal{R}_i\begin{pmatrix}X_1,\dots,X_l\\ Y\end{pmatrix}\right\}$, *которые по первой строке (то есть при любой фиксированной второй строке) являются полилинейными и монотонными, а по второй строке (то есть при любой фиксированной первой строке) — колинейными и комонотонными. Тогда предикат*

$$\mathcal{Q}\circ\mathcal{R}(N_1,\dots,N_{kl})=\left(\exists M_1,\dots,M_k\quad \mathcal{Q}(M_1,\dots,M_k)\text{ и для }i\in\{1,\dots,k\}\ \ \mathcal{R}_i\begin{pmatrix}N_{(i-1)l+1},\dots,N_{li}\\ M_i\end{pmatrix}\right),$$

называемый композицией предикатов $\mathcal{Q}$ *и* $\mathcal{R}$, *является полилинейным и монотонным.*

Доказательство. Проверим монотонность, например, по первому аргументу. Если $N_1'\leqslant N_1$ и свойство $\mathcal{Q}\circ\mathcal{R}(N_1,\dots,N_{kl})$ выполнено (с некоторыми M_i из определения композиции), то свойство $\mathcal{Q}\circ\mathcal{R}(N_1',\dots,N_{kl})$, разумеется, тоже выполнено (с теми же самыми M_i) в силу монотонности $\mathcal{R}_1$ относительно первой строки.

Проверим полилинейность, например, опять по первому аргументу. Пусть свойства $\mathcal{Q}\circ\mathcal{R}(N_1',N_2,\dots,N_{kl})$ и $\mathcal{Q}\circ\mathcal{R}(N_1'',N_2,\dots,N_{kl})$ выполняются, то есть выполнены свойства

$$\mathcal{R}_1\begin{pmatrix}N_1',N_2,\dots,N_l\\ M_1'\end{pmatrix},\ \mathcal{R}_2\begin{pmatrix}N_{l+1},\dots,N_{2l}\\ M_2'\end{pmatrix},\dots,\qquad \mathcal{Q}(M_1',\dots,M_k'),$$
$$\mathcal{R}_1\begin{pmatrix}N_1'',N_2,\dots,N_l\\ M_1''\end{pmatrix},\ \mathcal{R}_2\begin{pmatrix}N_{l+1},\dots,N_{2l}\\ M_2''\end{pmatrix},\dots\quad\text{и}\quad \mathcal{Q}(M_1'',\dots,M_k'')$$

для некоторых $M_1',\dots,M_k',M_1'',\dots,M_k''$. Мы утверждаем, что тогда выполнены свойства

$$\mathcal{R}_1\begin{pmatrix}\sup(N_1',N_1''),N_2,\dots,N_l\\ \sup(M_1',M_1'')\end{pmatrix},\ \mathcal{R}_2\begin{pmatrix}N_{l+1},\dots,N_{2l}\\ \inf(M_2',M_2'')\end{pmatrix},\dots,\quad\text{и}\quad \mathcal{Q}(\sup(M_1',M_1''),\inf(M_2',M_2''),\dots,\inf(M_k',M_k'')),$$

(то есть свойство $\mathcal{Q}\circ\mathcal{R}(\sup(N_1',N_1''),N_2,\dots,N_k)$ выполнено, а в качестве $M_1,\dots,M_k$ достаточно взять $\sup(M_1',M_1'')$, $\inf(M_2',M_2'')$,..., $\inf(M_k',M_k'')$, соответственно). Действительно,

- первое свойство ($\mathcal{R}_1(\dots)$) выполнено в силу линейности предиката $\mathcal{R}_1$ по первому элементу первой строки и комонотонности по второй строке;
- второе свойство ($\mathcal{R}_2(\dots)$) выполнено в силу колинейности предиката $\mathcal{R}_2$ по второй строке;
- ...
- а последнее свойство ($\mathcal{Q}(\dots)$) выполнено в силу линейности предиката $\mathcal{Q}$ по первому аргументу и монотонности по остальным аргументам.

Лемма доказана.

Оставшаяся часть работы посвящена применением основной теоремы для групп, алгебр, графов и других структур. В качестве полугруппы Ф в этой работе будет всегда рассматриваться какая-нибудь естественная подгруппа группы $\mathrm{Aut}\,\mathcal{L}$.

2. Решётка больших нормальных подгрупп

Напомним, что абстрактный класс групп $\mathcal{K}$ называют *радикальным* (или *классом Фиттинга*), если он замкнут относительно нормальных подгрупп и конечных произведений нормальных подгрупп, то есть

1) всякая нормальная подгруппа группы из $\mathcal{K}$ лежит в $\mathcal{K}$;
2) группа, раскладывающаяся в произведение двух нормальных подгрупп, лежащих в $\mathcal{K}$, также лежит в $\mathcal{K}$.

Корадикальным классом (или *формацией*) называют абстрактный класс групп $\mathcal{K}$, замкнутый относительно гомоморфных образов и подпрямых произведений, то есть такой, что:

1′) факторгруппа группы из $\mathcal{K}$ лежит в $\mathcal{K}$;
2′) подпрямое произведение двух групп, лежащих в $\mathcal{K}$, также лежит в $\mathcal{K}$.

Подробнее о радикальных и корадикальных классах можно прочитать, например, в книге [Шем78].

Следующие классы групп являются *радикальными формациям*, то есть они и радикальны, и корадикальны:

- конечные группы;
- конечные p-группы;
- локально конечные группы (радикальность вытекает из теоремы О. Ю. Шмидта: *расширение локально конечной группы при помощи локально конечной локально конечно*, см. [КаМ82]);
- периодические группы;
- нётеровы группы;
- артиновы группы;
- нильпотентные группы (радикальность имеет место по теореме Фиттинга, см. [КаМ82]);
- локально нильпотентные группы (радикальность имеет место по теореме Плоткина, см. [КаМ82]);

– разрешимые группы;
– почти разрешимые группы;
– локально полициклические группы (радикальность имеет место по теореме 18.1.2 из [KaM82]);
– группы, удовлетворяющие нетривиальному тождеству;
– группы, не содержит неабелевых свободных подгрупп;
– аменабельные (дискретные) группы;
– ...

Кроме того, корадикальными классами являются все многообразия групп, класс всех бинарно конечных групп, группы с условием максимальности (или минимальности) для нормальных подгрупп и другие классы.

Теорема о больших подгруппах. *Пусть N — нормальная подгруппа группы G и факторгруппа G/N удовлетворяет условию максимальности для нормальных подгрупп. Тогда G содержит характеристические подгруппы $H_1, H_2, \ldots$ такие, что*

1) *факторгруппы G/H_t лежат в корадикальном классе (формации) $\mathcal{F}$, порождённом группой G/N; более того подгруппы H_t содержатся в решётке подгрупп группы G, порождённой образами N при всевозможных автоморфизмах группы G;*
2) *для любого полилинейного коммутаторного слова w степени $k \leqslant t$ группа $w(H_t, \ldots, H_t)$ содержится в радикальном классе $\mathcal{R}_w$, порождённом группой $w(N, \ldots, N)$;*
3) *если при этом codim — обобщённая коразмерность, определённая на решётке подгрупп, факторгруппы по которым лежат в $\mathcal{F}$, то $\mathsf{codim}\, H_t \leqslant f^{t-1}(\mathsf{codim}\, N)$, где $f^k(x)$ означает k-ю итерацию функции $f(x) = x(x+1)$.*

Доказательство. Пусть $K_1, \ldots, K_t$ — нормальные подгруппы группы G и $w(x_1, \ldots, x_t)$ — внешний коммутатор. Тогда

а) подгруппа $w(K_1, \ldots, K_t) \overset{\text{опр}}{=} \langle w(h_1, \ldots, h_t) : h_i \in K_i \rangle$ нормальна в группе G;
б) $w(K_1, \ldots, K_t) = [u(K_1, \ldots, K_r), v(K_{r+1}, \ldots, K_t)]$, если $w(x_1, \ldots, x_t) = [u(x_1, \ldots, x_r), v(x_{r+1}, \ldots, x_t)]$;
в) $w(K_1, \ldots, K_{i-1}, \prod\limits_{N \in \mathcal{N}} N, K_{i+1}, \ldots, K_t) = \prod\limits_{N \in \mathcal{N}} w(K_1, \ldots, K_{i-1}, N, K_{i+1}, \ldots, K_t)$ для произвольного семейства $\mathcal{N}$ нормальных подгрупп группы G.

Эти факты хорошо известны и легко доказываются по индукции.

Осталось применить основную теорему, взяв в качестве $\mathcal{L}$ решётку нормальных подгрупп группы G, порождённую образами N при всевозможных автоморфизмах группы G (эта решётка нётерова, и даже вся формация $\mathcal{F}$ состоит из групп, нётеровых по нормальным подгруппам). В качестве Φ следует взять группу автоморфизмов группы G, а в качестве $\mathcal{P}(N_1, \ldots, N_t)$ — следующее свойство:

для каждого полилинейного коммутаторного слова w степени не больше t группа $w(N_1, \ldots, N_k)$ содержится в $\mathcal{R}_w$.

Монотонность свойства $\mathcal{P}$ вытекает из замкнутости радикального класса относительно нормальных подгрупп, а полилинейность — из замкнутости радикального класса относительно произведений нормальных подгрупп и свойства в) внешних коммутаторов. Теорема доказана.

Теорема о больших подгруппах обобщает теорему Макаренко–Хухро в трёх направлениях:

– конечность индексов подгрупп N и H, то есть конечность факторгрупп G/N и G/H, заменяется на принадлежность этих факторгрупп любой формации с условием максимальности для нормальных подгрупп, понятие индекса (точнее логарифма индекса) при этом заменяется на абстрактное понятие коразмерности; это обобщение не является новым, оно было впервые получено в [KhKMM09];
– тождество (то есть единичность вербальной подгруппы) заменяется на принадлежность этой вербальной подгруппы произвольному радикальному классу; например, наша теорема показывает, что *группа, содержащая подгруппу конечного индекса с периодическим сотым коммутантом, содержит характеристическую подгруппу конечного индекса с тем же свойством*;
– наконец, вместо одного полилинейного слова w рассматриваются сразу все полилинейные слова, что даёт значительный выигрыш в оценке, если, например, мы хотим построить характеристическую подгруппу конечного индекса, в которой выполняются все полилинейные тождества степени не выше чем сто, выполненные в данной подгруппе конечного индекса (этого можно добиться многократным применением теоремы Макаренко–Хухро, но оценка индекса станет очень плохой).

Следующие простые факты позволяют применить лемму о композиции, обобщить теорему Макаренко–Хухро ещё в одном направлении и ответить на вопрос Макаренко и Шумяцкого.

Лемма о факторгруппах. *Каждое из следующих двух свойств, $\mathcal{A}(N,M)$ и $\mathcal{B}(N,M)$, пар нормальных подгрупп произвольной группы G может быть записано в виде $\mathcal{R}\binom{N,\dots,N}{M}$, где предикат $\mathcal{R}$ на решётке нормальных подгрупп является по первой строке монотонным и полилинейным, а по второй строке — комонотонным и колинейным:*

$$\mathcal{A}(N,M) = \Big(N/(N\cap M) \text{ удовлетворяет (фиксированному) внешнему коммутаторному тождеству } w=1\Big),$$
$$\mathcal{B}(N,M) = \Big(N/(N\cap M) \text{ принадлежит (фиксированной) радикальной формации } \mathcal{F}\Big).$$

Доказательство. Для свойства $\mathcal{A}$ предикат

$$\mathcal{R}\binom{N_1,\dots,N_t}{M} = \Big(w(N_1,\dots,N_t)\subseteq M\Big)$$

очевидно удовлетворяет всем условиям.

А для свойства $\mathcal{B}$ в качестве $\mathcal{R}$ можно взять само свойство $\mathcal{B}$:

$$\mathcal{R}\binom{N_1}{M} = \mathcal{B}(N_1,M).$$

Линейность и монотонность по первой строке вытекают из радикальности класса $\mathcal{F}$, а колинейность и комонотонность по второй строке вытекают из корадикальности класса $\mathcal{F}$.

Лемма о расширениях. *Пусть $\mathcal{Q}(M_1,\dots,M_l)$ — монотонный полилинейный предикат на решётке нормальных подгрупп группы G, w — внешнее коммутаторное слово степени d и $\mathcal{F}$ — радикальная формация. Тогда каждое из следующих двух свойств, $\mathcal{C}(N)$ и $\mathcal{D}(N)$, нормальных подгрупп группы G может быть записано в виде $\mathcal{P}(N,\dots,N)$, где предикат $\mathcal{P}(N_1,\dots,N_t)$ на решётке нормальных подгрупп является монотонным и полилинейным, причём $t=ld$ для свойства $\mathcal{C}$ и $t=l$ для свойства $\mathcal{D}$:*

$$\mathcal{C}(N) = \Big(\exists M\lhd G \quad M\subseteq N,\ \mathcal{Q}(M,\dots,M) \text{ и } N/M \text{ удовлетворяет тождеству } w=1\Big),$$
$$\mathcal{D}(N) = \Big(\exists M\lhd G \quad M\subseteq N,\ \mathcal{Q}(M,\dots,M) \text{ и } N/M\in\mathcal{F}\Big).$$

Доказательство. Ясно, что свойство $\mathcal{C}(N)$ можно переписать в эквивалентном виде

$$\mathcal{C}(N) = \big(\exists M\lhd G \quad \mathcal{A}(N,M) \text{ и } \mathcal{Q}(M,\dots,M)\big), \quad \text{где } \mathcal{A} \text{ из леммы о факторгруппах.}$$

Теперь заметим, что последняя формула эквивалентна такой:

$$\mathcal{C}(N) = \Big(\exists M_1,\dots,M_l\lhd G \quad \mathcal{A}(N,M_1),\ \dots,\ \mathcal{A}(N,M_l) \text{ и } \mathcal{Q}(M_1,\dots,M_l)\Big).$$

Чтобы в этом убедиться (в неочевидную сторону) достаточно положить $M=\bigcap M_i$ и вспомнить, что многообразие групп, заданных тождеством $w=1$, замкнуто относительно подпрямых произведений, а свойство $\mathcal{Q}$ монотонно. В силу леммы о факторгруппах мы можем это свойство переписать в виде

$$\mathcal{C}(N) = \left(\exists M_1,\dots,M_l\lhd G \quad \mathcal{R}\binom{N,\dots,N}{M_1},\ \dots,\ \mathcal{R}\binom{N,\dots,N}{M_l} \quad \text{и } \mathcal{Q}(M_1,\dots,M_l)\right),$$

где предикат $\mathcal{R}$ на решётке нормальных подгрупп является по первой строке монотонным и полилинейным, а по второй строке — комонотонным и колинейным.

Ссылка на лемму о композиции завершает доказательство. Для свойства $\mathcal{D}$ рассуждения полностью аналогичны.

Следующее утверждение доказано в работе [MSh12] для случая, когда группа G локально конечна, а каждый класс $\mathcal{K}_i$ является классом всех локально нильпотентных групп.

Теорема о рядах. *Пусть группа G содержит подгруппу N конечного индекса, обладающую нормальным в G рядом*

$$\{1\} = A_0 \subseteq \ldots \subseteq A_n = N,$$

в котором каждый фактор A_i/A_{i-1} либо удовлетворяет полилинейному коммутаторному тождеству $w_i = 1$ веса t_i, либо лежит в радикальном классе $\mathcal{K}_i$, причём все эти классы, кроме быть может $\mathcal{K}_1$, являются одновременно корадикальными. Тогда G содержит характеристическую подгруппу конечного индекса с тем же свойством (то есть с рядом такой же длины, каждый фактор которого удовлетворяет тому же тождеству или лежит в том же классе, что соответствующий фактор исходного ряда), причём $\log_2 |G : H| \leqslant f^{t-1}(\log_2 |G : N|)$, где $f^k(x)$ — это k-ая итерация функции $f(x) = x(x+1)$ и $t = \prod t_i$.

Доказательство. Лемма о расширениях и очевидная индукция показывают, что наличие у нормальной подгруппы N такого нормального ряда записывается в виде $\mathcal{P}(N, \ldots, N)$, где $\mathcal{P}$ — некоторый полилинейный монотонный предикат от t аргументов на решётке нормальных подгрупп группы G. Осталось сослаться на основную теорему.

Отметим, что для случая, когда группа G локально конечна, а каждый класс $\mathcal{K}_i$ является классом всех локально нильпотентных групп, в работе [MSh12] доказано несколько более сильное утверждение: в группе G найдётся характеристическая подгруппа конечного индекса, обладающая характеристическим рядом с указанным свойством. В общем случае, такое усиление невозможно, как показывает следующий пример, принадлежащий Иву Корнулье.

Пример [Corn13]. *Существует группа, обладающая нормальной абелевой подгруппой счётного индекса, но не имеющая абелевых характеристических подгрупп счётного индекса.*
Возьмём счётномерное векторное пространство V с базисом $\{e_q\}$, где $q \in \mathbb{Q}$, над конечным полем K и рассмотрим группу G «унитреугольных» операторов, то есть таких операторов g в V, что $ge_q - e_q \in \langle\{e_r : r < q\}\rangle$. В группе G рассмотрим подгруппу H, состоящую из матриц A, обладающих тем свойством, что для любого вещественного числа r лишь конечное число их ненулевых элементов a_{pq} таковы, что $p \neq q$ и либо $p > r$, либо $q < r$. Тогда группа H обладает абелевой нормальной подгруппой счётного индекса, состоящей из матриц A, у которых все ненулевые недиагональные элементы a_{pq} таковы, что либо $p < 0$, либо $q > 0$. А нетривиальных характеристических абелевых подгрупп группа H не имеет. Действительно, если $1 \neq h \in N \lhd H$, то коммутатор c элемента h и любой трансвекции снова лежит в N и имеет лишь конечное число ненулевых недиагональных элементов и, следовательно, c лежит в конечномерной унитреугольной группе $\mathbf{UT}_n(K)$, которая является нильпотентной и, значит, любая её нетривиальная нормальная подгруппа нетривиально пересекается с центром (который состоит из трансвекций). Таким образом, любая нетривиальная нормальная подгруппа группы H содержит трансвекции. Осталось заметить, что все трансвекции переводятся друг в друга автоморфизмами группы H, то есть нетривиальная характеристическая подгруппа группы H обязана содержать все трансвекции и, значит, не может быть абелевой.

3. Решётка маленьких подгрупп. «Котеорема Макаренко–Хухро»

Рассмотрим произвольную универсальную позитивную замкнутую формулу первого порядка в групповом языке, например,

$$(\forall x)(\forall y)\left(\left(x^3 = y^3 \ \wedge\ (xy)^4 = (yx)^4\right) \ \vee\ (xy)^{2022} = 1 \ \vee\ [x,y]^5 = 1\right).$$

Каждая такая формула определяет класс групп, состоящий из групп, в которых выполняется данная формула. Например, формула $(\forall x)\,(x^2 = 1 \ \vee\ x^3 = 1)$ выполняется в симметрической группе порядка шесть, но не выполняется в абелевой группе порядка шесть.

Следующая теорему можно рассматривать как двойственную к теореме Макаренко–Хухро.

Теорема о конечных подгруппах. *Если в группе G есть конечная нормальная подгруппа, в факторгруппе по которой выполняется некоторая универсальная позитивная замкнутая формула, то в группе G есть характеристическая конечная подгруппа с тем же свойством.*

Мы будем доказывать более общее утверждение, похожее на теорему о больших подгруппах. Рассмотрим свойство $\mathcal{D}(N)$ нормальной подгруппы N группы G, имеющее вид

$$(\forall x)(\forall y)\ldots\left(\mathcal{S}(x,y,\ldots) \Longrightarrow \bigvee_{i=1}^{t}(G/N, xN, yN, \ldots) \in \mathcal{F}_i\right), \qquad (*)$$

где $\mathcal{S}$ — любое $(\operatorname{Aut} G)$-инвариантное свойство наборов элементов группы G и $\mathcal{F}_i$ — произвольные формации групп с отмеченными элементами.

Формация групп с отмеченными элементами — это класс наборов $(H, h_1, h_2, \ldots)$, где H — группа и $h_i \in H$, замкнутый относительно гомоморфных образов и подпрямых произведений (которые определяются естественным образом). Примером такой формации может служить класс аменабельных групп с двумя выделенными элементами, коммутатор которых лежит в центре.

Свойства вида $(*)$ нормальных подгрупп мы называем *t-дизъюнктными*.

Теорема о маленьких подгруппах. *Если радикальный класс, порождённый нормальной подгруппой N группы G, состоит из групп с условием минимальности для нормальных подгрупп, то G содержит характеристические подгруппы $H_1, H_2, \ldots$ такие, что*

1) *H_t лежат в радикальном классе $\mathcal{R}$, порождённом группой N; более того, подгруппы H_t содержатся в решётке подгрупп группы G, порождённой автоморфными образами подгруппы N;*
2) *факторгруппа G/H_t удовлетворяет всем t-дизъюнктным свойствам, которым удовлетворяет факторгруппа G/N;*
3) *если при этом* codim *— обобщённая коразмерность* (которую логичнее называть размерностью в данном случае), *определённая на решётке двойственной к решётке подгрупп, лежащих в $\mathcal{R}$, то* $\operatorname{codim} H_t \leqslant f^{t-1}(\operatorname{codim} N)$, *где $f^k(x)$ означает k-ю итерацию функции $f(x) = x(x+1)$.*

Доказательство. Каждое t-дизъюнктное свойство $\mathcal{D}(N)$ можно переписать в виде $\mathcal{D}(N) = \mathcal{P}_{\mathcal{D}}(N, \ldots, N)$, где $\mathcal{P}_{\mathcal{D}}(N_1, \ldots, N_t)$ представляет собой следующее свойство набора нормальных подгрупп:

$$(\forall x)(\forall y)\ldots\left(\mathcal{S}(x, y, \ldots) \Longrightarrow \bigvee_{i=1}^{t} (G/N_i, xN_i, yN_i, \ldots) \in \mathcal{F}_i\right).$$

Теперь всё вытекает из основной теоремы. В качестве решётки $\mathcal{L}$ следует взять решётку подгрупп группы G, порождённую образами подгруппы N при всевозможных автоморфизмах группы G, но порядок на этой решётке надо рассматривать противоположный естественному:

$$A \leqslant B, \quad \text{если} \quad A \supseteq B.$$

Эта решётка нётерова, так как состоит из нормальных подгрупп в G, артиновых по нормальным подгруппам. В качестве Φ надо взять группу автоморфизмов группы G, а в качестве свойства $\mathcal{P}$ следует взять конъюнкцию всех свойств $\mathcal{P}_{\mathcal{D}}$, где $\mathcal{D}$ пробегает все t-дизъюнктные свойства, выполненные в N.

Монотонность свойства $\mathcal{P}$ очевидным образом вытекает из замкнутости формаций относительно факторгрупп, а полилинейность — из замкнутости формаций относительно подпрямых произведений. Проверим, например, линейность по первому аргументу. Надо доказать, что свойство $\mathcal{P}_{\mathcal{D}}(N_1' \cap N_1'', N_2, \ldots)$ выполнено, если известно, что выполнены свойства $\mathcal{P}_{\mathcal{D}}(N_1', N_2, \ldots)$ и $\mathcal{P}_{\mathcal{D}}(N_1'', N_2, \ldots)$. Это значит, что нам известно, что для любого набора элементов $g, h, \ldots \in G$, обладающего свойством $\mathcal{S}$,

– либо $(G/N_i,\ gN_i,\ hN_i, \ldots) \in \mathcal{F}_i$ при некотором $i \geqslant 2$,
– либо формация $\mathcal{F}_1$ содержит две группы с отмеченными элементами:
$(G/N_1',\ gN_1',\ hN_1', \ldots)$ и $(G/N_1'',\ gN_1'',\ hN_1'', \ldots)$,
а значит, и их подпрямое произведение $(G/(N_1' \cap N_1''),\ g(N_1' \cap N_1''),\ h(N_1' \cap N_1''), \ldots)$.

Это означает, что свойство $\mathcal{P}_{\mathcal{D}}(N_1' \cap N_1'', N_2, \ldots)$ выполнено и теорема доказана.

Теорема о конечных подгруппах получается из теоремы о маленьких подгруппах, если в качестве каждой из формаций $\mathcal{F}_i$ взять класс всех групп, выделенные элементы которых удовлетворяют какой-то системе уравнений (зависящей от i). Мы ограничимся одним конкретным примером.

Теорема о спектре. *Для любой конечной нормальной подгруппы N группы G ограниченного периода найдётся характеристическая конечная подгруппа H такая, что спектр* (то есть множество всех порядков элементов) *факторгруппы G/H содержится в спектре факторгруппы G/N.*

Доказательство. Достаточно применить теорему о конечных подгруппах к формуле $\forall x \bigvee_{i=1}^{t} (x^{n_i} = 1)$, где $\{n_1, \ldots, n_t\}$ — это спектр группы G/N.

Порядок характеристической подгруппы H явно оценивается через порядок подгруппы N и мощность спектра факторгруппы G/N (поскольку логарифм порядка подгруппы — это естественный пример коразмерности на решётке конечных нормальных подгрупп). Слово «конечная» (оба раза) в теореме о спектре можно заменить на «артинова» или, например, «черниковская» и т.п. Слово «спектр» (оба раза) можно заменить, например, на «спектр коммутанта», для этого надо в качестве свойства $\mathcal{S}(x)$ написать, что x лежит в коммутанте.

В заключение мы приведём пример, показывающий, что теорему о конечных подгруппах нельзя распространить на произвольные позитивные (неуниверсальные) формулы первого порядка.

Пример. В группе $G = \langle a\rangle_2 \times B$, где B — абелева делимая группа, содержащая бесконечное число элементов порядка два (например, $B = (\mathbb{Z}_{2^\infty})^\infty$), есть очевидная конечная нормальная подгруппа $N = \langle a\rangle_2$, в факторгруппе по которой любой элемент является квадратом (то есть выполнена формула $\forall x\ \exists y\ x = y^2$), но нет характеристической конечной подгруппы с таким свойством. Действительно, понятно, что такая характеристическая подгруппа H не может содержаться в B. Возьмём элемент $(a, b) \in H$ и рассмотрим его образы при автоморфизмах, которые элементы из B оставляют на месте, а a переводят в (a, x), где x — произвольный элемент порядка два из B. Эти образы (a, bx) образуют бесконечное подмножество в H.

4. Решётки идеалов и подпространств

Под *алгеброй* в этом параграфе понимается необязательно ассоциативная алгебра над произвольным полем. *Характеристическим* подпространством в алгебре мы называем подпространство, инвариантное относительно всех автоморфизмов этой алгебры.

Теорема о больших подпространствах. *Пусть N — подпространство алгебры G и*
- *либо N имеет конечную коразмерность,*
- *либо N левый идеал и фактормодуль G/N нётеров,*
- *либо N двусторонний идеал и факторалгебра G/N удовлетворяет условию максимальности для двусторонних идеалов.*

Тогда G содержит характеристические подпространства $H_1, H_2, \ldots$ такие, что

1) *подпространства H_t содержатся в решётке подпространств алгебры G, порождённой образами N при всевозможных автоморфизмах алгебры G; в частности, подпространства H_t являются идеалами (односторонними или двусторонними), если N является идеалом, и факторалгебра (фактормодуль) G/H_t лежат в формации $\mathcal{F}$, порождённой алгеброй (модулем) G/N;*
2) *для любого полилинейного элемента $w(x_1, \ldots, x_n)$ свободной (неассоциативной) алгебры, имеющего степень $n \leqslant t$, множество $w(H_t, \ldots, H_t)$ содержится в линейной оболочке конечного числа образов множества $w(N, \ldots, N)$ при автоморфизмах алгебры G;*
3) *Если при этом codim — это либо обычная коразмерность (подпространства в G), либо обобщённая коразмерность, определённая на решётке идеалов, факторалгебры (фактормодули) по которым лежат в $\mathcal{F}$, то $\mathsf{codim}\, H_t \leqslant f^{t-1}(\mathsf{codim}\, N)$, где $f^k(x)$ означает k-ю итерацию функции $f(x) = x(x+1)$.*

Доказательство почти дословно повторяет доказательство теоремы о больших подгруппах; надо только сделать очевидные замены (слово «группа» заменять на «алгебра» и так далее).

Подобным же образом можно сформулировать и доказать аналог теоремы о маленьких подгруппах. Мы ограничимся формулировкой аналога теоремы о конечных подгруппах.

Теорема о конечномерных идеалах. *Если в алгебре G есть конечномерный двусторонний идеал, в факторалгебре по которому выполняется некоторая фиксированная универсальная позитивная замкнутая формула первого порядка (в языке алгебр над данным полем), то в алгебре G есть характеристический конечномерный двусторонний идеал с тем же свойством.*

5. Решётка конечных подграфов

Слово *граф* в этом параграфе можно понимать в любом разумном смысле: все утверждения верны и для ориентированных графов, и для неориентированных; кратные рёбра и петли можно допускать, а можно и запрещать; можно считать вершины и/или рёбра раскрашенными. В теореме о запрещённых подграфах и в теореме о локальной вложимости можно даже понимать слово «граф» как гиперграф. Все эти вариации не влияют на доказательства, если конечно автоморфизмы графа понимать в соответствующем смысле.

Теорема о запрещённых подграфах. *Пусть $\{\Gamma_1, \ldots, \Gamma_l\}$ — конечный набор конечных графов, называемых запрещёнными и рассматриваемых с точностью до изоморфизма, и G — некоторый граф. Если из графа G можно удалить конечное множество ребер $\overline{N}$ таким образом, что $G \setminus \overline{N}$ не содержит запрещённых подграфов, то из G можно удалить конечное инвариантное относительно всех автоморфизмов графа G множество ребер $\overline{H}$ с тем же свойством: $G \setminus \overline{H}$ не содержит запрещённых подграфов. При этом $|\overline{H}| \leqslant f^{t-1}(|\overline{N}|)$, где $f^k(x)$ означает k-ю итерацию функции $f(x) = x(x+1)$, а t — максимальное (по i) число рёбер в Γ_i. Кроме того, если $\overline{H} \neq \varnothing$, то $\overline{H} \cap \overline{N} \neq \varnothing$.*

Доказательство. Достаточно применить основную теорему к решётке, элементы которой суть коконечные подмножества множества рёбер графа G. Ясно, что эта решётка нётерова, а функция

$$\mathsf{codim}\,(X) \stackrel{\text{опр}}{=} \text{число рёбер графа } G \setminus X$$

удовлетворяет всем условиям из определения коразмерности. В качестве полугруппы Φ следует взять группу автоморфизмов графа G, а в качестве $\mathcal{P}(N_1, \ldots, N_t)$ можно взять следующее свойство:
в G не существует запрещённого подграфа, у которого первое ребро лежит в N_1, второе ребро лежит в N_2,...

Мы имеем в виду, что мы каким-то образом занумеровали рёбра каждого запрещённого графа. Ясно, что свойство $\mathcal{P}$ монотонно:

$$\mathcal{P}(N_1, \ldots, N_t) \Longrightarrow \mathcal{P}(N_1', \ldots, N_t'), \quad \text{если } N_i' \subseteq N_i.$$

Полилинейность тоже очевидна:

$$\big(\mathcal{P}(N_1', N_2 \ldots, N_t) \wedge \mathcal{P}(N_1'', N_2 \ldots, N_t)\big) \Longrightarrow \mathcal{P}(N_1' \cup N_1'', N_2 \ldots, N_t).$$

Осталось применить основную теорему и заметить, что свойство $\mathcal{P}(N, \ldots, N)$ означает в точности отсутствие запрещённых подграфов в N.

То что $\overline{H} = G \setminus H$ пересекается с $\overline{N} = G \setminus N$ следует из того, что согласно основной теореме H содержится в подрешётке, порождённой всеми образами множества N при автоморфизмах графа G. В частности, $H \supseteq \bigcap\limits_{\varphi \in \operatorname{Aut} G} \varphi(N)$, то есть $\overline{H} \subseteq \bigcup\limits_{\varphi \in \operatorname{Aut} G} \varphi(\overline{N})$. Следовательно, если $\overline{H} \neq \varnothing$, то $\overline{H} \cap \varphi(\overline{N}) \neq \varnothing$ для некоторого $\varphi \in \operatorname{Aut} G$. В силу инвариантности $\overline{H}$ это означает, что $\overline{H} \cap \overline{N} \neq \varnothing$, что и требовалось. Теорема доказана.

Эту теорему можно значительно усилить, если не заботиться об оценке числа выбрасываемых рёбер. Скажем, что граф X *локально вложим* в граф Y, если любой конечный подграф графа X изоморфен некоторому подграфу графа Y.

Теорема о локальной вложимости. *Для любого графа G и любого конечного множества $\overline{N}$ его рёбер найдётся конечное множество рёбер $\overline{H}$, инвариантное относительно всех автоморфизмов графа G и такое, что граф $H = G \setminus \overline{H}$ локально вложим в граф $N = G \setminus \overline{N}$.*

Доказательство. Пусть $\Gamma_1, \Gamma_2, \ldots$ — все конечные графы, не вложимые в N. Нам надо показать, что
> *все подграфы графа G, изоморфные Γ_i, можно разрушить путём удаления из G конечного ($\operatorname{Aut} G$)-инвариантного множества рёбер $\overline{H}$; если известно, что эти подграфы можно разрушить путём удаления из G какого-то конечного множества рёбер $\overline{M}$.*

Доказывать это утверждение мы будем индукцией по $|\overline{M}|$. Вначале $\overline{M} = \overline{N}$.

По теореме о запрещённых подграфах для каждого натурального n существует конечное множество рёбер $\overline{H}_n$ графа G такое, что
1) $\overline{H}_n$ инвариантно относительно всех автоморфизмов графа G;
2) графы $\Gamma_1, \ldots, \Gamma_n$ не вложимы в $H_n = G \setminus \overline{H}_n$;
3) $\overline{H}_n \cap \overline{M} \neq \varnothing$, если $\overline{H}_n \neq \varnothing$.

Если все множества $\overline{H}_n$ пусты, то доказывать нечего. Если же найдётся непустое множество $\overline{H}_k$, то рассмотрим граф $G' = H_k = G \setminus \overline{H}_k$. В этом графе есть конечное множество рёбер $\overline{M}' = \overline{M} \setminus (\overline{M} \cap \overline{H}_k)$ такое, что в $G' \setminus \overline{M}'$ не вложим ни один из Γ_i.

При этом $|M'| < |M|$ по свойству 3) множества $\overline{H}_k$. Значит, по предположению индукции в G' содержится конечное инвариантное множество рёбер $\overline{H}'$ такое, что ни один из графов Γ_i не вложим в $G' \setminus \overline{H}' = G \setminus (\overline{H}_k \cup \overline{H}')$, что и требовалось, так как $\overline{H}_k \cup \overline{H}'$ — это инвариантное множество. Действительно, $\overline{H}_k$ по определению инвариантно относительно всех автоморфизмов графа G, а $\overline{H}'$ инвариантно относительно $\operatorname{Aut} G'$, и, тем более, относительно $\operatorname{Aut} G$, поскольку G' — это ($\operatorname{Aut} G$)-инвариантный подграф в G. Теорема доказана.

Пример. Рассмотрим неориентированный граф G, гомеоморфный прямой, и граф N, получающийся из G удалением одного ребра. Ясно, что из G нельзя удалить конечное инвариантное относительно всех автоморфизмов множество рёбер так, чтобы получившийся граф H был вложим в N (поскольку группа автоморфизмов графа G действует транзитивно на рёбрах). Этот пример показывает, что в теореме нельзя заменить локальную вложимость на вложимость. (А для локальной вложимости H в N в этом простейшем случае достаточно взять $H = G$, то есть удалить пустое множество рёбер.)

Теорема о планарности. *Если граф можно сделать планарным путём удаления конечного числа рёбер, то его можно сделать планарным путём удаления конечного множества рёбер, инвариантного относительно всех автоморфизмов графа.*

Доказательство. По теореме Куратовского–Эрдёша–Вагнера [Wag67] граф планарен тогда и только тогда, когда
- число его рёбер не превосходит континуума;
- число его вершин степени большей чем два счётно (или конечно);
- он не содержит подграфов гомеоморфных полному графу на пяти вершинах K_5 или полному двудольному графу с тремя вершинами в каждой доле $K_{3,3}$ (рис. 1), то есть подграфов, которые получаются из K_5 или $K_{3,3}$ при помощи разбиения ребер.

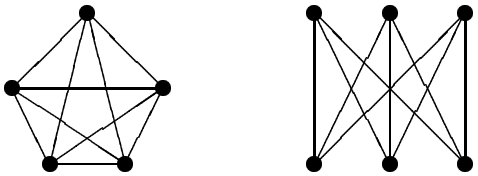


Рис. 1

На первые два свойства удаление или добавление конечного числа рёбер не влияет, а третье свойство переносится с графа на все графы, локально вложимые в него. Поэтому утверждение немедленно вытекает из теоремы о локальной вложимости.

Следующее утверждение показывает, что в теореме о планарности не может быть никакой оценки мощности инвариантного выбрасываемого множества рёбер.

Утверждение. *Для каждого натурального n существует конечный граф G_n, который становится планарным после удаления пяти рёбер, но который нельзя сделать планарным путём удаления инвариантного множества, состоящего менее чем из n рёбер.*

Доказательство. Возьмём граф K_5 и разобьём каждое ребро одного из циклов длины пять в этом графе на n частей. Склеим теперь n копий получившегося графа вдоль этого цикла длины $5n$ с поворотом (рис. 2).

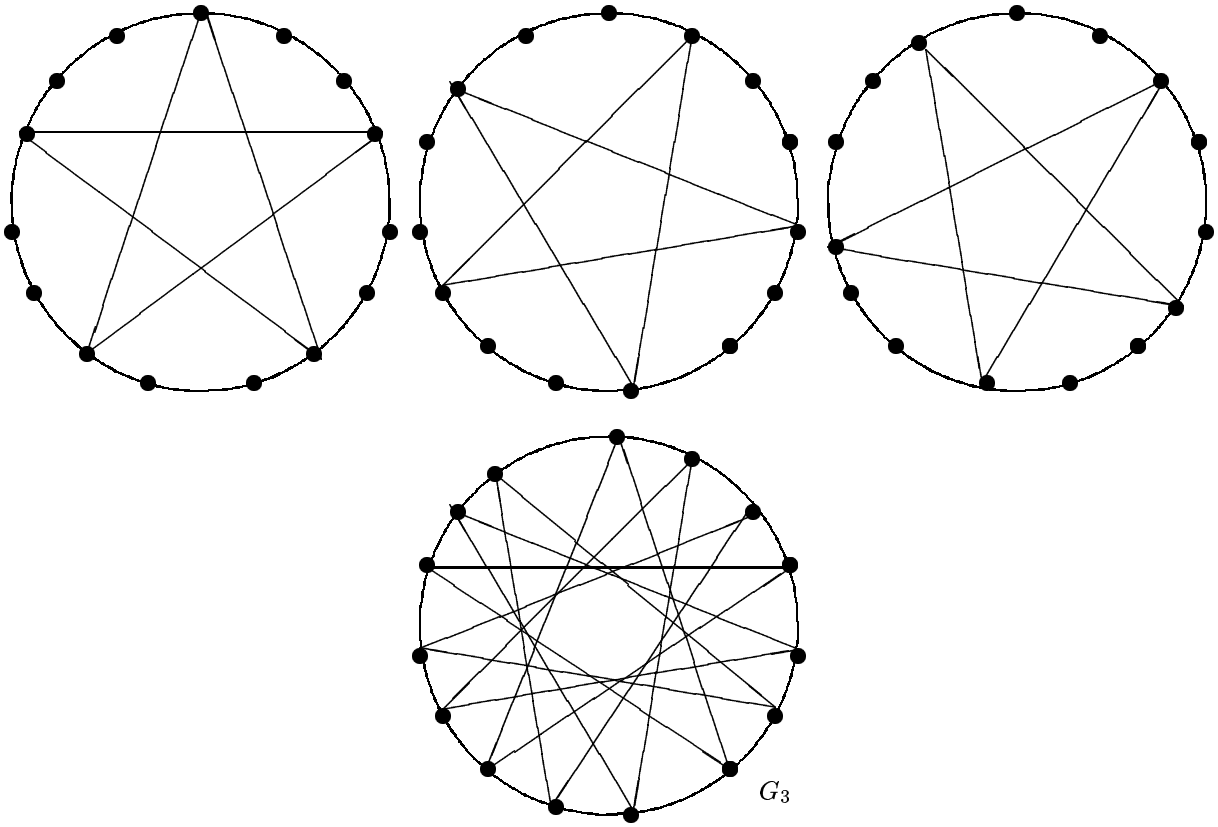


Рис. 2

Полученный граф G_n становится планарным после удаления пяти рёбер — каждого n-го ребра на упомянутом цикле длины $5n$ (рис. 3). Однако удаление маленького инвариантного множества рёбер не сделает этот граф планарным, поскольку среди автоморфизмов графа G_n есть поворот на одно ребро вдоль нашего цикла длины $5n$ и, следовательно, орбита каждого ребра состоит не менее чем из n элементов. Поэтому инвариантное множество рёбер, содержащее меньше чем n элементов, обязано быть пустым. Осталось заметить, что сам граф G_n непланарен, так как он содержит подграф, гомеоморфный K_5.

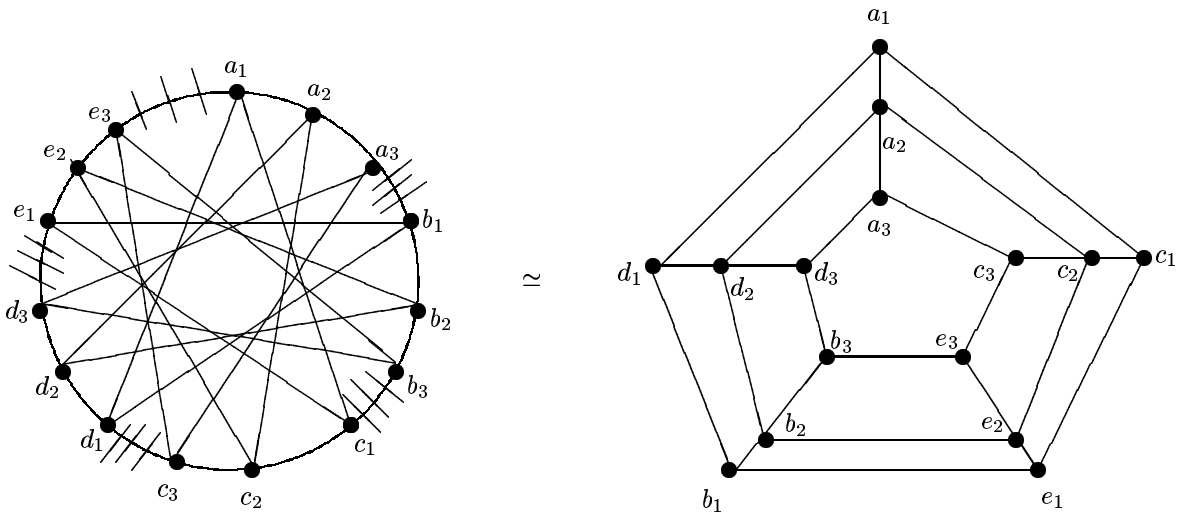


Рис. 3

В заключение отметим, что по крайней мере для счётных графов, верен аналог теоремы о планарности, в котором планарность заменяется на вложимость в любую фиксированную поверхность. Чтобы в этом убедиться достаточно вспомнить теорему Эрдёша, которая говорит, что счётный граф вкладывается в поверхность S тогда и только тогда, когда каждый его конечный подграф вкладывается в S.

6. Элементарная математика

Задача 1. *В трёхмерном евклидовом пространстве имеется некоторое множество точек X. Известно, что из этого множества можно удалить конечное множество точек так, что никакие 2022 из оставшихся точек не будут лежать на одной сфере. Покажите, что это конечное множество можно выбрать инвариантным относительно всех симметрий(=изометрий) множества X.*

Решение. Достаточно применить основную теорему, взяв в качестве решётки $\mathcal{L}$ решётку коконечных подмножеств множества X (она очевидно нётерова), в качестве Φ — группу симметрий множества X, а в качестве $\mathcal{P}$ следующий 2022-линейный Φ-инвариантный монотонный предикат:

$$\mathcal{P}(N_1,\dots,N_{2022}) = (\text{никакие точки } x_1\in N_1,\dots,x_{2022}\in N_{2022} \text{ не лежат на одной сфере}).$$

В данном случае имеется и естественная коразмерность: $\operatorname{codim}(X\setminus K)\overset{\text{опр}}{=}|K|$, что позволяет оценить мощность симметричного выкидываемого множества через мощность исходного множества K.

Задача 2. *Для полёта на Марс отобрали 10^{100} прекрасных во всех отношениях претендентов. Единственная проблема состоит в том, что они не очень уважительно друг к другу относятся. Но организаторы заметили, что если десять человек исключить, то получится работоспособный коллектив в том смысле, что среди любых пяти найдётся по крайней мере один, которого большинство (из этой пятёрки) уважает. Покажите, что из претендентов можно сформировать непустой работоспособный коллектив, исключив несколько человек справедливо, то есть так, что множество исключённых будет инвариантно относительно любой перестановки претендентов, сохраняющей отношение «уважает». (Разумеется, бинарное отношение «уважает» необязано быть ни транзитивным, ни симметричным, ни даже рефлексивным.)*

Решение. Достаточно применить основную теорему, взяв в качестве решётки $\mathcal{L}$ решётку всех подмножеств множества претендентов X (она очевидно нётерова), в качестве Φ — группу перестановок множества X, сохраняющих отношение «уважает», а в качестве $\mathcal{P}$ следующий пенталинейный Φ-инвариантный монотонный предикат:

$$\mathcal{P}(N_1,\dots,N_5) = (\text{любые претенденты } x_1\in N_1,\dots,x_5\in N_5 \text{ образуют работоспособную пятёрку}).$$

Имеется естественная коразмерность: $\operatorname{codim}(X\setminus K)\overset{\text{опр}}{=}|K|$, что позволяет оценить число справедливо исключаемых претендентов:

$$\operatorname{codim} H \leqslant f^{t-1}(\operatorname{codim} N) = f^{5-1}(10) < \frac{11}{10}\cdot\left(\frac{11}{10}\cdot\left(\frac{11}{10}\cdot\left(\frac{11}{10}\cdot 10^2\right)^2\right)^2\right)^2 = \left(\frac{11}{10}\right)^{15}\cdot 10^{16} = 11^{15}\cdot 10 \ll 10^{100},$$

то есть оставшийся работоспособный коллектив будет непустым.

ГЛАВА 14.
ИНВАРИАНТНЫЕ СИСТЕМЫ ПРЕДСТАВИТЕЛЕЙ, ИЛИ ЦЕНА СИММЕТРИИ

0. Введение

Рассмотрим следующую «прикладную» задачу.

> Мы отбираем участников для экспедиции на Марс и хотим соблюсти (например) следующее *требование совместимости*: среди любых пяти участников найдутся двое, каждый из которых уважает хотя бы троих из этой пятёрки. Наши досье показывают, что можно десять кандидатов исключить так, чтобы это требование совместимости оказалось выполненным. Проблема в том, что мы хотим быть *справедливыми* и *непредвзятыми*, то есть мы хотим, чтобы множество исключённых было инвариантно относительно всех перестановок множества кандидатов, сохраняющих отношение «уважает». Сколько кандидатов мы должны исключить (в худшем случае)?

Какова цена справедливости? Вопрос сложнее, чем может показаться на первый взгляд. Например, если мы попытаемся исключить всех кандидатов, которые получаются из исходных десяти «плохих» кандидатов под действием всех допустимых перестановок, то такой подход может привести к исключению вообще всех кандидатов, даже если их было бесконечно много. На самом деле, оптимальное множество справедливо исключаемых кандидатов всегда конечно и не обязано ни содержать исходное множество «плохих» кандидатов, ни содержаться в нём.

В алгебре известно много теорем такого сорта, например,

- если группа G содержит абелеву подгруппу конечного индекса, то G содержит *характеристическую* (то есть инвариантную относительно всех автоморфизмов) абелеву подгруппу конечного индекса [KaM82];
- если группа G содержит нильпотентную подгруппу конечного индекса, то G содержит характеристическую нильпотентную (той же ступени) подгруппу конечного индекса [BrNa04];
- если группа G содержит разрешимую подгруппу конечного индекса, то G содержит характеристическую разрешимую (той же ступени) подгруппу конечного индекса [KhM07a];
- если группа G содержит центрально метабелеву подгруппу конечного индекса, то G содержит характеристическую центрально метабелеву подгруппу конечного индекса [KhM07a];
- если группа G содержит паранильпотентную подгруппу конечного индекса, то G содержит характеристическую паранильпотентную подгруппу конечного индекса [dGT19b];
- если группа G содержит подгруппу конечного индекса с конечным коммутантом, то G содержит характеристическую подгруппу конечного индекса с конечным коммутантом [KMi15];
- если группа G конечного периода содержит конечную нормальную подгруппу N, то G содержит характеристическую конечную подгруппу H такую, что *спектр* (то есть множество порядков всех элементов) факторгруппы G/H содержится в спектре факторгруппы G/N [KMi15];
- если алгебра G (ассоциативная или лиевская) над полем содержит разрешимый идеал конечной коразмерности, то G содержит инвариантный относительно всех автоморфизмов разрешимый (той же ступени) идеал конечной коразмерности [KhM08].

Список можно долго продолжать, смотрите, например, [Вд00], [KhM07b], [KhM08], [KM09], [KhKMM09], [MSh12], [KMi15], [Fr18], [dGT18a], [dGT18b], [dGT19a], [dGT19b] и литературу там цитируемую. Утверждения такого сорта называют иногда ([KMi15], [Fr18]) *теоремами типа Макаренко–Хухро* в честь одного из таких результатов [KhM07a] (смотрите также [KMe09]), включающего в себя в качестве частных случаев первые четыре из упомянутых фактов.

Первый из этих фактов (об абелевых подгруппах) несложный в том смысле, что существует короткое и элементарное доказательство. Однако совсем уж наивные подходы здесь не работают. Как из данной абелевой подгруппы $N \subset G$ конечного индекса сделать характеристическую?

- Можно взять пересечение всех автоморфных образов подгруппы N. Полученная подгруппа $\bigcap\limits_{\varphi\in\operatorname{Aut} G} \varphi(N)$ будет характеристической и абелевой (поскольку содержится в N), но, к сожалению, не обязана иметь конечный индекс.
- Можно, наоборот, взять группу, порождённую всеми автоморфными образами подгруппы N. Полученная подгруппа $\left\langle \bigcup\limits_{\varphi\in\operatorname{Aut} G} \varphi(N) \right\rangle$ будет характеристической и иметь конечный индекс (поскольку содержит N), но, к сожалению, не обязана быть абелевой.

На самом деле, искомая характеристическая абелева подгруппа конечного индекса не обязана ни содержать исходную подгруппу, ни содержаться в ней. Похожая ситуация и с другими теоремами типа Макаренко–Хухро (и с задачей о марсианской экспедиции тоже).

Почти все упомянутые теоремы типа Макаренко–Хухро и сама теорема Макаренко–Хухро являются частными случаями некоторого очень общего факта, установленного в [KMi15], который мы будем здесь называть *теоремой о полилинейных свойствах*. Эта общая теорема даёт и некоторую общую оценку на соответствующий параметр (индекс характеристической подгруппы, коразмерность инвариантного относительно автоморфизмов идеала...). Такая общая оценка, однако, бывает далека от оптимальной в конкретных случаях. Например, для абелевых подгрупп теорема о полилинейных свойствах даёт следующее количественное уточнение:

> *если группа G содержит абелеву подгруппу конечного индекса n, то G содержит характеристическую абелеву подгруппу индекса, не превосходящего* $(n!)^{\log_2(n!)+1}$.

Тогда как на самом деле оптимальная оценка здесь n^2, смотрите [PSz02].*) В принципе, теорема о полилинейных свойствах применима и к чисто комбинаторным вопросам (смотрите [KMi15]); например, для задачи о марсианской экспедиции эта теорема даёт такой практически бесполезный ответ:

> *заведомо достаточно исключить* $22229709804712410 = f(f(f(f(10))))$ *кандидатов, где* $f(x) = x(x+1)$.

Эта оценка (сильно превышающая население Земли) тоже очень завышена. Следующая теорема говорит, что правильный ответ — 50 (и это уже неулучшаемо).

Основная теорема. *Пусть группа G действует на множестве U и $\mathcal{F}$ — G-инвариантное семейство конечных подмножеств множества U, мощности которых ограничены в совокупности, а $X \subseteq U$ — конечная система представителей для этого семейства (то есть $X \cap F \neq \varnothing$ для любого $F \in \mathcal{F}$). Тогда найдётся G-инвариантная система представителей Y такая, что* $|Y| \leqslant |X| \cdot \max\limits_{F\in\mathcal{F}} |F|$.

Слово *семейство* здесь понимается как *неупорядоченное семейство*, то есть $\mathcal{F}$ — это просто некоторое множество подмножеств множества U. *Инвариантность* семейства $\mathcal{F}$ следует понимать естественным образом: $g\mathcal{F} = \mathcal{F}$ для всех $g \in G$ или, более подробно, $gF \stackrel{\text{опр}}{=} \{gf \mid f \in F\} \in \mathcal{F}$ для всех $g \in G$ и $F \in \mathcal{F}$.

Доказательство основной теоремы вполне элементарно (смотрите последний параграф), но использует одну нетривиальную теорему Б. Неймана о покрытиях группы смежными классами [Neu54]. Из основной теоремы немедленно вытекает следующий факт о графах.

Следствие 1. *Пусть Γ — граф и K — конечный граф. Тогда*

1) *если в графе Γ можно выбрать конечное множество вершин X так, чтобы каждый подграф графа Γ, изоморфный графу K, имел хоть одну вершину из X, то в графе Γ можно выбрать конечное множество вершин Y, инвариантное относительно всех автоморфизмов графа Γ, так, чтобы опять каждый подграф графа Γ, изоморфный графу K, имел хоть одну вершину из Y, причём $|Y| \leqslant |X| \cdot$ (число вершин графа K);*
2) *если в графе Γ можно выбрать конечное множество рёбер X так, чтобы каждый подграф графа Γ, изоморфный графу K, имел хоть одно ребро из X, то в графе Γ можно выбрать конечное множество рёбер Y, инвариантное относительно всех автоморфизмов графа Γ, так, чтобы опять каждый подграф графа Γ, изоморфный графу K, имел хоть одно ребро из Y, причём $|Y| \leqslant |X| \cdot$ (число рёбер графа K).*

Слово *граф* здесь (и во всей главе) можно понимать в любом разумном смысле:
- граф может быть ориентированным, неориентированным или смешанным,
- кратные рёбра и/или петли могут допускаться или не допускаться.

Разумеется, слово «изоморфизм» (и «автоморфизм») следует понимать соответствующим образом, то есть изоморфизм должен сохранять ориентацию рёбер, если речь идёт об ориентированных графах.

---

*) Смотрите также работу [dGT18a], авторы которой передоказали оценку n^2, по-видимому не зная о работе [PSz02]. На самом деле для конечных групп G эта оценка была известна и раньше ([ChD89], смотрите также [Is08], теорема 1.41). А качественный факт: *если группа содержит абелеву подгруппу конечного индекса, то она содержит и характеристическую абелеву подгруппу конечного индекса*, был известен ещё раньше, смотрите [KaM82].

Замечание. Аналог следствия 1 справедлив в ситуации, когда имеется несколько (конечное число) «запрещённых» конечных графов $K_1, \dots, K_n$ (вместо одного графа K). В этом случае оценка получается такой: $|Y| \leqslant |X| \cdot \max\limits_i$(число вершин [рёбер] графа K_i).

Доказательство выглядит так же, как доказательство следствия 1: достаточно сослаться на основную теорему, взяв в качестве множества U множество всех вершин [рёбер] графа Γ, в качестве группы G группу автоморфизмов графа Γ, а в качестве семейства $\mathcal{F}$ следующее семейство

$$\mathcal{F} = \Big\{ \{\text{вершины [рёбра] графа } S\} \;\Big|\; S \text{ — подграф в } \Gamma, \text{ изоморфный одному из } K_i \Big\}.$$

В параграфах 1 и 2 мы обсуждаем точность оценок из следствия 1; ситуация здесь такая:
- оценки из обоих утверждений следствия 1 неулучшаемы в том смысле, что в этих утверждениях нельзя заменить функцию $|X| \cdot$ (число вершин [рёбер] графа K) ни на какую меньшую функцию от $|X|$ и числа вершин [рёбер] графа K;
- если же граф K фиксировать и задаться вопросом о неулучшаемости оценок при данном K, то задача становится интереснее:
  - графы K, для которых оценка из утверждения о вершинах неулучшаема, имеют простое описание (но всё равно остаются интересные открытые вопросы); смотрите следующий параграф;
  - что касается утверждения о рёбрах, то здесь вопросов явно больше, чем ответов; смотрите параграф 2.

В заключение отметим, что не в любой ситуации можно доказать теорему типа Макаренко–Хухро. Например,

> *из наличия в группе подгруппы конечного индекса с тождеством* $x^{2019} = 1$ *не вытекает существование характеристической подгруппы конечного индекса с таким тождеством* [KhKMM09].

В [KMi15] можно найти забавный пример пограничной ситуации: с одной стороны,

> *если граф сделать планарным путём удаления конечного числа рёбер, то такое конечное множество рёбер всегда можно выбрать инвариантным относительно всех автоморфизмов графа*;

а с другой стороны, *никакой оценки здесь быть не может* (то есть существует такое n, что для любого m существует граф, который можно сделать планарным путём удаления n рёбер, но нельзя сделать планарным путём удаления множества, состоящего из менее чем m рёбер и инвариантного относительно всех автоморфизмов графа).

Обозначения и соглашения, которые мы используем, в целом стандартны. Отметим только, что слово *граф* везде, где не оговорено противное, можно понимать в любом из шести смыслов, указанных выше. Индекс подгруппы H группы G обозначается $|G{:}H|$. Буква $\mathbb{Z}$ обозначает множество целых чисел. Символ $|X|$ обозначает мощность множества X.

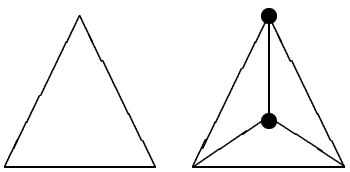
1. Вершинная представительность

Назовём *вершинной представительностью* $\Upsilon_{\mathrm{v}}(K, \Gamma)$ графа K в графе Γ минимальное число n такое, что в графе Γ найдётся множество вершин X мощности n, удовлетворяющее следующему условию:

$$\text{каждый подграф графа } \Gamma, \text{ изоморфный } K, \text{ содержит вершину из } X. \qquad (*)$$

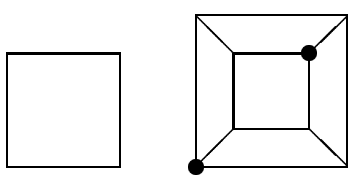
Определим *симметричную вершинную представительность* $\Upsilon_{\mathrm{v}}^{\mathrm{sym}}(K, \Gamma)$ графа K в графе Γ как минимальное число n такое, что в графе Γ найдётся инвариантное относительно всех автоморфизмов множество вершин X мощности n с условием $(*)$.

Например, для граней тетраэдра и куба имеем:



K $\qquad$ Γ

$\Upsilon_{\mathrm{v}}(K, \Gamma) = 2, \quad \Upsilon_{\mathrm{v}}^{\mathrm{sym}}(K, \Gamma) = 4$



K $\qquad$ Γ

$\Upsilon_{\mathrm{v}}(K, \Gamma) = 2, \quad \Upsilon_{\mathrm{v}}^{\mathrm{sym}}(K, \Gamma) = 8$

Ясно, что $\Upsilon_{\mathrm{v}}(K,\Gamma) \leqslant \Upsilon_{\mathrm{v}}^{\mathrm{sym}}(K,\Gamma)$. Согласно следствию 1, $\Upsilon_{\mathrm{v}}^{\mathrm{sym}}(K,\Gamma) \leqslant \Upsilon_{\mathrm{v}}(K,\Gamma) \cdot$ (число вершин графа K). Следующее утверждение показывает, что для связных графов K эта оценка не может быть улучшена.

Граф K будем называть *дорогим в смысле симметричной вершинной представительности* или просто *дорогим* (или *вершинно дорогим*), если

$$\forall m \in \mathbb{Z} \text{ найдётся граф } \Gamma_m \text{ такой, что } \Upsilon_{\mathrm{v}}^{\mathrm{sym}}(K,\Gamma_m) = \Upsilon_{\mathrm{v}}(K,\Gamma_m) \cdot (\text{число вершин графа } K) \geqslant m. \qquad (**)$$

Таким образом, граф K дорогой, если оценка из следствия 1 (по сути) не может быть улучшена для графа K. Назовём дорогой граф K (*вершинно*) *дорогим в классе графов* $\mathcal{K}$, если графы Γ_m в $(**)$ могут выбраны из класса $\mathcal{K}$.

Теорема 1. *Конечный граф K является дорогим тогда и только тогда, когда он связный. Более того, связный граф K без висячих рёбер является дорогим в классе связных графов.*

Доказательство. Заметим, что

всякий граф K вкладывается в вершинно транзитивный граф $\widetilde{K}$ с таким же числом вершин.

Действительно, если под словом *граф* понимается неориентированный граф без кратных рёбер и без петель, то в качестве графа $\widetilde{K}$ достаточно взять полный граф с таким же (как у K) числом вершин; в остальных случаях этот факт тоже остаётся верным (оставляем это читателям в качестве упражнения, смотрите графы K и $\widetilde{K}$ на рисунке 1).

Если граф K связный, то возьмём в качестве графа Γ_m несвязное объединение m копий графа $\widetilde{K}$. Покажем, что достигается нужная оценка. Действительно, чтобы избавиться от подграфов, изоморфных запрещенному, достаточно (и необходимо) удалить в каждой копии графа $\widetilde{K}$ одну вершину. Таким образом, $\Upsilon_{\mathrm{v}}(K,\Gamma_m) = m$. Но граф Γ_m является вершинно транзитивным, поэтому $\Upsilon_{\mathrm{v}}^{\mathrm{sym}}(K,\Gamma_m) = mk$ где k — это число вершин графа K.

Чтобы доказать утверждение «Более того» достаточно добавить к построенному графу Γ_m цепи длины N, соединяющие каждую вершину i-й копии графа $\widetilde{K}$ с соответствующей вершиной $(i+1)$-й копии графа $\widetilde{K}$, где $i \in \{1,\ldots,m-1\}$, а число N (одинаковое для всех добавленных цепей) больше, чем число вершин графа K, смотрите рисунок 1.

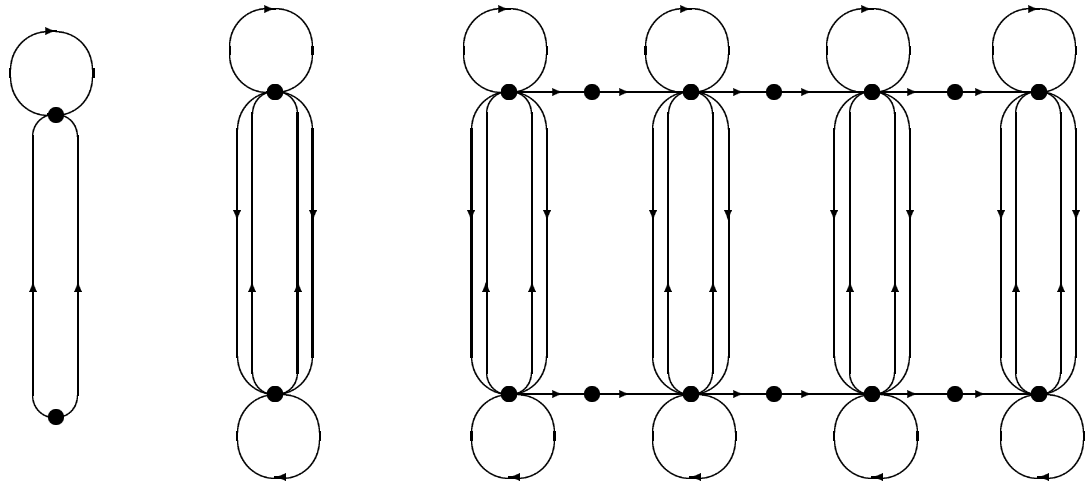


Рис. 1

Опять $\Upsilon_{\mathrm{v}}(K,\Gamma_m) = m$, поскольку чтобы избавиться от запрещённых подграфов K достаточно удалить по одной вершине из каждой копии графа $\widetilde{K}$ (здесь мы пользуемся тем, что граф K не имеет висячих рёбер, и число N выбрано достаточно большим). А $\Upsilon_{\mathrm{v}}^{\mathrm{sym}}(K,\Gamma_m) = mk$, поскольку на вершинах каждой (фиксированной) копии графа $\widetilde{K}$ группа автоморфизмов графа Γ_m действует транзитивно.

Осталось показать, что никакой несвязный граф K не является дорогим. Мы докажем чуть больше:

$$\Upsilon_{\mathrm{v}}^{\mathrm{sym}}(K,\Gamma) \leqslant k_1(\Upsilon_{\mathrm{v}}(K,\Gamma) + k_2),$$

если $K = K_1 \sqcup K_2$ где k_1 — число вершин в K_1, а $k_2 \leqslant k_1$ — число вершин в K_2.

Отметим $\Upsilon_{\mathrm{v}}(K, \Gamma)$ вершин в графе Γ так, чтобы каждый подграф, изоморфный графу $K = K_1 \sqcup K_2$, имел отмеченную вершину. Если теперь в Γ найдётся подграф $\widehat{K}_2 \simeq K_2$, без отмеченных вершин, то он обязан пересекать каждый подграф в Γ, изоморфный графу K_1 и не имеющий отмеченных вершин. Следовательно, отметив ещё все вершины графа $\widehat{K}_2$, мы добьёмся того, что всякий подграф графа Γ, изоморфный K_1, имеет отмеченную вершину. Таким образом, $\Upsilon_{\mathrm{v}}(K_1, \Gamma) \leqslant \Upsilon_{\mathrm{v}}(K, \Gamma) + k_2$ и

$$\Upsilon_{\mathrm{v}}^{\mathrm{sym}}(K, \Gamma) \leqslant \Upsilon_{\mathrm{v}}^{\mathrm{sym}}(K_1, \Gamma) \leqslant k_1 \Upsilon_{\mathrm{v}}(K_1, \Gamma) \leqslant k_1(\Upsilon_{\mathrm{v}}(K, \Gamma) + k_2) \text{ (где предпоследнее неравенство есть следствие 1),}$$

что и требовалось. Если же в Γ нет подграфов, изоморфных K_2, без отмеченных вершин, то мы получаем неравенство $\Upsilon_{\mathrm{v}}(K_2, \Gamma) \leqslant \Upsilon_{\mathrm{v}}(K, \Gamma)$ (которое на самом деле является равенством) и

$$\Upsilon_{\mathrm{v}}^{\mathrm{sym}}(K, \Gamma) \leqslant \Upsilon_{\mathrm{v}}^{\mathrm{sym}}(K_2, \Gamma) \leqslant k_2 \Upsilon_{\mathrm{v}}(K_2, \Gamma) \leqslant k_2 \Upsilon_{\mathrm{v}}(K, \Gamma) \leqslant k_1 \Upsilon_{\mathrm{v}}(K, \Gamma) < k_1(\Upsilon_{\mathrm{v}}(K, \Gamma) + k_2),$$

что и требовалось. Это завершает доказательство.

Вопрос 1. *Верно ли, что любой конечный связный граф является дорогим в классе связных графов?*

Согласно теореме 1, все конечные связные графы без вершин степени один являются дорогими в классе связных графов. Цепи также являются дорогими в классе связных графов; в качестве Γ_m можно взять в этом случае многоугольники.

Четырёхвершинные графы *треугольник с хвостиком* и *лапа*, изображённые на рисунке 2 слева, также являются дорогими в классе связных графов; соответствующие графы Γ_m устроены так, как показано на рисунке 2 справа. Точнее говоря, на этом рисунке изображён бесконечный вершинно транзитивный граф, в котором отмечена каждая четвёртая вершина таким образом, чтобы каждый треугольник с хвостиком и каждая лапа имели отмеченную вершину; поскольку полученный узор на плоскости является дважды периодическим, мы можем из него получить сколь угодно большие конечные узоры на торе с тем же свойством (то есть вершинно транзитивные графы, в которых четверть вершин отмечены таким образом, что каждый треугольник с хвостиком и каждая лапа имеет отмеченную вершину).

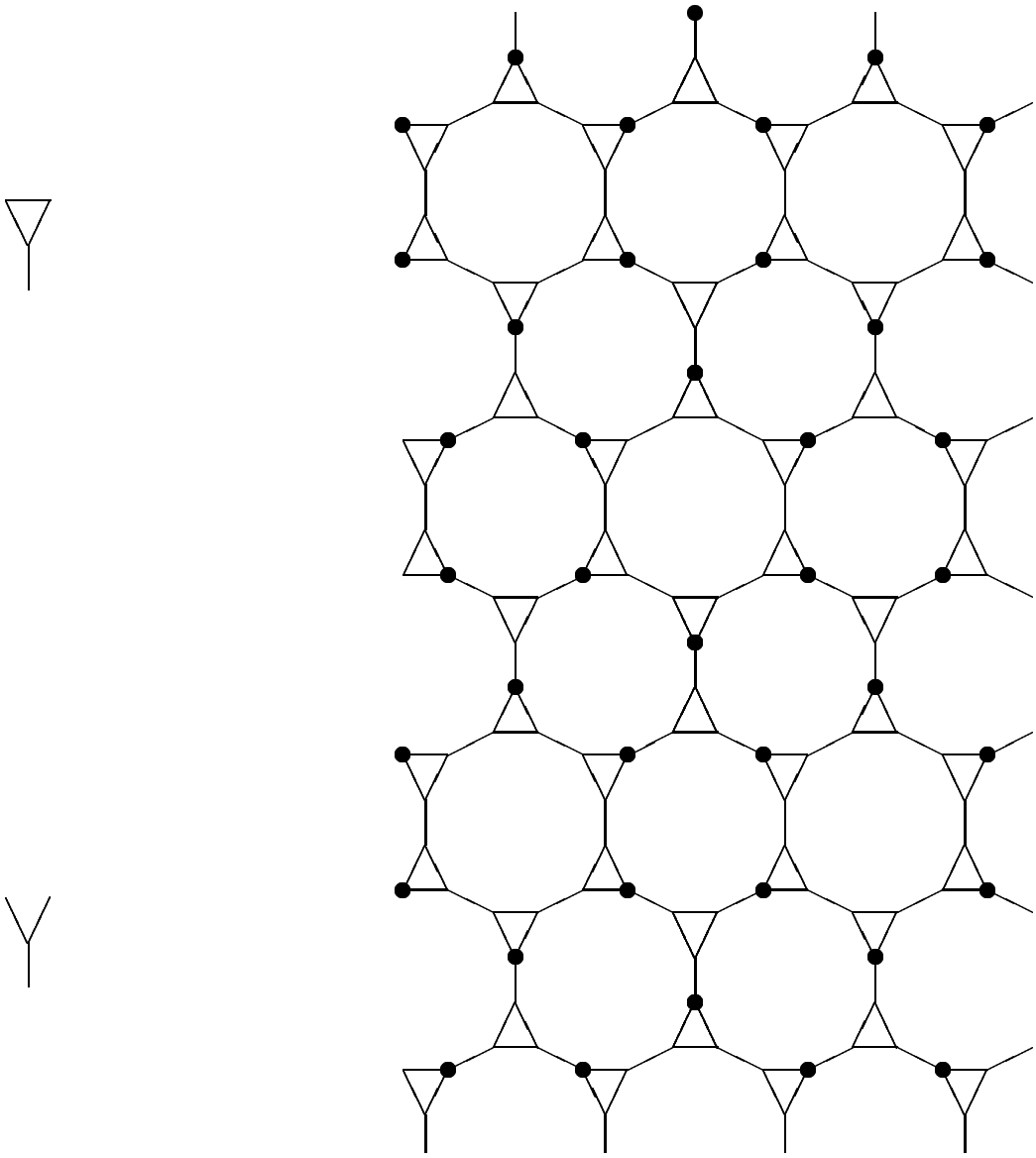


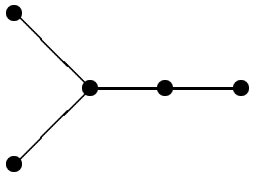
Рис. 2

Таким образом,

все связные графы, имеющие не более четырёх вершин, являются дорогими в классе связных графов.

(Строго говоря, рисунок 2 доказывает это утверждение лишь в случае, когда слово *граф* понимается как неориентированный граф без петель и кратных рёбер; но очевидная модификация этого рисунка позволяет доказать утверждение и в других случаях.)

Тем не менее мы полагаем, что ответ на вопрос 1 отрицательный, причём контрпримером вероятно служит пятивершинный граф D_5, изображённый на рисунке 3 (то есть гипотетически $\Upsilon_{\mathrm{v}}^{\mathrm{sym}}(D_5,\Gamma) < 5\Upsilon_{\mathrm{v}}(D_5,\Gamma)$ для любого связного графа Γ с достаточно большой представительностью $\Upsilon_{\mathrm{v}}(D_5,\Gamma)$).



D_5

Рис. 3

Частичным подтверждением этой гипотезы является следующий факт.

Теорема 2. *Граф D_5 не является дорогим в классе вершинно транзитивных связных графов. Более точно, если $\Gamma \supseteq D_5$ — вершинно транзитивный неориентированный связный граф, имеющий больше пяти вершин, и представительность $\Upsilon_{\mathrm{v}}(D_5, \Gamma)$ конечна, то $\Upsilon_{\mathrm{v}}^{\mathrm{sym}}(D_5, \Gamma) < 5\Upsilon_{\mathrm{v}}(D_5, \Gamma)$.*

(Граф Γ называется *вершинно транзитивным*, если группа его автоморфизмов действует транзитивно на множестве вершин, то есть для любых двух вершин u и v существует автоморфизм φ графа такой, что $\varphi(u) = v$.)

Доказательство. Сперва заметим, что мы можем (и будем) считать, что в графе Γ нет петель и кратных рёбер. Действительно, если убрать в графе Γ все петли, а все кратные рёбра заменить на одно ребро, то условия теоремы останутся выполненными, а из утверждение теоремы для полученного графа будет следовать и утверждение для исходного графа.

Заметим ещё, что граф Γ обязан быть конечным, поскольку по следствию 1 конечность величины $\Upsilon_{\mathrm{v}}(D_5, \Gamma)$ влечёт конечность величины $\Upsilon_{\mathrm{v}}^{\mathrm{sym}}(D_5, \Gamma)$, которая равна числу вершин графа в силу транзитивности.

Пусть степень каждой вершины графа Γ равна $k \geqslant 3$ (если $k < 3$, то доказывать нечего). Пусть в Γ выделено некоторое конечное множество вершин X (где $|X| = \Upsilon_{\mathrm{v}}(D_5, \Gamma)$) таким образом, что каждый подграф, изоморфный графу D_5, содержит выделенную вершину. Это означает, что граф Γ', полученный из Γ удалением всех выделенных вершин и инцидентных им рёбер не содержит подграфов, изоморфных D_5. Классифицировать такие графы несложно.

Лемма 1. *Конечный связный неориентированный граф без петель и кратных рёбер, не содержащий подграфов, изоморфных D_5 является*

- *либо l-угольником (циклом) (с $l \geqslant 3$);*
- *либо цепью (с $l \geqslant 0$ рёбрами);*
- *либо звездой $K_{1,l}$ (с $l \geqslant 3$ рёбрами);*
- *либо связным четырёхвершинным графом.*

На рисунке 4 изображены представители трёх бесконечных серий, а на рисунке 5 — три оставшихся четырёхвершинных графа (на чёрные вершины и инцидентные им рёбра пока не надо обращать внимание).

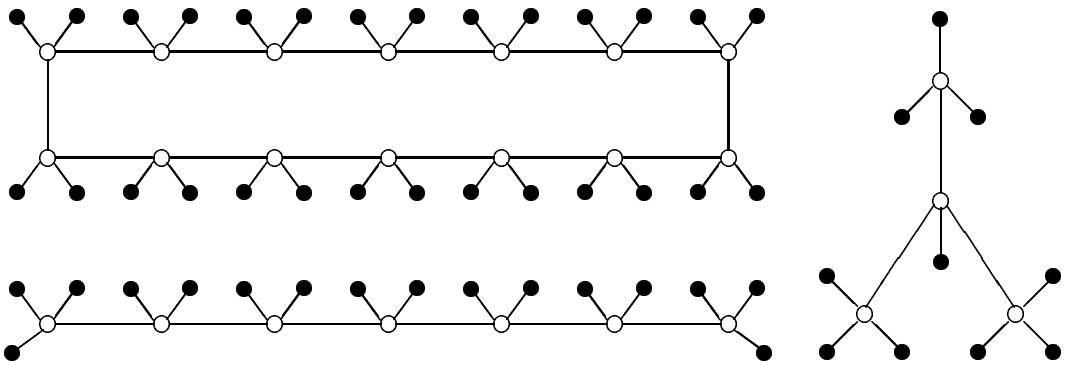


Рис. 4

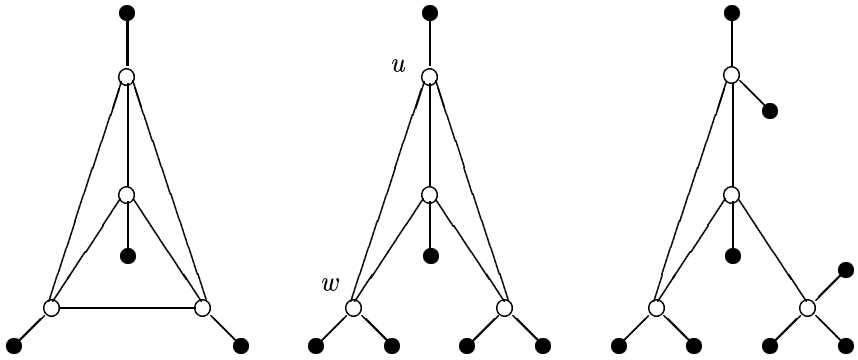


Рис. 5

Доказательство. Если связный конечный граф не содержит вершин степени больше двух, то это либо многоугольник, либо цепь. Если же имеется вершина v степени три или больше, то соседние с ней вершины могут быть соединены рёбрами только между собой (и ещё с v), поскольку иначе мы получаем D_5 в качестве подграфа. Таким образом, все вершины нашего графа, кроме v, являются соседними с v (в силу связности).

Если никакие из соседних с v вершины не соединены ребром, то наш граф — звезда.

Если же некоторое ребро соединяет две соседние с v вершины u и w, то, кроме v, u и w может только одна ещё вершина быть, поскольку иначе мы опять получим подграф D_5. Таким образом, наш граф не более четырёх вершин содержит, что завершает доказательство леммы.

Продолжим доказательство теоремы. Посчитаем теперь число p рёбер, соединяющих выделенные вершины с невыделенными. С одной стороны, $p \leqslant k|X|$ (поскольку каждая выделенная вершина имеет степень k), причём равенство достигается лишь в случае, когда никакие две выделенные вершины не соединены ребром. А с другой стороны, $p \geqslant (k-3)|Z|$, где Z — множество невыделенных вершин, поскольку на каждую невыделенную вершину, находящуюся в компоненте графа Γ' приходится в среднем не менее $(k-3)$-х рёбер, соединяющих эту компоненту с выделенными вершинами (смотрите рисунки 4 и 5, на которых выделенные вершины чёрные и $k=4$), причём равенство достигается только на компоненте, представляющей собой полный граф на четырёх вершинах.

Отсюда получаем: $k|X| \geqslant p \geqslant (k-3)|Z|$, то есть $|X| \geqslant (1-\frac{3}{k})|Z|$. Это означает, что

1) либо $|X| > \frac{1}{4}|Z|$,
2) либо $k=3$,
3) либо $k=4$ и $|X| = \frac{1}{4}|Z|$, причём, как было отмечено, это равенство возможно лишь в случае, когда все компоненты графа Γ' представляют собой полные графы на четырёх вершинах, и никакие две выделенные вершины графа Γ не соединены ребром.

Рассмотрим эти случаи.

1) В этом случае мы имеем $\Upsilon_{\mathrm{v}}^{\mathrm{sym}}(D_5,\Gamma) \leqslant$ (число вершин графа Γ) $= |X|+|Z| < |X|+4|X| = 5|X| = 5\Upsilon_{\mathrm{v}}(D_5,\Gamma)$, что и требовалось.
2) В этом случае никакая компонента графа Γ' не может быть полным графом на четырёх вершинах, изображённом на рисунке 5 слева (поскольку степень каждой вершины графа Γ равна трём). Никакая компонента графа Γ' не может быть также *ромбом*, изображённом на рисунке 5 в центре; действительно, окрестность вершины u (в графе Γ) в этом случае представляет собой цепочку, а окрестность вершины w — несвязный граф; в вершинно транзитивном графе это невозможно. Под *окрестностью* вершины v мы понимаем граф, состоящий из вершин соседних с v и всех рёбер их соединяющих. Обратите внимание, что в рассматриваемом случае степень каждой вершины три (а не четыре, как на рисунке 5).

   Таким образом, рассуждение, приведшее нас к неравенству $k|X| \geqslant (k-3)|Z|$, модифицируется следующим образом. На каждую невыделенную вершину, находящуюся в компоненте графа Γ' приходится в среднем не менее одного ребра, соединяющего эту компоненту с выделенными вершинами (равенство достигается на компонентах, изображённых на рисунке 5 справа, и на циклах, рисунок 4). Отсюда получаем $3|X| \geqslant |Z|$ и приходим к случаю 1).
3) Окрестность отмеченной вершины должна быть по условию несвязным объединением нескольких клик (состоящих из неотмеченных вершин). В силу транзитивности окрестность неотмеченной вершины должна иметь такой же вид. Поскольку окрестность неотмеченной вершины обязана содержать треугольник, состоящий из неотмеченных вершин, мы приходим к выводу, что
   а) либо окрестность каждой вершины представляет собой полный граф на четырёх вершинах,

б) либо не существует треугольника, содержащего отмеченную вершину.

В первом случае понятно, что граф Γ представляет собой полный граф с пятью вершинами и всё доказано. А случай б) очевидно невозможен в вершинно транзитивном графе, содержащем клики порядка четыре.

2. Рёберная представительность

Назовём *рёберной представительностью* $\Upsilon_{\mathrm{e}}(K,\Gamma)$ графа K в графе Γ минимальное число n такое, что в графе Γ найдётся множество рёбер X мощности n, удовлетворяющее следующему условию:

$$\textit{каждый подграф графа } \Gamma, \textit{ изоморфный } K, \textit{ содержит ребро из } X. \qquad (***)$$

Аналогичным образом определим *симметричную рёберную представительность* $\Upsilon_{\mathrm{e}}^{\mathrm{sym}}(K,\Gamma)$ графа K в графе Γ как минимальное число n такое, что в графе Γ найдётся инвариантное в классе всех автоморфизмов множество рёбер X мощности n с условием $(***)$.

Ясно, что $\Upsilon_{\mathrm{e}}(K,\Gamma) \leqslant \Upsilon_{\mathrm{e}}^{\mathrm{sym}}(K,\Gamma)$. Следствие 1 говорит, что $\Upsilon_{\mathrm{e}}^{\mathrm{sym}}(K,\Gamma) \leqslant \Upsilon_{\mathrm{e}}(K,\Gamma)\cdot(\text{число рёбер графа } K)$.

Граф K будем называть *дорогим в смысле симметричной рёберной представительности* или просто *рёберно дорогим*, если

$$\forall m \in \mathbb{Z} \text{ найдётся граф } \Gamma_m \text{ такой, что } \Upsilon_{\mathrm{e}}^{\mathrm{sym}}(K,\Gamma_m) = \Upsilon_{\mathrm{e}}(K,\Gamma_m)\cdot(\text{число рёбер графа } K) \geqslant m. \qquad (****)$$

Таким образом, граф K рёберно дорогой, если оценка из следствия 1 (о рёбрах) не может быть улучшена для графа K. Назовём рёберно дорогой граф K *рёберно дорогим в классе графов* $\mathcal{K}$, если графы Γ_m в $(****)$ могут выбраны из класса $\mathcal{K}$.

Утверждение 1. *Всякий конечный рёберно транзитивный связный граф K является рёберно дорогим в классе связных графов.*

Доказательство. Если граф K не имеет висячих рёбер (то есть не имеет вершин степени один), то мы можем поступить так же, как в вершинном случае. Возьмём в качестве графа Γ_m несвязное объединение m копий графа K. Покажем, что достигается нужная оценка. Действительно, чтобы избавиться от подграфов, изоморфных запрещенному, достаточно (и необходимо) удалить в каждой копии графа K одно ребро. Таким образом, $\Upsilon_{\mathrm{e}}(K,\Gamma_m) = m$. Но граф Γ_m является рёберно транзитивный, поэтому $\Upsilon_{\mathrm{e}}^{\mathrm{sym}}(K,\Gamma_m) = mk$, где k — это число рёбер графа K. Это доказывает, что граф K рёберно дорогой (в классе всех графов).

Чтобы сделать граф Γ_m связным достаточно добавить к построенному графу Γ_m цепи длины N, соединяющие каждую вершину i-й копии графа K с соответствующей вершиной $(i+1)$-й копии графа K, где $i \in \{1,\dots,m-1\}$, а число N (одинаковое для всех добавленных цепей) больше, чем число вершин графа K.

Опять $\Upsilon_{\mathrm{e}}(K,\Gamma_m) = m$, поскольку чтобы избавиться от подграфов, изоморфных K, достаточно удалить по одному ребру из каждой копии графа K (здесь мы пользуемся тем, что граф K не имеет висячих рёбер, и число N выбрано достаточно большим). А $\Upsilon_{\mathrm{e}}^{\mathrm{sym}}(K,\Gamma_m) = mk$, поскольку на рёбрах каждой (фиксированной) копии графа K группа автоморфизмов графа Γ_m действует транзитивно.

Если же рёберно транзитивный связный граф K имеет висячие рёбра, то все рёбра висячие и граф K представляет собой звезду $K_{1,l}$.

Если при этом рёбра ориентированы, то они ориентированы «одинаково», то есть звезда $K = K_{1,l}$ имеет один источник и l стоков или наоборот. Считая, что имеется один источник, возьмём в качестве графа Γ_m полный двудольный граф $K_{m,l}$, в котором все рёбра направлены из первой доли (состоящей из m вершин) во вторую долю (состоящую из l вершин). Ясно, что $\Upsilon_{\mathrm{e}}(K,\Gamma_m) = m$ и $\Upsilon_{\mathrm{e}}^{\mathrm{sym}}(K,\Gamma_m) = ml$ (поскольку граф Γ_m рёберно транзитивный).

Осталось рассмотреть случай, когда граф $K = K_{1,l}$ представляет собой неориентированную звезду.

Если l равно единице или двойке, то в качестве графа Γ_m можно взять цикл длины $2m$.

Если $l = 3$, то в качестве графа Γ_m можно взять «пчелиные соты». На рисунке 6 слева изображён бесконечный граф, в котором каждое третье ребро помечено (вертикальные рёбра на рисунке 6), и все подграфы, изоморфные лапе $K = K_{1,3}$, содержат помеченные рёбра.

Чтобы сделать этот граф конечным, нужно воспользоваться тем, что «пчелиные соты» — это дважды периодический узор на плоскости, поэтому из него можно сделать сколь угодно большой конечный граф на торе с теми же свойствами (то есть рёберно транзитивный граф, в котором каждое третье ребро помечено, и все лапы содержат помеченные рёбра).

Если же $l > 3$, то мы можем поступить так, как показано на рисунке 6 справа: Γ_m состоит из m копий звезды K, соединённых рёбрами; $\Upsilon_{\mathrm{e}}(K,\Gamma_m) = m$ и $\Upsilon_{\mathrm{e}}^{\mathrm{sym}}(K,\Gamma_m) = ml$. Это завершает доказательство.

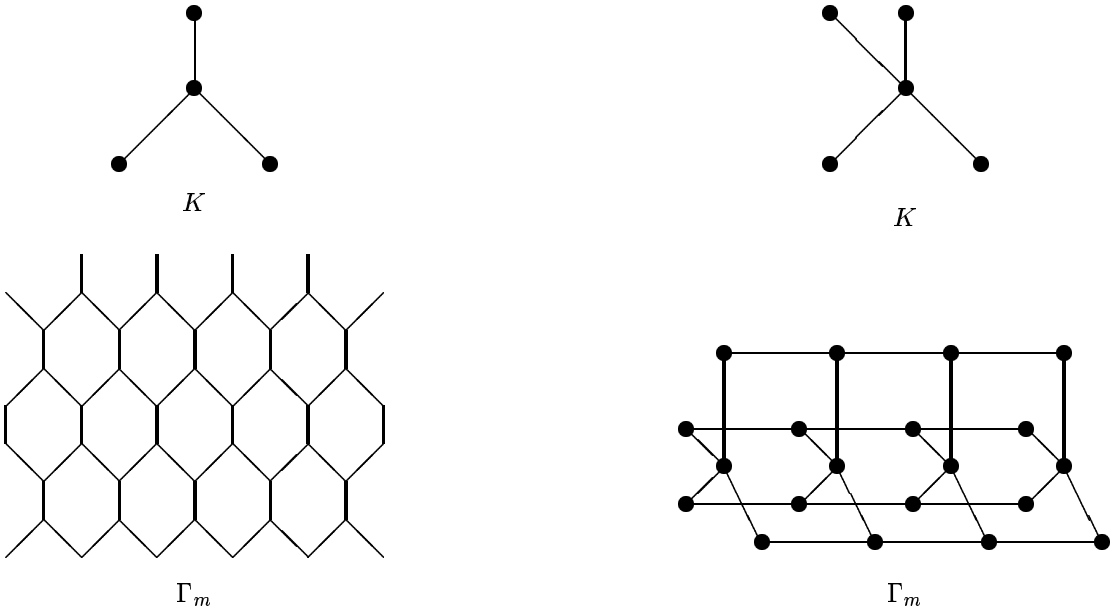


Рис. 6

Полный аналог теоремы 1 тут неверен:

существуют несвязные рёберно дорогие графы и даже несвязные графы, рёберно дорогие в классе связных графов.

Действительно, если взять в качестве K несвязное объединение двух рёбер, а в качестве Γ — полный двудольный граф $K_{2,m}$, то $\Upsilon_{\mathrm{e}}(K,\Gamma) = m$ (поскольку, чтобы избавиться от подграфов, изоморфных K, достаточно удалить все рёбра, инцидентные одной из вершин степени m, смотрите рисунок 7), а $\Upsilon_{\mathrm{e}}^{\mathrm{sym}}(K,\Gamma) = 2m$ (поскольку граф рёберно транзитивный).

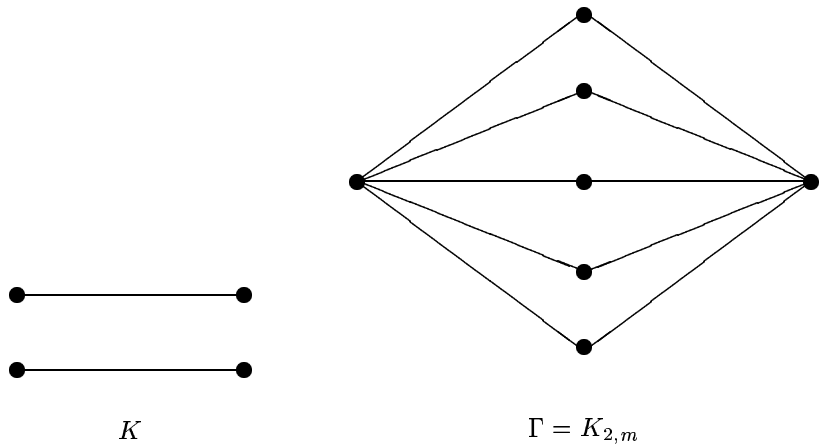


Рис. 7

Существуют ли вообще не рёберно дорогие графы? Да, но у нас есть только тривиальные примеры: если слово «граф» понимать как ориентированный граф, в котором петли разрешены, а кратные рёбра запрещены, то граф K, изображённый на рисунке 8 не будет рёберно дорогим по очевидным причинам: общее ребро двух подграфов такого вида в произвольном графе Γ обязано быть петлёй, поэтому $\Upsilon_{\mathrm{e}}^{\mathrm{sym}}(K,\Gamma) = \Upsilon_{\mathrm{e}}(K,\Gamma)$ (поскольку, если мы хотим избавиться от подграфов такого вида, нам выгоднее удалять только петли).

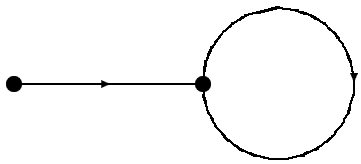


Рис. 8

Мы не знаем, например, ответ на следующий вопрос.

Вопрос 2. *Пусть слово граф понимается, как неориентированный граф без петель и кратных рёбер. Существует ли конечный не рёберно дорогой граф? Может ли такой граф быть связным? Существует ли конечный граф, не рёберно дорогой в классе связных графов? Может ли такой граф быть связным?*

Если слово *граф* понимать, как ориентированный граф без петель и кратных рёбер, ответов на аналогичные вопросы мы тоже не знаем. В общем, по поводу рёберной дороговизны у нас больше вопросов, чем ответов.

3. Доказательство основной теоремы

Положим $m = \max\limits_{F\in\mathcal{F}} |F|$ и рассмотрим следующее множество $Y = \left\{ y \in U \;\middle|\; |Gy \cap X| \geqslant \frac{1}{m}|Gy| \right\}$ (в частности, Y не содержит точек с бесконечной орбитой). Ясно, что это множество G-инвариантно. Ясно также, что $|Y| \leqslant m|X|$ (поскольку для каждой орбиты Gu имеет место неравенство $|Gu \cap Y| \leqslant m|Gu \cap X|$).

Осталось показать, что Y является системой представителей для $\mathcal{F}$. Возьмём какое-то множество $F \in \mathcal{F}$. Каждое множество gF (где $g \in G$) принадлежит $\mathcal{F}$ в силу инвариантности семейства $\mathcal{F}$ и, следовательно, пересекается с X. Значит,

$$G = \bigcup_{f\in F} \{g \in G \mid gf \in X\}.$$

Каждое из множеств $\{g \in G \mid gf \in X\}$ является либо пустым, либо объединением конечного числа левых смежных классов группы G по стабилизатору $\mathrm{St}(f)$ точки f:

$$\{g \in G \mid gf \in X\} = \bigcup_{x\in X} \{g \in G \mid gf = x\} = \bigcup_{x\in X\cap Gf} g_x \cdot \mathrm{St}(f), \quad \text{где } g_x \in G \text{ фиксированы так, что } g_x f = x.$$

Таким образом, мы получили разложение группы G в конечное объединение левых смежных классов по некоторым подгруппам. Воспользуемся теперь теоремой Б. Неймана [Neu54] (утверждение 4.5):

если группа G покрывается конечным числом смежных классов по некоторым (необязательно разным) подгруппам: $G = g_1G_1 \cup \ldots \cup g_sG_s$, то $\sum \dfrac{1}{|G : G_i|} \geqslant 1$ (*где обратный к бесконечному кардиналу считается нулём*).

Следовательно, (учитывая то, что индекс стабилизатора равен длине орбиты) мы получаем

$$1 \leqslant \sum_{f\in F} \frac{1}{|G : \mathrm{St}(f)|} \cdot |Gf \cap X| = \sum_{f\in F} \frac{|Gf \cap X|}{|Gf|}.$$

Поскольку число слагаемых в этой сумме равно $|F| \leqslant m$, по крайней мере одно из слагаемых должно быть не меньше чем $1/m$, то есть $|Gf \cap X|/|Gf| \geqslant 1/m$, что означает $f \in Y$ (по определению множества Y) и завершает доказательство.

ГЛАВА 15.
КОММУТАТОРНЫЕ, СТЕПЕННЫЕ И ПАРАБОЛИЧЕСКИЕ РАЗЛОЖЕНИЯ В СВОБОДНЫХ ПРОИЗВЕДЕНИЯХ ГРУПП

0. Введение

Хорошо известно, что в свободной группе неединичные коммутаторы не являются истинными степенями [Sch59]. Этот факт обобщался в разных направлениях, например, известно, что такой же результат остаётся верным в группах без кручения, удовлетворяющих (достаточно сильному) условию малого сокращения [FK12]. В свободных произведениях групп ситуация сложнее, но тоже полностью изучена [CCE91].

М. Каллер [Cull81] заметил, что в свободной группе $F(a,b)$ куб коммутатора $[a,b]$ является произведением двух коммутаторов: $[a,b]^3 = [a^{-1}ba, a^{-2}bab^{-1}][bab^{-1}, b^2]$. Более того, в работе [Cull81] показано, что $[a,b]^n$ раскладывается в произведение k коммутаторов, если $n \leqslant 2k-1$.

В работе [CCE91] доказано, что неединичное произведение двух коммутаторов в свободной группе не может быть более чем третьей степенью, то есть в свободной группе равенство $[x_1,y_1][x_2,y_2] = z^n$, где $n \geqslant 4$, влечёт, что $z = 1$.

Авторы [CCE91] высказали гипотезу, что оценка Каллера $n \leqslant 2k-1$ даёт для свободной группы максимальную степень n, которая может равняться неединичному произведению g коммутаторов. Другими словами, гипотеза Комерфорда, Комерфорда и Эдмундса говорит, что в свободной группе равенство $[x_1,y_1]\dots[x_k,y_k] = z^n$, где $n \geqslant 2k$, влечёт, что $z = 1$.

Эта гипотеза оказалась действительно верной. Теорема 3.3 работы [DuH91] говорит, что в свободном произведении $A * B$ локально индикабельных групп равенство $[x_1,y_1]\dots[x_k,y_k] = z^n$, где $n \geqslant 2k$, влечёт, что z сопряжён с элементом одного из свободных сомножителей A или B.

Наша основная теорема показывает, в частности, что то же самое верно для свободных произведений произвольных групп без кручения*) (и даже для групп с кручением, если это кручение не слишком маленькое). Заметим, что в случае маленького кручения аналогичное утверждение перестаёт быть верным: в бесконечной диэдральной группе $\langle c\rangle_2 * \langle d\rangle_2$ все степени коммутатора $[c,d]$ являются коммутаторами.

Основная теорема. *Если в свободном произведении нескольких групп без кручения*

$$c_1 \dots c_k d_1 \dots d_l = e_1^{n_1} \dots e_m^{n_m},$$

где c_i *являются коммутаторами,*
d_i *сопряжены элементам свободных сомножителей,*
e_i *сопряжены друг другу и не сопряжены элементам свободных сомножителей и*
n_i *— натуральные числа,*

$$\text{то} \quad \sum (n_i - 1) \leqslant 2k + l - 2.$$

(*То же самое верно для свободных произведений групп с кручением, в которых порядки всех неединичных элементов больше чем* $\sum n_i$.)

Следствие. *Если в свободном произведении нескольких групп без кручения*

$$c_1 \dots c_k d_1 \dots d_l = e_1 \dots e_m,$$

где c_i *являются коммутаторами,*
d_i *сопряжены элементам свободных сомножителей, а*
e_i *сопряжены друг другу и не сопряжены элементам свободных сомножителей,*
то в последовательности $(e_1, \dots, e_m)$ *никакой элемент не встречается больше чем* $2k + l - 1$ *раз.*

---

*) Этот факт был также доказан независимо, одновременно и другими методами в [Ch18].

Например, в свободной группе
- неединичный коммутатор часто можно разложить в произведение ста сопряжённых между собой элементов, но в таком случае все эти сто элементов должны быть разными;
- неединичное произведение двух коммутаторов часто можно разложить в произведение ста сопряжённых между собой элементов, но в таком случае среди этих ста элементов элементов, ни один не может встретиться больше трёх раз;
- ...

Другой пример: в свободном произведении $A * B$ групп без кручения
- неединичный элемент из A нельзя разложить в произведение нескольких сопряжённых между собой элементов, не лежащих в A;
- произведение ab неединичных элементов из A и из B часто можно разложить в произведение ста сопряжённых между собой элементов, но в таком случае все эти сто элементов обязаны быть разными;
- ...

Мы будем называть *двойным родом* элемента w свободного произведения групп $A*B$ минимальное s такое, что w представляется в виде произведения k коммутаторов и l элементов подгрупп, сопряжённых сомножителям A и B, причём $2k + l = s$. Например,
- двойной род ноль имеет только единичный элемент группы $A * B$;
- двойной род один имеют только неединичные элементы подгрупп, сопряжённых сомножителям;
- двойной род два имеют только не сопряжённые элементам сомножителей элементы вида $[u, v]$, $a^u a^v$, $b^u b^v$ и $a^u b^v$ (где $a \in A$, $b \in B$, $u \in A * B \ni v$);

Степенностью элемента $w \in A * B$ мы назовём максимальное s такое, что w раскладывается в произведение $e_1^{n_1} \dots e_m^{n_m}$, где все e_i сопряжены между собой и не сопряжены элементам сомножителей A и B, а $\sum(n_i - 1) = s$. Например, если $u, v \in A * B$ — сопряжённые элементы, не сопряжённые элементам свободных сомножителей, то
- элемент u^4v^2 имеет степенность по крайней мере четыре;
- элемент u^3vuv имеет степенность по крайней мере три, поскольку он переписывается в виде u^4v^uv.

Отметим ещё, что если в разложении $w = e_1^{n_1} \dots e_m^{n_m}$ в произведение сопряжённых элементов имеется p одинаковых сомножителей, то степенность элемента w не меньше $p - 1$, поскольку, пользуясь тождеством $uv = vu^v$, мы можем переставить сомножители, чтобы эти p одинаковых сомножителей шли подряд и образовывали p-ю степень.

Отсюда, в частности, вытекает, что если группа $A*B$ имеет кручение, то степенность единицы (а следовательно, и многих других элементов) бесконечна. Действительно, если, например, элемент $a \in A$ имеет порядок три, то

$$1 = [a,b][a,b]^{a^{-1}}[a,b]^{a^{-2}} \quad \text{и, следовательно, } 1 = \left([a,b][a,b]^{a^{-1}}[a,b]^{a^{-2}}\right)^{2022}$$

и мы получили разложение единицы в произведение сопряжённых элементов, в котором один из этих сопряжённых элементов ($[a, b]$, например) встречается сколь угодно много раз. В силу сделанного выше замечания это означает бесконечную степенность единицы. Основная теорема показывает, что в группах без кручения всё гораздо лучше:

> *если группа $A * B$ не имеет кручения, то степенность каждого элемента меньше бесконечности, а элементы свободных сомножителей вообще не раскладываются нетривиальным образом в произведения сопряжённых между собой элементов, не лежащих в сомножителях.*

Это означает, что степенность единицы равна нулю (поскольку для неё есть только пустое разложение), а степенность неединичных элементов сомножителей A и B можно считать минус бесконечностью (поскольку для них вообще нет никаких разложений).

Вообще, основную теорему можно переформулировать так:

> *степенность каждого элемента свободного произведения групп без кручения не превосходит двойного рода этого элемента минус два*

и улучшить эту оценку нельзя, как показывает упомянутый выше результат Каллера [Cull81] или даже более простое тождество $(ab)^n = a^n b^{a^{n-1}} b^{a^{n-2}} \dots b^a b$, из которого видно, что элемент $(ab)^n \in (A * B) \setminus (A \cup B)$ имеет степенность (по крайней мере) $n - 1$ и двойной род (не больше) $n + 1$.

Наше доказательство основано на использовании леммы о столкновениях [K93] (см. также [FeR96]), которая имеет несколько приложений к теории групп (см., например, [CG95], [FeR96], [K97], [FeR98], [CG00], [CR01], [FoR05], [K05], [K06a], [K06b], [K07], [K09], [Le09], [KL12], [FK12]).

Обозначения, которые мы используем, в целом стандартны. Отметим только, что если $k \in \mathbb{Z}$, а x и y — элементы некоторой группы, то x^y, x^{ky} и x^{-y} обозначают $y^{-1}xy$, $y^{-1}x^ky$ и $y^{-1}x^{-1}y$, соответственно. Символ g^G обозначает класс сопряжённости элемента g группы G. Коммутатор $[x, y]$ мы понимаем как $x^{-1}y^{-1}xy$. Эйлерову характеристику компактной поверхности S мы обозначаем $\chi(S)$. Буквы $\mathbb{R}$, $\mathbb{Z}$ и $\mathbb{N}$ обозначают множества вещественных, целых и натуральных (целых положительных) чисел, соответственно.

1. Диаграммы Хауи

Пусть имеется замкнутая ориентированная поверхность S (возможно несвязная) и карта на S, то есть (неориентированный) граф, который вложен в поверхность S и разбивает её на односвязные области, называемые *гранями* или *клетками*). Такую карту мы называем *диаграммой* над свободным произведением $A * B$, если

- граф двудольный, то есть вершины разделены на два класса: A-вершины и B-вершины и каждое ребро соединяет A-вершину с B-вершиной;
- углы при A-вершинах помечены элементами группы A, а углы при B-вершинах помечены элементами группы B;
- некоторые вершины выделены и называются *внешними*, остальные вершины называются *внутренним*;
- метка каждой внутренней A-вершины равна единице в группе A, а метка каждой внутренней B-вершины равна единице в группе B, где под *меткой вершины* понимается произведение меток углов при этой вершине, перечисленных по часовой стрелке.

Подобные диаграммы рассматривались в [How83], [How90], [K93], [Le09] и многих других работах, но наши определения слегка отличаются.

Метка грани такой диаграммы определяется естественным образом как произведение меток всех углов этой грани против часовой стрелки. Метка грани представляет собой элемент свободного произведения $A * B$, определённый с точностью до сопряжённости.

Например, на рисунке 1 изображена карта на торе (который нарисован в виде прямоугольника с отождествлёнными противоположными сторонами), содержащая две вершины, три ребра, одну грань и шесть углов с метками $a \in A$ и $b \in B$. Если вершины внутренние, то a^3 должно быть равно единице в группе A, а b^3 должно быть равно единице в группе B. Метка грани здесь равна $(ab)^3$. Эта диаграмма показывает, что куб произведения двух элементов порядка три всегда является коммутатором.

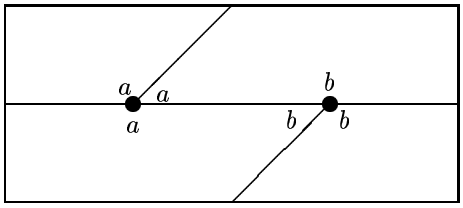


Рис. 1

Мы называем карту *несократимой* если у неё нет углов с единичными метками. *Двойным родом* карты мы называем сумму удвоенного рода поверхности*) и числа внешних вершин. Другими словами, для карты

$$\textit{двойной род} \;=\; 2 - (\textit{число граней}) + (\textit{число рёбер}) - (\textit{число внутренних вершин}).$$

Связь между двойным родом элемента свободного произведения и двойным родом диаграммы состоит в том, что

> *двойной род циклически несократимого элемента $u \in (A * B) \setminus (A \cup B)$ равен минимальному двойному роду несократимой диаграммы над $A * B$, состоящей из одной клетки с меткой u.*

Нам понадобится чуть более сильный факт.

Лемма о геометрическом смысле двойного рода. *Если в свободном произведении $G = A * B$ классы сопряжённости $u_1^G, \dots, u_m^G$ не пересекаются со свободным сомножителям A и B, то минимальный двойной род элемента произведения $u_1^G u_2^G \dots u_m^G$ этих классов совпадает с минимальным двойным родом несократимой диаграммы, состоящей из m клеток с метками $u_1, \dots, u_m$.*

Доказательство. Докажем, что минимальный двойной род диаграммы не превосходит минимального двойного рода элемента. Противоположное неравенство мы использовать не будем, поэтому его доказательство мы оставляем читателям в качестве упражнения

Во-первых заметим, что легко построить сократимую диаграмму нужного двойного рода, метки m клеток которой равны $u_1, \dots, u_m$, а метки оставшихся клеток равны единице, причём эта диаграмма будет связной (то есть поверхность будет связной).

Действительно, можно поступить, например, следующим образом. Пусть элемент минимального двойного рода из произведения классов сопряжённости имеет вид

$$w = u_1^{g_1} \dots u_m^{g_m} = [v_1, w_1] \dots [v_k, w_k] f_1 \dots f_l, \quad \text{где} \quad u_i, g_i v_i, w_i, f_i \in A * B,$$

*) Под *родом* необязательно связной замкнутой поверхности мы всегда понимаем $\frac{1}{2}(2 - \chi)$, где χ — эйлерова характеристика поверхности.

причём f_i сопряжены элементам сомножителей и $2k+l$ — это двойной род элемента w. Нарисуем на плоскости большую окружность, поставим на ней много вершин и поставим в качестве меток углов (внутри круга и против часовой стрелки) буквы слова

$$u_m^{-g_m} \dots u_1^{-g_1} [v_1, w_1] \dots [v_k, w_k] f_1 \dots f_l,$$

в котором мы не производим никаких сокращений и, более того, между словами u_i^{-1}, $g_i^{\pm 1}$, $v_i^{\pm 1}$, $w_i^{\pm 1}$, f_i мы ставим несколько дополнительных вершин, углам при которых (внутри круга) приписываем метки $1 \in A$ и $1 \in B$, заботясь о том, чтобы граф получился двудольный (то есть, чтобы углы с метками из A чередовались с углами с метками из B). Таким образом мы получили грань Г, метка которой равна единице (в $A * B$). Теперь для каждого u_i выберем A-вершину с единичной меткой перед началом слова u_i^{-1} и B-вершину с единичной меткой после конца u_i^{-1} и соединим дополнительным ребром на плоскости вне клетки Г. Отождествим теперь отрезки с метками v_i и v_i^{-1}, а также w_i и w_i^{-1} и получим карту на связной ориентированной поверхности рода k. Правда не все углы имеют метки. Более точно, у нас есть вершины степени три и два. Каждый угол при вершине степени три либо имеет метку один, либо не имеет пока метки, а у каждой вершины степени два либо оба угла имеют метки (причём эти метки взаимно обратны), либо один из углов имеет метку, а второй не имеет. Дорасставим теперь метки естественным образом:

- у всех углов при вершинах степени три поставим единичные метки;
- у вершин степени два, отвечающим серединам слов f_i припишем единичные метки углам, которые меток не имели; и объявим эти вершины внешними;
- с остальными вершинами степени два поступим так: если один из углов при такой вершине имеет метку c, то второму углу припишем метку c^{-1}.

Понятно, что мы получили диаграмму на связной ориентированной поверхности рода k с l внешними вершинами; m клеток этой диаграммы имеют метки $u_1, \dots, u_m$, а остальные клетки имеют единичные метки.

Теперь будем делать эту диаграмму несократимой. Связность при наших преобразованиях может нарушиться, но мы будем заботиться о том, чтобы каждая компонента связности содержала хоть одну клетку с неединичной меткой.

Пусть имеется два смежных ребра α и β, исходящих из вершины x и угол между этими рёбрами имеет единичную метку. Пусть ребро α соединяет вершины x и y, а ребро β соединяет x и z. Заметим, что $y \neq x \neq z$, поскольку наш граф двудольный. Возможны три случая.

Случай 1: $y \neq z$. В этом случае мы просто «схлопнем» рёбра α и β, вершины y и z при этом склеятся, а метки соответствующих углов при этих вершинах мы перемножим (рис. 2).

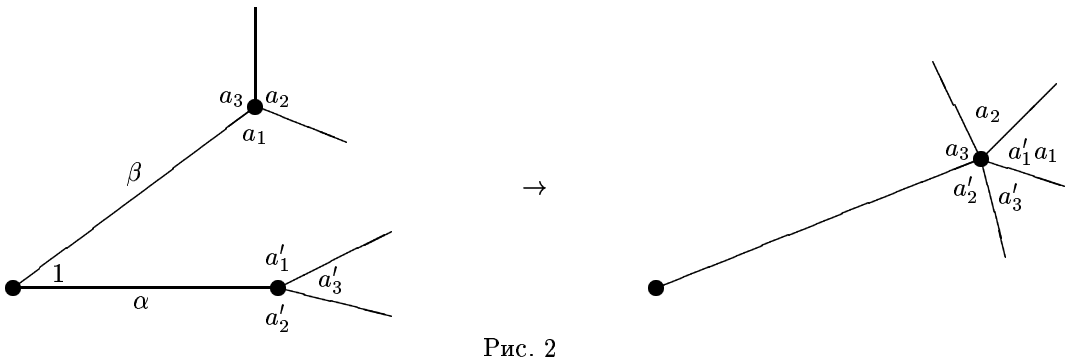


Рис. 2

Случай 2: $y = z$, но $\alpha \neq \beta$. В этом случае мы разрежем поверхность по циклу состоящему из рёбер α и β и получим (возможно несвязную) поверхность с двумя дырами (то есть с краем, состоящим из двух окружностей). На одной дыре есть две вершины x' и y', которые соединены рёбрами α' и β', а на другой дыре есть две вершины x'' и y'', которые соединены рёбрами α'' и β'', причём из вершины x'' других рёбер не исходит.

Если обе получившиеся компоненты содержат клетки с неединичной меткой (или если разрезание не привело к образованию новых компонент связности), то схлопнем рёбра α' и β', а также α'' и β''. Вершины y' и y'' объявим внешними, вершину x' оставим в том же статусе, который был у вершины x, а вершину x'' (которая имеет степени один, и единственный угол при ней имеет единичную метку) объявим внутренней (рис. 3).

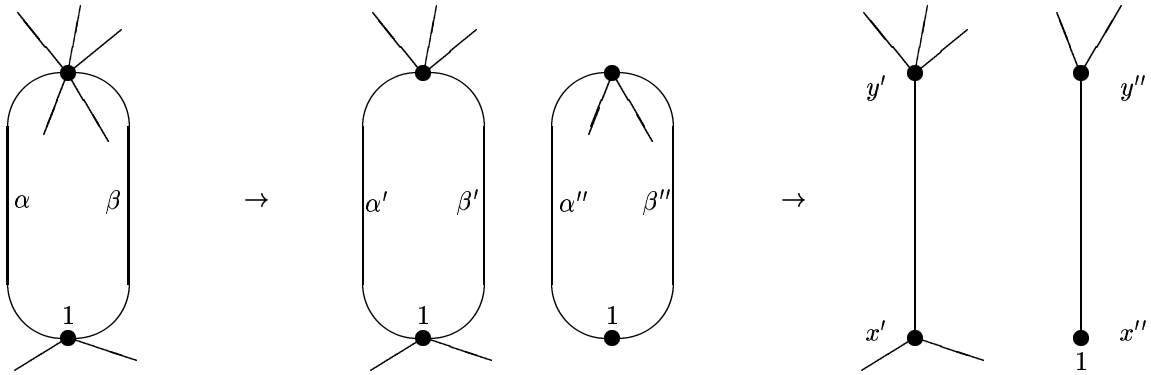


Рис. 3

Двойной род диаграммы может при этом только уменьшиться. Действительно,

$$\textit{двойной род диаграммы} \;=\; 2-\chi(S)+(\textit{число внешних вершин}).$$

При разрезании мы увеличили количество рёбер на два и увеличили количество вершин на два (то есть не изменили эйлерову характеристику). При схлопывании двух пар рёбер мы уменьшили количество рёбер на два (то есть увеличили эйлерову характеристику на два). При объявлении двух вершин внешними мы увеличили двойной род на два или на один (в зависимости от того, была ли вершина y внешней). В итоге двойной род не вырос.

Если же в результате разрезания образовалась компонента, все клетки которой имеют единичные метки, то мы удалим эту компонент. На оставшейся компоненте остались рёбра $\widetilde{\alpha}$ и $\widetilde{\beta}$, соединяющие вершины $\widetilde{x}$ и $\widetilde{y}$ (где $\widetilde{\alpha}$, $\widetilde{\beta}$, $\widetilde{x}$ и $\widetilde{y}$ — это α', β', x' и y' или α'', β'', x'' и y'' в зависимости от того, какую компоненту мы удалили). Схлопнем рёбра $\widetilde{\alpha}$ и $\widetilde{\beta}$, вершину $\widetilde{x}$ оставим в том же статусе, который был у x, а с вершиной $\widetilde{y}$ поступим следующим образом: если удалённая компонента была диском без внешних вершин, то оставим $\widetilde{y}$ в том же статусе, какой был у y (вершины $\widetilde{y}$ и y имеют одинаковые метки в этом случае); если же удалённая компонента не была диском или содержала внешние вершины, то мы объявим вершину $\widetilde{y}$ внешней).

Понятно, что двойной род при этом не увеличится, а в случае, когда удалённая компонента была диском без внешних вершин (и все её клетки имели единичную метку), метка вершины $\widetilde{y}$ равна метки вершины y.

Случай 3: $\alpha=\beta$ (то есть вершина x имеет степень один). Заметим, что в этом случае степень вершины y больше единицы, поскольку в противном случае α было бы единственным ребром в своей компоненте поверхности, эта компонента была бы сферой и метка единственной грани была бы элементом свободного сомножителя A или B, что невозможно, поскольку каждая компонента содержит грань с неединичной меткой, а u_i не сопряжены элементам сомножителей по условию.

Таким образом, вершина y имеет степень больше чем один и мы можем просто удалить вершину x и ребро α, а метки двух углов при вершине y перемножить (рис. 4). Ясно, что двойной род при этом не увеличится и доказательство закончено.

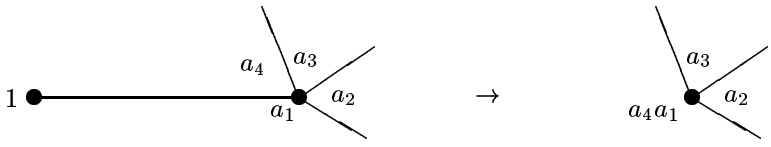


Рис. 4

2. Движения

Этот параграф почти дословно повторяет соответствующий параграф из работы [FK12] и состоит из определений и утверждений, которые мы позаимствовали из [K05] (слегка упростив их применительно к интересующему нас случаю).

Пусть на замкнутой ориентированной поверхности S имеется карта M. *Автомобилем*, объезжающим грань D этой карты, называют сохраняющее ориентацию накрытие границы ∂D грани D ориентированной окружностью R (*окружностью времени*).

Говоря по-простому, автомобиль объезжает границу своей грани против часовой стрелки (внутренность грани остается слева от автомобиля), не разворачиваясь и не останавливаясь. При этом движение периодично.

Если число автомобилей, оказавшихся в момент времени t в точке p одномерного остова поверхности S, равно кратности этой точки, то мы говорим, что в точке p в момент t происходит *полное столкновение*. При этом точка p называется *точкой полного столкновения*. Точки полного столкновения, лежащие на ребрах, мы называем просто *точками столкновения*.

Кратным движением периода T на карте M называется набор автомобилей $\alpha_{D,j}\colon R \to \partial D$, где $j = 1, \dots, d_D$, такой что

1) $d_D \geqslant 1$ (то есть каждую грань объезжает по крайней мере один автомобиль);
2) $\alpha_{D,j}(t+T) = \alpha_{D,j+1}(t)$ для любого $t \in R$ и $j = \{1, \dots, d_D\}$ (здесь индексы берутся по модулю d_D, а сложение точек окружности R производится естественным образом: $R = \mathbb{R}/l\mathbb{Z}$);
3) существует такое разбиение каждой из окружностей ∂D на d_D дуг (с непересекающимися внутренностями), что на протяжении интервала времени $[0, T]$ каждый автомобиль $\alpha_{D,j}$ движется по j-й дуге.

Лемма о столкновениях [K05], [K97]. *Для любого кратного движения на карте на замкнутой ориентированной поверхности S число точек полного столкновения не меньше чем*

$$\chi(S) + \sum_D (d_D - 1), \quad \text{где сумма распространяются на все грани карты.}$$

В упомянутых работах эта лемма была сформулирована и доказана для связных поверхностей, но она остаётся верной и в несвязном случае по очевидным причинам — и левая, и правая часть неравенства аддитивна относительно несвязного объединения.

3. Доказательство основной теоремы

Сперва заметим, что теорему достаточно доказать для свободных произведений двух сомножителей $A * B$, поскольку свободное произведение произвольного числа групп $*H_i$ можно вложить в свободное произведение некоторых двух групп таким образом, что

1) множество порядков элементов в $A * B$ такое же как в $*H_i$;
2) элемент $w \in *H_i$ сопряжён в этой группе элементу одного из сомножителей H_i тогда и только тогда, когда он сопряжён в $A * B$ элементу одного из сомножителей A или B.

Из второго свойства вытекает, что степенность элемента w в группе $*H_i$ не превосходит его степенности в группе $A * B$, а двойной род элемента w в группе $*H_i$ не меньше его двойного рода в группе $A * B$. Поэтому достаточно доказать требуемое неравенство для группы $A * B$.

Чтобы обеспечить условия 1) и 2), достаточно положить $A = *\widetilde{H}_i$, где $\widetilde{H}_i$ — изоморфные копии групп H_i (с изоморфизмом $x \mapsto \widetilde{x}$), в качестве группы B взять любую группу без кручения достаточно большой мощности, а в качестве вложения $*H_i \to A * B$ взять отображение

$$H_i \ni h_i \mapsto \left(\widetilde{h}_i\right)^{b_i} \in A * B, \quad \text{где } b_i \in B \text{ — какие-нибудь фиксированные попарно разные элементы.}$$

Будем теперь доказывать теорему для свободного произведения двух групп. Рассмотрим «степенное разложение» произвольного элемент $w \in A * B$:

$$w = u^{n_1 g_1} u^{n_2 g_2} \dots u^{n_m g_m}, \quad \text{где } u \in (A * B) \setminus (A \cup B) \text{ — циклически несократимый элемент, } g_i \in A * B \text{ и } n_i \in \mathbb{N},$$

причём $\sum(n_i - 1)$ равна степенности элемента w. По лемме о геометрическом смысле двойного рода мы получаем несократимую диаграмму, состоящую из m клеток с метками u^{n_1}, u^{n_2}, …, u^{n_m}, и двойной род этой диаграммы совпадает с двойным родом элемента w.

Пусть слово u имеет вид $u = a_1 b_1 \dots a_p b_p$, где $a_i \in A \setminus \{1\}$ и $b_i \in B \setminus \{1\}$. Организуем теперь движение на этой диаграмме следующим образом:

> клетку с меткой u^{n_i} объезжают n_i автомобилей с постоянной скоростью одно ребро в минуту; в нулевой момент времени все они находятся в (разных) углах с меткой b_p.

Ясно, что мы имеем дело с кратным периодическим движением с набором кратностей $n_1, \dots, n_m$ и периодом $2p$. Посмотрим, где могут происходить полные столкновения.

Столкновения на рёбрах (то есть не в вершинах) происходить не могут, поскольку в каждый момент времени мы имеем одну из следующих конфигураций:

- либо все автомобили находятся в A-вершинах (это происходит в нечётные моменты времени),
- либо все автомобили находятся в B-вершинах (это происходит в чётные моменты времени),
- либо каждый автомобиль едет от A-вершины к B-вершине (это происходит в нецелые моменты времени, целая часть которых нечётна),
- либо каждый автомобиль едет от B-вершины к A-вершине (это происходит в нецелые моменты времени, целая часть которых чётна).

Таким образом никогда два автомобиля не едут по ребру навстречу друг другу, а значит они не могут столкнуться на ребре.

Полные столкновения во внутренних вершинах тоже происходить не могут, поскольку в каждый целый момент времени, все автомобили находятся в углах с одинаковыми метками: в чётный момент времени $2i$ все автомобили проезжают углы с меткой b_i (индексы по модулю p), а в нечётный момент времени $2i+1$ все автомобили проезжают углы с меткой a_i. Следовательно, при вершине полного столкновения все углы должны иметь одинаковую метку. Во внутренней вершине такого быть не может, поскольку по определению диаграммы произведение меток углов при такой вершине должна быть единицей, а группа не имеет кручения по условию (и $a_i \neq 1 \neq b_i$).

Отметим, что это единственное место, в котором мы используем отсутствие кручения. Поэтому всё останется справедливым, если условие отсутствия кручения заменить на отсутствие неединичных элементов порядка $\leqslant \sum n_i$. В этом случае полное столкновение во внутренней вершине не может произойти, поскольку количество автомобилей, участвующих в таком гипотетическом столкновении превосходит общее количество автомобилей.

Получается, что полные столкновения могут происходить лишь во внешних вершинах. Но по лемме о столкновениях полные столкновения должны произойти по крайней мере в $\chi(S) + \sum(n_i - 1)$ различных точках. Следовательно,

$$\textit{число внешних вершин} \;\geqslant\; \chi(S) + \sum(n_i - 1), \quad \text{то есть} \quad (\textit{число внешних вершин}) - \chi(S) \;\geqslant\; \sum(n_i - 1).$$

Левая часть последнего неравенства есть двойной род минус два, а правая часть равна степенности и доказательство закончено.

ГЛАВА 16.
УРАВНОВЕШЕННЫЕ РАЗЛОЖЕНИЯ НА МНОЖИТЕЛИ

0. Введение

Покажите, что всякое рациональное число можно разложить в произведение нескольких рациональных чисел, сумма которых равна нулю.

Эта задача была придумана А. Н. Васильевым и предлагалась на Казахстанской республиканской математической олимпиаде для школьников в 2013 году [Вас13]. Аналогичный вопрос для произвольного поля характеристики не два предлагался на студенческой олимпиаде по алгебре в МГУ в 2014 году [Вас14]. Позже нам стало известно, что задача рассматривалась и раньше [Ива13] (также в контексте работы со способными школьниками).*)

В первом параграфе мы доказываем несколько общих фактов об уравновешенных разложениях и полностью решаем вопрос о возможном количестве сомножителей во всех конечных полях. Ответ получается неожиданным и довольно сложным (теорема 1). Например, оказывается, что во всех конечных полях, кроме ровно одного, каждый элемент допускает уравновешенное разложение в произведение не более чем трёх множителей. В роли единственного исключения выступает семиэлементное поле $\mathbb{F}_7$. Основным инструментом при работе в конечных полях нам служит оценка Хассе числа рациональных точек эллиптической кривой над конечным полем.

Кроме того, в первом параграфе мы показываем, что в каждом поле характеристики не 2 есть «универсальные» формулы, позволяющие получить уравновешенное разложение почти любого элемента. Например, формула (1) даёт уравновешенное разложение на пять множителей для любого ненулевого элемента (в любом поле характеристики не два). Мы доказываем, что такие формулы существуют для разложение на любое число сомножителей, начиная с пяти, но не существуют для разложение на три сомножителя. Этот факт мы выводим из теоремы Мейсона–Стотерса (то есть из abc-теоремы для многочленов).

Во втором параграфе мы показываем, что вопрос об уравновешенных разложениях в конечномерных алгебрах по существу сводится к аналогичному вопросу о полях и полностью решаем вопрос о количестве множителей в некоторых естественных алгебрах, например, в матричных алгебрах над $\mathbb{C}$ и $\mathbb{R}$.

В третьем параграфе мы приводим много примеров, показывающих, что результаты параграфа 2 не могут быть усилены в разных направлениях.

Последний параграф посвящён открытым вопросам.

Мы завершаем это краткое введение формальным определением нашего предмета изучения. Пусть некоторый элемент a некоторого кольца некоторым образом разложен на множители в этом кольце: $a = a_1 a_2 \dots a_k$. Мы называем это разложение *уравновешенным* или *сбалансированным*, если $\sum a_i = 0$.

1. Поля

Теорема 0. *В поле характеристики, отличной от двух, каждый элемент раскладывается в произведение k сомножителей, сумма которых равна нулю, для каждого $k \geqslant 5$. А для каждого $k < 5$ найдётся поле характеристики не два, в котором аналогичное утверждение неверно.*

Доказательство. Докажем первое утверждение. Для нулевого элемента доказывать нечего, а для ненулевого элемента a мы можем торжественно написать

$$a = \frac{a}{2} \cdot \frac{a}{2} \cdot (-a) \cdot \frac{2}{a} \cdot \left(-\frac{2}{a}\right). \tag{1}$$

Это даёт сбалансированное разложение на пять сомножителей. Лёгкая модификация разложения (1) даёт сбалансированное разложение произвольного элемента b на шесть сомножителей:

$$b = c^2 - ca = \frac{a}{2} \cdot \frac{a}{2} \cdot (c-a) \cdot \frac{2}{a} \cdot \left(-\frac{2}{a}\right) \cdot (-c), \quad \text{где } c \text{ — любой элемент такой, что } 0 \neq c^2 \neq b, \text{ а } a = \tfrac{c^2-b}{c}.$$

(Такое c обязательно найдётся, кроме случая, когда поле состоит из трёх элементов и $b = 1$; а в этом исключительном случае можно взять очевидное разложение $b = 1 = 1^3(-1)^3$.)

Сбалансированные разложения на $k \geqslant 7$ сомножителей можно получать, умножая полученные разложения на сбалансированные разложений минус единицы на два сомножителя: $-1 = (-1) \cdot 1$. Например, мы получаем такое сбалансированное разложение произвольного элемента в произведение ста сомножителей:

$$-b = -(c^2 - ca) = \frac{a}{2} \cdot \frac{a}{2} \cdot (c-a) \cdot \frac{2}{a} \cdot \left(-\frac{2}{a}\right) \cdot (-c) \cdot (-1)^{47} \cdot 1^{47}.$$

Первое утверждение доказано.

Второе утверждение вытекает из теоремы 1 (см. ниже): если $k \leqslant 3$, то в качестве примера годится поле $\mathbb{F}_7$, а если $k = 4$, то годится $\mathbb{F}_3$. Теорема доказана.

*) А ещё позже выяснилось, что этой задачей занимался ещё Эйлер, смотрите следующую главу.

Теорема 1. *Пусть $k \geqslant 2$ — целое число и F — конечное поле. В поле F всякий элемент можно разложить в произведение k сомножителей, сумма которых равна нулю, тогда и только тогда, когда*

либо $|F| = 2$ и k чётно,
либо $|F| = 4$ и $k \neq 3$,
либо $|F|$ — степень двойки, но не двойка и не четвёрка (и k любое),
либо $|F| \in \{3, 5\}$ и $k \notin \{2, 4\}$,
либо $|F| = 7$ и $k \notin \{2, 3\}$,
либо $|F|$ не степень двойки, не три, не пять и не семь и $k \neq 2$.

Другими словами, ситуация в конечных полях такая:

	$k=2$	$k=3$	$k=4$	$k=5,7,9,\ldots$	$k=6,8,10,\ldots$
$\mathbb{F}_2$	да	нет	да	нет	да
$\mathbb{F}_3$	нет	да	нет	да	да
$\mathbb{F}_4$	да	нет	да	да	да
$\mathbb{F}_5$	нет	да	нет	да	да
$\mathbb{F}_7$	нет	нет	да	да	да
$\mathbb{F}_8, \mathbb{F}_{16}, \mathbb{F}_{32}, \mathbb{F}_{64}, \ldots$	да	да	да	да	да
$\mathbb{F}_9, \mathbb{F}_{11}, \mathbb{F}_{13}, \mathbb{F}_{17}, \ldots$	нет	да	да	да	да

Доказательство. Будем доказывать по столбцам этой таблицы.

Случай $k = 2$. В конечном поле характеристики два всякий элемент является квадратом (поскольку порядок мультипликативной группы такого поля нечётный), то есть каждый элемент является произведением двух одинаковых сомножителей, сумма которых равна нулю, поскольку характеристика равна двум. Если же характеристика конечного поля не равна двум, то не каждый элемент является квадратом и, следовательно, не каждый элемент раскладывается в произведение двух сомножителей, сумма которых равна нулю.

Случай $k = 3$. Если характеристика равна трём, то порядок мультипликативной группы поля $q - 1 = 3^k - 1$ не делится на три и, следовательно, каждый элемент является кубом и разложение $a = bbb$ является искомым (поскольку $b + b + b = 0$ в поле характеристики три).

Для доказательства в случае другой характеристики нам понадобится известная оценка Хассе (или Хассе–Вейля).

Оценка Хассе (см., например, [Sil86], теорема V.1.1)**.** *Число точек эллиптической кривой (то есть неособой и неприводимой над замыканием поля проективной кривой рода один) над конечным полем из q элементов не меньше чем $q + 1 - 2\sqrt{q}$.*
В частности, это верно для неособых и неприводимых (над замыканием поля) кубических кривых в проективной плоскости над $\mathbb{F}_q$.

Продолжим доказательство, считая, что характеристика поля отлична от трёх. Мы хотим показать, что система уравнений

$$\begin{cases} x + y + z = 0 \\ xyz = a \end{cases} \tag{2}$$

над конечным полем $\mathbb{F}_q$ имеет по крайней мере одно решение для любого $a \in \mathbb{F}_q$. Другими словами, мы хотим показать, что кубическая (аффинная) кривая, заданная уравнением

$$xy(x + y) = -a,$$

имеет по крайней мере одну точку над $\mathbb{F}_q$. В однородных координатах соответствующая проективная кривая задаётся уравнением

$$XY(X + Y) = -aZ^3, \tag{3}$$

а особые точки этой кривой задаются системой уравнений, состоящей из уравнения (3) и его частных производных по X, Y и Z:

$$\begin{cases} XY(X + Y) = -aZ^3 \\ 2XY + Y^2 = 0 \\ 2XY + X^2 = 0 \\ -3aZ^2 = 0 \end{cases}. \tag{4}$$

Мы считаем, что $a \neq 0$, поскольку при $a = 0$ система (2) очевидно имеет решение (нулевое). Поэтому (и поскольку характеристика поля отлична от трёх) из последнего уравнения системы (4) мы получаем $Z = 0$. Разность второго и третьего уравнения показывает, что $X = \pm Y$ и тогда второе уравнение показывает, что X и Y нулевые (мы опять воспользовались тем, что $\operatorname{char} \mathbb{F}_q \neq 3$). Таким образом, система (4) не имеет ненулевых решений, то есть наша проективная кривая не имеет особых точек над замыканием поля (если $\operatorname{char} \mathbb{F}_q \neq 3$). Это

автоматически означает, что наша кривая неприводима (и, следовательно, эллиптична), поскольку приводимая кубическая кривая обязательно имеет особые точки (над замыканием поля)— это точки пересечения компонент.

Таким образом, мы можем применить оценку Хассе и получить, что проективная кубика (3) имеет больше трёх точек над полем $\mathbb{F}_q$, если характеристика этого поля не равна трём и $q+1 > 2\sqrt{q}+3$. Это неравенство выполнено при $q \geqslant 8$. Таким образом, при $q \geqslant 8$ проективная кривая содержит больше трёх точек, что означает, что соответствующая аффинная кривая содержит по крайней мере одну точку, поскольку пересечение неприводимой кубики с бесконечно удалённой прямой не может содержать больше трёх точек*), то есть система (2) имеет решение, что и требовалось.

Осталось разобраться с полями $\mathbb{F}_2$, $\mathbb{F}_4$, $\mathbb{F}_5$ и $\mathbb{F}_7$.

В $\mathbb{F}_2$ единица очевидно не имеет сбалансированных разложений в произведение трёх сомножителей.

В $\mathbb{F}_4$ ненулевое сбалансированное произведение xyz трёх сомножителей не может содержать повторяющихся множителей (поскольку $x+x=0$), поэтому такое произведение всего одно — это произведение всех ненулевых элементов поля, оно равно единице; следовательно, элементы, отличные от единицы и нуля, не допускают сбалансированных разложений в произведение трёх сомножителей.

В $\mathbb{F}_5$ система (2) имеет решение: $x=y=b$, $z=-2b$, где b — кубический корень из $-\frac{a}{2}$ (в $\mathbb{F}_5$ любой элемент является кубом).

Поле из семи элементов действительно является исключением. В самом деле, элементы ± 3 не имеют сбалансированных разложений в произведение трёх сомножителей. Действительно, если

$$\begin{cases} x+y+z=0 \\ xyz=\pm 3 \end{cases},$$

то элементы x, y и z обязаны быть попарно разными, поскольку ± 3 не является удвоенным кубом (кубами в $\mathbb{F}_7$ являются элементы 0 и ± 1). Разумеется, никакие два из элементов x, y и z не могут отличаться знаком. Остаётся только одна возможность (с точностью до знаков и перестановок): $x=\pm 1$, $y=\pm 2$, и $z=\pm 3$. Но произведение таких трёх чисел даёт ± 1, а не ± 3. (Тройка имеет, правда, более короткое сбалансированное разложение: $3=2\cdot(-2)$, но элемент -3 не имеет таких разложений.)

Случай $k=4$. Будем искать сбалансированное разложение элемента $a \in F$ в произведение четырёх сомножителей, один из которых равен единице. Дальнейшие рассуждения (до некоторого момента) аналогичны доказательству при $k=3$. Мы хотим показать, что система уравнений

$$\begin{cases} x+y+z+1=0 \\ xyz=a \end{cases} \tag{2'}$$

над конечным полем $\mathbb{F}_q$ имеет по крайней мере одно решение для любого $a \in \mathbb{F}_q$. Другими словами, мы хотим показать, что кубическая (аффинная) кривая, заданная уравнением

$$xy(x+y+1)=-a,$$

имеет по крайней мере одну точку над $\mathbb{F}_q$. В однородных координатах соответствующая проективная кривая задаётся уравнением

$$XY(X+Y+Z)=-aZ^3, \tag{3'}$$

а особые точки этой кривой задаются системой уравнений, состоящей из уравнения (3′) и его частных производных по X, Y и Z:

$$\begin{cases} XY(X+Y+Z)=-aZ^3 \\ 2XY+Y^2+YZ=0 \\ 2XY+X^2+XZ=0 \\ XY=-3aZ^2 \end{cases}. \tag{4'}$$

Разность второго и третьего уравнения есть $Y^2-X^2+Z(Y-X)=0$. Таким образом, либо $X+Y+Z=0$, либо $X=Y$.

Если $X+Y+Z=0$, то из первого уравнения (4′) получаем $Z=0$. Из последнего уравнения тогда получаем, что $XY=0$, и, следовательно все неизвестные равны нулю (поскольку мы предположили, что $X+Y+Z=0$).

Если же $X=Y$, то второе уравнение системы (4′) показывает, что $3X^2+XZ=0$. Если здесь $X=0$, то и $Y=0$ и, следовательно, $Z=0$ (из первого уравнения системы (4′)). Значит, $X \neq 0$ и сокращая на X мы получаем $3X+Z=0$. Тогда из последнего уравнения системы (4′) мы получаем $27a=-1$. Таким образом, если $27a \neq -1$ и $|F| \geqslant 8$, то мы можем воспользоваться оценкой Хассе и заключить, что $a \in F$ имеет сбалансированное

*) В нашем случае бесконечно удалённых точек на кривой ровно три: $(1,0,0)$, $(0,1,0)$ и $(1,-1,0)$ (в однородных координатах).

разложение в произведение четырёх сомножителей (один из которых равен единице), Если же $27a = -1$, то мы действительно получаем особую точку на кривой, но сама эта особая точка, не будучи бесконечно удалённой, даёт сбалансированное разложение элемента a:

$$-\frac{1}{27} = \left(-\frac{1}{3}\right)\cdot\left(-\frac{1}{3}\right)\cdot\left(-\frac{1}{3}\right)\cdot 1.$$

Осталось рассмотреть маленькие поля F, где $|F| < 8$. В $\mathbb{F}_2$ и в $\mathbb{F}_4$ (как и в любом конечном поле характеристики два) любой элемент является четвёртой степенью некоторого другого элемента, что и даёт сбалансированное разложение в произведение четырёх (одинаковых) сомножителей.

В $\mathbb{F}_3$ единственное ненулевое сбалансированное произведение четырёх сомножителей — это $1\cdot 1\cdot(-1)\cdot(-1)$ и оно равно единице, поэтому -1 не допускает таких разложений.

В $\mathbb{F}_5$ произведение четырёх ненулевых сомножителей может быть одного из следующих видов:

$$(\pm1)(\pm1)(\pm1)(\pm1),\quad (\pm1)(\pm1)(\pm1)(\pm2),\quad (\pm1)(\pm1)(\pm2)(\pm2),\quad (\pm1)(\pm2)(\pm2)(\pm2),\quad (\pm2)(\pm2)(\pm2)(\pm2).$$

Первое, третье и пятое из этих произведений дают ±1, поскольку квадрат любого элемента равен ±1. А во втором и четвёртом произведении есть только по два способа расставить знаки так, чтобы сумма сомножителей оказалась нулевой:

$$1\cdot1\cdot1\cdot2,\quad (-1)\cdot(-1)\cdot(-1)\cdot(-2),$$
$$(-1)\cdot2\cdot2\cdot2,\quad 1\cdot(-2)\cdot(-2)\cdot(-2).$$

Все эти произведения равны двойке, поэтому $-2\in\mathbb{F}_5$ не допускает сбалансированного разложения в произведение четырёх сомножителей.

В поле $\mathbb{F}_7$ подбираем уравновешенные разложения:

$$0=0^4,\quad 1=1^2\cdot(-1)^2,\quad -1=1\cdot1\cdot2\cdot3,\quad 2=2^2\cdot(-2)^2,\quad -2=1\cdot(-2)^2\cdot3,\quad 3=(-1)\cdot2\cdot3^2,\quad -3=(-1)^3\cdot3.$$

Случай чётного $k > 4$. Если каждый элемент a имеет сбалансированное разложение в произведение k сомножителей: $a = a_1\dots a_k$, то каждый элемент имеет сбалансированное разложение в произведение $(k+2)$-х сомножителей: $-a = a_1\dots a_k\cdot 1\cdot(-1)$. Поэтому достаточно доказать утверждение для $k = 6$. Более того, для всех конечных полей, кроме $\mathbb{F}_3$ и $\mathbb{F}_5$, утверждение можно считать доказанным, поскольку у нас уже есть уравновешенное разложение каждого элемента в произведение четырёх сомножителей.

Для $\mathbb{F}_3$ имеем $0=0^6$, $1=1^6$, $-1=1^3\cdot(-1)^3$. А для $\mathbb{F}_5$ сбалансированное произведение $x\cdot x\cdot(-2x)\cdot1\cdot1\cdot(-2)$, равное $-x^3$, даёт произвольный элемент, поскольку все элементы являются кубами.

Случай нечётного $k > 4$. Такая же индукция, как в доказательстве при чётном большом k, позволяет свести дело к случаю $k = 5$. Более того, для всех конечных полей, кроме $\mathbb{F}_2$, $\mathbb{F}_4$ и $\mathbb{F}_7$, утверждение можно считать доказанным, поскольку у нас уже есть уравновешенное разложение каждого элемента в произведение трёх сомножителей.

В поле $\mathbb{F}_7$ искомое разложение существует по теореме 0. А в поле $\mathbb{F}_4$ мы можем написать $a = b^2xyz$, где b — квадратный корень из a и x, y, z — все ненулевые элементы поля (их произведение равно единице, а сумма — нулю). В поле $\mathbb{F}_2$ уравновешенного разложения единицы в произведение нечётного числа сомножителей, очевидно, нет. Это завершает доказательство теоремы.

Формулу (1) можно рассматривать как «универсальную формулу», позволяющую сбалансировано разложить почти любой элемент поля характеристики не два в произведение пяти сомножителей (где *почти любой* означает любой, кроме конечного числа исключительных элементов). Теорема 0 показывает, что такие универсальные формулы существуют для каждого $k \geqslant 5$. Из доказательства теоремы 0 можно извлечь явный вид таких формул:

$$t = \underbrace{\frac{t}{2}\cdot\frac{t}{2}\cdot(-t)\cdot\frac{2}{t}\cdot\left(-\frac{2}{t}\right)}_{5\ \textit{множителей}} = \underbrace{\frac{1-t}{2}\cdot\frac{1-t}{2}\cdot t\cdot\frac{2}{1-t}\cdot\frac{2}{t-1}\cdot(-1)}_{6\ \textit{множителей}} = \underbrace{\left(-\frac{t}{2}\right)\cdot\left(-\frac{t}{2}\right)\cdot t\cdot\left(-\frac{2}{t}\right)\cdot\frac{2}{t}\cdot(-1)\cdot1}_{7\ \textit{множителей}} = \dots$$

Следующая теорема показывает, что «универсальной формулы» сбалансированного разложения на три сомножителя не существует (универсальных сбалансированных разложений на два множителя тоже, очевидно, не существует, а вопрос про четыре сомножителя остаётся открытым, смотрите последний параграф).

Теорема об отсутствии формул. *Элемент t поля рациональных дробей $F(t)$ не допускает сбалансированного разложения на три множителя ни для какого поля F.*

Доказательство. Предположив противное, после приведения к общему знаменателю получаем тождество

$$t^s = \frac{x(t)}{v(t)} \cdot \frac{y(t)}{v(t)} \cdot \frac{z(t)}{v(t)}, \quad \text{где } x, y, z \in F[t] \text{ и } x + y + z = 0.$$

Мы хотим показать, что s не может быть единицей, но удобно доказывать более общий факт:

написанные выше равенства влекут, что s делится на три.

Ясно, что многочлены x, y и z можно считать взаимно простыми, поскольку равенство $xyz = t^s v^3$ показывает, что их общий неприводимый делитель обязан делить v или совпадать с t; в обоих случаях всё можно сократить. Кроме того, можно считать, что $v(0) \neq 0$ (увеличивая s, если нужно).

Воспользуемся известной теоремой Мейсона–Стотерса ([Mas84], [Sto81]), изложенной во многих книгах (см., например, [Lang02]). Мы предпочитаем пользоваться версией Снайдера, которая работает в любой характеристике.

Теорема Мейсона–Стотерса (в форме Снайдера [Sny00]). *Если три многочлена $x, y, z \in F[t]$ над произвольным полем F взаимно просты и $x + y + z = 0$, то либо степень каждого из них строго меньше числа различных корней произведения xyz в алгебраическом замыкании поля F, либо все три производные x', y' и z' равны нулю (как многочлены).*

В нашей ситуации $xyz = t^s v^3$ и число различных корней этого многочлена не превосходит $\deg v + 1$, поэтому по теореме Мейсона–Стотерса либо степень каждого из многочленов x, y, z не превосходит степени многочлена v, либо $x' = y' = z' = 0$.

В первом случае $\deg(xyz) \leqslant 3 \deg v$, что означает, что $s = 0$ (поскольку $xyz = t^s v^3$) и всё доказано. А во втором случае производная произведения равна нулю: $0 = (xyz)' = (t^s v^3)' = st^{s-1}v^3 + 3t^s v^2 v' = v^2 t^{s-1}(sv + 3tv')$, сокращая на $v^2 t^{s-1}$, мы получаем $sv = -3tv'$. Это означает, что s делится на $\operatorname{char} F$, поскольку $v(0) \neq 0$. Значит, либо $\operatorname{char} F = 3$ и s делится на три, что и требовалось, либо $v' = 0$.

Если $v' = 0$, то вспомним, что равенство $f' = 0$ означает, что многочлен f представляет собой многочлен вида

$$f(x) = f_1(x^p), \quad \text{где } p \text{ — это характеристика поля, а } f_1 \text{ — это какой-то многочлен.}$$

Значит подставляя в равенство, с которого мы начали,

$$x(t) = x_1(t^p), \quad y(t) = y_1(t^p), \quad z(t) = z_1(t^p), \quad v(t) = v_1(t^p),$$

мы получаем, что s делится на p и, обозначая t^p буквой τ, мы получаем аналогичное равенство, но для многочленов меньшей степени (от τ):

$$\tau^{\frac{s}{p}} = \frac{x_1(\tau)}{v_1(\tau)} \cdot \frac{y_1(\tau)}{v_1(\tau)} \cdot \frac{z_1(\tau)}{v_1(\tau)}, \quad \text{где } x_1, y_1, z_1 \in F[\tau] \text{ и } x_1 + y_1 + z_1 = 0.$$

Здесь степени всех многочленов уменьшились в p раз. Очевидная индукция завершает доказательство.

2. Алгебры

Лемма 1. *Многочлен от одной переменной над ассоциативным коммутативным кольцом с единицей, у которого значение в некоторой точке d нильпотентно, а значение производной в этой точке обратимо, обязательно имеет корень в этом кольце. При этом для некоторого корня b разность $d - b$ делится на $f(d)$.*

Доказательство. Очевидная замена переменных сводит задачу к случаю, когда $d = 0$. Пусть наш многочлен над кольцом R имеет вид $f(x) = a_0 + a_1 x + \ldots + a_n x^n$ и нам известно, что a_1 обратим, $a_0^s = 0$. Будем доказывать индукцией по s, что *многочлен f имеет корень, делящийся на a_0*.

В факторкольце $\overline{R} = R/(a_0^{s-1}R)$ образ $\overline{f}$ нашего многочлена f имеет корень $\overline{ca_0}$ по предположению индукции. Возьмём какой-нибудь прообраз $c \in R$ элемента $\overline{c} \in \overline{R}$ и будем искать корень многочлена f в виде $b = ca_0 + ta_0^{s-1}$, где $t \in R$ — (неизвестный) элемент. Поскольку $a_0^s = 0$, мы имеем

$$f(b) = a_0 + a_1(ca_0 + ta_0^{s-1}) + \ldots + a_n(ca_0 + ta_0^{s-1})^n = f(ca_0) + a_1 t a_0^{s-1}. \tag{5}$$

Далее, поскольку ca_0 — корень многочлена f по модулю идеала $a_0^{s-1}R$, мы имеем $f(ca_0) \in a_0^{s-1}R$, то есть $f(ca_0) = ra_0^{s-1}$ при некотором $r \in R$. Осталось заметить, что $f(b)$ в выражении (5) будет нулём, если мы возьмём $t = -r/a_1$, что и доказывает лемму.

Следующая теорема сводит вопрос о сбалансированных разложениях в конечномерных алгебрах к аналогичному вопросу о полях, если интересоваться только *нестепенными* разложениями, то есть такими разложениями, в которых не все сомножители равны между собой.

Теорема 2. *Пусть F — поле и n — натуральное число большее двух. Если во всех конечных расширениях поля F каждый элемент обладает нестепенным сбалансированным разложением в произведение n элементов, то то же верно для каждого элемента каждой конечномерной ассоциативной алгебры с единицей над F.*

Доказательство. Ясно, что утверждения достаточно доказать для конечномерных однопорождённых алгебр с единицей (поскольку любой элемент любой алгебры содержится в однопорождённой подалгебре). Таким образом, мы считаем, что наша алгебра A над полем F имеет вид $A = F[x]/(f)$, где $f \in F[x]$. Такая алгебра A раскладывается, как известно, в прямую сумму

$$A \simeq \bigoplus_{i=1}^{m} F_i[x]/(x^{k_i}), \quad \text{где поля } F_i \text{ являются конечными расширениями поля } F$$

($F_i \simeq F[x]/(p_i)$, если $f = \prod p_i^{k_i}$ — разложение многочлена f на неприводимые (над F) множители). Сбалансированные разложения достаточно получить для каждого прямого слагаемого по отдельности. Поэтому мы будем считать, что $A = G[x]/(x^k)$, где поле G является конечным расширением поля F. Такая алгебра A является локальной, то есть имеет единственный максимальный идеал I (порождённый элементом x), $A/I \simeq G$ и все элементы, не лежащие в I, обратимы.

Мы хотим разложить произвольный элемент $a \in A$ в произведение n элементов с нулевой суммой.

Случай I. $a \notin I$. В этом случае найдём нестепенное сбалансированное разложение элемента a по модулю идеала I, то есть в поле G. Таким образом мы получим элементы $a_1, \ldots, a_n \in A$ такие, что

$$a - a_1 a_2 \ldots a_n \in I, \quad a_1 + \ldots + a_n \in I \quad \text{и (без ограничения общности)} \quad a_1 - a_n \notin I.$$

Это означает, что для квадратного многочлена

$$g(t) = a + t a_2 a_3 \ldots a_{n-1}(t + a_2 + a_3 + \ldots + a_{n-1}) \quad \text{мы имеем} \quad g(a_1) \in I. \tag{6}$$

Для производной многочлена g мы получаем

$$g'(a_1) = a_2 a_3 \ldots a_{n-1}(a_1 + a_2 + a_3 + \ldots + a_{n-1}) + a_1 a_2 a_3 \ldots a_{n-1} \in a_2 a_3 \ldots a_{n-1}(a_1 - a_n) + I.$$

Идеал I состоит из нильпотентных элементов, а все не лежащие в нём элементы кольца A обратимы. Поэтому условия леммы 1 выполнены, так как $a_1 \neq a_n \pmod I$. Применяя лемму 1, мы находим корень $\widetilde{t} \in A$ многочлена g, что и требовалось, поскольку

$$a = \widetilde{t} a_2 a_3 \ldots a_{n-1}(-\widetilde{t} - a_2 - a_3 - \ldots - a_{n-1}) \quad \text{и сумма множителей в этом разложении равна нулю.} \tag{7}$$

Это разложение нестепенное, поскольку $\widetilde{t} = a_1 \pmod I$ по лемме 1, а $a_1 \neq a_n \pmod I$ по предположению.

Случай II. $a \in I$. Выберем обратимые (то есть не лежащие в I) элементы $a_2, \ldots, a_{n-1} \in A$ так, чтобы их сумма тоже оказалась обратимой. Это очевидно возможно, если в поле $G = A/I$ больше двух элементов. Если же в поле G два элемента, то единичный элемент этого поля не обладает в G никаким нестепенным разложением, что противоречит условию.

Тогда для многочлена $g(t)$ (см. формулу (6)) мы имеем $g(0) = a$ — нильпотентный элемент и

$$g'(0) = a_2 a_3 \ldots a_{n-1}(a_2 + a_3 + \ldots + a_{n-1}) \text{ — обратимый элемент.}$$

Поэтому, по лемме 1 многочлен g имеет корень $\widetilde{t} \in A$, что и требовалось (см. (7)). Разложение (7) не может быть степенным, поскольку элемент a_2 обратим, а элемент a — нет.

Теорема доказана.

Следствие 1. *Каждый элемент конечномерной ассоциативной алгебры (над полем) с единицей раскладывается в произведение*

а) *трёх элементов, сумма которых равна нулю, если поле алгебраически замкнуто;*

б) *пяти элементов, сумма которых равна нулю, если характеристика поля не два.*

Доказательство. Первое утверждение немедленно вытекает из теоремы 2, поскольку в алгебраически замкнутом поле каждый элемент обладает нестепенным сбалансированным разложением в произведение трёх сомножителей (чтобы получить нестепенное сбалансированное разложение $a = a_1 a_2 a_3$ для данного элемента a, можно просто выбрать любой элемент a_1 такой, что $a_1^3 \neq a$, после чего a_2 и a_3 подобрать, воспользовавшись алгебраической (квадратичной) замкнутостью).

Чтобы доказать второе утверждение, достаточно сослаться на теоремы 2 и 0 и заметить, что формула (1) никогда не может представлять собой степенное разложение.

Следствие 2. *Для любого $k \geqslant 3$ всякую комплексную или вещественную матрицу можно разложить в произведение k матриц над тем же полем, сумма которых равна нулю.*

Доказательство. Утверждение немедленно вытекает из теоремы 2, поскольку каждое вещественное или комплексное число a допускает нестепенное сбалансированное разложение вида $a = x \cdot (x+1) \cdot 1^{k-3} \cdot (2 - k - 2x)$, поскольку это равенство представляет собой кубическое уравнение относительно x.

3. Алгебры. Примеры

В этом параграфе мы приведём примеры, показывающие, что никакие условия теоремы 2 и следствия 1 не могут быть отброшены.

Пример 1. Каждый элемент поля $\mathbb{F}_3$ из трёх элементов обладает сбалансированным разложением в произведение трёх сомножителей: $0 = 0\cdot 0\cdot 0$, $\quad 1 = 1\cdot 1\cdot 1$, $\quad 2 = 2\cdot 2\cdot 2$. Однако в двумерной алгебре $A = \mathbb{F}_3[x]/(x^2)$ над этим полем элемент $1+x$ не допускает уравновешенных разложений в произведение трёх множителей, поскольку, как нетрудно заметить, разложение $1 = 1\cdot 1\cdot 1$ является единственным сбалансированным разложением единицы в поле $\mathbb{F}_3$; следовательно, разложение элемента $1+x \in A$ обязано иметь вид $1+x = (1+kx)(1+lx)(1+mx)$ (где $k, l, m \in \mathbb{F}_3$), откуда получаем $k+l+m = 1$ и разложение не является сбалансированным. Этот пример показывает, что теорема 2 перестанет быть верной, если из неё исключить оговорку о том, что рассматриваются только нестепенные разложения.

Пример 2. В алгебре многочленов $F[x]$ над произвольным полем элемент x вообще не обладает сбалансированными разложениями. Этот пример показывает, что условие конечномерности нельзя исключить из формулировки теоремы 2 и следствия 1.

Пример 3. В алгебре с нулевым умножением вообще никакой ненулевой элемент не обладает сбалансированными разложениями. Этот пример показывает, что условие наличия единицы нельзя исключить из формулировки теоремы 2 и следствия 1.

Что же касается условия $n > 2$, то его, в принципе, можно исключить из формулировки теоремы 2 по той причине, что оно очевидным образом вытекает из остальных условий: в поле всякое сбалансированное разложение нуля в произведение двух сомножителей обязано быть степенным. С другой стороны, в любом ненулевом кольце ноль обладает нестепенными разложениями в произведение трёх и любого большего числа сомножителей: $0 = 0^{2022}\cdot b\cdot(-b)$, где b — ненулевой элемент. Однако есть следующий простой пример.

Пример 4. В поле комплексных чисел всякий ненулевой элемент обладает нестепенным сбалансированным разложением в произведение двух сомножителей, но нильпотентная жорданова клетка очевидно не обладает сбалансированным разложением в произведение двух сомножителей (ни над каким полем).

Пример 4 также показывает, что в следствии 2 нельзя исключить условие $k > 2$, а в следствии 1(а), нельзя заменить тройку на двойку. Следующий пример показывает, что в следствии 1(б) нельзя заменить пятёрку на меньшее число.

Пример 5. Как уже отмечалось (смотрите пример 1), в двумерной алгебре $A = \mathbb{F}_3[x]/(x^2)$ элемент $1+x$ не допускает уравновешенного разложения на три сомножителя. В той же алгебре (как и просто в поле $\mathbb{F}_3$) минус единица не допускает, очевидно, уравновешенного разложения в произведение четырёх сомножителей, а единица не имеет уравновешенных разложений в произведение двух сомножителей.

Пример 6. В поле $\mathbb{F}_2$ единица, разумеется, не допускает сбалансированных разложений в произведение пяти сомножителей. Этот простой пример показывает, что условие на характеристику не может быть отброшено в следствии 1(б) (и в теореме 0).

ГЛАВА 17.
УРАВНОВЕШЕННЫЕ РАЗЛОЖЕНИЯ НА МНОЖИТЕЛИ В НЕКОТОРЫХ АЛГЕБРАХ

0. Введение

> *„Покажите, что всякое рациональное число можно разложить в произведение нескольких рациональных чисел, сумма которых равна нулю.“*

Эта задача предлагалась на Казахстанской республиканской олимпиаде для школьников в 2013 году [Вас13]. Аналогичный вопрос для произвольного поля характеристики не два предлагался на студенческой олимпиаде по алгебре в МГУ в 2014 году [Вас14]. Задача рассматривалась и раньше [Ива13] (также в контексте работы со способными школьниками).

Вопрос о наличии таких *уравновешенных* разложений (то есть разложения в произведение нескольких множителей, сумма которых равна нулю) решается легко в любом поле характеристики не два. Гораздо труднее выяснить, сколько множителей могут содержать такие уравновешенные разложения. На самом деле (см. [KV16]),

> *в любом поле характеристики не два каждый элемент допускает уравновешенное разложение в произведение k сомножителей для каждого $k \geqslant 5$. (А для каждого $k < 5$ найдётся поле, в котором это утверждение перестаёт быть верным.)*

При $k < 5$ вопрос становится более тонким, например, в поле рациональных чисел не всякий элемент допускает уравновешенное разложение в произведение трёх множителей [Ива13], а вопрос о четырёх множителях оставался открытым*). В [Ива13] приводится следующее письмо М. А. Цфасмана А. В. Иванищуку:

> $3 = (363/70) \cdot (20/77) \cdot (-49/110) \cdot (-5)$. *Уф...*
>
> *Ваш М.А.*

Это письмо содержит (первое открытое) уравновешенное разложение тройки в произведение четырёх множителей в поле рациональных чисел. Аналогичные разложения для единицы и двойки выглядят не так впечатляюще: $1 = 1 \cdot 1 \cdot (-1) \cdot (-1)$ и $2 = \frac{1}{6} \cdot \frac{9}{2} \cdot (-\frac{2}{3}) \cdot (-4)$. Статья [Ива13] содержит полученные с помощью компьютера уравновешенные разложения первых пятидесяти натуральных чисел в произведение четырёх рациональных множителей.

Мы доказываем, что любое рациональное число допускает уравновешенное разложение в произведение четырёх рациональных сомножителей.*)

Более того, имеет место следующая теорема, отвечающая на два вопроса из [KV16] (один из которых был известен и раньше [Ива13]).

Теорема 1. *Во всяком поле характеристики не два и не три, кроме пятиэлементного поля $\mathbb{F}_5$, каждый элемент допускает уравновешенное разложение в произведение четырёх множителей; если это поле бесконечно, то каждый элемент допускает бесконечно много таких разложений.*

Автор просит не считать эту теорему частью результатов диссертации (по причинам, описанным в сноске), но советует читателям заглянуть в доказательство, состоящее из красивой явной формулы для таких разложений.

Следующая теорема из [KV16] описывает для каждого k все конечные поля, в которых каждый элемент допускает уравновешенное разложение в произведение k множителей.

---

*) Как позже выяснилось, задачу решил ещё Эйлер! Но полученная нами формула для разложения значительно проще и эйлеровой, и вообще всех известных, смотрите
`https://mathoverflow.net/q/268336/24165` и `https://mathoverflow.net/a/302958/24165` .

Теорема об уравновешенных разложениях в конечных полях [KV16]. *Пусть $k \geqslant 2$ — целое число и F — конечное поле. В поле F всякий элемент можно разложить в произведение k сомножителей, сумма которых равна нулю, тогда и только тогда, когда*

либо $|F| = 2$ и k чётно,
либо $|F| = 4$ и $k \neq 3$,
либо $|F|$ — степень двойки, но не двойка и не четвёрка (и k любое),
либо $|F| \in \{3, 5\}$ и $k \notin \{2, 4\}$,
либо $|F| = 7$ и $k \notin \{2, 3\}$,
либо $|F|$ не степень двойки, не три, не пять и не семь и $k \neq 2$.

Другими словами, ситуация в конечных полях такая:

	$k=2$	$k=3$	$k=4$	$k=5,7,9,\ldots$	$k=6,8,10,\ldots$
$\mathbb{F}_2$	да	нет	да	нет	да
$\mathbb{F}_3$	нет	да	нет	да	да
$\mathbb{F}_4$	да	нет	да	да	да
$\mathbb{F}_5$	нет	да	нет	да	да
$\mathbb{F}_7$	нет	нет	да	да	да
$\mathbb{F}_8, \mathbb{F}_{16}, \mathbb{F}_{32}, \mathbb{F}_{64}, \ldots$	да	да	да	да	да
$\mathbb{F}_9, \mathbb{F}_{11}, \mathbb{F}_{13}, \mathbb{F}_{17}, \ldots$	нет	да	да	да	да

Таблица 1

Следующая теорема дополняет этот результат из [KV16].

Теорема 2. *Пусть $k, n \geqslant 2$ — целые числа и F — конечное поле. Каждая матрица $n \times n$ над полем F раскладывается в произведение k коммутирующих матриц, сумма которых равна нулю, тогда и только тогда, когда либо $k = 3$ и $|F| = 5$, либо $k = 3$ и $|F| \geqslant 8$, либо $k = 4$ и $|F| = 4$, либо $k = 4$ и $|F| \geqslant 7$, либо $k \geqslant 5$ и $|F| \geqslant 3$.*
Другими словами, ситуация в матричных алгебрах над конечными полями такая (на верхние индексы пока не нужно обращать внимание):

	$k=2$	$k=3$	$k=4$	$k=5,6,7,8,\ldots$
$\mathbb{F}_2$	нет^1	нет^0	нет^2	нет^2
$\mathbb{F}_3$	нет^1	нет^8	нет^0	да^{3,4}
$\mathbb{F}_4, \mathbb{F}_7$	нет^1	нет^0	да^{5,7}	да^{3,4,5,7}
$\mathbb{F}_5$	нет^1	да^5	нет^0	да^{3,4}
$\mathbb{F}_8, \mathbb{F}_9, \mathbb{F}_{11}\mathbb{F}_{13}\mathbb{F}_{16}, \ldots$	нет^1	да^{5,6}	да^{5,7}	да^{3,4,5,7}

Таблица 2

Обратите внимание, что от размера матриц ответ не зависит, если этот размер по крайней мере двойка.

В первом параграфе мы доказываем теорему 1 и ещё одну теорему о конечных полях (теорема 3), которая играет ключевую роль в доказательстве теоремы 2. Все рассуждения первого параграфа вполне элементарны, за исключением того, что доказательство теоремы 3 существенно опирается на результаты работы [KV16] (которые, в свою очередь, опираются на теорию эллиптических кривых). Во втором параграфе мы доказываем теорему 2.

Обозначения, которые мы используем в целом стандартны. Отметим только, что символ $\mathbb{F}_q$ обозначает поле из q элементов, а буква E всегда обозначает единичную матрицу.

1. Поля

Доказательство теоремы 1. Имеет место тождество

$$x = \frac{2(1-4x)^2}{3(1+8x)} \cdot \frac{-(1+8x)}{6} \cdot \frac{-(1+8x)}{2(1-4x)} \cdot \frac{18x}{(1-4x)(1+8x)}.$$

Мы можем только предложить читателю проверить непосредственно это тождество и тот факт, что сумма множителей равна нулю. В исключительных случаях, когда знаменатели обращаются в ноль, то есть при $x \in \{\frac{1}{4}, -\frac{1}{8}\}$, следует умножить x на y^4, подобрав y так, чтобы $xy^4 \notin \{\frac{1}{4}, -\frac{1}{8}, 0\}$ (в любом поле характеристики не два и не три, кроме $\mathbb{F}_5$, это возможно), написать аналогичное разложение для xy^4 и потом разделить каждый сомножитель на y:

$$x = \frac{2(1-4xy^4)^2}{3y(1+8xy^4)} \cdot \frac{-(1+8xy^4)}{6y} \cdot \frac{-(1+8xy^4)}{2y(1-4xy^4)} \cdot \frac{18xy^4}{y(1-4xy^4)(1+8xy^4)}.$$

Таким образом мы получаем уравновешенное разложение любого элемента в произведение четырёх множителей. Бесконечность числа таких разложений в случае бесконечного поля вытекает из последнего тождества и следующего элементарного факта, доказательство которого мы оставляем читателям в качестве упражнения:

не равная константе рациональная дробь над бесконечным полем принимает бесконечное число значений.

(Отметим, что, например, второй сомножитель в последнем тождестве при каждом x представляет собой не равную константе рациональную дробь $f(y)$.) Это завершает доказательство теоремы. Поле из пяти элементов действительно является исключением, как видно из таблицы 1.

Аналогичным образом можно получить бесконечно много уравновешенных разложений в произведение любого большего числа сомножителей, то есть

в любом бесконечном поле характеристики не два каждый элемент допускает бесконечно много уравновешенных разложений в произведение k сомножителей для каждого $k \geqslant 5$.

Например, следующее тождество получается лёгкой модификацией из тождества, приведённого в [KV16], и даёт бесконечно много уравновешенных разложений произвольного ненулевого элемента бесконечного поля характеристики не два в произведение 2017-ти сомножителей:

$$x = \frac{xy^{2016}}{2} \cdot \frac{xy^{2016}}{2} \cdot (-xy^{2016}) \cdot \frac{2}{xy^{2018}} \cdot \left(-\frac{2}{xy^{2018}}\right) \cdot \left(\frac{1}{y}\right)^{1006} \cdot \left(-\frac{1}{y}\right)^{1006}.$$

Разложение на множители $x = x_1 x_2 \dots x_k$ называется *степенны́м*, если все сомножители равны друг другу: $x_1 = \dots = x_k$ [KV16].

Теорема 3. *Пусть $k \geqslant 2$ — целое число и F — конечное поле. В поле F всякий элемент допускает нестепенное уравновешенное разложение в произведение k множителей тогда и только тогда, когда*
либо $k = 3$ и $|F| = 5$, либо $k = 3$ и $|F| \geqslant 8$, либо $k = 4$ и $|F| = 4$, либо $k = 4$ и $|F| \geqslant 7$, либо $k \geqslant 5$ и $|F| \geqslant 3$.
Другими словами, ответ здесь такой же как в теореме 2 (таблица 2).

Доказательство. Верхние индексы у частиц *да* и *нет* в таблице 2 обозначают ссылку на случай доказательства ниже.
Случай 0: нет, так как в этих случаях у некоторых элементов нет никаких сбалансированных разложений (по теореме об уравновешенных разложениях в конечных полях).
Случай 1: $k = 2$ — нет. Для любого элемента a рассмотрим его уравновешенное разложение $a = xy$, $x + y = 0$. Если у поля характеристика 2, то наше разложение $a = (-x)x$ является степенным; если же характеристика конечного поля не два, то не всякий элемент является квадратом и, следовательно, не всякий элемент допускает уравновешенное разложение в произведение двух множителей.
Случай 2: $|F| = 2$ — нет. В разложении единицы могут участвовать только единицы, поэтому оно будет степенным.
Случай 3: $k = 5 + 2n$, где $n \geqslant 0$ и $\operatorname{char} F \neq 2$ — да. Здесь можно использовать универсальную формулу для уравновешенных разложений в произведение $5 + 2n$ сомножителей из [KV16]:

$$\pm a = (-a) \cdot \frac{a}{2} \cdot \frac{a}{2} \cdot \frac{2}{a} \cdot \frac{-2}{a} \cdot 1^n \cdot (-1)^n \quad (\text{при } a \neq 0).$$

$\operatorname{char} F \neq 2$, поэтому $\frac{2}{a} \neq -\frac{2}{a}$ и, значит, это разложение нестепенное. А нулевой элемент очевидно имеет уравновешенное нестепенное разложение: $0 = (-1) \cdot 1 \cdot 0^{k-2}$.
Случай 4: $k = 6 + 2n$, где $n \geqslant 0$ и $\operatorname{char} F \neq 2$ — да. Воспользуемся общей формулой для уравновешенных разложений в произведение $6 + 2n$ множителей из [KV16]: Рассмотрим ненулевое $c \in F$ такое, что $c^2 \neq a$ (такое c всегда найдётся, кроме случая, когда $F = \mathbb{F}_3$ и $a = 1$; но в этом случае всё очевидно). Положим $b = \frac{c^2 - a}{c}$. Тогда

$$\pm a = (-c) \cdot (c - b) \cdot \frac{b}{2} \cdot \frac{b}{2} \cdot \frac{2}{b} \cdot \frac{-2}{b} \cdot 1^n \cdot (-1)^n.$$

Так как $\operatorname{char} F \neq 2$, мы имеем $\frac{2}{b} \neq -\frac{2}{b}$, поэтому разложение нестепенное.
Случай 5: В этих случаях уравновешенное разложение существует по теореме об уравновешенных разложениях в конечных полях и оно не может быть степенным, поскольку число сомножителей не делится на характеристику поля.
Случай 6: $|F| \geqslant 9$, $\operatorname{char} F \neq 2$ и $k = 3$ — да.

Здесь нужно рассмотреть два случая. Если $\operatorname{char} F \neq 3$, то по теореме об уравновешенных разложениях в конечных полях уравновешенное разложение у любого элемента существует, а так как $\operatorname{char} F \neq 3$, то оно точно нестепенное.

Для доказательства в случае характеристики три нам понадобится вспомогательное утверждение.

Лемма. *В поле $\mathbb{F}_{3^n}$, где $n \geqslant 2$, существует такой ненулевой квадрат u, что $u+1$ — тоже ненулевой квадрат.*

Доказательство. Если 2 — квадрат, то $u = 1$ — искомый элемент. Иначе предположим, что для любого $u \notin \{0, 1, 2\}$ верно следующее утверждение:

$$\text{если } u \text{ — квадрат, то } u+1 \text{ — не квадрат.}$$

Тогда в любом множестве вида $\{u, u+1, u+2\}$ не более одного квадрата. Значит всего квадратов не больше $3^{n-1}+1$. С другой стороны, в поле характеристики 3 квадратов ровно $\frac{3^n+1}{2}$. Отсюда получаем неравенство $\frac{3^n+1}{2} \leqslant 3^{n-1}+1$, которое выполняется только при $n = 1$. Полученное противоречие завершает доказательство леммы.

Вернемся к доказательству теоремы 3. Итак, мы хотим показать, что в конечном поле характеристики три и порядка по крайней мере девять каждый элемент имеет уравновешенное нестепенное разложение в произведение трёх множителей.

Отметим, что в таком поле любой элемент является кубом. Будем искать сбалансированное разложение элемента $a = b^3 \neq 0$:

$$a = xyz, \quad x+y+z = 0. \quad \text{Избавляясь от } z, \text{ получаем} \quad yx^2 + y^2x + a = 0. \tag{$*$}$$

Будем решать это уравнение относительно x. По Лемме существует $\tau^2 \neq 0$ такой, что $\tau^2+1 \neq 0$ — тоже квадрат: $\tau^2+1 = \pi^2 \neq 0$. Возьмём $y = \frac{b+b\pi}{2}$. Отметим, что $y \neq b$, поскольку равенство $y = b$ означало бы, что $\pi = 1$ и $\tau = 0$. Значит дискриминант квадратного уравнения $(*)$ является квадратом:

$$D = y^4 - 4ay = y(y^3 - b^3) = y(y-b)^3 = \frac{b\pi+b}{2} \cdot \left(\frac{b\pi-b}{2}\right)^3 = (b^2(1+\tau^2) - b^2)(b\pi-b)^2 = b^2\tau^2(b\pi-b)^2$$

и у уравнения $(*)$ есть решение. Полученное разложение не будет степенным, так как $y^3 \neq a$ (поскольку $y \neq b$).

Осталось найти нестепенное уравновешенное разложение нуля, но это легко: $0 = (-1) \cdot 1 \cdot 0$.

Случай 7: $|F| = 2^n$ и $k = 4+2m$, где $m \geqslant 0$. Так как $\operatorname{char} F = 2$, любой элемент поля является квадратом: $a = b \cdot b$. Если $a \neq 1$, то $b \neq 1$ и $a = b^2 \cdot 1^{2m+2}$ — искомое разложение. Если $a = 1$, то $a = 1 = c^2 \cdot \left(\frac{1}{c}\right)^2 \cdot 1^{2m}$ — искомое разложение, где c — любой элемент, отличный от нуля и единицы.

Случай 8: $|F| = 3$ и $k = 3$ — нет. В разложении единицы не может участвовать ноль, а 1 и -1 обязаны участвовать, чтобы разложение было нестепенным. Тогда третий множитель обязан быть нулём, так как разложение уравновешенное. Это противоречие завершает доказательство теоремы 3.

2. Матрицы

Доказательство теоремы 2. Сперва заметим, что при $k = 2$ теорема верна по простой причине:

жорданова клетка J с собственным значением ноль и размера $n \times n$ не является квадратом в кольце матриц $n \times n$ при $n \geqslant 2$

(доказательство этого утверждения мы оставляем читателям в качестве простого упражнения) и, следовательно, матрица $-J$ не обладает сбалансированным разложением в произведение двух сомножителей.

В случае $k \geqslant 3$ по теореме 3 нам достаточно доказать следующее утверждение.

Теорема 2′. *Пусть $n \geqslant 2$ и $k \geqslant 3$ — целые числа и F — поле (необязательно конечное). Тогда следующие условия равносильны:*

а) каждая матрица $n \times n$ над F обладает уравновешенным разложением в произведение k коммутирующих множителей;

б) каждый элемент поля F обладает нестепенным уравновешенным разложением в произведение k множителей.

Доказательство.

Импликация *б)* $\Longrightarrow$ *а)* сразу вытекает из следующего факта, доказанного в [KV16]:

Пусть F — поле и k — натуральное число большее двух. Если во всех конечных расширениях поля F каждый элемент обладает нестепенным сбалансированным разложением в произведение k элементов, то то же верно для каждого элемента каждой конечномерной ассоциативной алгебры с единицей над F.

Импликация *а)* $\Longrightarrow$ *б)*. Заметим, что $0 \in F$ имеет нестепенное уравновешенное разложение в произведение k множителей для любого $k \geqslant 3$: $0 = 0^{k-2} \cdot 1 \cdot (-1)$. Чтобы разложить ненулевой элемент $a \in F$, нам понадобится следующий простой факт из линейной алгебры, доказательство которого мы тоже оставляем читателям в качестве упражнения:

централизатор нильпотентной жордановой клетки J размера $n \times n$ в алгебре матриц $n \times n$ состоит из многочленов от J,

то есть $C(J) = \{a_0E + a_1J + \ldots + a_{n-1}J^{n-1} \mid a_i \in F\}$.

Теперь если жорданова клетка $aE + J$ обладает сбалансированным разложением $aE + J = X_1 \ldots X_k$ в произведение коммутирующих матриц, то все эти матрицы X_i лежат в централизаторе матрицы J и, в силу упомянутого выше факта, мы получаем уравновешенное разложение элемента a в поле F:

$$a = x_1 \ldots x_k, \quad \text{где } x_i \text{ — это единственное собственное значение матрицы } X_i.$$

Остаётся заметить, что это разложение не может быть степенным при $a \neq 0$. Действительно, предположив противное, мы бы получили такое уравновешенное разложение в кольце матриц:

$$aE + J = (xE + J_1) \ldots (xE + J_k), \quad \text{где } J_i \text{ — некоторые нильпотентные коммутирующие матрицы.}$$

Уравновешенность этого разложения означает, что k делится на $\operatorname{char} F$ и $\sum J_i = 0$. Но тогда, раскрывая скобки мы получаем

$$aE + J = (xE + J_1) \ldots (xE + J_k) = aE + f(J_1, \ldots, J_k),$$

где многочлен f не имеет членов первой степени, то есть в правой части равенства стоит матрица $aE + J'$, где $(J')^{n-1} = 0$. Полученное противоречие завершает доказательство теорем $2'$ и 2.

Если не требовать никакой коммутативности, то вопрос об уравновешенных разложениях в алгебрах матриц над конечными полями остаётся открытым.

Вопрос. *При каких q, k и n верно, что всякая матрица $n \times n$ над полем из q элементов имеет уравновешенное разложение в произведение k матриц того же размера?*

Мы можем сказать лишь следующее.

1. В некоторых случаях разложение существует по теореме 2.
2. При $k = 2 \leqslant n$ разложения не существует, например, потому, что сомножители такого уравновешенного разложения обязаны коммутировать.

Кроме того, компьютерные эксперименты показывают следующие факты.

3. Над полем из двух элементов все матрицы 2×2, кроме $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$ и (подобной ей матрицы) $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$, допускают уравновешенное разложение в произведение трёх сомножителей, а эти две матрицы не имеют таких разложений.
4. Матрица $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ и две подобные ей матрицы над полем из двух элементов не имеют уравновешенных разложений в произведение четырёх множителей, а остальные матрицы 2×2 над $\mathbb{F}_2$ имеют такие разложения.
5. Матрица $\begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ и подобные ей матрицы над полем из двух элементов не имеют уравновешенных разложений в произведение трёх множителей, а остальные матрицы 3×3 над $\mathbb{F}_2$ имеют такие разложения.
6. Все матрицы 3×3 над $\mathbb{F}_2$ имеют уравновешенные разложения в произведение четырёх множителей.
7. Все матрицы 2×2 над полями $\mathbb{F}_3$, $\mathbb{F}_4$, $\mathbb{F}_5$ и $\mathbb{F}_7$ имеют уравновешенные разложения в произведение трёх и четырёх множителей. Отсюда вытекает, что и для любого большего числа множителей это верно, поскольку мы можем увеличивать количество множителей на два, умножая имеющееся разложение на E и $-E$.

ГЛАВА 18.
ФИНИТНО АППРОКСИМИРУЕМЫЕ АЛГОРИТМИЧЕСКИ КОНЕЧНЫЕ ГРУППЫ, ИХ ПОДГРУППЫ И ПРЯМЫЕ ПРОИЗВЕДЕНИЯ

0. Введение

В работе [MO11] был построен первый пример конечно порождённой рекурсивно представленной бесконечной группы, которая является *алгоритмически конечной*, в том смысле, что не существует алгоритма, выписывающего бесконечное количество попарно различных элементов этой группы. Группы, обладающие этими свойствами (то есть конечно порождённые рекурсивно представленные бесконечные и алгоритмически конечные), авторы [MO11] предлагают называть *монстрами Дэна*.

Монстры Дэна, построенные в [MO11], обладают ещё дополнительным свойством конечности-бесконечности — у них есть бесконечные финитно аппроксимируемые гомоморфные образы. В связи с этим в [MO11] был задан вопрос: *существуют ли финитно аппроксимируемые монстры Дэна?* Мы отвечаем на этот вопрос положительно,*) но задаём другой вопрос.

Вопрос 1. *Верно ли, что прямое произведение двух алгоритмически конечных групп алгоритмически конечно?*

Ответа мы не знаем (и предполагаем, что он отрицательный), но построенный в нашей работе финитно аппроксимируемый монстр обладает приятным свойством: все его конечные декартовы степени алгоритмически конечны. Ещё более интригующий, на наш взгляд, вопрос звучит так.

Вопрос 2. *Верно ли, что сплетение двух алгоритмически конечных групп алгоритмически конечно? Верно ли хотя бы, что прямое сплетение конечной группы (например, группы из двух элементов) и алгоритмически конечной группы алгоритмически конечно?*

По этому поводу мы ничего не можем сказать и не знаем даже ответа на «противоположный вопрос».

Вопрос 3. *Существует ли такой монстр Дэна D, что прямое сплетение $\mathbb{Z}_2 \wr D$ алгоритмически конечно?*

Отметим однако, что построенный в этой работе монстр в некотором смысле похож на такое сплетение — он является полупрямым произведением бесконечной элементарной абелевой нормальной подгруппы и некоторого другого монстра.

Основная теорема. *Существует бесконечная конечно порождённая рекурсивно представленная финитно аппроксимируемая группа G, все конечные декартовы степени которой алгоритмически конечны, то есть ни для какого n не существует алгоритма, выписывающего бесконечное число попарно различных элементов группы G^n.*
При этом группа G может быть выбрана содержащей в качестве нормальной подгруппы бесконечную прямую степень циклической группы $\mathbb{Z}_p$ (где p — произвольное фиксированное простое число), причём соответствующее расширение расщепляется: $G = H \leftthreetimes \left(\bigtimes\limits_{i=1}^{\infty} \langle a \rangle_p \right)$.

Сам по себе вопрос о возможных подгруппах монстров Дэна заслуживает отдельного внимания. Ясно, что все конечно порождённые подгруппы монстров сами являются алгоритмически конечными, в частности, все циклические подгруппы конечны и, следовательно, например, все разрешимые конечно порождённые подгруппы также конечны.

Вопрос 4. *Какие группы (или какие абелевы группы) могут быть вложены в алгоритмически конечные группы? Какие могут быть вложены в качестве нормальных подгрупп?*

Основную теорему мы выводим из следующего результата об алгебрах, который имеет самостоятельный интерес.

Теорема о сильно алгоритмически конечных алгебрах. *Над любым конечным полем существует бесконечная конечно порождённая рекурсивно представленная финитно аппроксимируемая ассоциативная алгебра A (с единицей), все конечные декартовы степени которой алгоритмически конечны, то есть ни для какого n не существует алгоритма, выписывающего бесконечное число попарно различных элементов алгебры A^n.*
При этом можно считать, что алгебра A порождается конечным множеством нильпотентных элементов.

Наш подход к построению монстров Дэна основан на идеях работы [MO11], то есть на использовании теоремы Голода–Шафаревича. Однако представленное здесь доказательство существования монстров Дэна проще чем в [MO11], несмотря на то, что нам приходится специально заботиться о том, чтобы построенный монстр обладал дополнительными свойствами (финитная аппроксимируемость, впрочем, получается сама собой при нашем подходе).

*) Когда эта работа была написана, мы обнаружили, что ответ на этот вопрос содержится также в статье [KhM14].

1. Признак бесконечномерности

Мы будем рассматривать свободную ассоциативную алгебру $F\langle X\rangle$ (с единицей) с конечным множеством свободных порождающих X над полем F. Эта алгебра состоит из многочленов от некоммутирующих переменных с коэффициентами из F. Под степенью $\deg u$ многочлена $u \in F\langle X\rangle$ мы будем всегда понимать минимальную из степеней мономов этого многочлена. Например, $\deg(xy - yx + xy^{2022}x) = 2$.

Следующий удобный признак бесконечномерности градуированной алгебры легко выводится из известного результата Голода–Шафаревича [ГШ64] и принадлежит, по-видимому, М.Ершову, см. [Er12], следствие 2.2.

Признак бесконечномерности. *Если в множестве R, состоящем из однородных элементов конечно порождённой свободной ассоциативной алгебры $F\langle X\rangle$ число элементов степени n равно r_n, причём $r_0 = r_1 = 0$ и ряд*

$$1 - |X|t + H_R(t) \stackrel{\text{опр}}{=} 1 - |X|t + \sum_{i=2}^{\infty} r_i t^i$$

сходится к отрицательному числу при некотором $t \in (0,1)$, то факторалгебра $A = F\langle X\rangle/(R)$ бесконечномерна.

Нам понадобится также следующий очевидный факт.

Лемма 1. *Если поле F и множество X конечны, то для любых натуральных n и d существует лишь конечное наборов $(u_{11},\dots,u_{n1}),(u_{12},\dots,u_{n2}),\dots$ длины n элементов свободной ассоциативной алгебры $F\langle X\rangle$, обладающих тем свойством, что для любых различных i и l найдётся s такое, что $\deg(u_{si} - u_{sl}) < d$.*

Доказательство. Такое неравенство означает, что все наборы представляют различные элементы алгебры $\left(F\langle X\rangle/(X)^d\right)^n$, которая, очевидно, конечна. Здесь (X) — это идеал, порождённый всеми свободными порождающими и, таким образом, $(X)^d$ состоит из всех многочленов, степень которых не меньше d.

2. Построение алгебры A

Зафиксируем натуральное число α и рекурсивную всюду определённую функцию $f : \mathbb{N}\times\mathbb{N} \to \mathbb{N}$ (по поводу конкретного выбора α и f смотрите следующий параграф) и зафиксируем также рекурсивную нумерацию $P_1, P_2, \dots$ всех программ без входа с выходным алфавитом, состоящим из элементов некоторого конечного поля F, некоторого конечного множества X, содержащего не меньше двух элементов, и трёх дополнительных символов: «+» (плюс), «,» (запятая) и «;» (точка с запятой). Выходную последовательность каждой такой программы мы будем интерпретировать как последовательность наборов элементов свободной ассоциативной алгебры $F\langle X\rangle$: элементы каждого набора разделены запятыми, а различные наборы отделяются друг от друга точками с запятой; последовательно написанные символы из $F \sqcup X$ мы интерпретируем как их произведение, лишние плюсы и запятые мы игнорируем. Например, при $F = \mathbb{Z}_3 = \{0,1,2\}$ и $X = \{x,y\}$, последовательность

$$++xy2y+,,,,221++1+++++0xy1yyy++,,;;,;xxx2112+++yxyxy22+++$$

мы понимаем как четыре набора (два из которых пустые, а один незаконченный):

$$(2xy^2, 2);\ ();\ ();\ (x^3 + yxyxy + \dots$$

Мы будем строить алгебру A в виде $A = F\langle X\rangle/(R)$. Алгоритм построения определяющих R соотношений выглядит просто.

Основной алгоритм. Сперва множество определяющих соотношений R состоит из одночленов x^α для всех $x \in X$. Далее на шаге k запускаем программу $N(k)$ (параллельно со всем, что уже работает) и переходим к шагу $k+1$.

Программа $N(k)$ (то есть программа N, получившая на вход натуральное число k) делает следующие действия.

Программа $N(k)$:

1. Запускает программу P_k (параллельно со всем, что уже работает).
2. Следит за работой программы P_k: как только программа P_k напишет точку с запятой, N делает следующее:
   а) приостанавливает работу программы P_k;
   б) проверяет, что все наборы элементов алгебры $F\langle X\rangle$, которые программа P_k выдала до сих пор, имеют одинаковую длину n, то есть на выходе программы P_k имеется последовательность вида:

   $$u_{11},\dots,u_{n1};u_{12},\dots,u_{n2};\dots;u_{1l},\dots,u_{nl};\quad \text{для некоторых } u_{ij} \in F\langle X\rangle \text{ и некоторого } n \in \mathbb{N};$$

   если это не так, то программа N выключает программу P_k и завершает свою работу;

в) проверяет, существует ли $i < l$ такое, что $\deg(u_{si} - u_{sl}) \geqslant f(n,k)$ для всех s; если нет, то программа N велит программе P_k продолжить работу и продолжает за ней следить; если же такое $i < l$ нашлось, то N переходит к следующему шагу;

г) добавляет все однородные компоненты соответствующих разностей $u_{si} - u_{sl}$ (для всех $s \in \{1, \ldots, n\}$) в множество соотношений R, выключает программу P_k и завершает свою работу.

Отметим, что в каждый момент времени у нас параллельно работает некоторое конечное число программ P_i (не более k на k-м шаге основного алгоритма) и столько же копий программы N (каждая копия следит за одной программой P_i). При этом каждая копия программы N

- либо работает вечно и ничего не добавляет в множество соотношений R,
- либо завершает свою работу на шаге 2б) и, в этом случае, также ничего не добавляет в множество соотношений R,
- либо завершает свою работу на шаге 2г) и, в этом случае, добавляет в R некоторое конечное множество однородных соотношений $w_1, w_2, \ldots$ большой степени: $\deg w_i \geqslant f(n,k)$ (где k — номер этой копии программы N); при этом число добавленных соотношений каждой конкретной степени не превосходит n. Более точно, имеет место неравенство:

$$r_i(k) \leqslant \begin{cases} 0, & \text{если } i < f(n(k),k); \\ n(k), & \text{если } i \geqslant f(n(k),k); \end{cases}$$

где $r_i(k)$ — это число соотношений степени i, которые k-я копия программы N добавляет в R, а $n(k)$ — это длина наборов, которые выписывает программа P_k (если P_k выписывает наборы разных длин или пишет что-то неправильное, или вообще ничего не пишет, то мы считаем $n(k) = \infty$).

3. Бесконечномерность алгебры A

Чтобы воспользоваться признаком бесконечномерности, надо оценить сумму ряда Голода–Шафаревича.

$$H_R(t) \stackrel{\text{опр}}{=} \sum_{i=2}^{\infty} r_i t^i = |X|t^\alpha + \sum_{k=1}^{\infty} \left(\sum_{i=2}^{\infty} r_i(k) t^i \right) \leqslant |X|t^\alpha + \sum_{k=1}^{\infty} \left(\sum_{i=f(n(k),k)}^{\infty} n(k) t^i \right) =$$

$$= |X|t^\alpha + \sum_{k=1}^{\infty} \left(t^{f(n(k),k)} n(k) \frac{1}{1-t} \right) = |X|t^\alpha + \frac{1}{1-t} \sum_{k=1}^{\infty} \left(t^{f(n(k),k)} n(k) \right).$$

Полагая $t = \frac{1}{2}$ и учитывая, что $x < 2^x$ при $x \in \mathbb{N}$, получаем

$$H_R\left(\frac{1}{2}\right) = \frac{|X|}{2^\alpha} + 2\sum_{k=1}^{\infty} \left(\frac{n(k)}{2^{f(n(k),k)}} \right) < \frac{1}{2^{\alpha - |X|}} + 2\sum_{k=1}^{\infty} \left(\frac{1}{2^{f(n(k),k) - n(k)}} \right).$$

Положим теперь $f(n,k) = n + k + 2$ и $\alpha = |X| + 1$ и получим

$$H_R\left(\frac{1}{2}\right) < \frac{1}{2} + 2\sum_{k=1}^{\infty} \left(\frac{1}{4 \cdot 2^k} \right) = 1, \quad \text{то есть} \quad 1 - \frac{1}{2}|X| + H_R\left(\frac{1}{2}\right) < 0 \quad \text{при } |X| \geqslant 4$$

и по признаку из параграфа 1 градуированная алгебра $A = F\langle X \rangle / (R)$ бесконечномерна. Разумеется, эта алгебра финитно аппроксимируема, так как всякая конечно порождённая градуированная алгебра над конечным полем аппроксимируется своими конечными факторалгебрами $A/(X)^n$.

4. Алгоритмическая конечность декартовых степеней алгебры A

Допустим, что существует программа P, выписывающая бесконечное число попарно различных элементов алгебры A^n. Разумеется, можно считать, что программа P имеет выходной алфавит $X \sqcup F \sqcup \{«+», «,», «;»\}$ и выписывает попарно различные элементы алгебры A^n в принятом у нас формате:

$$u_{11}, \ldots, u_{n1}; u_{12}, \ldots, u_{n2}; \ldots, \quad \text{где } u_{ij} \in F(X)$$

(всякая программа может быть преобразована к такому виду).

Программа P получит при нашей нумерации программ некоторый номер k, то есть $P = P_k$. Тогда на k-м шаге нашего основного алгоритма будет запущена программа $N(k)$ (параллельно с другими работающими программами), которая, в свою очередь, запустит программу $P_k = P$ и будет за ней следить. Возможно два варианта.

Случай I: $\deg(u_{si} - u_{sl}) \geqslant f(n,k)$ для некоторых различных i и l и всех s. Будем считать, что $i < l$ и l минимальное возможное с этими свойствами. Тогда после написания l-й точки с запятой программа $P = P_k$ будет приостановлена на шаге 2а) работы программы-надсмотрщика $N(k)$. Далее, на шаге 2б) и 2в) проверки завершатся успешно, а на шаге 2г) в множество определяющих соотношений R будут добавлены все однородные компоненты разностей $u_{si} - u_{sl}$ (для всех $s \in \{1, \ldots, n\}$). Это означает, что наборы $(u_{1i}, \ldots, u_{ni})$ и $(u_{1l}, \ldots, u_{nl})$, выписанные программой P, представляют один и тот же элемент алгебры A^n, противоречие.

Случай II: для любых различных i и l найдётся s такое, что $\deg(u_{si} - u_{sl}) < f(n,k)$. Этого не может быть по лемме 1.

Теорема о сильно алгоритмически конечных алгебрах доказана.

5. Доказательство основной теоремы

Возьмём алгебру A над полем вычетов $\mathbb{Z}_p$ с конечным множеством порождающих X, существование которой утверждается в теореме о сильно алгоритмически конечных алгебрах, и рассмотрим множество матриц

$$G = \begin{pmatrix} H & A \\ 0 & 1 \end{pmatrix},$$

где H — подгруппа мультипликативной группы алгебры A, порождённая элементами вида $1 + x$, где $x \in X$ (эти элементы обратимы, так как элементы множества X нильпотентны). Ясно, что G — это группа:

$$\begin{pmatrix} h & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} h' & a' \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} hh' & a + ha' \\ 0 & 1 \end{pmatrix},$$

причём G является полупрямым произведением

$$\text{нормальной подгруппы } \begin{pmatrix} 1 & A \\ 0 & 1 \end{pmatrix} \simeq \bigoplus_{i=1}^{\infty} \mathbb{Z}_p \quad \text{и ненормальной подгруппы } \begin{pmatrix} H & 0 \\ 0 & 1 \end{pmatrix} \simeq H.$$

Группа G конечно порождена ($(|X| + 1)$-порождена), она порождается матрицами $\begin{pmatrix} 1 + X & 0 \\ 0 & 1 \end{pmatrix}$ и $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, так как элементы $1 + X$ очевидным образом порождают алгебру A как кольцо. Все декартовы степени G^n алгоритмически конечны, так как все декартовы степени алгебры A алгоритмически конечны. Понятно также, что рекурсивная представленность группы G вытекает из рекурсивной представленности алгебры A. Финитная аппроксимируемость группы G также немедленно вытекает из финитной аппроксимируемости алгебры A, так как группа обратимых матриц (и алгебра всех матриц) над финитно аппроксимируемой алгеброй финитно аппроксимируема.

Основная теорема доказана.

ГЛАВА 19.
ТОЖДЕСТВА АДДИТИВНОЙ ДВОИЧНОЙ АРИФМЕТИКИ

0. Введение

На множестве чисел $\{0, 1, \ldots, q-1\} = \mathbb{Z}_q$, где q является степенью двойки, рассматриваются две естественные операции: сложение по модулю q и побитовое сложение по модулю 2. В компьютерной литературе эти операции принято обозначать `ADD` и `XOR`; они аппаратно реализованы на всех современных ЭВМ, насколько мы знаем.*)

Мы рассматриваем два естественных вопроса.

1. *Какие функции $\mathbb{Z}_q^k \to \mathbb{Z}_q$ выражаются через эти две операции?*
2. *Какие тождества связывают эти две операции?*

На первый вопрос мы даём исчерпывающий ответ (теорема 1) — простой алгоритм, позволяющий по любой функции быстро ответить, выражается ли она через `ADD` и `XOR`, и вычисляем общее число функций от k аргументов, выражающихся через эти две операции (следствие 1).

На второй вопрос явного ответа мы не даём, но доказываем, что при каждом q все тождества, связывающие `ADD` и `XOR`, следуют из конечного числа таких тождеств (теорема 2) и существует алгоритм, выписывающий такой конечный базис тождеств для любого заданного q (следствие 2). Вопрос о наличии конечного базиса тождеств интенсивно исследовался для групп, полугрупп, колец, линейных алгебр (см., например, [БаОл88], [Нейм69], [Бело99], [ВаЗе89], [Гриш99], [Зайц78], [Кеме87], [Крас90], [Латы73], [Льво73], [О70], [О89], [Щиго99], [GuKr03], [Kras09], [Speht52] и литературу там цитируемую), но «прикладная» алгебра с операциями `ADD` и `XOR` никогда не изучалась с этой точки зрения, насколько нам известно.

На алгебраическом языке теорема 1 представляет собой явное описание свободных алгебр многообразия, порождённого алгеброй $\mathbb{Z}_q$ с двумя бинарными операциями `ADD` и `XOR`, а теорема 2 утверждает, что это многообразие конечно базируемо (то есть имеет конечный базис тождеств). Необходимые сведения о многообразиях универсальных алгебр можно прочитать, например, в [БаОл88] или в [ОА91].

Обозначения, которые мы используем в целом стандартны. Отметим только, что операцию сложения по модулю q (то есть `ADD`) мы будем обозначать символом $+$, а операцию побитового сложения по модулю 2 (то есть `XOR`) мы будем обозначать символом $\oplus$. Символ a_i обозначает i-й бит числа $a \in \mathbb{Z}_q$, причём биты с отрицательными номерами считаются нулевыми. Множество $\{0, 1, \ldots, q-1\} = \mathbb{Z}_q$, рассматриваемое как универсальная алгебра с операциями $+$ и $\oplus$, мы обозначаем символом A_q. Умножение на целые числа в алгебре A_q мы всегда трактуем как умножение по модулю q. Эти умножения очевидным образом выражаются через сложение $+$, например, $3x = x + x + x$, а $-3x = (-3)x = -(3x) = \underbrace{x + x + \ldots + x}_{3(q-1)\ слагаемых}$.

1. Определения и результаты

Функцию $f\colon A_q^k \to A_q$ мы называем *алгебраической*, если она выражается через операции $+$ и $\oplus$. Более точно, множеством $F_{k,q}$ алгебраических функций от k аргументов мы называем минимальное по включению множество функций, удовлетворяющее следующим условиям:

1) функции $f(x, y, \ldots) = x$, $f(x, y, \ldots) = y, \ldots$ принадлежат $F_{k,q}$;
2) если функции f и g принадлежат $F_{k,q}$, то функции $f + g$ и $f \oplus g$ принадлежат $F_{k,q}$.

Множество $F_{k,q}$ всех алгебраических функций от k аргументов образует универсальную алгебру относительно операций $+$ и $\oplus$, которая является *свободной алгеброй ранга k многообразия, порождённого алгеброй A_q.*

Теорема 1. *Функция $f\colon A_q^k \to A_q$ является алгебраической тогда и только тогда, когда i-й бит её значения для любого i выражается через биты аргументов при помощи формулы вида*

$$(f(x, y, \ldots))_i = g(x_i, y_i, \ldots; x_{i-1}, y_{i-1}, \ldots; x_{i-2}, y_{i-2}, \ldots; \ldots) \qquad (*)$$

(биты с отрицательными номерами считаются нулевыми), где g — некоторый не зависящий от i многочлен (Жегалкина) без свободного члена над $\mathbb{Z}_2$, вес которого не превосходит единицы.

Весом или *приведённой степенью* многочлена от переменных $x_i, y_i, \ldots, x_{i-1}, y_{i-1}, \ldots, x_{i-2}, y_{i-2}, \ldots$ мы называем максимум весов его мономов, под весом монома мы понимаем сумму весов входящих в него переменных, а под весом переменных $x_{i-l}, y_{i-l}, \ldots$ мы понимаем число 2^{-l}. (Здесь i считается формальным параметром.)

*) Команду `ADD` называют обычно просто сложением, поскольку она используется чаще всего для получения обычной суммы натуральных чисел, однако в действительности процессор выполняет сложение по некоторому большому модулю q (например, $q = 2^{32}$ для 32-разрядных процессоров и т.д.).

Пример 1. Если $q = 8$ и $k = 1$, то имеется всего четыре монома Жегалкина вес которых не превосходит единицы: x_i (вес 1), x_{i-1} (вес $\frac{1}{2}$), x_{i-2} (вес $\frac{1}{4}$) и $x_{i-1}x_{i-2}$ (вес $\frac{3}{4}$). (Здесь мы пользуемся тем, что степень монома Жегалкина по каждой переменной не превосходит единицы.) Следовательно, имеется 2^4 многочленов веса не больше единицы. Таким образом, алгебра $F_{1,8}$ состоит из шестнадцати элементов. Например, алгебраическая функция, соответствующая многочлену Жегалкина $x_i \oplus x_{i-1}x_{i-2}$ имеет вид

$$f(x) = f(x_0,\ x_1,\ x_2) = (x_0 \oplus x_{-1}x_{-2},\ x_1 \oplus x_0x_{-1},\ x_2 \oplus x_1x_0) = (x_0,\ x_1,\ x_2 \oplus x_1x_0)$$

(поскольку биты с отрицательными номерами считаются нулевыми). Другими словами,

$$f(0) = 0, \quad f(1) = 1, \quad f(2) = 2, \quad f(3) = 7, \quad f(4) = 4, \quad f(5) = 5, \quad f(6) = 6, \quad f(7) = 3.$$

Теорема 1 позволяет построить следующий простой

АЛГОРИТМ, выясняющий по данной функции $f\colon \mathbb{Z}_{2^\varkappa}^k \to \mathbb{Z}_{2^\varkappa}$, является ли она алгебраической (то есть выражается ли она через `ADD` и `XOR`).

1. Записать старший бит $(f(x, y, \ldots))_{\varkappa-1}$ значения функции f в виде многочлена Жегалкина $g_{\varkappa-1}(x_0, y_0, \ldots, x_1, y_1, \ldots)$ от битов аргументов и проверить, что вес этого многочлена (для $i = \varkappa - 1$) не превосходит единицы и свободный член нулевой. Если вес больше или свободный член ненулевой, то завершить программу с ответом `НЕТ`.
2. Сделать в многочлене $g_{\varkappa-1}$ следующие подстановки:

$$x_0 \to 0,\ x_1 \to x_0,\ x_2 \to x_1, \ldots,\ x_{\varkappa-1} \to x_{\varkappa-2},\ y_0 \to 0,\ y_1 \to y_0,\ y_2 \to y_1, \ldots,\ y_{\varkappa-1} \to y_{\varkappa-2}, \ldots \qquad (**)$$

и проверить, совпадает ли полученный многочлен $g_{\varkappa-2}$ с многочленом, задающим $(\varkappa-2)$-й бит функции f. Если нет, то завершить программу с ответом `НЕТ`; если да, то продолжить.

$\ldots \quad \ldots \quad \ldots$

$\varkappa - 1$. Сделать в многочлене g_2 подстановки $(**)$ и проверить, совпадает ли полученный многочлен g_1 с многочленом, задающим первый бит функции f. Если нет, то завершить программу с ответом `НЕТ`; если да, то продолжить.

$\varkappa$. Сделать в многочлене g_1 подстановки $(**)$ и проверить, совпадает ли полученный многочлен g_0 с многочленом, задающим младший бит функции f. Если нет, то завершить программу с ответом `НЕТ`; если да, то завершить программу с ответом `ДА`.

Понятно, что этот алгоритм легко сделать однородным по $\varkappa$.

Например, функция умножения двух чисел по модулю q не выражается через `ADD` и `XOR` (наш алгоритм оборвётся на первом шаге из-за условия на вес), что, конечно, неудивительно. Однако функция одного аргумента $x \mapsto xy$ при каждом фиксированном $y \in \mathbb{Z}_q$ является алгебраической, как уже отмечалось.

Доказательство теоремы 1 конструктивное и оно даёт некоторый алгоритм, позволяющий выразить данную функцию f через `ADD` и `XOR` (при условии, что она выражается), но этот алгоритм далеко не такой простой и быстрый.

Пример 1 нетрудно обобщить, пересчитав мономы при произвольных q и k, и получить следующее утверждение.

Следствие 1. *Свободная алгебра $F_{k,q}$ состоит из*

$$2^{\frac{1}{k!}(\frac{q}{2}+1)(\frac{q}{2}+2)\ldots(\frac{q}{2}+k)-1} \qquad (1)$$

элементов.

Доказательство. В случае $k = 1$ имеется ровно $\frac{q}{2}$ мономов веса не больше единицы. Действительно, в силу однозначности двоичного разложения числа существует ровно один моном каждого веса $s \cdot \frac{2}{q}$, где $s \in \{1, 2, \ldots, \frac{q}{2}\}$. А именно, моном

$$x_{i-l_1}x_{i-l_2}\ldots x_{i-l_p}, \quad \text{где} \quad s = 2^{\varkappa-1-l_1} + 2^{\varkappa-1-l_2} + \ldots + 2^{\varkappa-1-l_p}, \quad \text{а } 2^\varkappa = q.$$

Отсюда следует, что число мономов веса не больше единицы при произвольном целом k совпадает с числом ненулевых наборов неотрицательных целых чисел $(n_1, \ldots, n_k)$, сумма которых не превосходит $\frac{q}{2}$ (здесь, $n_i \cdot \frac{2}{q}$ — это вес относительно i-й переменной). Количество таких наборов, как известно, равно

$$\frac{(\frac{q}{2}+1)(\frac{q}{2}+2)\ldots(\frac{q}{2}+k)}{k!} - 1.$$

Значит, общее количество многочленов веса не больше единицы задаётся формулой (1).

Следующее утверждение представляет собой переформулировку теоремы 1.

Теорема 1′. *Функция $f\colon A_q^k \to A_q$ является алгебраической тогда и только тогда, когда она может быть записана в виде*

$$f(x,y,\ldots) = \bigoplus_i \left((2^{k_{i,1}}x) \odot (2^{k_{i,2}}x) \odot \ldots \odot (2^{l_{i,1}}y) \odot (2^{l_{i,2}}y) \odot \ldots\right),$$

где для каждого i имеет место неравенство $2^{-k_{i,1}} + 2^{-k_{i,2}} + \ldots + 2^{-l_{i,1}} + 2^{-l_{i,2}} + \ldots \leqslant 1$.

Здесь и далее символ $\odot$ обозначает побитовое умножение по модулю два (конъюнкцию).

Что касается тождеств, в первую очередь можно заметить, что относительно каждой из операций $+$ и $\oplus$ алгебра A_q является абелевой группой экспоненты q и 2, соответственно. Поэтому все тождества, включающие только одну из двух операций являются следствиями следующей системы тождеств:

$$(x+y)+z = x+(y+z),\ x+qy = x,\ x+y = y+x, \quad (x\oplus y)\oplus z = x\oplus(y\oplus z),\ x\oplus(y\oplus y) = x,\ x\oplus y = y\oplus x.$$

С тождествами, включающими обе операции, дело обстоит сложнее. Простейшим примером такого рода может служить тождество $qx = x \oplus x$, выражающее тот факт, что нулевые элементы двух групповых структур совпадают. Менее тривиальный пример тождества выглядит так: $\frac{q}{2}(x+y) = \frac{q}{2}(x\oplus y)$ (это тождество выражает то, что сложения $+$ и $\oplus$ совпадают в младшем бите).

Теорема 2. *Для любой целой степени двойки q алгебра A_q обладает конечным базисом тождеств. Более того, алгебра A_q порождает шпехтово многообразие.**)

Конечность алгебры сама по себе не влечёт конечности базиса её тождеств. Конечным базисом тождеств обладает каждая конечная группа [ОаРо64] (см. также [Неим69]), каждое конечное ассоциативное или лиево кольцо ([Льво73], [Kruse73], [БаОл75]), но не каждая конечная полугруппа и не каждое конечное кольцо (см. [БаОл88]).

Для доказательства теоремы 2 мы используем не столько конечность, сколько хорошо известные соображения нильпотентности. Например, известно, что конечным базисом тождеств обладает всякое нильпотентное кольцо (то есть кольцо, в котором все достаточно длинные произведения равны нулю) и всякая нильпотентная группа (то есть группа, в которой все достаточно длинные кратные коммутаторы равны единице) (см. [Неим69]). Алгебра A_q не является конечно же ни группой, ни кольцом. Однако оказывается, что эта алгебра *рационально эквивалентна* (в смысле Мальцева) некоторому нильпотентному кольцу, то есть на алгебре A_q можно ввести структуру нильпотентного кольца так, что сложение и умножение кольца будут выражаться через операции $+$ и $\oplus$ и наоборот: операции $+$ и $\oplus$ будут выражаться через сложение и умножение этого кольца.

Теорема 3. *Алгебра A_q рациональна эквивалентна нильпотентному коммутативному неассоциативному кольцу $(\mathbb{Z}_q, \oplus, \circ)$. Сложение $\oplus$ есть обычное побитовое сложение по модулю два, умножение $\circ$ определяется следующей формулой $x \circ y = 2(x \odot y)$, где $\odot$ — побитовое умножение по модулю два (конъюнкция), а умножение на два есть умножение на два по модулю q, то есть сдвиг разрядов.*

В следующем параграфе мы доказываем теорему 1. В параграфе 3 мы доказываем теорему 3, из которой теорема 2 немедленно вытекает в силу упомянутой выше конечной базируемости тождеств нильпотентных колец.

2. Доказательство теоремы 1

Коммутатором элементов $x, y \in A_q$ назовем элемент $[x,y] \stackrel{\text{опр}}{=} x \oplus y \oplus (x+y)$. Коммутатор представляет собой разницу между суммой $\oplus$ и суммой $+$ двух элементов; i-й бит коммутатора $[x,y]$ — это перенос в i-й разряд при суммировании $x+y$ «в столбик».

Следующая хорошо известная лемма широко используется в электронных сумматорах.

Утверждение 1. *Для битов коммутатора имеет место равенство*

$$[x,y]_i = x_{i-1}y_{i-1} \oplus [x,y]_{i-1}(x_{i-1} \oplus y_{i-1}). \tag{2}$$

Доказательство. Перенос $c_i = [x,y]_i$ в i-й разряд образуется следующим образом:

$$c_i = \begin{cases} 1, & \text{если среди трёх битов } x_{i-1}, y_{i-1}, c_{i-1} \text{ большинство (то есть два или три) составляют единицы;} \\ 0, & \text{если среди трёх битов } x_{i-1}, y_{i-1}, c_{i-1} \text{ большинство составляют нули.} \end{cases}$$

В виде многочлена Жегалкина эта булева функция записывается так:

$$c_i = x_{i-1}y_{i-1} \oplus y_{i-1}c_{i-1} \oplus c_{i-1}x_{i-1} = x_{i-1}y_{i-1} \oplus c_{i-1}(x_{i-1} \oplus y_{i-1}),$$

*) Это значит, что любая алгебра сигнатуры $(+, \oplus)$, в которой выполнены все тождества алгебры A_q, имеет конечный базис тождеств.

что и требовалось.

Формулу (2) можно переписать в виде $[x,y] = 2(x \odot y \oplus [x,y] \odot (x \oplus y))$ или (воспользовавшись дистрибутивностью умножения на двойку относительно $\odot$ и $\oplus$ и дистрибутивностью $\odot$ относительно $\oplus$) в виде

$$(2x) \odot (2y) = [x,y] \oplus (2[x,y]) \odot (2x) \oplus (2[x,y]) \odot (2y). \qquad (2')$$

С помощью формулы (2) нетрудно показать, что i-й бит суммы $x + y = x \oplus y \oplus [x,y]$ записывается в виде многочлена Жегалкина от битов слагаемых следующим образом:

$$(x+y)_i = x_i \oplus y_i \oplus x_{i-1}y_{i-1} \oplus x_{i-1}x_{i-2}y_{i-2} \oplus y_{i-1}x_{i-2}y_{i-2} \oplus \ldots = \textit{сумма всех мономов веса } 1. \qquad (2'')$$

Приступим к доказательству теоремы 1. Пусть M — множество всех функций $A_q^k \to A_q$ вида $(*)$. Необходимо доказать два утверждения.

1. Любая функция из $F_{k,q}$ принадлежит M;
2. Любая функция из M принадлежит $F_{k,q}$.

Первое утверждение проверяется непосредственно. Функции $f(x,y,\ldots) = x$, $f(x,y,\ldots) = y, \ldots$ принадлежат M, так как соответствующие многочлены Жегалкина x_i, $y_i, \ldots$ имеют вес один. Допустим, что функции $f(x,y,\ldots)$ и $g(x,y,\ldots)$ лежат в M, то есть

$$(f(x,y,\ldots))_i = F(x_i,y_i,\ldots;x_{i-1},y_{i-1},\ldots;\ldots), \quad (g(x,y,\ldots))_i = G(x_i,y_i,\ldots;x_{i-1},y_{i-1},\ldots;\ldots),$$

где F и G — многочлены Жегалкина веса не больше единицы и без свободного члена. Тогда

$$(f(x,y,\ldots) \oplus g(x,y,\ldots))_i = F(x_i,y_i,\ldots;x_{i-1},y_{i-1},\ldots;\ldots) \oplus G(x_i,y_i,\ldots;x_{i-1},y_{i-1},\ldots;\ldots)$$

и вес многочлена Жегалкина, стоящего в правой части этого равенства, не превосходит, стало быть, единицы, то есть $f \oplus g \in M$. Для функции $f + g$ i-й бит, согласно формуле $(2'')$, записывается следующим образом:

$$(f+g)_i = F \oplus G \oplus F'G' \oplus F'F''G'' \oplus F''G'G'' \oplus \ldots,$$

где многочлен H' получается из многочлена $H = H(x_i,y_i,\ldots;x_{i-1},y_{i-1},\ldots;\ldots)$, сдвигом всех битов:

$$H'(x_i,y_i,\ldots;x_{i-1},y_{i-1},\ldots;\ldots) = H(x_{i-1},y_{i-1},\ldots;x_{i-2},y_{i-2},\ldots;\ldots).$$

Вес многочлена H' по крайней мере вдвое меньше, чем вес многочлена H. Поэтому вес многочлена

$$F \oplus G \oplus F'G' \oplus F'F''G'' \oplus F''G'G'' \oplus \ldots$$

не превосходит единицы и $f + g \in M$.

Оставшаяся часть параграфа посвящена доказательству второго утверждения.

Кратные коммутаторы сложности n определим индуктивно как следующие формальные выражения от переменных $x, y, \ldots$:

каждую из этих переменных будем считать кратным коммутатором сложности 1;

выражение $[u,v]$ назовём кратным коммутатором сложности n, если выражения u и v являются кратными коммутаторами и сумма их сложностей есть n.

Очевидная индукция показывает, что кратный коммутатор равен нулю, если хотя бы одна из переменных, входящих в него, равна нулю.

Глубину $d(w)$ кратного коммутатора w также определим индуктивно:

$d(x) = 0$, если x — переменная;

$d([u,v]) = \max(d(u),d(v)) + 1$.

Например, кратный коммутатор $[[x,y],[[z,t],x]]$ имеет сложность 5 и глубину 3.

Лемма 1. *В кратном коммутаторе биты с номерами, меньшими чем его глубина, равны нулю.*

Доказательство. Индукция по глубине. При глубине 1 утверждение верно. Если в кратных коммутаторах u и v равны нулю $d(u)$ и $d(v)$ младших битов, соответственно, то по формуле (2) мы получаем, в $[u,v]$ равны нулю $\max(d(u),d(v)) + 1$ младших битов, что и требовалось.

Лемма 2. *Кратный коммутатор сложности* $\geqslant 2^n$ *имеет глубину не меньше* n.

Доказательство. Докажем это индукцией по n. Действительно, кратный коммутатор сложности 1 (то есть переменная) имеет глубину 0. Кратный коммутатор w сложности $\geqslant 2^n$, где $n \geqslant 1$, имеет вид $w = [u,v]$. При этом хотя бы хотя бы один из кратных коммутаторов u или v имеет сложность $\geqslant 2^{n-1}$ (иначе у w сложность была бы меньше 2^n). По предположению индукции, глубина этого кратного коммутатора не меньше $n-1$, а это значит, что глубина w не меньше n по определению глубины.

Лемма 3. *В A_q любой кратный коммутатор сложности $\geqslant q$ равен нулю.*

Доказательство. По лемме 2 глубина такого кратного коммутатора не меньше $\log_2 q$ и, следовательно, по лемме 1 все биты этого кратного коммутатора нулевые.

Доказательство теоремы 1′. Достаточно доказать, что произвольное выражение

$$(2^{k_1}x)\odot(2^{k_2}x)\odot\ldots\odot(2^{l_1}y)\odot(2^{l_2}y)\odot\ldots,\quad\text{где}\quad 2^{-k_{i,1}}+2^{-k_{i,2}}+\ldots+2^{-l_{i,1}}+2^{-l_{i,2}}+\ldots\leqslant 1,$$

выражается через операции $\oplus$ и $+$. Мы будем доказывать более общий факт: *всякое выражение вида*

$$f=(2^k u)\odot(2^l v)\odot(2^m w)\odot\ldots,\quad \text{где } 2^{-k}+2^{-l}+2^{-m}+\ldots\leqslant 1,\ \text{а } u,v,w,\ldots \text{ — кратные коммутаторы} \tag{3}$$

(а не только переменные), выражается через операции $\oplus$ и $+$ (от переменных).

Допустим противное. Тогда найдётся выражение вида (3), не выражающихся через $\oplus$ и $+$, и в котором неравенство превращается в равенство:

$$2^{-k}+2^{-l}+2^{-m}+\ldots=1, \tag{4}$$

Это следует из того, что $1-(2^{-k}+2^{-l}+2^{-m}+\ldots)$ представляет собой дробь вида $\frac{s}{2^k}$, где k — максимальное из чисел $k,l,m,\ldots$, а значит выражение

$$f\odot\underbrace{(2^k u)\odot(2^k u)\odot\ldots\odot(2^k u)}_{s\text{ сомножителей}}$$

задаёт ту же функцию, что f, но неравенство превращается в равенство. Заметим, что $2x=[x,x]$ и, следовательно, $2^k u$ есть кратный коммутатор, если u есть кратный коммутатор.

Выберем из всех неалгебраических (не выражающихся через $\oplus$ и $+$) выражений (3), удовлетворяющих равенству (4), минимальные по числу сомножителей, а из всех минимальных по числу сомножителей выражений, выберем выражение с максимальной суммарной сложностью коммутаторов $u,v,w,\ldots$. Такое выражение f существует по лемме 3.

Число сомножителей в этом выражении, разумеется, больше единицы, так как кратный коммутатор выражается через $\oplus$ и $+$ по определению. Далее, из равенства (4) следует, что два самых больших среди показателей $k,l,m,\ldots$ равны. Будем считать, что $k=l$.

Воспользовавшись тождеством $(2')$, мы получаем

$$\begin{aligned}(2^k u)\odot(2^k v)&=(2\cdot 2^{k-1}u)\odot(2\cdot 2^{k-1}v)=\\&=[2^{k-1}u,2^{k-1}v]\oplus(2[2^{k-1}u,2^{k-1}v])\odot(2\odot 2^{k-1}u)\oplus(2[2^{k-1}u,2^{k-1}v])\odot(2\cdot 2^{k-1}v)=\\&=2^{k-1}[u,v]\oplus(2^k[u,v])\cdot(2^k u)\oplus(2^k[u,v])\odot(2^k v)\end{aligned}$$

Следовательно, выражение (3) переписывается в виде суммы трёх слагаемых:

$$f=\Big((2^{k-1}t)\odot(2^m w)\odot\ldots\Big)\oplus\Big((2^k t)\odot(2^k u)\odot(2^m w)\odot\ldots\Big)\oplus\Big((2^k t)\odot(2^k v)\odot(2^m w)\odot\ldots\Big),\quad\text{где } t=[u,v].$$

Каждое из этих слагаемых удовлетворяет равенству (4).

Первое слагаемое алгебраическое, так как его длина меньше, чем у исходного выражения f, которое по построению является минимальным по длине среди неалгебраических выражений (3), удовлетворяющих равенству (4).

Второе и третье слагаемые имеют ту же длину, что f, но их сложность больше (так как сложность коммутатора $t=[u,v]$ на единицу больше суммы сложностей u и v). Следовательно, они также являются алгебраическими по выбору f. Таким образом, выражение f алгебраично, как сумма трёх алгебраических слагаемых. Полученное противоречие завершает доказательство теоремы $1'$ (а значит, и теоремы 1).

3. Доказательство теорем 3 и 2

Для доказательства теоремы 3 заметим, что алгебра $\mathbb{Z}_q$ с операциями $\oplus$ и $\circ$ действительно является нильпотентным коммутативным неассоциативным кольцом. Коммутативность умножения $\circ$ очевидны, дистрибутивность умножения относительно сложения $\oplus$ — тоже, нильпотентность также имеется: $((\dots(x\circ y)\circ z)\circ\dots=0$, если число сомножителей не меньше $\log_2 q$. Заметим, что ступень нильпотентности этого кольца обычно больше, чем $\log_2 q$, но она не превосходит q, то есть произведение любых q элементов (с любой расстановкой скобок) равно нулю. Это доказывается аналогично лемме два (глубина не меньше логарифма от длины для любой расстановки скобок).

Умножение $x\circ y=2(x\odot y)=(2x)\odot(2y)$ выражается через $+$ и $\oplus$ по теореме $1'$. Осталось доказать, что сложение $+$ выражается через кольцевые операции $\oplus$ и $\circ$.

Заметим, что сложение $+$ выражается через коммутатор и $\oplus$ (по определению коммутатора): $x+y=x\oplus y\oplus[x,y]$. Поэтому достаточно выразить коммутатор через $\oplus$ и $\circ$.

Лемма 4. *Для любого натурального k коммутатор $[x,y]$ может быть записан в виде*

$$[x,y]=f_k(x,y)\oplus\underbrace{[x,y]\circ(x\oplus y)\circ(x\oplus y)\circ\dots\circ(x\oplus y)}_{k+1\ \text{сомножитель}},\tag{5}$$

где f_k — многочлен (в смысле умножения $\circ$ и сложения $\oplus$). Здесь и далее мы считаем, что в кратных произведениях все скобки сдвинуты влево, например, $a\circ b\circ c\circ d\overset{\text{опр}}{=}((a\circ b)\circ c)\circ d$.

Доказательство. При $k=1$ нужное разложение даёт тождество $(2')$:

$$[x,y]=x\circ y\oplus[x,y]\circ(x\oplus y).\tag{6}$$

Далее по индукции: имея при некотором k тождество (5), мы подставляем в его правую часть тождество (6) и получаем

$$\begin{aligned}[x,y]&=f_k(x,y)\oplus(x\circ y\oplus[x,y]\circ(x\oplus y))\circ(x\oplus y)\circ(x\oplus y)\circ\dots\circ(x\oplus y)=\\&=\underbrace{f_k(x,y)\oplus x\circ y\circ(x\oplus y)\circ(x\oplus y)\circ\dots\circ(x\oplus y)}_{f_{k+1}(x,y)}\oplus\underbrace{[x,y]\circ(x\oplus y)\circ(x\oplus y)\circ(x\oplus y)\circ\dots\circ(x\oplus y)}_{k+2\ \text{сомножителя}},\end{aligned}$$

что и требовалось.

Применяя лемму 4 при $k=\log_2 q$ и пользуясь нильпотентностью кольца, мы получаем выражение коммутатора через $\oplus$ и $\circ$, а именно, $[x,y]=f_{\log_2 q}(x,y)$. Теорема 3 доказана.

Теорема 2 немедленно вытекает из теоремы 3 и следующего хорошо известного утверждения.

Теорема (см. [БаОл88]). *Каждое нильпотентное кольцо обладает конечным базисом тождеств.*

Замечание. Доказательство теоремы о конечной базируемости тождеств нильпотентного кольца показывает, что все тождества такого кольца следуют из тождеств, включающих не более n переменных, где n — степень нильпотентности, то есть такое число, что все произведения n элементов (с любой расстановкой скобок) равны нулю. Это влечёт следующий факт:

Следствие 2. *Все тождества алгебры A_q следуют из тождеств, зависящих от не более чем q элементов. Существует алгоритм, который по любому числу $q=2^{\varkappa}$ выписывает конечный базис тождеств алгебры A_q.*

Этот базис представляет собой просто таблицы сложения (для $+$ и $\oplus$) свободной алгебры $F_{q,q}$.

ГЛАВА 20.
ЭКОНОМНОЕ ПРИСОЕДИНЕНИЕ КВАДРАТНЫХ КОРНЕЙ К ГРУППАМ

0. Введение

Исследованию разрешимости уравнений над группами посвящено множество работ (см., например, [GR62], [Le62], [Ly80], [Б84], [EH91], [How91], [K93], [КП95], [FeR96], [K97], [CG00], [EdJu00], [Juhá03], [K06] и литературу там цитируемую). В этих статьях доказывается, что при тех или иных условиях уравнение $w(x) = 1$ с коэффициентами из группы G *разрешимо над* G, то есть найдётся группа H, содержащая G в качестве подгруппы, и элемент $h \in H$ такой, что $w(h) = 1$. В настоящей работе мы пытаемся исследовать количественный вопрос: *насколько большой должна быть такая группа* H*?* Даже для простых уравнений, разрешимость которых давно известна, этот вопрос оказывается весьма трудным и мы ограничиваемся изучением простейшего нетривиального уравнения $x^2 = g$.

Разумеется, ответ сильно зависит от исходной группы G. Например, если порядок группы G нечётный, то при любом $g \in G$ в качестве H можно взять саму группу G; если группа G циклическая, то при любом $g \in G$ в качестве H достаточно взять группу вдвое большего порядка и т. д. Наиболее интересно, конечно, оценить порядок группы H «в худшем случае». Нам удаётся получить оценку, отличающуюся от наилучшей не более, чем в два раза в следующем смысле.

Основная теорема. *Каждая конечная группа G вкладывается в группу порядка $2|G|^2$, в которой все элементы группы G являются квадратами. Существует бесконечно много попарно неизоморфных конечных групп G_i таких, что для некоторого $g_i \in G_i$ группа, содержащая G_i в качестве подгруппы и содержащая элемент, квадрат которого равен g_i, имеет порядок не меньше чем $|G_i|^2$.*

Кроме задачи решения одного уравнения $x^2 = g$, можно рассмотреть и задачу одновременного решения всех уравнений такого вида. Из основной теоремы ясно, что и в этом случае также всегда достаточно группы порядка $2|G|^2$, но не всегда достаточно группы порядка меньшего $|G|^2$.

Про поведение множества решений уравнений в конечных группах многое известно (см., например, [Frob03], [Hall36b], [Solo69], [Стру95] и литературу там цитируемую). К сожалению, нам не удалось воспользоваться этими нетривиальными результатами.

Первое утверждение теоремы не является новым и легко доказывается (см. параграф 1). Во втором параграфе мы доказываем второе утверждение. В последнем параграфе мы формулируем несколько открытых вопросов об экономном присоединении решений уравнений к группам.

Обозначения, которые мы используем, в целом стандартны. Отметим только, что если $k \in \mathbb{Z}$, а x и y — элементы некоторой группы, то x^y, x^{ky}, x^{-y} обозначают $y^{-1}xy$, $y^{-1}x^ky$ и $y^{-1}x^{-1}y$, соответственно. Если X — подмножество некоторой группы, то $|X|$, $\langle X\rangle$ и $\langle\langle X\rangle\rangle$ означают, соответственно, мощность множества X, подгруппу, порождённую множеством X, и нормальную подгруппу, порождённую множеством X. Буква $\mathbb{Z}$ обозначают множество целых чисел. Символ $\mathbb{Z}_n$ обозначает группу или кольцо $\mathbb{Z}/n\mathbb{Z}$ вычетов по модулю n. Мультипликативная группа кольца $\mathbb{Z}_n$ обозначается $\mathbb{Z}_n^*$. Группа автоморфизмов группы G обозначается $\mathrm{Aut}\, G$. Символ D_p обозначает диэдральную группу порядка $2p$. Стабилизатор точки a при действии группы G обозначается $\mathrm{St}_G(a)$. *Отражением* мы называем элемент группы D_p, не лежащий в её подгруппе $\mathbb{Z}_p$.

1. Сплетения и доказательство первого утверждения теоремы

Первое утверждение теоремы хорошо известно [Le62]: сплетение

$$G \wr \mathbb{Z}_2 = \left\{ \begin{pmatrix} g_1 & 0 \\ 0 & g_2 \end{pmatrix} \;\middle|\; g_1, g_2 \in G \right\} \cup \left\{ \begin{pmatrix} 0 & g_1 \\ g_2 & 0 \end{pmatrix} \;\middle|\; g_1, g_2 \in G \right\}$$

группы G и циклической группой порядка 2 является группой порядка $2|G|^2$ и содержит квадратные корни из всех элементов группы G, если считать, что группа G вложена в сплетение $G \wr \mathbb{Z}_2$ диагональным образом:

$$g \mapsto \begin{pmatrix} g & 0 \\ 0 & g \end{pmatrix}.$$

Действительно, $\left(\begin{smallmatrix} 0 & g \\ 1 & 0 \end{smallmatrix}\right)^2 = \left(\begin{smallmatrix} g & 0 \\ 0 & g \end{smallmatrix}\right)$. Это простейший частный случай теоремы Левина, полную формулировку мы приводим в последнем параграфе.

2. Диэдральные группы и доказательство второго утверждения теоремы

Второе утверждение основной теоремы немедленно вытекает из следующего факта.

Теорема 1. *Пусть $p \in 4\mathbb{Z}+3$ — простое число, $\widetilde{G}$ — группа, содержащая диэдральную подгруппу $G = D_p$, и отражение $g \in G$ является квадратом некоторого элемента $x \in \widetilde{G}$. Тогда $|\widetilde{G}| \geqslant |G|^2$.*

Для доказательства нам потребуются несколько несложных лемм.

Лемма 1. *Если H_1 и H_2 — подгруппы некоторой группы H, то $|H| \geqslant \frac{|H_1||H_2|}{|H_1 \cap H_2|} = |H_1 H_2|$.*

Доказательство этой несложной леммы мы оставляем читателю в качестве упражнения.

Лемма 2. *Пусть $D_p = G \subseteq \langle G, x\rangle = \widetilde{G}$ и $x^2 = g$, где $g \in G$ — отражение. Тогда либо $G \lhd \widetilde{G}$, либо $G \cap G^x = \langle g\rangle$.*

Доказательство. Очевидно, что $g \in G \cap G^x$. В D_p существуют всего две подгруппы, содержащие g. Если $G \cap G^x = \langle g\rangle$, то всё доказано. Если же $G \cap G^x = G$, то $G = G^x$. Но тогда $G \lhd \widetilde{G}$, так как $\langle G, x\rangle = \widetilde{G}$.

Лемма 3. *Пусть $D_p = G \lhd \widetilde{G}$, где $p \in 3+4\mathbb{Z}$ — простое число. Тогда никакое отражение $g \in G$ не является квадратом в $\widetilde{G}$.*

Доказательство. Подгруппа $\mathbb{Z}_p \subset D_p = G \lhd \widetilde{G}$ является коммутантом группы G и, следовательно, характеристична в G и нормальна в $\widetilde{G}$. Группа $\widetilde{G}$ действует на $\mathbb{Z}_p$ сопряжениями. При этом отражение g действует как $-1 \in \mathbb{Z}_p^* = \operatorname{Aut}\mathbb{Z}_p$, а -1 не является, как известно, квадратом в $\mathbb{Z}_p^*$, если $p \in 3+4\mathbb{Z}$, что и доказывает лемму.

Приступим теперь к доказательству теоремы 1. Можно считать, что $\widetilde{G} = \langle G, x\rangle$. Пусть K — множество всех подгрупп группы $\widetilde{G}$, сопряжённых с G. Тогда $\widetilde{G}$ транзитивно действует на K сопряжениями.

Лемма 4. $|\widetilde{G}| \geqslant |K| \cdot |G|$.

Доказательство. $|\widetilde{G}| = |K| \cdot |\mathrm{St}_{\widetilde{G}}(G)| \geqslant |K| \cdot |G|$, так как $G \subseteq \mathrm{St}_{\widetilde{G}}(G)$.

Рассмотрим полный неориентированный граф Γ с множеством вершин K. Назовём ребро (G^{h_1}, G^{h_2})

зелёным, если $|G^{h_1} \cap G^{h_2}| = 2$; жёлтым, если $|G^{h_1} \cap G^{h_2}| = p$; красным, если $|G^{h_1} \cap G^{h_2}| = 1$.

Ясно, что все рёбра покрашены. Если есть хотя бы одно ребро красного цвета, то утверждение сразу же следует из леммы 1. Поэтому далее считаем, что красных рёбер нет.

Лемма 5. *Все вершины K и жёлтые рёбра образуют граф Y, каждая компонента связности которого — полный граф. Все компоненты связности содержат одно и то же число вершин.*

Доказательство. Первое утверждение леммы немедленно вытекает из того, что в D_p есть всего одна подгруппа порядка p. То, что все компоненты связности содержат одинаковое количество вершин, следует из того, что действие $\widetilde{G}$ на K транзитивно и сохраняет цвета рёбер.

Лемма 6. *Число зелёных рёбер, выходящих из вершины G, положительно и делится на p.*

Доказательство. Каждое зелёное ребро, выходящее из G, соответствует одному из p отражений $g \in G$. Таким образом, рёбра, выходящие из G делятся на p классов. В каждом из этих классов одинаковое число рёбер, так как все отражения в группе G сопряжены и, следовательно, автоморфизмом графа можно перевести любой из этих классов в любой другой из этих классов. Это значит, что число зелёных рёбер, выходящих из G делится на p.

Одно зелёное ребро в графе существует, это ребро (G, G^x), где $x^2 = g \in G$ — отражение. Действительно, $G^x \cap G \ni g$, но $G^x \neq G$ (так как иначе группа G была бы нормальной подгруппой в $\widetilde{G} = \langle G, x\rangle$, чего не может быть по лемме 3). Значит, $G^x \cap G = \langle g\rangle_2$ и лемма доказана.

Продолжим доказательство теоремы. Предположим, что из G выходит по крайней мере $2p$ зелёных рёбер. Тогда граф имеет по крайней мере $2p+1$ вершину, то есть $|K| > 2p$ и по лемме 4 $|\widetilde{G}| \geqslant |K| \cdot |G| > 2p|G| = |G|^2$ и всё доказано.

Согласно лемме 6 остаётся рассмотреть случай, когда из каждой вершины графа выходит ровно p зелёных рёбер.

Пусть u — число вершин в каждой из компонент связности графа Y (лемма 5), а v — количество этих компонент связности. Тогда

$$p = (\text{число зелёных рёбер выходящих из } G) = (v-1)u$$

(так как каждая вершина, не соединённая с G жёлтым ребром, соединена с G зелёным ребром).

Равенство $p=(v-1)u$ означает (в силу простоты числа p), что либо $v=2$ и $u=p$, либо $v=p+1$ и $u=1$.

В первом случае $|K|=2p$ и всё доказано по лемме 4: $|\widetilde{G}|\geqslant 2p|G|=|G|^2$.

Во втором случае $|K|=p+1$ и граф Γ представляет собой полный граф, все рёбра которого зелёные. Группа $\widetilde{G}$ действует на этом графе, причём действие группы G на множестве вершин, отличных от G, изоморфно действию G сопряжениями на множестве своих подгрупп порядка два (этот изоморфизм сопоставляет группе G^h подгруппу $G^h\cap G$). В частности, сопряжение при помощи отражения g представляет собой перестановку вершин графа, которая оставляет на месте ровно две точки (G и группу G^h, для которой $G\cap G^h=\langle g\rangle$) и, следовательно, раскладывается в произведение $\frac{p-1}{2}$ независимых транспозиций. Эта перестановка нечётная, так как $p\in 3+4\mathbb{Z}$, что противоречит тому, что g является квадратом в $\widetilde{G}$. Теорема доказана.

3. Корни высших степеней и другие открытые вопросы

Возникает вопрос: какова же на самом деле точная оценка?

Вопрос 1. *Бесконечно ли множество таких конечных групп G, что для некоторого $g\in G$ каждая группа, содержащая G в качестве подгруппы и содержащая элемент, квадрат которого равен g, имеет порядок не меньше чем $2|G|^2$?*

Следующее утверждение показывает, что для диэдральных групп наша теорема не может быть усилена, а для ответа на вопрос 1 надо изучать группы, близкие к простым.

Утверждение 1. *Если конечная группа G и её элемент g удовлетворяют хотя бы одному из следующих условий*

а) *G не совпадает со своим коммутантом;*

б) *G не совпадает с нормальным замыканием элемента g;*

в) *в G есть нетривиальная нормальная подгруппа нечётного порядка;*[*)]

то G вкладывается в группу H порядка не превосходящего $|G|^2$, в которой элемент g является квадратом.

Доказательство. Следующая лемма показывает, что при выполнении условия а) или б) в качестве группы H можно взять не всё сплетение $G\wr\mathbb{Z}_2$ (см. параграф 1), а его собственную подгруппу. Если же выполнено условие в), то в качестве H можно взять собственную факторгруппу этого сплетения, как показывает лемма 8 (см. ниже).

Лемма 7. *В сплетении $G\wr\mathbb{Z}_2$ подгруппа H, порождённая группой G, вложенной диагонально, и квадратным корнем $\left(\begin{smallmatrix}0&g\\1&0\end{smallmatrix}\right)$ из элемента $g\in G$ имеет вид*

$$H=\left\{\begin{pmatrix}g_1&0\\0&g_2\end{pmatrix}\ ;\ g_1g_2^{-1}\in[\langle\!\langle g\rangle\!\rangle,G]\right\}\cup\left\{\begin{pmatrix}0&g_1\\g_2&0\end{pmatrix}\ ;\ g_1g_2^{-1}\in g\,[\langle\!\langle g\rangle\!\rangle,G]\right\},$$

где $[\langle\!\langle g\rangle\!\rangle,G]$ — взаимный коммутант нормального замыкания элемента g в группе G и группы G.

Доказательство. Эпиморфизм $\varphi\colon G\to G/[\langle\!\langle g\rangle\!\rangle,G]$ индуцирует гомоморфизм $\Phi\colon G\wr\mathbb{Z}_2\to(G/[\langle\!\langle g\rangle\!\rangle,G])\wr\mathbb{Z}_2$. Множество, стоящее в правой части доказываемого равенства, есть $\Phi^{-1}(\Phi(H))$. Поэтому достаточно доказать, что H содержит ядро гомоморфизма Φ. Но $\ker\Phi$ порождается (как подгруппа) элементами вида

$$\begin{pmatrix}[g^x,y]&0\\0&1\end{pmatrix}\quad\text{и}\quad\begin{pmatrix}1&0\\0&[g^x,y]\end{pmatrix},\quad\text{где } x,y\in G,$$

которые лежат в H, как показывают следующие равенства:

$$\begin{pmatrix}x^{-1}&0\\0&x^{-1}\end{pmatrix}\begin{pmatrix}0&g\\1&0\end{pmatrix}\begin{pmatrix}x&0\\0&x\end{pmatrix}=\begin{pmatrix}0&g^x\\1&0\end{pmatrix},\quad\left[\begin{pmatrix}0&g^x\\1&0\end{pmatrix},\begin{pmatrix}y&0\\0&y\end{pmatrix}\right]=\begin{pmatrix}0&1\\g^{-x}&0\end{pmatrix}\begin{pmatrix}0&g^{xy}\\1&0\end{pmatrix}=\begin{pmatrix}1&0\\0&[g^x,y]\end{pmatrix},$$

$$\begin{pmatrix}1&0\\0&[g^x,y]\end{pmatrix}\begin{pmatrix}[g^x,y]&0\\0&[g^x,y]\end{pmatrix}^{-1}=\begin{pmatrix}[g^x,y]&0\\0&1\end{pmatrix}^{-1}.$$

Лемма 8. *Если N — нормальная абелева подгруппа группы G, то множество*

$$K=\left\{\begin{pmatrix}x&0\\0&x^{-1}\end{pmatrix}\ ;\ x\in N\right\}$$

[*)] Из теоремы Фейта–Томпсона о разрешимости групп нечётного порядка [FeTh63] следует, что свойство в) эквивалентно наличию в G нетривиальной абелевой нормальной подгруппы нечётного порядка.

является нормальной подгруппой в сплетении $G \wr \mathbb{Z}_2$. Если порядок подгруппы N нечётный, то подгруппа K тривиально пересекается с группой G (вложенной в сплетение диагональным образом).
Наоборот: каждая нетривиальная нормальная подгруппа этого сплетения, тривиально пересекающаяся с G, содержит нетривиальную абелеву нормальную подгруппу указанного вида.

Доказательство. То, что множество K является нормальной подгруппой, очевидно. Ясно, что

$$K \cap G = \{x \in N \,;\, x^2 = 1\},$$

поэтому K тривиально пересекается с G, если порядок подгруппы N нечётный.

Произвольная нетривиальная нормальная подгруппа X сплетения, как известно, нетривиально пересекается с базой (см, например, [КаМ82]). Пусть

$$1 \neq u = \begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix} \in X.$$

Тогда

$$\left[u, \begin{pmatrix} y & 0 \\ 0 & y \end{pmatrix}\right] = \begin{pmatrix} [x,y] & 0 \\ 0 & 1 \end{pmatrix} = v \in X \ni \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^{-1} v \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & [x,y] \end{pmatrix} = w$$

и, следовательно,

$$vw = \begin{pmatrix} [x,y] & 0 \\ 0 & [x,y] \end{pmatrix} \in X \cap G = \{1\}, \quad \text{то есть } [x,y] = 1.$$

Но тогда

$$X \ni \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^{-1} u \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} y & 0 \\ 0 & x \end{pmatrix} = t$$

и, следовательно,

$$ut = \begin{pmatrix} xy & 0 \\ 0 & xy \end{pmatrix} \in X \cap G = \{1\}, \quad \text{то есть } xy = 1.$$

Таким образом, пересечение подгруппы X с базой сплетения имеет вид

$$K = \left\{ \begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix} \,;\, x \in N \right\},$$

где N — некоторое подмножество группы G. Отсюда, разумеется, вытекает, что множество N обязано быть абелевой нормальной подгруппой. Лемма доказана.

Эти леммы доказывают утверждение 1 и, кроме того, показывают, что если группа G не удовлетворяет ни одному из условий а), б) и в) (например, если группа G является неабелевой простой), то сплетение $G \wr \mathbb{Z}_2$ не имеет ни собственных подгрупп, ни собственных факторгрупп, содержащих группу G и квадратный корень $\left(\begin{smallmatrix} 0 & g \\ 1 & 0 \end{smallmatrix}\right)$ из элемента g.

Перейдём теперь к корням высших степеней и решениям других уравнений. Отправной точкой нашего исследования послужила теорема Левина, которая в полном объёме выглядит так:

Теорема Левина ([Le62]). *Сплетение $G \wr \mathbb{Z}_n$ группы G и циклической группы порядка n (имеющее порядок $n|G|^n$) содержит решения всех положительных уравнений степени n над группой G.*

Под *положительным уравнением степени n над группой G* понимается уравнение вида

$$g_1 x g_2 x \dots g_n x = 1 \quad \text{где } g_1, \dots, g_n \in G.$$

В связи с этим возникает вопрос: верно ли, что теорема Левина даёт неулучшаемую оценку?

Вопрос 2. *Бесконечно ли множество таких конечных групп G, что каждая группа, содержащая G в качестве подгруппы и содержащая решение каждого положительного уравнения степени n над G, имеет порядок не меньше чем $n|G|^n$?*

Можно выдвинуть и более смелую гипотезу.

Вопрос 3. *Бесконечно ли множество таких конечных групп G, что каждая группа H, содержащая G в качестве подгруппы, каждый элемент которой является n-й степенью в H, имеет порядок не меньше чем $n|G|^n$?*

Что можно сказать об экономном присоединении решений других (то есть неположительных) уравнений? Например, теорема Герстенхабера–Ротхауза [GR62] в комбинации с теоремой Мальцева о финитной аппроксимируемости конечно порождённых линейных групп [Маль40] даёт следующее утверждение.

Утверждение 2. ([GR62]+[Маль40]). *Каждая конечная группа G может быть вложена в конечную группу H, содержащую решения всех невырожденных уравнений длины n над G.*

Под *невырожденным уравнением длины n над группой G* понимается уравнение вида

$$g_1 x^{\varepsilon_1} g_2 x^{\varepsilon_2} \dots g_n x^{\varepsilon_n} = 1, \quad \text{где } g_i \in G, \quad \varepsilon_i \in \{\pm 1\}, \quad \text{и } \sum \varepsilon_i \neq 0.$$

Доказательство теоремы Герстенхабера–Ротхауза красивое, но неконструктивное. Поэтому трудно написать не только неулучшаемую, но даже хоть какую-нибудь оценку на порядок группы H.

Вопрос 4. *Можно ли оценить $|H|$ через $|G|$ и n в утверждении 2?*

При $n = 1$ ответ на вопросы 2, 3 и 4, очевидно, положительный. Невырожденное уравнение длины два имеет вид $g_1 x^{\varepsilon} g_2 x^{\varepsilon} = 1$, где $\varepsilon \in \{\pm 1\}$, и линейной заменой переменных приводится к виду $x^2 = g$, поэтому основной результат этой работы даёт ответ на «ослабленные вдвое» версии этих вопросов при $n = 2$. Что происходит при других n, нам неизвестно.

ГЛАВА 21.
КАК ОБОБЩИТЬ ИЗВЕСТНЫЕ РЕЗУЛЬТАТЫ ОБ УРАВНЕНИЯХ НАД ГРУППАМИ

1. Введение

Напомним, что *уравнением над группой G с неизвестным* (или *переменной*) t называют формальное выражение вида

$$g_1 t^{\varepsilon_1} g_2 t^{\varepsilon_2} \dots g_n t^{\varepsilon_n} = 1, \qquad (*)$$

где $g_i \in G$, $\varepsilon_i \in \mathbb{Z}$. Уравнение $(*)$ называют *разрешимым над* группой G, если найдётся бóльшая группа $\widetilde{G}$, содержащая группу G в качестве подгруппы, и элемент $\widetilde{t} \in \widetilde{G}$ (называемый решением уравнения $(*)$) такой, что
$g_1 \widetilde{t}^{\varepsilon_1} g_2 \widetilde{t}^{\varepsilon_2} \dots g_n \widetilde{t}^{\varepsilon_n} = 1$ в группе $\widetilde{G}$.

Имеется множество теорем, которые говорят, что уравнение $(*)$ разрешимо при тех или иных условиях на группу G и на левую часть уравнения.

В настоящей главе предлагается рассмотреть некоторое обобщение понятия уравнения.

Обобщённым уравнением над группой G с переменной группой T мы назовём формальное выражение вида

$$g_1 t_1 g_2 t_2 \dots g_n t_n = 1, \qquad (*')$$

где $g_i \in G$, $t_i \in T$. Обобщённое уравнение $(*')$ называют *разрешимым над* группой G, если найдётся бóльшая группа $\widetilde{G}$, содержащая группу G в качестве подгруппы, и гомоморфизм $T \to \widetilde{G}$, $t \mapsto \widetilde{t}$ (называемый решением обобщённого уравнения $(*')$) такой, что $g_1 \widetilde{t}_1 g_2 \widetilde{t}_2 \dots g_n \widetilde{t}_n = 1$ в группе $\widetilde{G}$.

Ясно, что в случае, когда переменная группа является бесконечной циклической, определение разрешимости обобщённого уравнения превращается в определение разрешимости обычного уравнения. Предлагается доказывать обобщённые аналоги известных теорем о разрешимости уравнений. Такие обобщённые теоремы могут включать в себя помимо условий на группу G и на левую часть уравнения некоторые условия, говорящие о том, что переменная группа в некотором смысле похожа на бесконечную циклическую.

Приведём несколько примеров. Мы называем уравнение

$$w(G,t) \equiv \prod g_i t^{\varepsilon_i} = 1, \quad \text{где } \ g_i \in G,\ \varepsilon_i \in \mathbb{Z}, \qquad (1)$$

или обобщённое уравнение

$$w(G,T) \equiv \prod g_i t_i = 1, \quad \text{где } \ g_i \in G,\ t_i \in T, \qquad (1')$$

нетривиальным, если его левая часть не сопряжена с константой (то есть с элементом исходной группы G) в свободном произведении $G * \langle t \rangle_\infty$ (соответственно, в $G * T$).

Гипотеза Левина [Le62]. *Над группой без кручения разрешимо любое нетривиальное уравнение.*

Эта гипотеза остаётся недоказанной, однако известно, что она эквивалентна своему обобщённому аналогу.

Обобщённая гипотеза Левина. *Над группой без кручения разрешимо любое нетривиальное обобщённое уравнение с переменной группой без кручения.*

Действительно, рассмотрим группу без кручения G_1, содержащую группы G и T в качестве подгрупп (например, $G_1 = G \times T$ или $G_1 = G * T$). По нетривиальному обобщённому уравнению $(1')$ над группой G построим нетривиальное обычное уравнение

$$v(G_1, t) \equiv w(G_1, t^{-1} T t) = 1$$

над группой G_1. Если (обычная) гипотеза Левина верна, то это уравнение имеет решение $\widetilde{t} \in \widetilde{G_1} \supseteq G_1$. Но тогда группа $\widetilde{T} = \widetilde{t}^{-1} T \widetilde{t} \subseteq \widetilde{G_1}$ будет решением обобщённого уравнения $(1')$ над группой G, что доказывает обобщённую гипотезу Левина в предположении справедливости обычной гипотезы Левина.

Отметим, что условие похожести переменной группы на бесконечную циклическую состоит, в случае обобщённой гипотезы Левина, в отсутствии кручения.

Самым известным результатом в направлении доказательства гипотезы Левина является следующая теорема Бродского–Хауи ([Б84], [How81]). Напомним, что группа называется *локально индикабельной*, если каждая её нетривиальная конечно порождённая подгруппа обладает эпиморфизмом на бесконечную циклическую.

Теорема Б. *Над локально индикабельной группой разрешимо любое нетривиальное уравнение.*

Обобщённым аналогом этого факта служит следующая теорема (которая на самом деле и была доказана Бродским).

Теорема Б′. *Над локально индикабельной группой разрешимо любое нетривиальное обобщённое уравнение с локально индикабельной переменной группой.*

Эквивалентность этих двух теорем легко доказывается дословным повторением приведённого выше рассуждения по поводу гипотезы Левина; надо лишь заменить слова «без кручения» на слова «локально индикабельная».

Отметим, что в случае теоремы Бродского условием похожести переменной группы на бесконечную циклическую служит локальная индикабельность.

Можно привести ещё много примеров столь же тривиального обобщения различных утверждений. Не так просто дело обстоит с другой известной гипотезой. Напомним, что уравнение (1) называется *невырожденным*, если сумма показателей при t в $w(G,t)$ отлична от нуля; если $\sum \varepsilon_i = \pm 1$, то уравнение называется *унимодулярным*.

Гипотеза Кервера–Лауденбаха (см. [ЛШ80]). *Унимодулярное уравнение над любой группой разрешимо над ней.*

Иногда гипотезой Кервера–Лауденбаха называют утверждение о разрешимости любого *невырожденного* уравнения (или даже системы уравнений) над любой группой. На сегодняшний день ни одна из версий этой гипотезы не доказана и не опровергнута.

Пытаясь сформулировать обобщённый аналог гипотезы Кервера–Лауденбаха или каких-либо известных фактов в этом направлении, мы сталкиваемся с проблемой: *что делать с условием унимодулярности (невырожденности)?*

В этой главе мы доказываем обобщённый аналог следующей теоремы.

Теорема 1 ([K93], см. также [FeR96]). *Унимодулярное уравнение над группой без кручения разрешимо над ней.*

Обобщённый аналог, который мы собираемся доказывать, выглядит так.

Теорема 1′. *Унимодулярное обобщённое уравнение над группой без кручения разрешимо над ней.*

Здесь унимодулярность обобщённого уравнения понимается в смысле следующего определения, которое, хотя и выглядит не самым естественным образом, однако работает и, разумеется, превращается в точности в обычную унимодулярность, если переменная группа является бесконечной циклической.

Определение 1. Обобщённое уравнение (1′) называется *унимодулярным*, если
1) $\prod t_i$ является элементом бесконечного порядка в группе T;
2) циклическая подгруппа $\langle \prod t_i \rangle$ нормальна в T;
3) факторгруппа $T/\langle \prod t_i \rangle$ является группой с сильно однозначным умножением.

Напомним, что группа H называется *группой с однозначным умножением* (или *UP-группой*), если для любых двух её конечных непустых подмножеств $X, Y \subseteq H$ их произведение XY содержит по крайней мере один элемент, раскладывающийся в произведение элемента из X и элемента из Y однозначно. Известно, что в групповом кольце группы с однозначным умножением отсутствуют делители нуля. Одно время была гипотеза, что всякая группа без кручения является группой с однозначным умножением (обратное, очевидно, верно). Если бы эта гипотеза подтвердилась, то проблема Капланского о делителях нуля в групповых кольцах была бы решена. Однако выяснилось, что существует контрпример ([RS87], [P88]).

Мы называем группу H *группой с сильно однозначным умножением*, если для любых двух её конечных непустых подмножеств $X, Y \subseteq H$ таких, что $|Y| \geqslant 2$, их произведение XY содержит по крайней мере два однозначно разложимых элемента x_1y_1 и x_2y_2 таких, что $x_1, x_2 \in X$, $y_1, y_2 \in Y$ и $y_1 \neq y_2$.

Отметим, что смысл этого определения состоит в условии $y_1 \neq y_2$, поскольку согласно теореме Стройновского [Str80] произведение любых двух конечных непустых и неодноэлементных подмножеств в UP-группе всегда содержит по меньшей мере два однозначно разложимых элемента.

Насколько мы знаем, все известные примеры UP-групп обладают сильно однозначным умножением. Например, этим свойством обладают все правоупорядочиваемые группы, локально индикабельные группы, диффузные группы в смысле Бовдича.

Кроме того заметим, что сильная однозначность умножения вытекает из следующего свойства UP_4: произведение любых четырёх непустых конечных подмножеств $A, B, C, D \subseteq H$ содержит по меньшей мере один элемент, раскладывающийся однозначно в произведение $abcd$, где $a \in A$, $b \in B$, $c \in C$ и $d \in D$. Действительно, если все однозначно разложимые элементы xy множества XY имеют общий сомножитель y, то произведение четырёх множеств $XYY^{-1}X^{-1}$ не содержит однозначно разложимых элементов: из однозначной разложимости элемента $u = x_1y_1y_2^{-1}x_2^{-1}$ вытекает, что $y_1 = y$ (иначе x_1y_1 будет иметь другое разложение $x_1y_1 = x_1'y_1'$, а значит и u будет иметь другое разложение $u = x_1'y_1'y_2^{-1}x_2^{-1}$); по аналогичным причинам y_2 обязан быть равным

элементу y; но тогда u имеет два разложения $u = x_1 y y^{-1} x_2^{-1} = x_1 y'(y')^{-1} x_2^{-1}$, где $y' \in Y$ – любой элемент отличный от y.

Из теоремы $1'$ вытекает следующий факт об обычных уравнениях с несколькими переменными, который можно рассматривать как многомерный аналог теоремы 1.

Следствие. *Уравнение*

$$g_1 x_{j_1}^{\varepsilon_1} g_2 x_{j_2}^{\varepsilon_2} \dots g_n x_{j_n}^{\varepsilon_n} = 1 \qquad (**)$$

над группой без кручения G с неизвестными $x_1, x_2, \dots$ разрешимо над G, если $\prod x_{j_i}^{\varepsilon_i}$ не является истинной степенью в свободной группе $F(x_1, x_2, \dots)$.

Доказательство. Рассмотрим в качестве группы T группу

$$T = \left\langle x_1, x_2, \dots \mid [x_1, \prod x_{j_i}^{\varepsilon_i}] = 1,\ [x_2, \prod x_{j_i}^{\varepsilon_i}] = 1, \dots \right\rangle.$$

Эта группа является универсальным центральным расширением группы с одним соотношением

$$T_1 = \left\langle x_1, x_2, \dots \mid \prod x_{j_i}^{\varepsilon_i} = 1 \right\rangle.$$

Хорошо известно, что, если $\prod x_{j_i}^{\varepsilon_i}$ не является истинной степенью в свободной группе $F(x_1, x_2, \dots)$, то группа T_1 является локально индикабельной ([Б84]), и, следовательно, группой с сильно однозначным умножением. Элемент $\prod x_{j_i}^{\varepsilon_i}$ имеет бесконечный порядок в группе T (см. [ЛШ80]). Таким образом, уравнение (**), рассматриваемое как обобщённое уравнение с переменной группой T, является унимодулярным. Следовательно, оно разрешимо по теореме $1'$. Следствие доказано.

Теорему $1'$ мы получаем как частный случай следующего утверждения.

Основная теорема. *Если всякое унимодулярное уравнение над любой свободной степенью группы G является магнусовым, то всякое унимодулярное обобщённое уравнение над группой G разрешимо над ней.*

Мы говорим, что уравнение (1) над группой G является *магнусовым**, если оно разрешимо над G и для всякого свободного сомножителя H группы G такого, что уравнение (1) не является уравнением над ним (в том смысле, что w не сопряжено в $G * \langle t \rangle$ с элементами группы $H * \langle t \rangle$), в некоторой надгруппе существует решение $\widetilde{t}$, трансцендентное над H, то есть такое, что $\langle H, \widetilde{t} \rangle = H * \langle \widetilde{t} \rangle_\infty$.

Теорема $1'$ является непосредственным следствием основной теоремы и следующей леммы, которая, по нашему мнению, интересна и сама по себе.

Лемма 1. *Любое унимодулярное уравнение над группой без кручения является магнусовым.*

На самом деле основная теорема не утверждает ничего большего, чем справедливость теоремы $1'$, так как очевидно, что над группой с кручением заведомо найдётся немагнусово унимодулярное уравнение (например, уравнение $t = g$, где g — нетривиальный элемент конечного порядка).

Обозначения, которые мы используем, в целом стандартны. Отметим только, что если x и y — элементы некоторой группы, а X — подмножество группы, то x^y означает $y^{-1}xy$, коммутатор $[x, y]$ понимается как $x^{-1}y^{-1}xy$, а символы $\langle X \rangle$ и $\langle\langle X \rangle\rangle$ означают, соответственно, подгруппу, порождённую множеством X и нормальную подгруппу, порождённую множеством X. Кроме того, если A и B — изоморфные подгруппы некоторой группы и $\varphi : A \to B$ — изоморфизм, то часто встречающиеся системы соотношений вида $\{a^x = a^\varphi \mid a \in A\}$ мы будем записывать в сокращённой форме $A^x = B$ в случае, когда ясно, о каком изоморфизме идёт речь.

---

* Имеется в виду теорема Магнуса о свободе, которую мы можем сформулировать так: *всякое уравнение над свободной группой магнусово.*

2. Доказательство основной теоремы

Положим $t = \prod t_i$. Разложим T в объединение смежных классов:

$$T = \coprod_{x \in T/\langle t \rangle} c_x \langle t \rangle, \quad \text{где } c_1 = 1.$$

Запишем обобщённое уравнение $(1')$ в виде

$$t \prod_i g_i^{c_{x_i} t^{k_i}} = 1. \tag{2}$$

Пусть $X_1 = \{x_i\}$ — это множество всех $x \in T/\langle t \rangle$, встречающихся в несократимой записи уравнения (2). Для каждого $x \in T/\langle t \rangle$ символом $G^{(c_x)}$ обозначим изоморфную копию группы G, подразумевая, что изоморфизм переводит $g \in G$ в $g^{(c_x)} \in G^{(c_x)}$.

Положим

$$H_1 = \mathop{*}_{y \in X_1} G^{(c_y)}$$

и рассмотрим уравнение (относительно t)

$$t \prod_i g_i^{(c_{x_i}) t^{k_i}} = 1$$

над группой H_1.

Сопряжём уравнение (2) при помощи элемента $x \in T/\langle t \rangle$ (имеется в виду, что мы сопрягаем при помощи элемента группы T, но в результате сопряжения при помощи t получается уравнение, эквивалентное исходному). Получим уравнение

$$t^{\varepsilon_x} \prod_i g_i^{c_{x_i x} t^{l_i(x)}} = 1,$$

где $\varepsilon_x = \pm 1$ в зависимости от того, коммутирует x с t или нет, а целые числа $l_i(x)$ однозначно определяются из равенства $c_{x_i} t^{k_i} c_x = c_{x_i x} t^{l_i(x)}$. Аналогичным образом положим $X_x = X_1 x = \{x_i x\}$ и напишем уравнение (относительно t)

$$w_x(t) \equiv t^{\varepsilon_x} \prod_i g_i^{(c_{x_i x}) t^{l_i(x)}} = 1$$

над группой

$$H_x = \mathop{*}_{y \in X_x} G^{(c_y)}.$$

Это унимодулярное уравнение над группой без кручения, согласно теореме 1, имеет решение $\widetilde{t} \in \widetilde{H_x} \supseteq H_x$.

Разумеется, мы можем считать, что

$$\widetilde{H_x} = \langle H_x,\ \widetilde{t} \mid w_x(\widetilde{t}) = 1 \rangle.$$

Положим

$$K = \langle \mathop{*}_{x \in T/\langle t \rangle} G^{(c_x)},\ \widetilde{t} \mid \{w_y(\widetilde{t}) = 1 \mid y \in T/\langle t \rangle\} \rangle.$$

Докажем, что естественное отображение $G \simeq G^{(1)} \to K$ инъективно. Для этого достаточно показать, что для любого конечного множества $Y \subseteq T/\langle t \rangle$ такого, что $X_1 Y \ni 1$, естественное отображение

$$G \simeq G^{(1)} \to K_Y = \langle \mathop{*}_{x \in X_1 Y} G^{(c_x)},\ \widetilde{t} \mid \{w_y(\widetilde{t}) = 1 \mid y \in Y\} \rangle$$

инъективно. Этот факт очевидным образом вытекает из следующего утверждения.

Лемма 2. *Пусть Y — конечное подмножество группы $T/\langle t\rangle$, $z \in T/\langle t\rangle$, $k = |X_1|$ и $y_1, \ldots, y_{k-1}$ — различные элементы множества $X_z \cap (X_1 Y)$. Тогда в группе K_Y имеет место разложение*

$$\left\langle \widetilde{t}, G^{(c_{y_1})}, \ldots, G^{(c_{y_{k-1}})} \right\rangle = \langle \widetilde{t} \rangle_\infty * G^{(c_{y_1})} * \ldots * G^{(c_{y_{k-1}})}.$$

(Отметим, что по условию элемент z может лежать в Y, а может и не лежать.)

Доказательство. Индукция по мощности множества Y. Если $Y = \{u\}$, то утверждение леммы немедленно следует из магнусовости унимодулярного уравнения $w_u(t) = 1$ над группой H_u (лемма 1), так как $K_Y = K_{\{u\}} = \widetilde{H_u}$.

Если $|Y| > 1$, то из сильной однозначности умножения в группе $T/\langle t\rangle$ следует, что существует $y \in Y \setminus \{z\}$ такой, что $X_y = X_1 y \not\subseteq X_1 \cdot (\{z\} \cup Y \setminus \{y\})$, то есть $|(X_1 \cdot (\{z\} \cup Y \setminus \{y\})) \cap X_y| < k$; значит, в группе $K_{Y\setminus\{y\}}$ по предположению индукции мы имеем

$$\left\langle \widetilde{t},\ \{G^{(c_x)}\ ;\ x \in (X_1 \cdot (Y \setminus \{y\})) \cap X_y\} \right\rangle = \langle \widetilde{t} \rangle_\infty * \left(\mathop{*}_{(X_1 \cdot (Y\setminus\{y\})) \cap X_y} G^{(c_x)} \right).$$

Следовательно в группе

$$N = K_{Y\setminus\{y\}} * \left(\mathop{*}_{x \in (X_z \cap X_y) \setminus (X_1 (Y\setminus\{y\}))} G^{(c_x)} \right)$$

имеет место разложение

$$M = \left\langle \widetilde{t},\ \{G^{(c_x)}\ ;\ x \in (X_1 \cdot (\{z\} \cup Y \setminus \{y\})) \cap X_y\} \right\rangle = \\ = \langle \widetilde{t} \rangle_\infty * \left(\mathop{*}_{x \in (X_1 \cdot (\{z\} \cup Y\setminus\{y\})) \cap X_y} G^{(c_x)} \right).$$

Такое же разложение группы M имеет место в группе $\widetilde{H}_y$ по лемме 1. Тем самым мы получаем корректное разложение в свободное произведение с объединённой подгруппой:

$$K_Y = N \mathop{*}_M \widetilde{H}_y.$$

При этом интересующая нас подгруппа $\left\langle \widetilde{t}, G^{(c_{y_1})}, \ldots, G^{(c_{y_{k-1}})} \right\rangle$ лежит в группе N и доказываемое равенство имеет место по предположению индукции. Лемма 2, а вместе с ней и инъективность естественного отображения $G \simeq G^{(1)} \to K$, доказана.

Группа T действует на K следующим образом:

$$\widetilde{t}^{\,y} = \widetilde{t}^{\,\varepsilon_y}, \quad (g^{(c_x)})^y = (g^{(c_f)})^{\widetilde{t}^{\,k}}, \tag{3}$$

где $y \in T$ — произвольный элемент, а $f \in T/\langle t\rangle$ и $k \in \mathbb{Z}$ определяются из равенства $c_x y = c_f t^k$. Ясно, что это — корректно определённое действие автоморфизмами.

Возьмём соответствующее полупрямое произведение $T \leftthreetimes K$ и профакторизуем его по циклической нормальной подгруппе $\langle \widetilde{t} t^{-1} \rangle$. Это и будет искомая группа, содержащая решение:

$$\widetilde{G} = (T \leftthreetimes K) / \langle \widetilde{t} t^{-1} \rangle .$$

Действительно, G вкладывается в $\widetilde{G}$ в качестве подгруппы: $G = G^{(1)} \subseteq K \subseteq \widetilde{G}$. Согласно определению действия (3), мы имеем

$$G^{(c_x)} = G^{c_x},$$

значит, соотношение $w_1(\widetilde{t}) = 1$, выполненное в K, и равенство $t = \widetilde{t}$ в $\widetilde{G}$ дают соотношение (2). То есть группа T, рассматриваемая как подгруппа группы $\widetilde{G}$, является решением уравнения (2). Основная теорема доказана.

3. Доказательство леммы 1

Отметим один простой факт.

Лемма 3. *Пусть A — нетривиальная подгруппа группы B и $b \in B$. Тогда b трансцендентен над A в том и только том случае, когда*

$$\left\langle \{A^{b^i} \mid i \in \mathbb{Z}\} \right\rangle = \underset{i\in\mathbb{Z}}{*} A^{b^i}.$$

Доказательство. В одну сторону утверждение очевидно, а в другую сторону следует из того, что, если $u \in A * \langle b \rangle_\infty$ — нетривиальное соотношение между A и b в группе B и $a \in A \setminus \{1\}$, то $[a, u]$ — нетривиальное соотношение между группами A^{b^i}. Лемма 3 доказана.

До конца этого раздела будем предполагать, что $G = H * K$, уравнение (1) является унимодулярным уравнением над G и w не лежит в подгруппе, сопряжённой с $H * \langle t \rangle$ в группе $G * \langle t \rangle_\infty$. Кроме того, положим $U = G * \langle t \rangle_\infty / \langle\langle w \rangle\rangle$ (это так называемая «универсальная группа решений»). Будем доказывать, что уравнение (1) обладает решением, трансцендентным над H, или, что то же самое, элемент $t \in U$ трансцендентен над H.

Лемма 4. *Если*

$$\left\langle \{H^{t^i} \mid i \in \mathbb{Z}\} \right\rangle = \underset{i\in\mathbb{Z}}{*} H^{t^i} \tag{4}$$

в группе U, то элемент $t \in U$ является трансцендентным над H решением уравнения (1).

Доказательство. В случае, когда группа H нетривиальна, утверждение немедленно вытекает из леммы 3. Если же $H = \{1\}$, то утверждается лишь то, что элемент $t \in U$ имеет бесконечный порядок (если w не сопряжено с $t^{\pm 1}$); в явном виде этот факт отмечен в [6]. Лемма 4 доказана.

Положим

$$\overline{H} = (\underset{i\in\mathbb{Z}}{*} H_i), \quad \overline{G} = \overline{H} * K,$$

где H_i — это изоморфные копии группы H. Считая группу G вложеной в $\overline{G}$ в качестве $H_0 * K$, рассмотрим систему уравнений над группой $\overline{G}$, состоящую из исходного уравнения (1) и вспомогательных уравнений

$$\begin{cases} w(t) = 1, \\ t^{-1} H_i t = H_{i+1}, \quad i \in \mathbb{Z}. \end{cases}$$

С помощью очевидных преобразований эту систему можно переписать в виде

$$\begin{cases} w_1(t) = 1, \\ t^{-1} H_i t = H_{i+1}, \quad i \in \mathbb{Z}, \end{cases}$$

причём w_1 не содержит фрагментов вида $t^{-1}\overline{h}t$ и $t\overline{h}t^{-1}$, где $\overline{h} \in \overline{H}$.

Если $w_1(t)$ имеет длину 1, то есть первое уравнение системы переписывается в виде $t = u$, где $u \in \overline{G}$, то вся система переписывается в виде

$$\{u^{-1} H_i u = H_{i+1}, \quad i \in \mathbb{Z}\}.$$

Естественное отображение группы $\overline{H}$ в группу

$$\overline{\overline{G}} = \langle \overline{G} \mid \{u^{-1} H_i u = H_{i+1}, \quad i \in \mathbb{Z}\} \rangle$$

является инъективным в силу следующей теоремы, доказанной в [K93] (см. также [FeR96]).

Теорема. *Пусть A и B — группы без кручения, $v \in (A * B) \setminus A$ и φ — автоморфизм группы A. Тогда естественные отображения*

$$A \to \langle A * B \mid \{a^v = a^\varphi \mid a \in A\} \rangle \leftarrow B$$

инъективны.

Элемент t HNN-расширения $\widetilde{G} = \left\langle \overline{\overline{G}}, t \mid H_i^t = H_{i+1} \; i \in \mathbb{Z} \right\rangle$, очевидно, является решением уравнения (1) над $G = H_0 * K$. Ясно также, что он трансцендентен над $H = H_0$ по лемме 4, так как разложение (4) имеет место в $\widetilde{G}$, а значит и в U. (На самом деле, нетрудно заметить, что $\widetilde{G} \simeq U$.)

Рассмотрим теперь случай, когда длина (то есть число вхождений $t^{\pm 1}$) слова w_1 больше единицы. Рассмотрим следующие подгруппы группы $G * \langle t \rangle_\infty$: $K_i = t^{-i} K t^i$, $H_i = t^{-i} H t^i$,

$$\overline{H} = \mathop{\ast}_{i=-\infty}^{\infty} H_i, \quad K^{(m)} = \mathop{\ast}_{i=0}^{m} K_i \quad \text{и} \quad G^{(m)} = \overline{H} * K^{(m)}. \tag{5}$$

Рассмотрим все возможные записи уравнения (1) в виде

$$ct \prod_{i=1}^{n} b_i t^{-1} a_i t = 1, \quad \text{где } a_i, b_i, c \in G^{(m)}. \tag{6}$$

Из всех таких записей выберем те, в которых m минимально, после чего из всех записей с минимальным m выберем запись с наименьшим n. Для такой минимальной записи (6) будем иметь:

1) $n \geqslant 1$ (то есть длина этой записи строго больше единицы);
2) $a_i \notin G^{(m-1)} = \overline{H} * K_0 * \ldots * K_{m-1}$, а $b_i \notin (G^{(m-1)})^t = \overline{H} * K_1 * \ldots * K_m$;
3) a_i трансцендентен над $G^{(m-1)}$, а b_i трансцендентен над $(G^{(m-1)})^t$.

Первое свойство обеспечивается тем, что длина w_1 больше единицы, значит в записи длины 1 $m > 0$, следовательно, m можно уменьшить, заменив все вхождения элементов K_m на фрагменты вида $t^{-1} g t$, где $g \in K_{m-1}$. Второе свойство очевидным образом следует из условий минимальности n и m. Свойство 3) вытекает из свойства 2).

Пусть теперь символы H_i и K_i обозначают абстрактные изоморфные копии групп H и K, а группы $\overline{H}$, $K^{(m)}$ и $G^{(m)}$ определены формулами (5). Рассмотрим следующую систему уравнений над группой $G^{(m)}$:

$$\begin{cases} x^{-1} H_i x = H_{i+1}, & i \in \mathbb{Z}, \\ x^{-1} K_i x = K_{i+1}, & i \in \{0, \ldots m-1\}, \\ cx \prod_{i=1}^{n} b_i x^{-1} a_i x = 1. \end{cases} \tag{7}$$

Ясно, что всякое решение этой системы над $G^{(m)}$ будет решением уравнения (1) над G, трансцендентным над H (по лемме 4). Для завершения доказательства леммы 1 остаётся только заметить, что свойства 1) и 3) системы (7) влекут её разрешимость в силу следующей теоремы.

Теорема ([K84], см. также [FeR96]). *Пусть M и N — изоморфные подгруппы группы L, $\varphi : M \to N$ — изоморфизм, $n \in \mathbb{N}$, $a_1, \ldots, a_n$ — элементы группы L, трансцендентные над M, $b_1, \ldots, b_n$ — элементы группы L, трансцендентные над N, $c \in L$. Тогда система уравнений*

$$\begin{cases} x^{-1} g x = g^\varphi, & g \in M, \\ cx \prod_{i=1}^{n} b_i x^{-1} a_i x = 1 \end{cases}$$

разрешима над L.

4. Заключительные замечания

Определение унимодулярности обобщённых уравнений (определение 1) выглядело бы изящнее, если бы условие 3) имело вид

$\widetilde{3}$) группа $T / \langle \prod t_i \rangle$ не имеет кручения.

Назовём обобщённое уравнение (1′), удовлетворяющие условиям 1), 2) и $\widetilde{3}$) *слабо унимодулярными.*

Вопрос 1. *Верно ли, что всякое слабо унимодулярное обобщённое уравнение над группой без кручения разрешимо над ней?*

Если мы вовсе откажемся от условия 3) в определении 1, то получим понятие *невырожденного* обобщённого уравнения.

Вопрос 2. *Верно ли, что всякое невырожденное обобщённое уравнение над группой без кручения разрешимо над ней?*

Ответ на этот вопрос неизвестен и для обычных уравнений, но, надо полагать, в обобщённой ситуации легче построить контрпример.

Можно ли доказать обобщённые аналоги других известных фактов? например, теоремы Герстенхабера–Ротхауза ([GR62], см. также [ЛШ80])?

Вопрос 3. *Верно ли, что всякое (слабо) унимодулярное (или даже всякое невырожденное) обобщённое уравнение над конечной группой разрешимо над ней?*

Легко видеть, что из гипотезы Левина следует, что всякое разрешимое уравнение над группой без кручения магнусово. Поскольку до доказательства или опровержения этой гипотезы, судя по всему, ещё далеко, мы позволим себе сформулировать следующий условный вопрос.

Вопрос 4. *Верно ли, что утверждение о том, что всякое разрешимое уравнение над группой без кручения магнусово, равносильно гипотезе Левина?*

Нетрудно сообразить, что ответ на обобщённый вариант этого вопроса положителен.

ГЛАВА 22.
ГИПОТЕЗА КЕРВЕРА–ЛАУДЕНБАХА И КОПРЕДСТАВЛЕНИЯ ПРОСТЫХ ГРУПП

1. Соглашения

$G = \langle X \mid R \rangle$ — произвольная (если не оговорено противное) группа, $\widetilde{G} = \langle G, t \mid w = 1 \rangle \stackrel{\text{опр}}{=} \langle X \cup \{t\} \mid R \cup \{w\} \rangle$ — группа, полученая из группы G добавлением одного образующего и одного (произвольного) соотношения.

Под простой группой в этой главе понимается неабелева простая группа.

2. Введение

Напомним одну старую хорошо известную недоказанную теоретико-групповую гипотезу, имеющую топологическое происхождение.

Гипотеза Кервера–Лауденбаха (КЛ) (см., например, [ЛШ80], [МКС74]). *Если группа G нетривиальна, то и группа $\widetilde{G}$ нетривиальна.*

Мы позволим себе высказать другую похожую гипотезу.

«Простая» гипотеза Кервера–Лауденбаха (КЛп). *Если группа G непроста, то и группа $\widetilde{G}$ непроста.*

Сходство между этими вопросами не только внешнее.

Утверждение 1. *Гипотеза* **КЛ** *эквивалентна гипотезе* **КЛп**.

Наиболее известным результатом в направлении доказательства гипотезы **КЛ** является следующая замечательная теорема.

Теорема Герстенхабера–Ротхауза [GR62]. *Если группа G конечна и нетривиальна, то и группа $\widetilde{G}$ нетривиальна.***

Из этого результата нетрудно вывести аналогичную «простую» теорему.

Теорема 1. *Если группа G конечна и непроста, то и группа $\widetilde{G}$ непроста.*

Возьмём другой результат, частично подтверждающий гипотезу **КЛ**.

Теорема [K93]. *Если группа G без кручения и нетривиальна, то и группа $\widetilde{G}$ нетривиальна.*

Аналогичная «простая» теорема имеет вид.

Теорема 2. *Если группа G без кручения и непроста, то и группа $\widetilde{G}$ непроста.*

Теорема 1 и утверждение 1 доказываются очень просто. Основным содержанием этой главы является доказательство теоремы 2. На самом деле, мы установим более сильный факт.

Основная теорема. *Если группа G не имеет кручения, то группа $\widetilde{G}$ проста тогда и только тогда, когда группа G проста и слово w сопряжено в свободном произведении $G * \langle t \rangle_\infty$ со словом вида $t^{\pm 1} g$, где $g \in G$.*

Можно ли аналогичным образом усилить теорему 1, нам неизвестно.

Отметим, что из основной теоремы и того хорошо известного факта, что всякая группа без кручения вкладывается в простую группу без кручения, немедленно вытекает следующий результат Коэна и Рурка.

Теорема [CR01]. *Если группа G не имеет кручения, то естественное отображение $G \to \widetilde{G}$ сюръективно тогда и только тогда, когда слово w сопряжено в свободном произведении $G * \langle t \rangle_\infty$ со словом вида $t^{\pm 1} g$, где $g \in G$.*

Наше доказательство основной теоремы почти сразу распадается, в зависимости от слова w, на два случая — лёгкий и трудный. Забавно, что трудный случай в точности соответствует словам сложности 1 (в смысле Форестера и Рурка [FoR05]), со словами большей сложности дело обстоит гораздо проще.

Помимо прочего, глава содержит полное и замкнутое изложение метода кодвижений, который мы применяем для доказательства основной теоремы в трудном случае, тогда как в лёгком случае наши геометрические рассуждения сводятся к простому использованию леммы о движениях из [K93].

** На самом деле теорема Герстенхабера–Ротхауза утверждает нечто большее, мы сформулировали лишь важнейший частный случай (см. [ЛШ80]).

3. Доказательство утверждения 1 и теоремы 1

Пусть циклически несократимая форма слова w имеет вид

$$w \equiv g_1 t^{\varepsilon_1} \dots g_n t^{\varepsilon_n}, \quad \text{где } \varepsilon_i \in \{\pm 1\},\ g_i \in G.$$

(Эти обозначения мы считаем фиксированными до конца главы.)

Следующая переформулировка гипотезы Кервера–Лауденбаха хорошо известна.

Утверждение 2 (фольклор). *Гипотеза* **КЛ** *эквивалентна следующей гипотезе* **КЛ′**.

Гипотеза КЛ′. *Если* $\sum \varepsilon_i = \pm 1$, *то естественное отображение* $G \to \widetilde{G}$ *инъективно.*

Доказательство. Предположим, что гипотеза **КЛ′** верна, и докажем **КЛ**. Если $G \neq \{1\}$ и $\sum \varepsilon_i = \pm 1$, то группа $\widetilde{G}$ нетривиальна, так как содержит нетривиальную подгруппу, изоморфную группе G. Если же $\sum \varepsilon_i \neq \pm 1$, то группа $\widetilde{G}$ нетривиальна, так как допускает эпиморфизм на нетривиальную группу $\mathbb{Z}/(\sum \varepsilon_i)\mathbb{Z}$.

Предположим теперь, что гипотеза **КЛ′** неверна, и опровергнем **КЛ**. Пусть $\sum \varepsilon_i = \pm 1$ и $N \neq \{1\}$ есть ядро естественного отображения $G \to \widetilde{G}$. Хорошо известно, что любая группа G вкладывается в некоторую простую группу H (см., например, [ЛШ74]). Тогда группа $\widetilde{H} \stackrel{\text{опр}}{=} \langle H, t \mid w = 1 \rangle$ очевидным образом тривиальна:

$$\widetilde{H} \simeq \widetilde{H} / \langle\langle N \rangle\rangle \simeq \widetilde{H} / \langle\langle H \rangle\rangle \simeq \mathbb{Z} \Big/ (\textstyle\sum \varepsilon_i)\, \mathbb{Z} \simeq \{1\}.$$

Здесь и далее $\langle\langle X \rangle\rangle$ обозначает нормальную подгруппу, порождённую множеством X. Утверждение 2 доказано.

Доказательство утверждения 1. Предположим, что **КЛ** неверна, то есть для некоторой нетривиальной группы G группа $\widetilde{G}$ тривиальна. Пусть S – некоторая простая группа. Тогда группа $G \times S$ непроста, но группа $\langle G \times S, t \mid w = 1 \rangle \simeq S$ проста. Таким образом гипотеза **КЛп** также неверна.

Предположим теперь, что **КЛп** неверна, то есть для некоторой непростой группы G группа $\widetilde{G}$ проста. Заметим прежде всего, что группа G неабелева и $\sum \varepsilon_i = \pm 1$, так как иначе группа $\widetilde{G}$ не совпадала бы со своим коммутантом (или была бы тривиальной) и, следовательно, не была бы простой. Если естественное отображение $G \to \widetilde{G}$ не инъективно, то **КЛ** неверна в силу утверждения 2. Допустим, что естественное отображение $G \to \widetilde{G}$ инъективно. Пусть N – некоторая собственная нетривиальная нормальная подгруппа группы G. Тогда группа $\widetilde{G} / \langle\langle N \rangle\rangle$, с одной стороны, тривиальна (так как $\widetilde{G}$ проста, а $N \neq \{1\}$ в $\widetilde{G}$ в силу инъективности отображения $G \to \widetilde{G}$), а с другой стороны, изоморфна группе $\langle G/N, t \mid w' = 1 \rangle$, где w' получается из w приведением по модулю N. Таким образом, гипотеза **КЛ** также неверна. Утверждение 1 доказано.

Доказательство теоремы 1. Теорема 1 выводится из теоремы Герстенхабера–Ротхауза дословно так же, как гипотеза **КЛп** выводится из **КЛ**; надо только помнить, что факторгруппа конечной группы конечна и всякая конечная группа вкладывается в простую конечную группу (например, в знакопеременную).

Заметим, что доказать так же просто теорему 2 не удаётся по той причине, что класс групп без кручения, в отличие от класса конечных групп, не замкнут относительно перехода к факторгруппам. Вся оставшаяся часть главы представляет собой доказательство теоремы 2 (точнее, основной теоремы).

4. Алгебраические леммы

Обозначения, которые мы используем, в целом стандартны. Отметим только, что если $k \in \mathbb{Z}$, x и y — элементы некоторой группы, а φ — гомоморфмзм из этой группы в какую-нибудь другую группу, то x^y, x^{ky}, x^{-y}, x^φ, $x^{k\varphi}$ и $x^{-\varphi}$ обозначают $y^{-1}xy$, $y^{-1}x^k y$, $y^{-1}x^{-1}y$, $\varphi(x)$, $\varphi(x^k)$ и $\varphi(x^{-1})$ соответственно.

Лемма 1. *Пусть* A *и* B *— группы без кручения,* $u \in (A * B) \setminus A$. *Тогда* $\langle A, u \rangle = A * \langle u \rangle_\infty$. *Если при этом группа* A *нетривиальная, а* B *нециклическая, то найдётся такое слово* $v \in A * B$, *что* $\langle A, u, v \rangle = A * \langle u \rangle_\infty * \langle v \rangle_\infty$.

Доказательство. Ясно, что можно считать, что слово u в несократимой записи начинается и кончается на буквы из B.

Для таких u первое утверждение леммы очевидно, докажем второе утверждение. Если $u \in B$, то в качестве v можно взять слово $v = a^b$, где b — произвольный элемент группы B, не лежащий в циклической подгруппе, порождённой элементом u, а a — произвольный неединичный элемент группы A. Если же $u \notin B$, $u = b_1 a_1 \dots b_k$, то в качестве v можно взять слово $v = a^b$, где $b \in B \setminus \{b_1^{\pm 1}, b_k^{\pm 1}\}$, а $a \in A \setminus \{1\}$. Лемма доказана.

Следующая лемма представляет собой одну из возможных формулировок алгебраического трюка из [К93], который часто используется для исследования уравнений над группами и смежных вопросов (см. [КП95], [CG95], [CG00], [CR01], [FeR96], [FeR98], [FoR05]). Геометрическую интерпретацию этого приёма можно найти в [FoR05].

Лемма 2. *Предположим, что группа G не имеет кручения,*

$$\sum \varepsilon_i = 1 \quad \text{и} \quad n > 1. \tag{1}$$

Тогда группа $\widetilde{G}$ обладает (относительным) копредставлением вида

$$\widetilde{G} \simeq \left\langle H, t \;\middle|\; \{p^t = p^\varphi,\ p \in P \setminus \{1\}\},\ ct \prod_{i=0}^{m} (b_i a_i^t) = 1 \right\rangle, \tag{2}$$

где $a_i, b_i, c \in H$, P и P^φ — изоморфные подгруппы группы H, $\varphi\colon P \to P^\varphi$ — изоморфизм между ними. При этом

1) *$m \geqslant 0$ (то есть произведение в формуле (2) непустое);*
2) *$a_i \notin P$, а $b_i \notin P^\varphi$;*
3) *$\langle P, a_i \rangle = P * \langle a_i \rangle_\infty$ и $\langle P^\varphi, b_i \rangle = P^\varphi * \langle b_i \rangle_\infty$ в H;*
4) *если группа G нециклическая и $P \neq \{1\}$, то для каждого i найдутся такие элементы $a_i', b_i' \in H$, что $\langle P, a_i, a_i' \rangle = P * \langle a_i \rangle_\infty * \langle a_i' \rangle_\infty$ и $\langle P^\varphi, b_i, b_i' \rangle = P * \langle b_i \rangle_\infty * \langle b_i' \rangle_\infty$ в H;*
5) *группы H, P и P^φ являются свободным произведением конечного числа изоморфных копий группы G: $H = G^{(0)} * \ldots * G^{(s)}$, $P = G^{(0)} * \ldots * G^{(s-1)}$, $P^\varphi = G^{(1)} * \ldots * G^{(s)}$, где $s \geqslant 0$ (при $s = 0$ группы P и P^φ тривиальны), а изоморфизм φ представляет собой сдвиг: $\left(G^{(i)}\right)^\varphi = G^{(i+1)}$.*

Доказательство. Сначала покажем, что у группы $\widetilde{G}$ имеется по крайней мере одно копредставление вида (2), удовлетворяющее условию 5). Поскольку $\sum \varepsilon_i = 1$, слово w можно записать в виде

$$w = \left(\prod g_i^{t^{k_i}} \right) t.$$

Сопрягая, если надо, w при помощи t, мы можем считать, что $k_i \geqslant 0$. Полагая $g^{(i)} = g^{t^i}$ для $g \in G$, $G^{(i)} = G^{t^i}$, $s = \max k_i$ и $c = \prod g_i^{(k_i)}$. Мы видим, что $\widetilde{G}$ обладает копредставлением

$$\widetilde{G} \simeq \left\langle G^{(0)} * \ldots * G^{(s)}, t \;\middle|\; \left\{ \left(g^{(i)}\right)^t = g^{(i+1)},\ i = 0, \ldots, s-1,\ g \in G \right\},\ ct = 1 \right\rangle,$$

то есть копредставлением вида (2) (с $m = -1$), удовлетворяющим условию 5).

Теперь из всех копредставлений вида (2) группы $\widetilde{G}$, удовлетворяющих условию 5), выберем те, в которых s минимально, а из всех копредставлений с минимальным s выберем то, в котором m минимально. Полученное копредставление (2) будет искомым.

Действительно, если $m < 0$ (то есть $w = ct$, где $c \in H$), то $s = 0$, так как в противном случае мы могли бы уменьшить s, заменив в слове c все вхождения $g^{(s)}$ на $(g^{(s-1)})^t$. Но условия $m < 0$ и $s = 0$ означают, что исходное слово w имеет вид $w = ct$, $c \in G$, что противоречит тому, что $n > 1$. Таким образом условие 1) выполнено.

Условие 2) выполнено, поскольку в противном случае мы могли бы в копредставлении (2) заменить подслово $t^{-1} a_i t$, где $a_i \in P$ (или подслово $t b_i t^{-1}$, где $b_i \in P^\varphi$), на a_i^φ (соответственно, на $b_i^{\varphi^{-1}}$), уменьшив тем самым m (не увеличив при этом s).

Условия 3) и 4) следуют из условий 2) и 5) в силу леммы 1. Лемма 2 доказана.

5. Карты и движения

Под поверхностью в этой главе мы всегда понимаем замкнутую двумерную ориентированную поверхность.

Картой M на поверхности S называется конечный набор непрерывных отображений $\{\mu_i\colon D_i \to S\}$, где D_i — двумерный замкнутый ориентированный диск (круг), называемый i-й *гранью* или *клеткой* карты, на границе которого отмечено некоторое конечное непустое множество точек $c_{ij} \in \partial D_i$, называемых *углами* карты. Интервалы e_{ij}, на которые углы делят границу грани, мы называем *прорёбрами* карты. Образы углов $\mu_i(c_{ij})$ и прорёбер $\mu_i(e_{ij})$ называют *вершинами* и *рёбрами* карты соответственно. При этом предполагается, что

1) ограничения отображения μ_i на внутренность грани D_i является гомеоморфным вложением, сохраняющим ориентацию; ограничение μ_i на каждое проребро является гомеоморфным вложением;
2) различные ребра не пересекаются;
3) образы внутренностей разных граней не пересекаются;
4) $\bigcup \mu_i(D_i) = S$.

Карту M мы будем также иногда трактовать как непрерывное отображение $\mathrm{M}\colon \coprod D_i \to S$ из дискретного объединения дисков в поверхность.

Объединение всех вершин и рёбер карты представляет собой граф на поверхности, называемый *одномерным остовом*. *Кратностью* точки одномерного остова мы называем число инцидентных ей рёбер, если эта точка является вершиной; если же эта точка лежит на ребре, то её кратность считается равной двум. Другими словами, кратность точки p равна $\left|\mathrm{M}^{-1}(p)\right|$.

Мы говорим, что угол c является углом при вершине v, если $\mathrm{M}(c) = v$. На множестве всех углов при вершине v имеется естественный циклический порядок; мы называем два угла при вершине v *смежными*, если они являются соседними относительно этого порядка.

Допуская некоторую вольность речи, мы говорим, что точка или подмножество поверхности содержится в грани D_i, если она (оно) лежит в образе μ_i. Аналогично, мы говорим, что грань D_i содержится в некотором подмножестве $X \subseteq S$ поверхности S, если $\mathrm{M}(D_i) \subseteq X$.

На рисунке 1 представлена карта на сфере с пятью гранями: A, B, C, D и E, восемнадцатью углами: a_i, b_i, c_i, d_i и e_i, шестью вершинами, девятью рёбрами и восемнадцатью прорёбрами. Заметим, что число углов всегда равно числу прорёбер и вдвое больше числа рёбер, а величина

$$e(S) \stackrel{\text{опр}}{=} (\textit{число вершин}) - (\textit{число ребер}) + (\textit{число граней})$$

не зависит от выбора карты на поверхности S и называется *эйлеровой характеристикой* этой поверхности. Эйлерова характеристика сферы (единственной поверхности, которая нас на самом деле интересует в этой главе) равна двум.

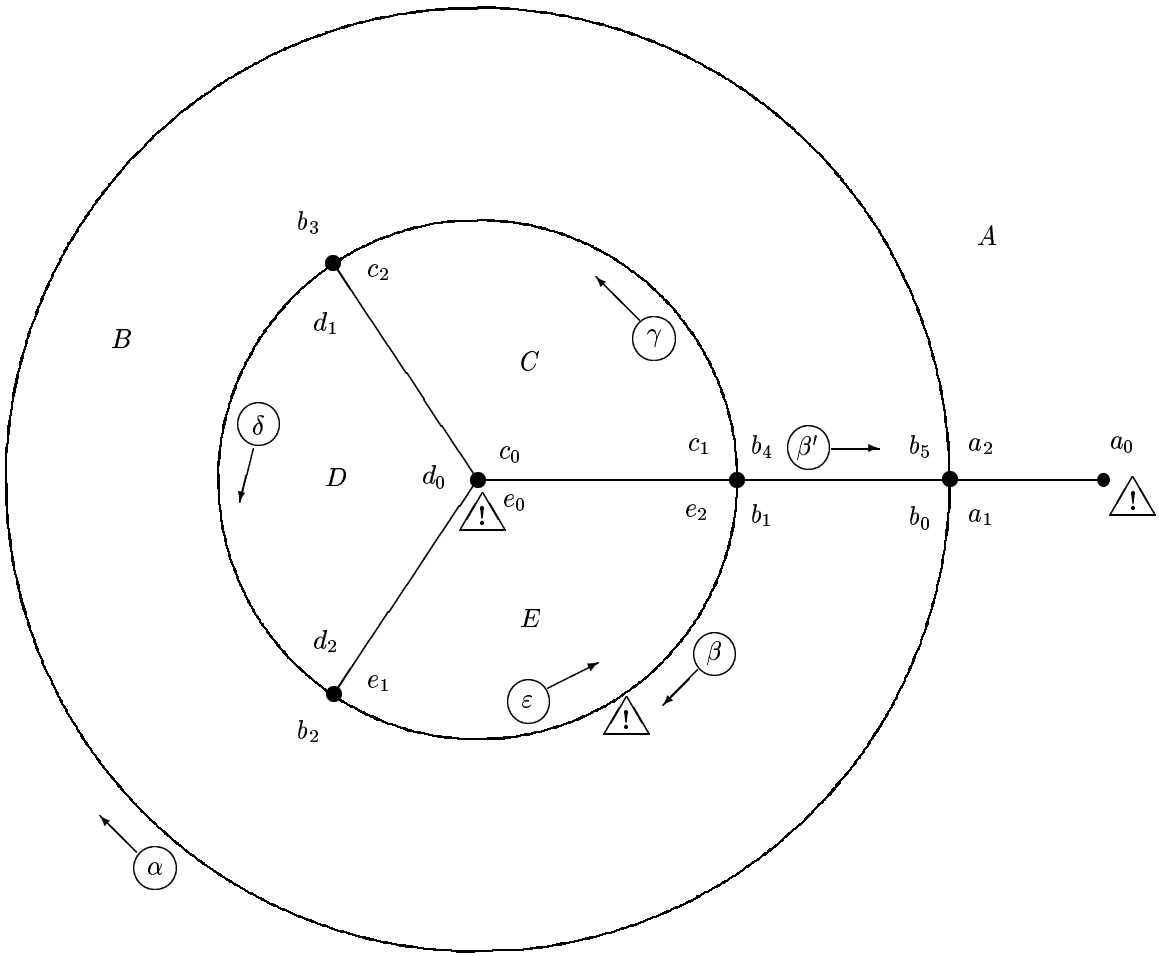


Рис. 1

Движением на ориентированной поверхности S называется карта $\mathrm{M}\colon \coprod D_i \to S$ на этой поверхности и набор непрерывных отображений $\alpha_i\colon \mathbb{R} \to \partial D_i$. Отображение α_i мы называем *автомобилем*, объезжающим грань D_i. Мы говорим, что автомобиль α_i находится в углу $c \in \partial D_i$ в момент времени $t \in \mathbb{R}$ если $\alpha_i(t) = c$, кроме того, мы говорим, что в момент времени $t \in \mathbb{R}$ автомобиль α_i *находится* в точке $p \in S$, если $\mu_i(\alpha_i(t)) = p$. Если число автомобилей, оказавшихся в момент времени t в точке p одномерного остова поверхности, S равно кратности этой точки (иными словами $\bigcup \alpha_i(t) \supseteq \mathrm{M}^{-1}(p)$), то мы говорим, что в точке p в момент t происходит *полное столкновение*. При этом точка p называется *точкой полного столкновения*. Точки полного столкновения, лежащие на рёбрах, мы называем просто *точками столкновеня*.

Движение называется *правильным*, если отображения α_i являются накрытиями, сохраняющими ориентацию. Говоря по-простому, при правильном движении автомобиль объезжает границу своей грани против часовой стрелки (внутренность грани остаётся слева от автомобиля) и при этом едет без разворотов, без остановок, и без «бесконечных замедлений и ускорений».

Пример 1. На карте, изображённой на рисунке 1, можно определить правильное движение так: автомобили α, β, γ, δ и ε, объезжающие грани A, B, C, D и E соответственно, движутся с единичной скоростью (одно ребро в единицу времени) в положительном направлении, находясь в нулевой момент времени в углах a_0, b_0, c_0, d_0 и e_0 соответственно (в углы с номером i автомобили при этом попадают в момент $t = i$). На рисунке 1 показано положение автомобилей и направление их движения в момент времени $t = 4/3$ (на автомобиль β' пока не нужно обращать внимание). При таком режиме движения имеется 3 точки полного столкновения, они помечены восклицательными знаками на рисунке 1: в моменты времени кратные трём происходит полное столкновение автомобилей γ, δ и ε; в моменты времени $t \in 3/2+6\mathbb{Z}$ происходит столкновение на ребре автомобилей β и ε; кроме того, в моменты времени кратные трём автомобиль α заезжает в тупик, что, согласно нашему определению, также является полным столкновением. Можно добиться того, что точек полного столкновения останется две, изменив расписание движения на этой карте (например, заставив автомобиль ε ехать со скоростью 2 на рёбрах

$[e_0, e_1]$ и $[e_1, e_2]$ и со скоростью $1/2$ на ребре $[e_2, e_0]$). Дальнейшая оптимизация расписания невозможна, как показывает следующее утверждение.

Лемма 3 [K93] (см. также [FeR96]). *При любом правильном движении на сфере по крайней мере в двух точках происходит полное столкновение.*

Так же как в [K93] (или в [FeR96]), нам будет удобно рассматривать движения чуть более общие, чем правильные.

Мы называем непрерывное отображение $\alpha\colon X \to Y$ ориентированной прямой или окружности X в ориентированную окружность Y (локально) *неубывающим*, если прообраз всякого интервала $U \subset Y$ есть объединение интервалов, ограничение α на каждый из которых является неубывающей функцией (в обычном смысле, как отображение одного ориентированного интервала в другой). Назовём отображение $\alpha\colon X \to Y$ прямой в окружность *собственным*, если образ всякого луча $U \subset X$ есть вся окружность Y.

Прообраз точки при собственном неубывающем отображении прямой в окружность является дискретным объединением точек и отрезков. Точку $y \in Y$, прообраз которой недискретен, будем называть *точкой остановки* отображения.

Движение на поверхности S называется *движением с разделёнными остановками*, если каждый автомобиль является собственной неубывающей функцией, каждая точка остановки которой является углом (то есть, говоря по-простому, каждый автомобиль едет без разворотов и бесконечных замедлений и ускорений, объезжая границу своей грани против часовой стрелки, возможно, останавливаясь на конечное время в некоторых углах). При этом можно выделить такое множество углов, называемых *остановочными углами*, что

1) автомобили останавливаются только в остановочных углах (возможно, не во всех остановочных углах автомобили действительно останавливаются);
2) в каждой вершине v, при которой имеется хотя бы один остановочный угол, остановки разделены в следующем смысле: пусть $c_1, \ldots, c_k$ — это все остановочные углы при вершине v, занумерованные против часовой стрелки. Требуется, чтобы для каждого i в углах c_i и c_{i+1} (индексы по модулю k) автомобили никогда не находились одновременно. (В частности, это условие означает, что $k \geqslant 2$.)

Лемма 4 [K93] (см. также [FeR96]). *При любом движении с разделёнными остановками на сфере по крайней мере в двух точках происходит полное столкновение.*

Доказательство. Во-первых, ясно, что движение автомобиля, проезжающего через остановочный угол, можно немного изменить в маленькой окрестности этого угла так, чтобы он действительно останавливался в этом углу, при этом не добавив новых точек полного столкновения и оставив выполненным условие разделённости остановок.

Предполагая теперь, что каждый раз, проезжая остановочный угол, автомобиль действительно останавливается, сделаем следующее преобразование карты, которое мы называем *раздутием остановочных углов* (см. рис. 2): возьмём вершину v, при которой имеется $k \geqslant 2$ остановочных углов $c_1, \ldots, c_k$; сделаем надрез поверхности вдоль небольшой дуги, ведущей из вершины v «внутрь» угла c_i; края этого надреза назовём x_i (левый край, если смотреть от вершины v) и y_i (правый край, если смотреть от вершины v); когда мы сделаем эти разрезы для всех $i = 1, \ldots, k$, на поверхности возникнет дыра с границей, состоящей из последовательных участков $y_1, x_1, y_2, x_2, \ldots, y_k, x_k$; заклеим эту дыру, склеив каждый из участков x_i с y_{i+1} (индексы по модулю k); получится новая карта M' на той же поверхности, которая отличается от старой наличием дополнительных прорёбер x_i и y_i в том месте границы грани, где был остановочный угол c_i, и дополнительных рёбер $\mathrm{M}'(x_i) = \mathrm{M}'(y_{i+1})$.

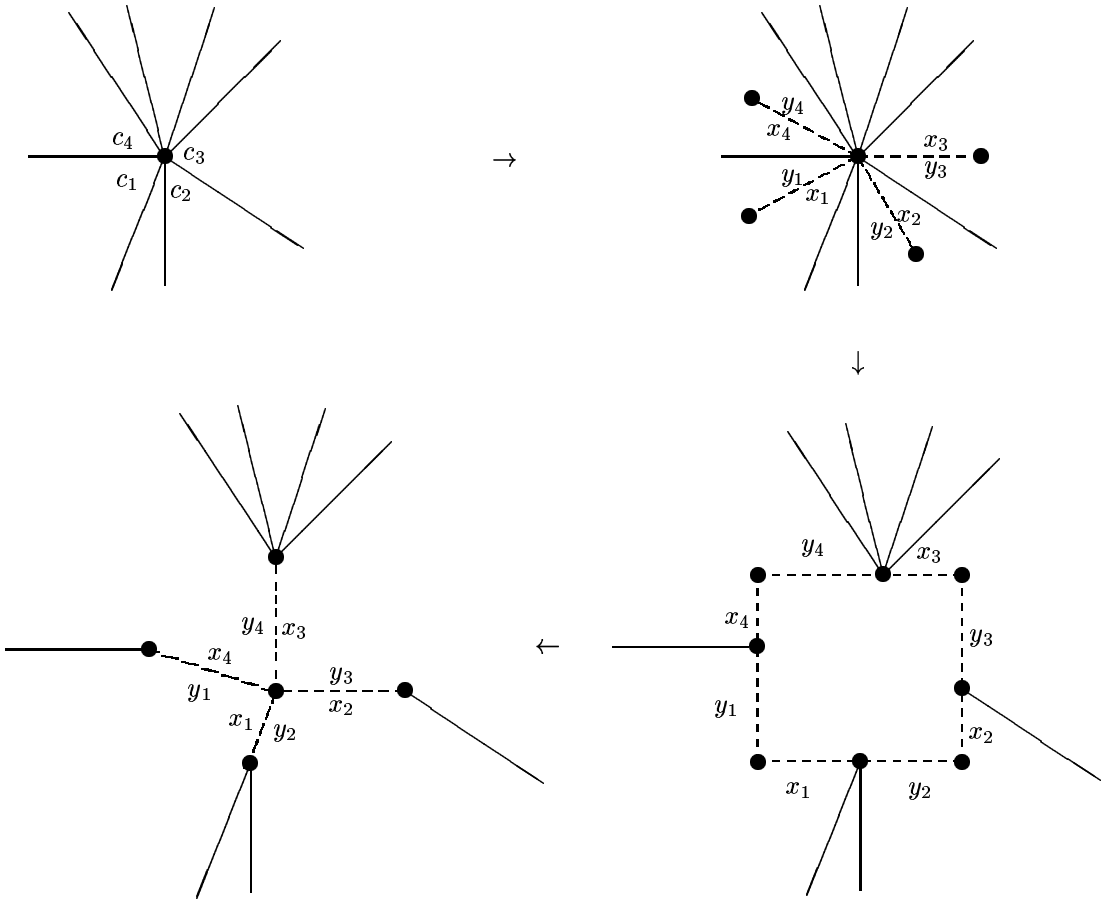


Рис. 2

Сделав описанное выше преобразование для каждой вершины v, при которой имеются остановочные углы, определим правильное движение на получившейся карте так: автомобили едут так же, как на исходной карте, но в то время, когда автомобиль на исходной карте стоит в остановочном углу c_i, соответствующий автомобиль на новой карте равномерно движется по возникшему на месте этого угла отрезку $x_i \cup y_i$. Из условия разделённости остановок следует, что при этом правильном движении на новой карте полные столкновения не могут происходить на дополнительных рёбрах и в их концах. Для завершения доказательства остаётся сослаться на лемму 3.

Отметим, что условие разделённости остановок означает, в частности, что полное столкновение не может произойти в вершине, при которой имеется хотя бы один остановочный угол.

6. Диаграммы Хауи

Пусть имеется карта M на поверхности S, углы которой помечены элементами некоторой группы H, а рёбра ориентированны (на рисунках на них имеются стрелки) и помечены элементами некоторого множества $\{t_1, t_2, \ldots\}$, не пересекающегося с группой H. Метку угла или ребра x будем обозначать $\lambda(x)$.

Метка вершины v в такой ситуации определяется формулой

$$\lambda(v) = \prod_{i=1}^{k} \lambda(c_i),$$

где $c_1, \ldots, c_k$ — это все углы при вершине v, перечисленные по часовой стрелке. Метка вершины является элементом группы H, определённым с точностью до сопряжённости.

Метка грани D определяется формулой

$$\lambda(D) = \prod_{i=1}^{k} \big(\lambda(\mathrm{M}(e_i))\big)^{\varepsilon_i} \lambda(c_i),$$

где $e_1, \ldots, e_k$ и $c_1, \ldots, c_k$ — это все прорёбра и все углы грани D, перечисленные против часовой стрелки, причём концами проребра e_i являются углы c_{i-1} и c_i (индексы по модулю k), а $\varepsilon_i = \pm 1$ в зависимости от того, сохраняет или обращает ориентацию гомеоморфизм $e_i \xrightarrow{\mathrm{M}} \mathrm{M}(e_i)$. Говоря по-простому, чтобы получить метку грани, надо обойти её границу против часовой стрелки, выписывая метки всех встречающихся углов и рёбер, причём метку ребра надо записывать в минус первой степени, если мы его проходим против стрелки.

Метка грани является элементом группы $H * F(t_1, t_2, \ldots)$ (свободного произведения H и свободной группы с базисом $\{t_1, t_2, \ldots\}$), определённым с точностью до циклической перестановки. Более точно, правую часть нашей формулы для $\lambda(D)$ мы называем *меткой грани D, написанной начиная с проребра e_1*.

Размеченную таким образом карту мы называем *диаграммой Хауи* (или просто *диаграммой*) над относительным копредставлением

$$\langle H, t_1, t_2, \ldots \mid w_1 = 1, w_2 = 1, \ldots \rangle, \qquad (*)$$

если

1) некоторые вершины и некоторые грани выделены и называются *внешними*, остальные вершины и грани называются *внутренними*;
2) метка каждой внутренней грани является циклической перестановкой одного из слов $w_i^{\pm 1}$;
3) метка каждой внутренней вершины равна единице в группе H.

Диаграмма Хауи называется *приведённой*, если она не содержит такого ребра e, что две грани, его содержащие, являются внутренними, эти грани различны, а их метки, написанные начиная с M-прообразов ребра e, взаимнообратны; такая пара клеток с общим ребром называется *сократимой парой*.

Следующая лемма является аналогом леммы ван Кампена для относительных копредставлений.

Лемма 5 [How83]. *Естетвенное отображение группы H в группу, заданную относительным копредставлением $(*)$, не является инъективным тогда и только тогда, когда существует сферическая диаграмма над этим копредставлением с единственной внешней вершиной и без внешних граней, причём метка внешней вершины не равна единице в группе H. Минимальная (по числу клеток) из таких диаграмм является приведённой. Если это естественное отображение инъективно, то имеет место эквивалентность: образ элемента*

$$u \in H * F(t_1, t_2, \ldots) \setminus \{1\}$$

равен единице в группе $(*)$ тогда и только тогда, когда существует сферическая диаграмма над этим копредставлением без внешних вершин и с единственной внешней гранью, метка которой равна u. Минимальная (по числу клеток) из таких диаграмм также является приведённой.

Диаграммы на сфере с единственной внешней гранью и без внешних вершин называют также *дисковыми* диаграммами, границу внешней грани такой диаграммы называют *контуром* диаграммы.

Пусть $\varphi\colon P \to P^\varphi$ — изоморфизм между двумя подгруппами группы H. Относительное копредставление вида

$$\langle H, t \mid \{p^t = p^\varphi;\ p \in P \setminus \{1\}\}, w_1 = 1,\ w_2 = 1,\ \ldots \rangle \qquad (**)$$

назовём *φ-копредставлением*. Диаграмму над φ-копредставлением $(**)$ назовём *φ-приведённой* если она приведена и различные внутренние клетки, метки которых имеют вид $p^t p^{-\varphi}$, $p \in P$, не имеют общих рёбер.

Лемма 6. *Минимальная (по числу клеток) из всех сферических диаграмм над данным φ-копредставлением без внешних граней и с единственной внешней вершиной, метка которой не равна единице, является φ-приведённой. Если таких диаграмм не существует, то минимальная дисковая диаграмма с данной меткой контура является φ-приведённой.* Другими словами, имеет место полный φ-аналог леммы 5.

Доказательство. Действительно, если в какой-то диаграмме над копредставлением $(**)$ пара клеток, соответствующих соотношениям вида $p^t p^{-\varphi}$, $p \in P$ имеет общее ребро, то либо такая пара клеток есть сократимая пара, либо общее ребро можно стереть, перемножив метки сливающихся при этом углов (рис. 3) и получить диаграмму с меньшим числом клеток и такими же метками внешних граней и вершин, что означает неминимальность исходной диаграммы и доказывает лемму.

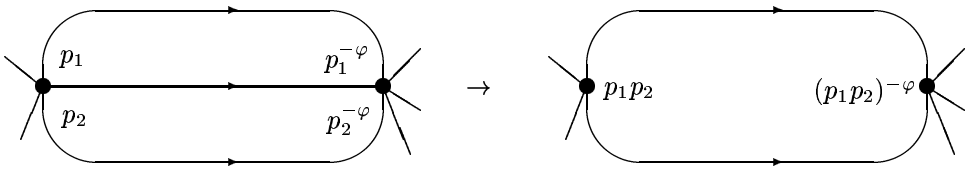


Рис. 3

Относительное копредставление (φ-копредставление), над которым не существует приведённых (соответственно, φ-приведённых) сферических диаграмм с единственной внешней вершиной и без внешних граней, будем называть *асферичными* (соответственно, *φ-асферичными*).

Лемма 7. *Пусть группа H в копредставлении $(*)$ нетривиальна и найдётся такое слово $w \in H * F(t_1, t_2, \ldots)$, несопряжённое в $H * F(t_1, t_2, \ldots)$ ни с одним из элементов множества $H \cup \{w_i^{\pm 1}\}$, что копредставление*

$$L = \langle H, t_1, t_2, \ldots \mid w = 1, w_1 = 1, w_2 = 1, \ldots \rangle$$

либо асферично, либо φ-асферично, если исходное копредставление $(*)$ является φ-копредставлением. Тогда группа K, заданная копредставлением $(*)$, непроста

Доказательство. Из (φ-)асферичности копредставления L следует (φ-)асферичность копредставления $(*)$.

Покажем, что $w \neq 1$ в группе K. Действительно, в противном случае, в силу (φ-)асферичности копредставления $(*)$ и лемм 5 и 6, над этим копредставлением существовала бы (φ-)приведённая дисковая диаграмма с меткой контура w. Но такую диаграмму можно рассматривать как (φ-)приведённую сферическую диаграмму над копредставлением L без внешних граней и вершин, а таких диаграмм не бывает по условию.

Естественное отображение группы H в группу L инъективно по лемме 5 (и лемме 6), значит,

$$L = K / \langle\langle w \rangle\rangle \neq \{1\},$$

то есть $\langle\langle w \rangle\rangle$ является собственной нетривиальной нормальной подгруппой в K, что и требовалось доказать.

7. Стандартное движение

Пусть имеется карта на поверхности, рёбра которой ориентированы (например, диаграмма Хауи). На такой карте бывает 4 сорта углов: $(++)$, $(--)$, $(+-)$ и $(-+)$ (рис. 4).

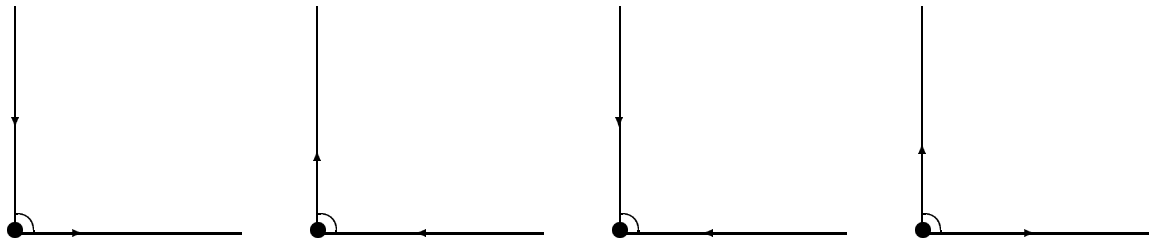


Рис. 4

Следующую лемму мы не доказываем ввиду её очевидности.

Лемма 8. *При обходе против часовой стрелки углов при любой вершине v углы типа $(++)$ и $(--)$ чередуются. Если же при вершине v углов типа $(++)$ нет, или, что то же самое, углов типа $(--)$ нет, то либо все углы при v имеют тип $(+-)$ (в этом случае вершина v называется стоком), либо все углы при v имеют тип $(-+)$ (в этом случае вершина v называется источником)* (рис. 5).

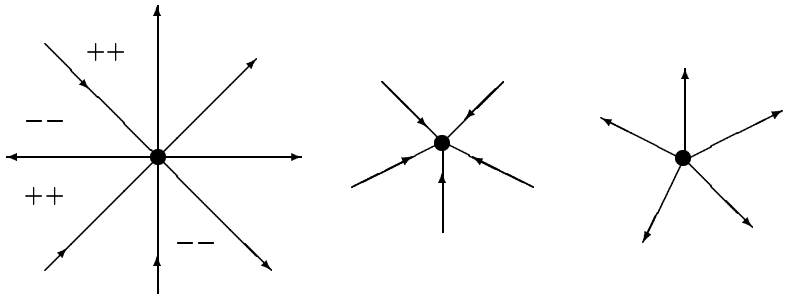


Рис. 5

Мы скажем, что карта с ориентированными рёбрами имеет тип A_m, $m \geqslant 0$, если последовательность ориентаций прорёбер каждой грани имеет одну из четырёх форм:

а) $+-$ (рисунок 6а);

б) $+(+-)^{m+1}$ (рисунок 6б);

в) $-(-+)^{m+1}$ (рисунок 6в);

г) $(+)^{k+1}(-)^{l+1}$, $k, l \geqslant 1$ (рисунок 6г).

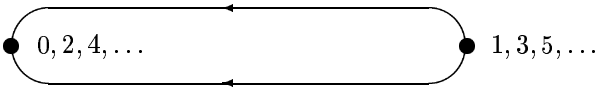
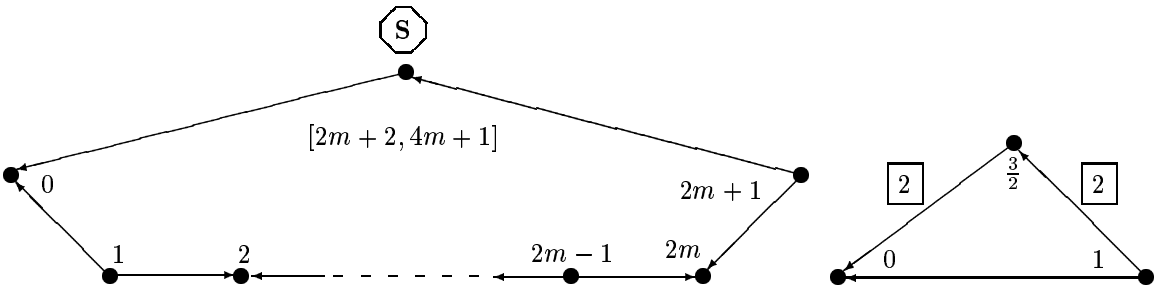
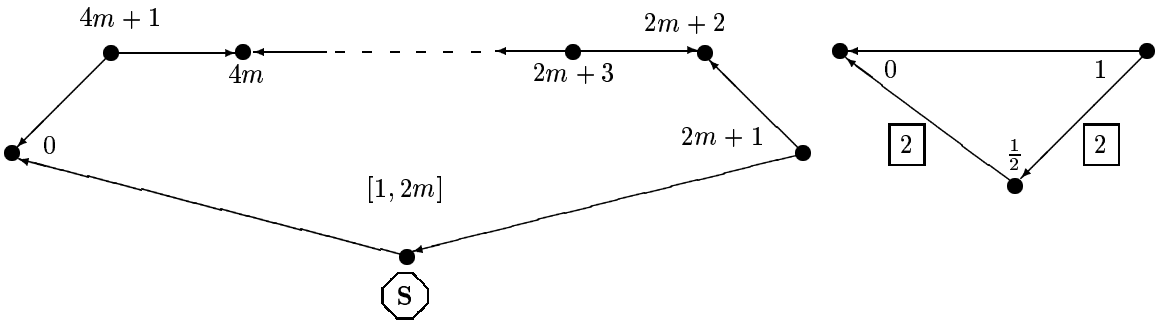


Рис. 6а



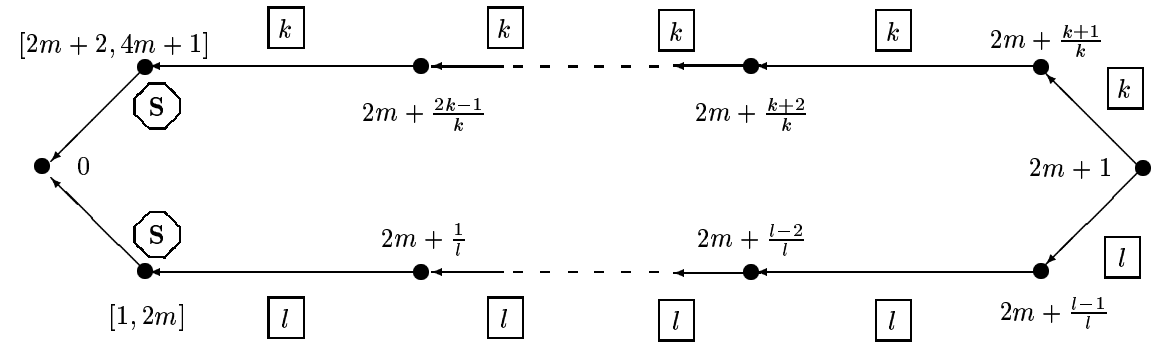
$m > 0$ $\qquad$ $m = 0$

Рис. 6б

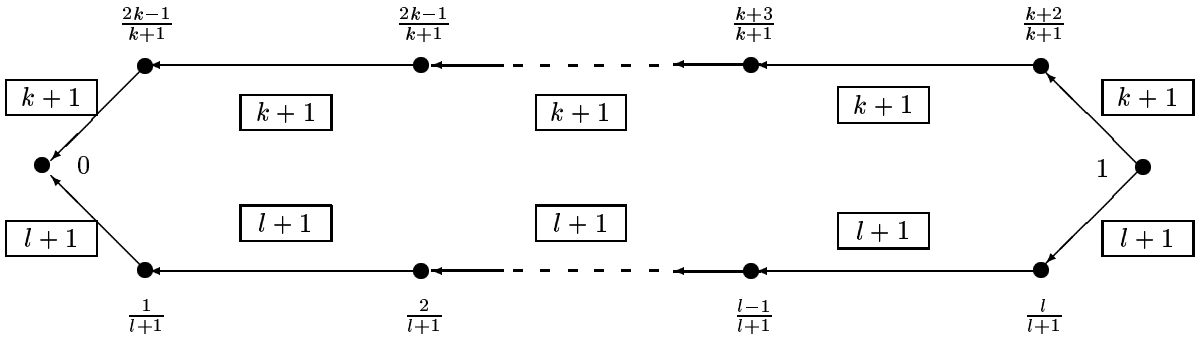


$m > 0$ $\qquad$ $m = 0$

Рис. 6в



$m > 0$



$m = 0$

Рис. 6г

Определим *стандартное движение* на карте типа A_m следующим образом:

а) автомобиль, объезжающий грань типа $+-$, движется против часовой стрелки равномерно с единичной скоростью (одно ребро в единицу времени), проезжая в нулевой момент времени угол типа $(+-)$ (рис. 6а);

б) при $m > 0$ автомобиль, объезжающий грань типа $+(+-)^{m+1}$, на протяжении промежутков времени

$$[2m+2, 4m+1] + (4m+2)\mathbb{Z}$$

стоит в углу типа $(++)$, а остальное время едет против часовой стрелки равномерно с единичной скоростью; при $m = 0$ такой автомобиль движется без остановок, проезжая положительные прорёбра со скоростью 2, отрицательное — со скоростью 1, и находясь в углу типа $(+-)$ в нулевой момент времени (рисунок 6б);

в) при $m > 0$ автомобиль, объезжающий грань типа $-(-+)^{m+1}$, на протяжении промежутков времени

$$[1, 2m] + (4m+2)\mathbb{Z}$$

стоит в углу типа $(--)$, а остальное время едет против часовой стрелки равномерно с единичной скоростью; при $m = 0$ такой автомобиль движется без остановок, проезжая отрицательные прорёбра со скоростью 2, положительное — со скоростью 1, и находясь в углу типа $(+-)$ в нулевой момент времени (рисунок 6в);

г) при $m > 0$ автомобиль, объезжающий грань типа $(+)^{k+1}(-)^{l+1}$, в нулевой момент времени находится в углу типа $(+-)$, далее проезжает первое из отрицательных прорёбер с единичной скоростью, после чего останавливается, стоит на протяжении интервала времени $[1, 2m]$, далее проезжает со скоростью l оставшиеся l отрицательных прорёбер, потом проезжает со скоростью k k положительных прорёбер, после чего останавливается и стоит на протяжении интервала времени $[2m+2, 4m+1]$, потом проезжает с единичной скоростью последнее положительное проребро и оказывается в момент $4m+2$ снова в углу типа $(+-)$, далее всё повторяется с периодом $4m+2$; при $m = 0$ такой автомобиль движется без остановок, проезжая отрицательные прорёбра со скоростью $l+1$, положительные — со скоростью $k+1$, и находясь в углу типа $(+-)$ в нулевой момент времени (рисунок 6г).

Стандартное движение является периодическим с периодом $4m+2$ (при этом на гранях типа $+-$ минимальный период равен двум). На рисунке 6 показано подробное расписание движения на протяжении интервала времени $[0, 4m+2)$, числа в рамочках около рёбер означают скорость автомобиля на этих рёбрах (по умолчанию скорость единичная). В углах, помеченных буквой **S**, автомобиль останавливается на время $2m-1$.

Лемма 9. *Стандартное движение на карте типа A_m является движением с разделёнными остановками. Полные столкновения могут происходить только в вершинах, являющихся источниками или стоками, и только в целые моменты времени.*

Доказательство. Объявим остановочными углами все углы типа $(++)$ и $(--)$. То, что остановки являются разделёнными, следует из леммы 8 и того, что расписание стандартного движения устроено так, что автомобили никогда не бывают одновременно в углах типа $(++)$ и $(--)$ (в углах типа $(--)$ автомобили бывают только в первую половину периода, то есть в моменты из интервалов $(0, 2m+1) + (4m+2)\mathbb{Z}$, а в углах типа $(++)$ — во вторую половину, то есть в моменты из интервалов $(2m+1, 4m+2) + (4m+2)\mathbb{Z}$).

Столкновение на ребре в момент времени t означает, что в этот момент направление движения одного из автомобилей совпадает с направлением ребра, а направление движения другого автомобиля противоположно направлению ребра (рис. 7).

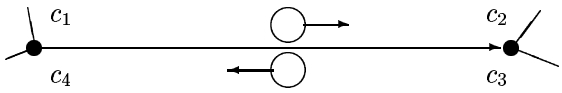


Рис. 7

Но расписание стандартного движения устроено таким образом, что в каждый момент времени t либо все автомобили, находящиеся на рёбрах, едут в направлении ребра (это происходит, когда целая часть t нечётна), либо все автомобили, находящиеся на рёбрах, едут в направлении, противоположном направлению ребра, (это происходит, когда целая часть t чётна). Значит, столкновения могут происходить только в вершинах; из условия разделённости остановок следует, что вершины, в которых происходят полные столкновения, не могут иметь остановочных углов и, следовательно, являются источниками или стоками. В таких вершинах автомобили появляются только в целые моменты времени (чётные для стоков и нечетные для источников). Лемма доказана.

8. Доказательство основной теоремы. Лёгкий случай

То, что указанные в основной теореме условия достаточны для простоты группы $\widetilde{G}$, очевидно. Будем доказывать их необходимость. Ясно, что из простоты группы $\widetilde{G}$ следует, что группа G совпадает с коммутантом и $\sum \varepsilon_i = \pm 1$ (так как иначе $\widetilde{G}$ не совпадала бы со своим коммутантом). Мы будем предполагать, что группа G совпадает с коммутантом и условия (1) выполнены. При этом нам достаточно доказать, что группа $\widetilde{G}$ непроста.

По лемме 2 группа $\widetilde{G}$ обладает копредставлением (2). Лёгкий случай, который мы рассматриваем в этом разделе, состоит в том, что $P \neq \{1\}$ в копредставлении (2), или, что то же самое, слово w не сопряжено слову вида $ct\prod_{i=0}^{m}(b_i a_i^t)$, где $c, a_i, b_i \in G$. Утверждение теоремы в этом случае очевидным образом вытекает из леммы 7 и следующего утверждения.

Лемма 10. *Если G — нециклическая группа без кручения, условия* (1) *выполнены и $P \neq \{1\}$ в копредставлении* (2), *то существуют такие элементы $a, b \in H$, что копредставление*

$$\widetilde{G}\Big/\Big\langle\Big\langle a^{t^2}b\Big\rangle\Big\rangle \simeq \left\langle H, t \;\middle|\; \{p^t = p^\varphi,\ p \in P \setminus \{1\}\},\ ct\prod_{i=0}^{m}(b_i a_i^t) = 1,\ a^{t^2}b = 1 \right\rangle, \tag{3}$$

полученное из копредставления (2) *добавлением соотношения $a^{t^2}b = 1$, φ-асферично.*

Доказательство. Возьмём в качестве a и b такие элементы группы H, что $\langle P, a_m, a\rangle = P * \langle a_m\rangle_\infty * \langle a\rangle_\infty$ и $\langle P^\varphi, b_0, b\rangle = P * \langle b_0\rangle_\infty * \langle b\rangle_\infty$. Такие элементы существуют по лемме 2 (свойство 4).

Надо показать, что над копредставлением (3) не существует φ-приведённой сферической диаграммы без внешних граней и с единственной внешней вершиной. Клетки такой диаграммы должны иметь вид, изображённый на рисунке 8. Мы видим, что диаграмма является картой типа A_m. Покажем, что при стандартном движении на этой карте полное столкновение может произойти только во внешней вершине.

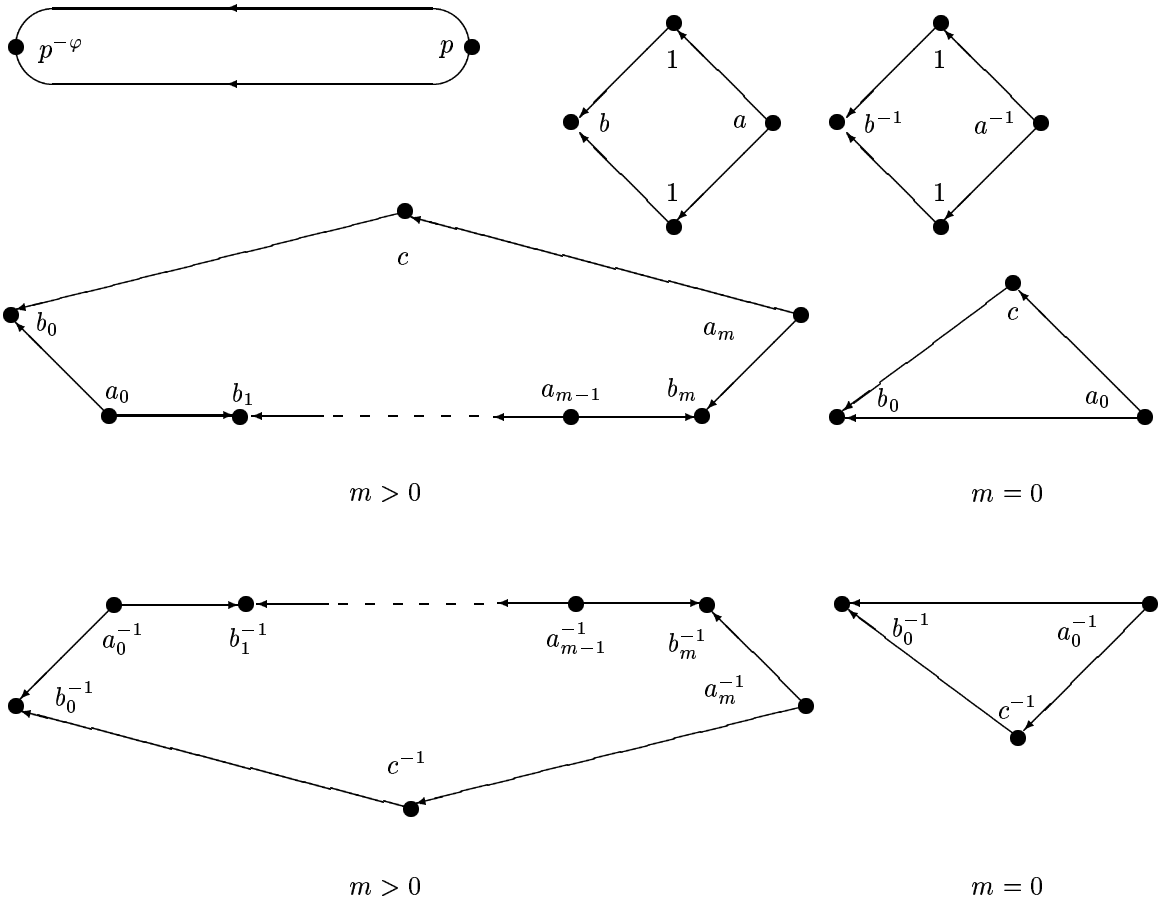


Рис. 8

Согласно лемме 9 полные столкновения могут происходить только в вершинах, являющихся стоками или источниками.

Допустим, что вершина полного столкновения является стоком. Тогда все углы при ней имеют тип $(+-)$; метка каждого из этих углов есть либо p^{φ}, где $p \in P$, либо $b_i^{\pm 1}$, либо $b^{\pm 1}$ (см. рис. 8). Если при вершине есть угол с меткой $b_i^{\pm 1}$ и угол с меткой $b_j^{\pm 1}$, где $i \neq j$, то полного столкновения в такой вершине не происходит, так как в этих углах автомобили никогда не находятся одновременно (сравните рисунки 8, 6б и 6в). Если присутствует угол с меткой $b^{\pm 1}$, то речь может идти только о столкновении в момент времени $0 \pmod{4m+2}$, только в этот момент времени автомобиль появляется в этом углу (рисунки 8 и 6г); но тогда в вершине полного столкновения не может быть углов с метками $b_i^{\pm 1}$, где $i \neq 0$, поскольку в таких углах автомобили не появляются в момент времени $0 \pmod{4m+2}$ (рисунки 8, 6б и 6в). Таким образом метка вершины, являющейся стоком, в которой происходит полное столкновение, есть либо

$$\prod_j (b_i^{\varepsilon_j} p_j^{\varphi}), \quad \text{либо} \quad \prod_j (x^{\varepsilon_j} p_j^{\varphi}),$$

где $\varepsilon_j \in \mathbb{Z}$, $p_j \in P$ и $x \in \{b, b_0\}$. Но метка внутренней вершины должна быть равна единице, значит мы имеем нетривиальное (в силу φ-приведённости диаграммы) соотношение указанного вида, что противоречит свойству 3 из леммы 2 и выбору b.

Аналогичным образом, предположив, что полное столкновение в момент времени t происходит во внутренней вершине, являющейся источником, мы получим нетривиальное соотношение вида

$$\prod_j (a_i^{\varepsilon_j} p_j) = 1 \ \ (\text{если } t \neq 2m+1 \pmod{4m+2}) \quad \text{или} \quad \prod_j (x^{\varepsilon_j} p_j) = 1 \ \ (\text{если } t = 2m+1 \pmod{4m+2}),$$

где $\varepsilon_j \in \mathbb{Z}$, $p_j \in P$ и $x \in \{a, a_m\}$, что противоречит свойству 3 из леммы 2 и выбору a.

Таким образом, полное столкновение может произойти только во внешней вершине, но по лемме 4 должно быть по меньшей мере две точки полного столкновения. Это противоречие завершает доказательство леммы 10 и лёгкого случая основной теоремы.

Замечание. Отметим, что попутно мы доказали следующий факт. *Пусть на φ-приведённой диаграмме над копредставлением* (2), *обладающим свойствами* 1 *и* 3 *из леммы* 2, *задано движение, являющееся стандартным на внутренних гранях. Тогда полные столкновения могут происходить только во внешних вершинах и на границах внешних граней.* Отсюда, в частности, вытекает (в силу лемм 2, 4, 5 и 6) основной результат статьи [K93]: *если группа G не имеет кручения и $\sum \varepsilon_i = 1$, то естественное отображение $G \to \widetilde{G}$ инъективно.*

9. Кодвижения и кратные движения

В этом разделе мы изложим теорию кодвижений, которые были введены в работах [K94] и [K97]; там же можно найти некоторые применения кодвижений к уравнениям над группами. Наше нынешнее изложение будет несколько отличаться по языку и по общности от того, что написано в упомянутых работах.

Понятие кодвижения двойственно понятию периодического движения.

Определение. *Кодвижением* A на ориентированной поверхности S называется карта $\mathrm{M}\colon \coprod D_i \to S$ на этой поверхности и набор непрерывных отображений $\{\alpha_i\colon \partial D_i \to \mathbf{T}\}$, где $\mathbf{T}$ — ориентированная окружность, называемая окружностью времени. Иногда мы будем трактовать кодвижение, как непрерывное отображение $\mathrm{A}\colon \coprod \partial D_i \to \mathbf{T}$. Отображение α_i мы называем *коавтомобилем*, объезжающим грань D_i. Мы говорим, что в момент времени $t \in \mathbf{T}$ коавтомобиль α_i *находится* в точке $p \in S$, если $\alpha_i(\mu_i^{-1}(p)) \ni t$. Мы говорим, что в момент $t \in \mathbf{T}$ в точке p одномерного остова поверхности S происходит *полное столкновение* если $\mathrm{A}^{-1}(t) \supseteq \mathrm{M}^{-1}(p)$. При этом точка p называется *точкой полного столкновения.* Точки полного столкновения, лежащие на рёбрах, мы называем просто *точками столкновеня.*

Кодвижение называется *правильным*, если отображения α_i являются неубывающими.

Отметим, что при непрерывном неубывающем отображении окружности в окружность число односвязных компонент связности прообраза точки всегда является конечным, не зависит от точки и совпадает со степенью отображения.

Основное свойство кодвижений, которое нам понадобится в этой главе, состоит в следующем:

Лемма 11. *При правильном кодвижении $\{\alpha_i\}$ на поверхности S*

$$(\textit{число точек полного столкновения}) + \sum_i (1 - \deg \alpha_i) \geqslant e(S).$$

На самом деле это неравенство есть простое следствие некоторого равенства, для формулировки которого нам понадобится несколько дополнительных обозначений.

Зафиксируем взаимнооднозначное непрерывное сохраняющее ориентацию отображение $f\colon [0;T) \to \mathbf{T}$ полуинтервала $[0;T)$ ($T \in \mathbb{R}$) на окружность. Определим функции $\chi\colon \mathbf{T} \times \mathbf{T} \to \mathbb{Z}$ и $\psi\colon \coprod\limits_{k \in \mathbb{N}} \mathbf{T}^k \to \mathbb{Z}$ формулами

$$\chi(x,y) = \begin{cases} 0, & \text{если } f^{-1}(x) \leqslant f^{-1}(y); \\ 1, & \text{если } f^{-1}(x) > f^{-1}(y); \end{cases}$$

$$\psi(t_1, \ldots, t_k) = \chi(t_1,t_2) + \chi(t_2,t_3) + \ldots + \chi(t_k,t_1); \quad \psi(t_1) = 0.$$

Лемма 12. *Функция ψ обладает следующими свойствами:*

1) *ψ не зависит от выбора функции f и может быть определена инвариантно так: рассмотрим ориентированную окружность X, точки $x_1, \ldots, x_k \in X$, расположенные на ней по порядку в положительном направлении, и непрерывное неубывающее отображение $F\colon X \to \mathbf{T}$, которое отображает точки x_i в точки t_i, а дуги $[x_i, x_{i+1}]$ в дуги $[t_i, t_{i+1}]$ (здесь индексы по модулю k и дуга с совпадающими концами считается состоящей из одной точки); тогда $\psi(t_1, \ldots, t_k) = \deg F$;*
2) *ψ принимает целые неотрицательные значения;*
3) *$\psi(t_1, \ldots, t_k) = 0$ тогда и только тогда, когда все t_i равны.*

Доказательство. Свойства 2) и 3) очевидны. Чтобы доказать свойство 1), заметим, что по определению $\psi(t_1, \ldots, t_k)$ равно числу полуоткрытых дуг вида $(t_i, t_{i+1}]$, содержащих $f(0)$ (здесь индексы по модулю k и полуоткрытая дуга с совпадающими концами считается пустым множеством). А это число, в свою очередь, есть число прообразов при отображении F точки $f(T - \varepsilon)$, где ε — достаточно маленькое положительное вещественное число. Лемма доказана.

Лемма 13. *Пусть* $\mathrm{A}: \coprod \partial D_i \to \mathbf{T}$ *есть правильное кодвижение на поверхности* S. *Определим вес* ν *грани* D_i, *ребра* e *и вершины* v *следующими формулами*

$$\begin{aligned}\nu(D_i) &= 1 - \deg \alpha_i,\\ \nu(e) &= -1 + (\text{число компонент связности множества точек ребра } e, \text{ не являющихся точками столкновения}),\\ \nu(v) &= 1 - \psi(\mathrm{A}(c_0), \ldots, \mathrm{A}(c_k)),\end{aligned}$$

где в последней формуле $c_0, \ldots, c_k$ — *это все углы при вершине* v, *занумерованные против часовой стрелки. Тогда суммарный вес всех граней, рёбер и вершин равен эйлеровой характеристике поверхности* S. (Напоминаем, что, согласно нашему определению, концы ребра не принадлежат ребру.)

Доказательство. Заметим, что суммарный вес граней, рёбер и вершин не меняется при измельчении рёбер, то есть при добавлении вершины v, которая разделяет ребро e на два ребра e_1 и e_2. В самом деле, если вершиной v объявляется точка ребра e, не являющаяся точкой столкновения, то суммарное число компонент связности множества точек рёбер e_1 и e_2, не являющихся точками столкновения, будет на единицу больше аналогичной величины для ребра e, а вес вершины v окажется нулевым. Таким образом, суммарный вес не изменится: $\nu(e_1) + \nu(e_2) + \nu(v) = \nu(e)$. Если же вершиной v объявляется точка ребра e в которой происходит столкновение, то суммарное число компонент связности множества точек рёбер e_1 и e_2, не являющихся точками столкновения, будет равно аналогичной величине для ребра e, а вес вершины v окажется единицей. Таким образом, суммарный вес снова не изменится.

Измельчая рёбра, можно добиться того, чтобы каждое ребро e обладало следующими свойствами:

1) в некоторый момент времени на замыкании ребра e нет ни одного коавтомобиля;
2) либо на ребре e не происходит столкновений, либо они происходят в каждой точке ребра e (последнее означает, что функция A является постоянной на $\mathrm{M}^{-1}(e)$).

Заметим, что вес ребра e, обладающего этими свойствами, равен либо нулю, либо -1 и может быть записан в виде

$$\nu(e) = \psi(\mathrm{A}(c_1), \mathrm{A}(c_2), \mathrm{A}(c_3), \mathrm{A}(c_4)) - 1,$$

где c_1, c_2, c_3, c_4 — углы при ребре e, занумерованные по часовой стрелке (как на рисунке 7). Справедливость этой формулы легко усматривается из свойств функции ψ (лемма 12), если заметить, что свойства 1) и 2) ребра e означают, что интервалы $(\mathrm{A}(c_1), \mathrm{A}(c_2))$ и $(\mathrm{A}(c_3), \mathrm{A}(c_4))$ не пересекаются.

Согласно лемме 12 вес грани может быть записан в виде

$$\nu(D_i) = 1 - \psi(\alpha_i(c_0), \ldots, \alpha_i(c_k)),$$

где $c_0, \ldots, c_k$ — это все углы грани D_i, занумерованные против часовой стрелки. Для завершения доказательства осталось сослаться на следующий очевидный факт.

Лемма 14. *Пусть имеется произвольная карта на произвольной поверхности* S *и две произвольные функции* g *и* h, *сопоставляющие паре углов число. Определим вес* ν *грани* D, *ребра* e *и вершины* v *следующими формулами:*

$$\begin{aligned}\nu(D) &= 1 - \sum_{i=0}^{k} g(c_i, c_{i+1}),\\ \nu(e) &= -1 + g(c_1, c_2) + h(c_2, c_3) + g(c_3, c_4) + h(c_4, c_1),\\ \nu(v) &= 1 - \sum_{i=0}^{k} h(c_i, c_{i+1}),\end{aligned}$$

где в первой формуле $c_0, \ldots, c_k$ — *это все углы грани* D, *занумерованные против часовой стрелки, во второй формуле* $c_1, \ldots, c_4$ — *это углы при ребре* e, *занумерованные по часовой стрелке (рис. 7), а в последней формуле* $c_0, \ldots, c_k$ — *это все углы при вершине* v, *занумерованные против часовой стрелки. Тогда суммарный вес всех граней, рёбер и вершин равен эйлеровой характеристике поверхности* S.

Для доказательства этого утверждения достаточно понять, что при суммировании всех весов все значения функций g и h сократятся: каждое встречающееся выражение $g(x, y)$ один раз входит в вес грани со знаком минус и один раз в вес ребра со знаком плюс; аналогично, каждое встречающееся выражение $h(x, y)$ один раз входит в вес вершины со знаком минус и один раз в вес ребра со знаком плюс.

Для завершения доказательства леммы 13 надо положить в лемме 14 $g(c_1, c_2) = h(c_1, c_2) = \chi(\mathrm{A}(c_1), \mathrm{A}(c_2))$.

Лемма 11 немедленно вытекает из леммы 13; надо только заметить, что вес ребра (из леммы 13) не больше числа точек полного столкновения на этом ребре, а вес вершины равен единице, если в этой вершине происходит полное столкновение, и неположителен в противном случае.

Кратным движением периода $T \in \mathbb{R}$ на поверхности S называется карта $\{\mu_i \colon D_i \to S \mid i \in I\}$ на этой поверхности и набор отображений $\{\alpha_{i,j} \colon \mathbb{R} \to \partial D_i;\ i \in I, j = 1, \ldots, d_i\}$ (называемых автомобилями), удовлетворяющих следующим условиям периодичности:

1) $\alpha_{i,j}(t+T) = \alpha_{i,j+1}(t)$ для любого $t \in \mathbb{R}$ и $j \in \{1, \ldots, d_i\}$ (индексы по модулю d_i);
2) существует такое разбиение каждой из окружностей ∂D_i на d_i дуг, что на протяжении интервала времени $[0, T]$ каждый автомобиль $\alpha_{i,j}$ движется по j-й дуге.

Натуральные числа d_i называются *кратностями* кратного движения. Кратное движение называется *правильным*, если все функции $\alpha_{i,j}$ являются накрытиями, сохраняющими ориентацию.

Пример 2. На карте, изображённой на рисунке 1, определим кратное движение так: автомобили α, β, γ, δ и ε, объезжающие грани A, B, C, D и E, соответсвенно, движутся так же, как в примере 1, то есть с единичной скоростью (одно ребро в единицу времени) в положительном направлении, находясь в нулевой момент времени в углах a_0, b_0, c_0, d_0 и e_0, соответственно; кроме того, имеется ещё один автомобиль β', объезжающий грань B в положительном направлении с единичной скоростью, находясь в нулевой момент времени в углу b_3. На рисунке 1 показано положение автомобилей и направление их движения в момент времени $t = 4/3$. Это кратное движение является правильным, имеет период 3 и набор кратностей $\{1, 2, 1, 1, 1\}$. Полные столкновения происходят в тех же трёх точках, что в примере 1 (они помечены восклицательными знаками на рисунке 1). Однако на этот раз никакие изменения расписания движения не помогут уменьшить число точек полного столкновения.

Лемма 15. *Число точек полного столкновения правильного кратного движения с кратностями* $\{d_i;\ i \in I\}$ *на поверхности* S *не может быть меньше чем*

$$e(S) + \sum_{i \in I} (d_i - 1).$$

Доказательство. Правильное кратное движение $\{\alpha_{i,j}\}$ очевидным образом позволяет определить кодвижение $\{\beta_i \colon \partial D_i \to \mathbb{R}/T\mathbb{Z}\}$. Достаточно положить $\beta_i(x)$ равным такому t, что $\alpha_{i,j}(t) = x$; это выражение не зависит от j, корректно определено по модулю T и является накрытием степени d_i. Для завершения доказательства осталось заметить, что точки полного столкновения этого кодвижения совпадают с точками полного столкновения исходного кратного движения, и сослаться на лемму 11.

Кратное движение $\{\alpha_{i,j}\}$ называется *кратным движением с разделёнными остановками*, если все автомобили $\alpha_{i,j}$ являются неубывающими функциями и остановки разделены в смысле определения из раздела 5.

Лемма 16. *Число точек полного столкновения кратного движения с разделёнными остановками на поверхности* S *не может быть меньше чем*

$$e(S) + \sum_{i \in I} (d_i - 1),$$

где d_i *суть кратности кратного движения.*

Эта лемма выводится из леммы 15 так же, как лемма 4 выводится из леммы 3.

Назовём карту на поверхности 2-*градуированной*, если на ней имеется следующая дополнительная структура: некоторые из вершин и некоторые из граней выделены и называются *внешними*, остальные вершины и грани называются *внутренними*; кроме того, некоторые из граней называются *большими*, остальные грани называются *малыми*.

Пусть на 2-градуированной карте M на поверхности S задано (кратное) движение. Скажем, что две различные большие грани A и B *плохо примыкают друг к другу*, если они имеют
такие углы $a_1, a_2 \in \partial A$ и $b_1, b_2 \in \partial B$, что

1) a_i и b_i являются несмежными углами при некоторой внутренней вершине полного столкновения

$$v_i = \mathrm{M}(a_i) = \mathrm{M}(b_i)$$

(при $i = 1, 2$);
2) $v_1 \neq v_2$;
3) замкнутый путь на поверхности S, состоящий из участка $[a_1, a_2]$ границы грани A и участка $[b_2, b_1]$ границы грани B не проходит через внешние вершины и является контуром дисковой подкарты, каждая вершина которой является внутренней, а каждая клетка — малой внутренней.

Скажем, что большая грань A *плохо примыкает к самой себе* если либо она имеет такие углы $a_1, a_2, b_2, b_1 \in \partial A$ (все различные и расположенные именно в таком порядке), что выполнены условия 1), 2) и 3), либо она имеет углы $a, b \in \partial A$, являющиеся несмежными (и несовпадающими) углами при некоторой внутренней вершине полного столкновения $v = \mathrm{M}(a) = \mathrm{M}(b)$, причём участок $[a, b]$ границы грани A на поверхности S не проходит через

внешние вершины и является контуром дисковой подкарты, каждая вершина которой является внутренней, а каждая клетка — малой внутренней.

Рисунок 9 иллюстрирует все случаи плохого примыкания; звёздочкой на этом рисунке отмечены подкарты, не содержащие ни внешних вершин, ни внешних граней, ни больших граней; в вершинах, отмеченных восклицательным знаком, происходят полные столкновения.

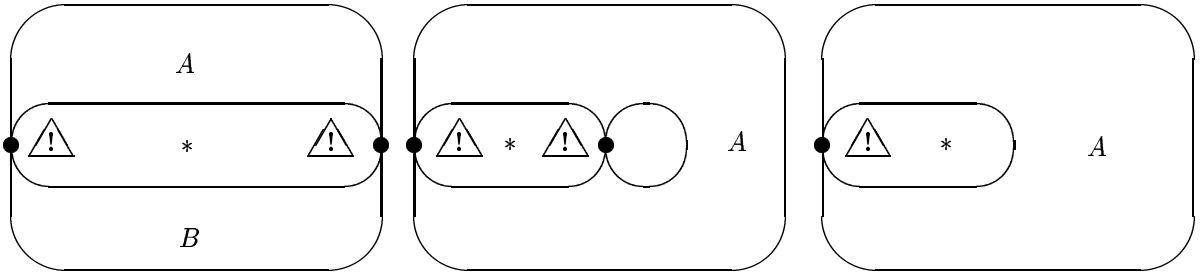


Рис. 9

Лемма 17. *На сферической 2-градуированной карте с единственной внешней вершиной и без внешних граней не может существовать кратного движения с разделёнными остановками, удовлетворяющего следующим условиям:*

1) *кратность движения на каждой большой грани не меньше четырёх, а на каждой малой грани не меньше одного;*
2) *при каждой из внутренних точек полного столкновения имеется по меньшей мере два несмежных угла больших клеток;*
3) *не существует плохо примыкающих (к себе или другим) больших клеток.*

Доказательство. Чтобы получить противоречие с леммой 16, достаточно показать, что из условий 2) и 3) следует, что

$$(\textit{число внутренних точек полного столкновения}) < 3 \cdot (\textit{число больших граней}) + 1.$$

Отметим внутри каждой большой грани D точку v_D. При каждой внутренней точке полного столкновения p выделим 2 несмежных угла a и b, лежащих на больших гранях, которые мы назовём A и B соответственно. Проведём на сфере дугу от точки v_A по внутренности грани A через угол a до точки p и далее через угол b по внутренности грани B до точки v_B. Если мы позаботимся о том, чтобы различные построенные дуги не пересекались, то мы получим граф Γ на сфере, число вершин которого равно числу больших клеток карты, а число рёбер равно числу внутренних точек полного столкновения. Для завершения доказательства осталось заметить, что условие 3) означает, что граф Γ удовлетворяет условиям следующей леммы.

Лемма 18. *Пусть имеется конечный (необязательно связный) граф* Γ *на сфере* S^2 *такой, что периметр каждой односвязной компоненты связности множества* $S^2 \setminus \Gamma$*, кроме, быть может, одной — исключительной, не меньше трёх. Тогда число рёбер этого графа не больше утроенного числа его вершин.*

Здесь под периметром области мы понимаем число рёбер на её границе, причём ребро считается дважды, если область лежит по обе стороны от этого ребра.

Доказательство. Если граф не имеет рёбер, то доказывать нечего. Считая, что рёбра есть, воспользуемся индукцией по числу компонент связности графа Γ. В случае, когда граф связный, по формуле Эйлера мы имеем $V - E + F = 2$, где V, E и F — это число вершин, рёбер и граней соответствующей карты на сфере. Добавив одну вершину внутри исключительной компоненты и соединив её ребром с вершиной границы этой компоненты, мы добьёмся того, что каждая грань станет по меньшей мере треугольником. Следовательно, $F \leqslant \frac{2}{3}(E+1)$. Значит, $V - E + \frac{2}{3}E = V - \frac{1}{3}E \geqslant 2 - \frac{2}{3} = \frac{4}{3}$. Тем самым для связных графов лемма доказана.

Если рёбра есть, но граф несвязный, то соединим компоненту связности, отличную от точки, с какой-нибудь другой компонентой новым ребром. При этом число компонент связности графа уменьшится, число вершин не изменится, число рёбер увеличится, а возникающая односвязная компонента дополнения к графу будет иметь периметр не меньше трёх. Ссылка на предположение индукции завершает доказательство леммы 18, а заодно и леммы 17.

Мы скажем, что карта с ориентированными рёбрами имеет тип B_m, $m \geqslant 0$, если последовательность ориентаций прорёбер каждой грани имеет одну из трёх форм:

а) $+(+-)^{m+1}$ (рисунок 6б);

б) $-(-+)^{m+1}$ (рисунок 6в);
в) $((+)^{k+1}(-)^{l+1})^s$, $k, l, s \geqslant 1$ (рисунок 10).

Определим *стандартное кратное движение* на карте типа B_m следующим образом. На гранях типов $+(+-)^{m+1}$ и $-(-+)^{m+1}$ стандартное движение (однократное) определяется так же, как для карты типа A_m. На грани типа $((+)^{k+1}(-)^{l+1})^s$ определим s-кратное движение как поднятие стандартного движения на грани типа $(+)^{k+1}(-)^{l+1}$ (из определения стандартного движения на карте типа A_m). Более точно: имеется естественное сохраняющее ориентацию прорёбер s-листное накрытие $\pi\colon \partial B \to \partial A$, где B — грань типа $((+)^{k+1}(-)^{l+1})^s$, а A — грань типа $(+)^{k+1}(-)^{l+1}$; у стандартного автомобиля $\alpha\colon \mathbb{R} \to \partial A$ имеется ровно s поднятий, то есть таких функций $\alpha_1, \ldots, \alpha_s\colon \mathbb{R} \to \partial B$, что $\alpha = \pi\alpha_i$; эти функции мы и называем стандартными автомобилями, объезжающими ∂B.

На рисунке 10 представлено расписание стандартного кратного движения на грани типа $((+)^{k+1}(-)^{l+1})^s$ при $k = l = 2$ и $s = 4$: около вершин указано когда $(\mathrm{mod}\, 4m+2)$ в этих вершинах находится один из четырёх автомобилей. Это расписание, разумеется, относится к случаю $m > 0$; при $m = 0$ все 4 автомобиля движутся равномерно со скоростью $k + 1 = l + 1 = 3$ и находятся в вершинах, помеченных числом 0, в нулевой момент времени.

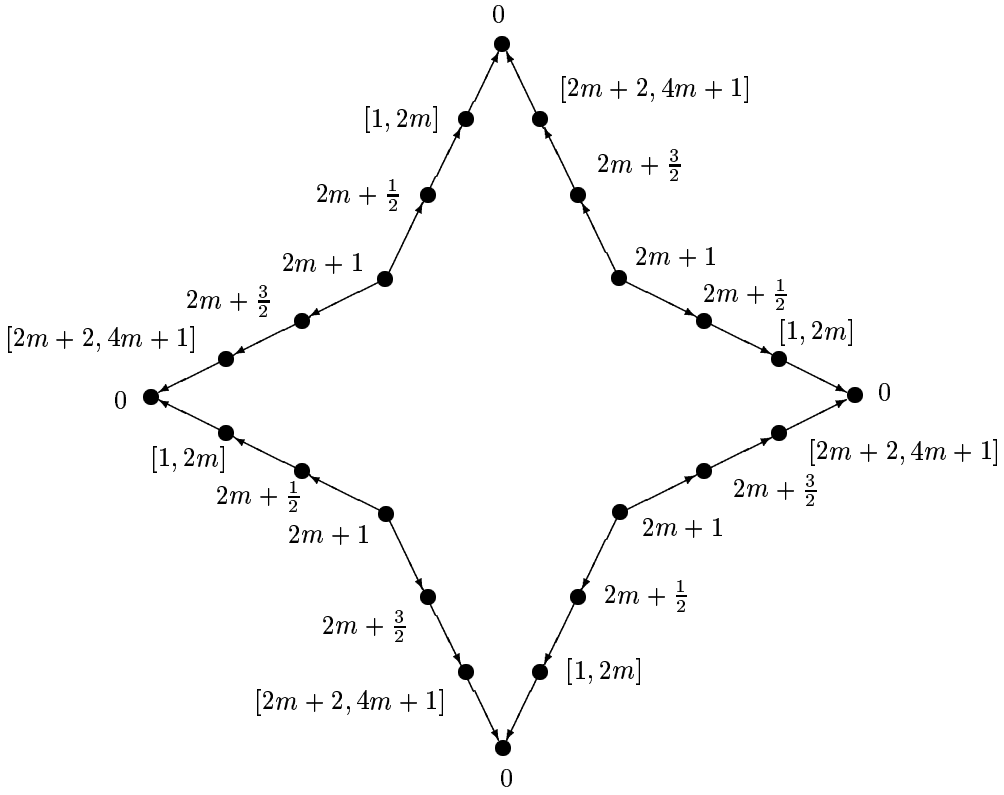


Рис. 10

Лемма 19. *Стандартное движение на карте типа B_m является кратным движением с разделёнными остановками. Полные столкновения могут происходить только в вершинах, являющихся источниками или стоками, и только в целые моменты времени.*

Чтобы доказать эту лемму, надо дословно повторить доказательство леммы 9.

10. Доказательство основной теоремы. Трудный случай

Мы по-прежнему считаем, что группа G без кручения и условия (1) выполнены. При этом нам достаточно доказать, что группа $\widetilde{G}$ непроста. Группа $\widetilde{G}$ обладает копредставлением (2), и мы теперь считаем, что $P = \{1\}$, то есть копредставление (2) имеет вид

$$\widetilde{G} \simeq \left\langle G, t \;\middle|\; ct\prod_{i=0}^{m}(b_i a_i^t) = 1 \right\rangle, \quad m \geqslant 0. \tag{4}$$

Лемма 20. *$G^t \cap G = \{1\}$ в группе $\widetilde{G}$.*

Доказательство. Предполагая противное, по лемме 5 (и в силу замечания после леммы 10) мы получаем, что существует приведённая сферическая диаграмма над копредставлением (4) с единственной внешней гранью, метка которой есть $g^t h$, где $g, h \in G \setminus \{1\}$. Эта диаграмма является картой типа A_m. Она имеет одну клетку (внешнюю) типа $+-$ (рис.6а), а остальные клетки имеют тип $+(+-)^{m+1}$ (рис. 6б) и $-(-+)^{m+1}$ (рис. 6в). Рассмотрим стандартное движение периода $4m + 2$ на этой карте. Согласно замечанию после леммы 10, полные столкновения могут происходить только в вершинах A и B, лежащих на границе внешней грани. По лемме 4 в обеих этих вершинах должны происходить полные столкновения. По лемме 9 столкновения могут происходить только в источниках и стоках. Значит, вершина A, при которой расположен угол типа $(-+)$ внешней грани, является источником, а вершина B, при которой расположен угол типа $(+-)$ внешней грани, является стоком. При $m = 0$ из этого немедленно вытекает, что метки всех внутренних углов при вершине A равны $a_0^{\pm 1}$ (поскольку A — источник), но не все эти метки одинаковы (поскольку B — сток) (рис.11); значит, диаграмма содержит сократимую пару клеток, то есть не является приведённой.

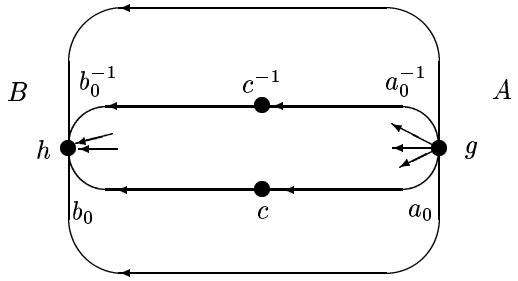


Рис. 11

Если $m > 0$, то полные столкновения не могут произойти в обеих вершинах. Действительно, допустим, что в вершине A происходит полное столкновение в момент t. Тогда один из автомобилей, объезжающих внутреннюю грань, окажется в вершине B в момент $t_1 = t + 1$, а другой автомобиль — в момент $t_2 = t - 1$. Но t_1 никогда не бывает равен t_2 по модулю периода движения, так как при $m > 0$ период больше чем 2, то есть в вершине B столкновения не происходит. Полученное противоречие завершает доказательство.

Лемма 21. *Для любых $g, h \in G$ мы имеем одно из двух:*
либо $\langle g \rangle^{t^2} \cap \langle h \rangle = \{1\}$ в группе $\widetilde{G}$,
либо $\langle g \rangle^{t^3} \cap \langle h \rangle = \{1\}$ в группе $\widetilde{G}$.

Доказательство. Допустим противное:

$$g^{kt^2} = h^l, \quad g^{k't^3} = h^{l'}.$$

Возведём эти равенства в степени k' и k соответственно:

$$g^{kk't^2} = h^{lk'}, \quad g^{kk't^3} = h^{kl'}.$$

Сопрягая первое равенство при помощи t, получаем

$$h^{lk't} = h^{kl'},$$

откуда $h = 1$ в силу леммы 20 и отсутствия кручения в G.

Лемма 22. *Существует такое* $d \in \{2,3\}$, *что*

$$u \equiv \prod_{i=1}^{s} y_i x_i^{t^d} \neq 1 \text{ в } \widetilde{G}$$

для любого натурального s *и любых* $x_i, y_i \in G$ *таких, что* $\left|\{i \mid x_i \in \langle a_m \rangle\}\right| + \left|\{i \mid y_i \in \langle b_0 \rangle\}\right| \leqslant 2$ *и* $u \neq 1$ *в* $G * \langle t \rangle_\infty$.

Доказательство. В качестве d выберем такое число, что $\langle a_m \rangle^{t^d} \cap \langle b_0 \rangle = \{1\}$; такое $d \in \{2,3\}$ существует по лемме 21.

Доказывая от противного, рассмотрим контрпример с наименьшим возможным s. По лемме 5 (и замечанию после леммы 10) существует диаграмма над копредставлением (4) на сфере с единственной внешней гранью, метка контура которой равна u.

Покажем сперва, что ни при какой вершине не может быть более одного угла типа $(+-)$ внешней грани. Действительно, предположив, что углы внешней грани с метками y_1 и y_r являются углами при одной и той же вершине и рассмотрев соответствующие поддиаграммы, мы получим, что равенство $u = 1$ распадается в произведение двух равенств

$$\left(\prod_{i=1}^{r-1} y_i x_i^{t^d}\right) g = 1 \quad \text{и} \quad g^{-1} \prod_{i=r}^{s} y_i x_i^{t^d} = 1, \quad \text{где } g \in G,$$

(смотрите рис. 12, на котором $s = 5$, $d = 2$ и $r = 3$), по крайней мере одно из которых противоречит минимальности рассматриваемого контрпримера. Аналогичным образом можно показать, что ни при какой вершине не может быть более одного угла типа $(-+)$ внешней грани.

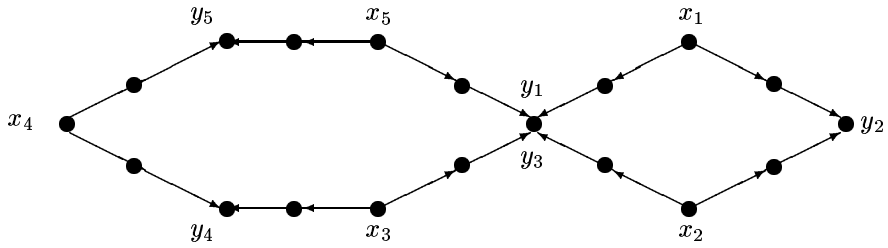


Рис. 12

Далее заметим, что диаграмма представляет собой карту типа B_m. Рассмотрим стандартное кратное движение на этой карте. Согласно замечанию после леммы 10, полные столкновения могут происходить только в вершинах, лежащих на контуре внешней грани. Кроме того, по лемме 19 вершины полных столкновений должны быть источниками или стоками. Следовательно, при каждой вершине полного столкновения имеется ровно один угол внешней грани и полные столкновения могут происходить только в моменты времени 0 и $2m+1 \pmod{4m+2}$, так как только в эти моменты автомобили, объезжающие внешнюю грань, оказываются в углах типа $(+-)$ или $(-+)$. Поскольку все остальные автомобили в эти моменты времени проезжают углы с метками $b_0^{\pm 1}$ (в момент 0) и $a_m^{\pm 1}$ (в момент $2m+1$), метка угла внешней грани при вершине полного столкновения должна лежать в $\langle b_0 \rangle$ (для угла типа $(+-)$) или в $\langle a_m \rangle$ (для угла типа $(-+)$). Но по условию внешняя грань имеет не более двух таких углов, значит, имеется не больше двух точек полного столкновения. Однако, согласно лемме 16, должна быть по меньшей мере $s+1$ точка полного столкновения. Значит, $s = 1$ и u имеет вид $b_0^k a_m^{lt^d}$, а такое слово не равно 1 в $\widetilde{G}$ в силу выбора d. Лемма доказана.

Лемма 23. *При* $m \geqslant 0$ *найдётся такое* $d \in \{2,3\}$, *что копредставление*

$$\left\langle G, t \;\middle|\; ct \prod_{i=0}^{m} (b_i a_i^t) = 1,\ (a^{t^d} b)^4 = 1 \right\rangle$$

асферично для любых элементов $a, b \in G$ *таких, что* $a^2 \notin \langle a_m \rangle$ *и* $b^2 \notin \langle b_0 \rangle$.

Доказательство. В качестве d выберем число, существование которого утверждается в лемме 22.

Доказывая от противного, рассмотрим приведённую сферическую диаграмму над нашим копредставлением с единственной внешней вершиной и без внешних граней. Эта диаграмма представляет собой карту типа

B_m. Рассмотрим стандартное кратное движение на этой карте. Клетки с меткой границы $(a^{t^d}b)^{\pm 4}$ назовём большими, остальные клетки будем считать малыми.

Покажем, что выполнены условия 1), 2) и 3) из леммы 17.

Условие 1) выполнено по определению стандартного кратного движения.

Покажем, что условие 2) выполнено. При каждой вершине полного столкновения по меньшей мере один угол должен быть углом большой клетки (смотрите замечание после леммы 10). По лемме 19 вершина полного столкновения должна быть источником или стоком, а в таких вершинах автомобиль, объезжающий большую клетку, бывает только в моменты времени 0 и $2m+1 \pmod{4m+2}$, так как только в эти моменты автомобили, объезжающие большие клетки, оказываются в углах типа $(+-)$ или $(-+)$. Автомобили, объезжающие малые клетки, в эти моменты времени проезжают углы с метками $b_0^{\pm 1}$ (в момент 0) и $a_m^{\pm 1}$ (в момент $2m+1$). Значит, метка каждого угла при вершине полного столкновения есть либо $a_m^{\pm 1}$, либо $a^{\pm 1}$, если эта вершина — источник, и либо $b_0^{\pm 1}$, либо $b^{\pm 1}$, если эта вершина — сток. При этом метки смежных углов не являются взаимнообратными в силу приведённости диаграммы. Предположим, что условие 2) не выполнено, то есть при некоторой внутренней вершине полного столкновения нет пары различных несмежных углов больших клеток, то есть углов с метками $a^{\pm 1}$ или $b^{\pm 1}$. Допустим для определённости, что эта вершина — источник. Тогда её метка имеет вид

$$\text{либо } a^{\pm 1}a_m^k, \quad \text{либо } a^{\pm 2}a_m^k, \quad \text{либо } a^{\pm 3}.$$

С другой стороны, эта метка должна быть равна единице в группе G, поскольку речь идёт о внутренней вершине. Таким образом, мы получаем, что в группе G выполнено одно из трёх равенств, первые два из которых противоречат тому, что, по условию, $a^2 \notin \langle a_m \rangle$, а третье противоречит отсутствию кручения в группе G. Это показывает, что условие 2) леммы 17 выполнено.

Допустим, что условие 3) не выполнено. Мы имеем дисковую поддиаграмму (не содержащую внешнюю вершину), внутренние клетки которой малы, а метка контура имеет вид

$$u = \prod_{i=1}^{s} y_i x_i^{t^d},$$

где $s \in \mathbb{N}$, $x_i, y_i \in G \setminus \{1\}$, $\left|\{i \mid x_i \neq a^{\pm 1}\}\right| + \left|\{i \mid y_i \neq b^{\pm 1}\}\right| \leqslant 2$, причём 1 или 2 исключительных коэффициента являются ненулевыми степенями b_0 или a_m (рис. 13). Это означает (по лемме 5), что $u = 1$ в $\widetilde{G}$, что невозможно по лемме 22.

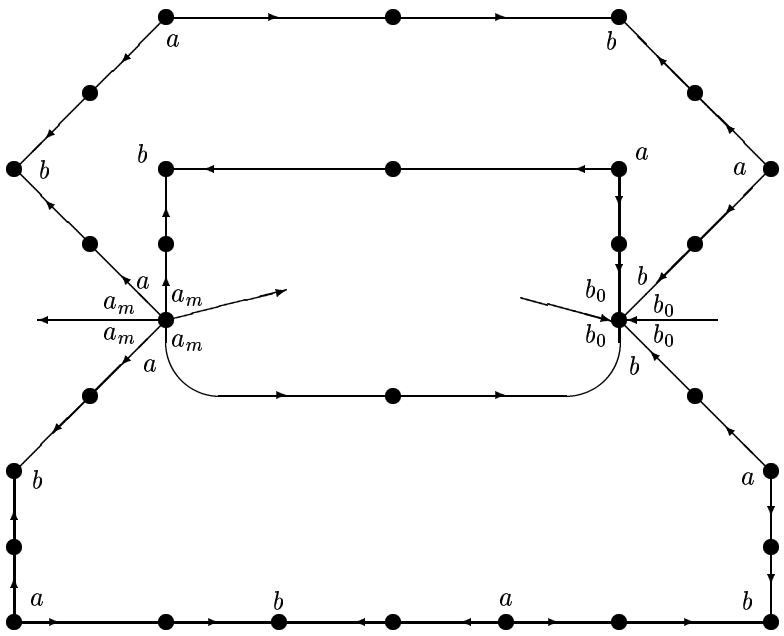


Рис. 13

Таким образом рассматриваемая диаграмма обладает свойствами 1), 2) и 3) из леммы 17, которая утверждает, что таких диаграмм не бывает. Это противоречие завершает доказательство леммы 23.

Справедливость основной теоремы (в трудном случае) вытекает из лемм 23 и 7 и того очевидного факта, что если в нетривиальной группе G квадраты всех элементов лежат в одной и той же циклической подгруппе, то G не совпадает со своим коммутантом (поскольку является метабелевой) и, следовательно, $\widetilde{G}$ также не совпадает с коммутантом.

ГЛАВА 23.
СВОБОДНЫЕ ПОДГРУППЫ ОТНОСИТЕЛЬНЫХ КОПРЕДСТАВЛЕНИЙ С ОДНИМ СООТНОШЕНИЕМ

0. Введение

Следующая теорема была сформулирована в [Ma32]; доказательство, насколько известно автору, впервые появилось в [Mo69].

Теорема о свободных подгруппах групп с одним соотношением. *Группа с одним соотношением*

$$\langle x_1, x_2, \ldots, x_n \mid w = 1 \rangle$$

не содержит неабелевых свободных подгрупп тогда и только тогда, когда она либо циклическая, либо изоморфна группе Баумслага–Солитэра $G_{1,k} = \langle x, y \mid y^{-1}xy = x^k \rangle$, *где* $k \in \mathbb{Z} \setminus \{0\}$.

Мы пытаемся решить ту же задачу для относительных копредставлений с одним соотношением, то есть для групп вида

$$\widetilde{G} = \langle G, x_1, x_2, \ldots, x_n \mid w = 1 \rangle \stackrel{\text{опр}}{=} (G * F(x_1, x_2, \ldots, x_n))/\langle\langle w \rangle\rangle .$$

Здесь G — произвольная группа, а w — произвольный элемент свободного произведения группы G и свободной группы $F(x_1, \ldots, x_n)$. Мы будем всегда предполагать, что группа G не имеет кручения.

В случае когда $n \geqslant 2$ ответ оказывается вполне ожидаемым.

Теорема 1. *Если группа* G *нетривиальна и не имеет кручения, а* $n \geqslant 2$, *то группа* $\widetilde{G} = \langle G, x_1, x_2, \ldots, x_n \mid w = 1 \rangle$ *содержит неабелеву свободную подгруппу.*

Отметим, что при $n \geqslant 3$ наличие свободных подгрупп в $\widetilde{G}$ непосредственно вытекает из теоремы о свободных подгруппах групп с одним соотношением. Таким образом, теорема 1 неочевидна только при $n = 2$.

Верно ли аналогичное утверждение, когда добавляются, скажем, два соотношения при $n \geqslant 3$, мы не знаем. Для свободных групп G такое обобщение заведомо верно по теореме Романовского о свободе [Ром77].

Случай $n = 1$ является самым трудным. Важную роль здесь играет сумма показателей при образующем. Слово $w = \prod g_i t^{\varepsilon_i} \in G * \langle t \rangle_\infty$ мы называем *унимодулярным*, если $\sum \varepsilon_i = 1$. Если сумма показателей в слове w равна любому другому числу $p \neq \pm 1$, то неизвестно даже, вкладывается ли группа G в $\widetilde{G} = \langle G, t \mid w = 1 \rangle$; другими словами, неизвестно, при каких условиях группа $\widetilde{G}$ отлична от $\mathbb{Z}/p\mathbb{Z}$. На эту тему имеется много работ, но ответ удаётся получить лишь при наложения дополнительных жёстких ограничений на группу G или/и на слово w (см., например, [Б84], [КП95], [C02], [C03], [CG95], [CG00], [EH91], [FeR98], [GR62], [IK00], [Le62], [Ly80], [Sta87]). Поэтому здесь мы ограничимся изучением унимодулярных копредставлений.

Инъективность естественного отображения $G \to \widetilde{G}$ в унимодулярном случае была доказана в [K93] (см. также [FeR96]). Более тонкие свойства группы $\widetilde{G}$ можно найти в [CR01], [FoR05], [K06] и [K05].

Теорема 2. *Если группа* G *не имеет кручения, а слово* $w \in G * \langle t \rangle_\infty$ *унимодулярно, то группа* $\widetilde{G} = \langle G, t \mid w = 1 \rangle$ *содержит неабелеву свободную подгруппу, за исключением следующих двух случаев:*

1) $w \equiv g_1 t g_2$, *где* $g_1, g_2 \in G$ *(при этом* $\widetilde{G} \simeq G$*), и группа* G *не содержит неабелевых свободных подгрупп;*
2) G *— циклическая группа, а* $\widetilde{G}$ *изоморфна группе Баумслага–Солитэра* $G_{1,2} = \langle g, t \mid g^{-1}tg = t^2 \rangle$.

В работе [K06] было предложено обобщение понятия унимодулярности на случай когда слово w является элементом свободного произведения группы G и произвольной (то есть не обязательно циклической) группы T. Слово $w \equiv g_1 t_1 \ldots g_n t_n \in G * T$ называется *унимодулярным*, если

1) $\prod t_i$ является элементом бесконечного порядка в группе T;
2) циклическая подгруппа $\langle \prod t_i \rangle$ нормальна в T;
3) факторгруппа $T/\langle \prod t_i \rangle$ является группой с сильно однозначным умножением.

Напомним, что группа H называется *группой с однозначным умножением* (или *UP-группой*), если для любых двух её конечных непустых подмножеств $X, Y \subseteq H$ их произведение XY содержит по крайней мере один элемент, раскладывающийся в произведение элемента из X и элемента из Y однозначно. Одно время была гипотеза, что всякая группа без кручения является группой с однозначным умножением (обратное, очевидно, верно). Однако выяснилось, что существует контрпример ([P88], [RS87]).

Мы называем группу H *группой с сильно однозначным умножением*, если для любых двух её конечных непустых подмножеств $X, Y \subseteq H$ таких, что $|Y| \geqslant 2$, их произведение XY содержит по крайней мере два однозначно разложимых элемента $x_1 y_1$ и $x_2 y_2$ таких, что $x_1, x_2 \in X$, $y_1, y_2 \in Y$ и $y_1 \neq y_2$.

Насколько мы знаем, все известные примеры UP-групп обладают сильно однозначным умножением. Например, этим свойством обладают все правоупорядочиваемые группы, локально индикабельные группы, диффузные группы в смысле Бовдича.

Следующая теорема, с одной стороны, обобщает (точнее, дополняет) теорему 2, а с другой стороны, является ключевым шагом в доказательстве теоремы 1.

Теорема 3. *Пусть группа G не имеет кручения, группа T нециклическая и слово $w \in G*T$ унимодулярно. Тогда группа $\widetilde{G} = \langle G, T \mid w = 1\rangle \overset{\text{опр}}{=} (G * T)/\langle\langle w\rangle\rangle$ не содержит неабелевых свободных подгрупп тогда и только тогда, когда группа G циклическая, группа T не содержит неабелевых свободных подгрупп, а слово w сопряжено в $G * T$ слову вида gt, где $t \in T$, а g – порождающий элемент группы G.*

Обозначения, которые мы используем, в целом стандартны. Отметим только, что если x и y — элементы некоторой группы, а X — подмножество группы, то x^y означает $y^{-1}xy$, коммутатор $[x, y]$ понимается как $x^{-1}y^{-1}xy$, а $\langle X\rangle$ и $\langle\langle X\rangle\rangle$ означают, соответственно, подгруппу, порождённую множеством X и нормальную подгруппу, порождённую множеством X. Символом $|X|$ мы обозначаем мощность множества X.

1. Доказательство теоремы 1

Пусть слово w имеет вид $w \equiv g_1 x_{j_1}^{\varepsilon_1} g_2 x_{j_2}^{\varepsilon_2} \dots g_p x_{j_p}^{\varepsilon_p}$ и слово $w' \in F(x_1, \dots, x_n)$ получается из w стиранием коэффициентов: $w' = x_{j_1}^{\varepsilon_1} x_{j_2}^{\varepsilon_2} \dots x_{j_p}^{\varepsilon_p}$.

Случай 1: w' является истинной степенью в свободной группе $F(x_1, \dots, x_n)$. В этом случае группа $\widetilde{G}$ содержит неабелеву свободную подгруппу, поскольку по теореме о свободных подгруппах групп с одним соотношением такую подгруппу содержит группа с одним соотношением $T_1 = \langle x_1, \dots, x_n \mid w' = 1\rangle$, являющаяся гомоморфным образом группы G.

Случай 2: w' не является истинной степенью. Рассмотрим группы

$$T = \langle x_1, \dots, x_n \mid [x_1, w'] = \dots = [x_n, w'] = 1\rangle \quad \text{и} \quad T_1 = \langle x_1, \dots, x_n \mid w' = 1\rangle = T/\langle\langle w'\rangle\rangle.$$

Группа T является свободным центральным расширением группы с одним соотношением T_1. Хорошо известно, что если w' не является истинной степенью в свободной группе $F(x_1, \dots, x_n)$, то группа T_1 является локально индикабельной ([Б84]) и, следовательно, группой с сильно однозначным умножением. Элемент w' имеет бесконечный порядок в группе T (см. [ЛШ80]). Таким образом, слово w, рассматриваемое как элемент свободного произведения $G * T$, является унимодулярным. Группа T не является циклической, поскольку её факторгруппа по коммутанту является свободной абелевой ранга n и $n \geqslant 2$. Осталось заметить, что группа $\langle G, T \mid w = 1\rangle$ является гомоморфным образом группы $\widetilde{G}$ и, таким образом, утверждение теоремы 1 немедленно вытекает из теоремы 3.

2. Доказательство теоремы 2

Согласно [FoR05] мы говорим, что элемент $v \in G * \langle t\rangle_\infty$ с циклически несократимой формой $v \equiv g_1 t^{\varepsilon_1} \dots g_n t^{\varepsilon_n}$, где $\varepsilon_i \in \{\pm 1\}$ и $g_i \in G$, имеет *сложность* 0, если все показатели ε_i равны между собой (то есть если слово либо положительно, либо отрицательно); мы говорим, что сложность слова v равна 1, если среди показателей встречаются и положительные, и отрицательные, но либо два положительных показателя никогда не идут подряд, либо два отрицательных показателя никогда не идут подряд (здесь $(\varepsilon_1, \dots, \varepsilon_n)$ рассматривается как циклическая последовательность). В остальных случаях мы считаем, что сложность слова v больше единицы. Полное определение сложности можно найти в [FoR05].

Теорема о минимальной сложности [FoR05]**.** *Если группа G не имеет кручения, циклически приведённое слово $w \in G * \langle t\rangle_\infty$ унимодулярно и сложность слова $v \in G * \langle t\rangle_\infty$ меньше сложности слова w, то $v \neq 1$ в группе $\widetilde{G} = \langle G, t \mid w = 1\rangle$.*

Из этой теоремы немедленно вытекает, что в случае когда сложность слова w больше единицы, $\widetilde{G}$ содержит свободный квадрат группы G (поскольку $\langle G, G^t\rangle = G * G^t$), а значит и неабелевы свободные подгруппы.

Остаётся рассмотреть копредставления с соотношением сложности 1:

$$\widetilde{G} = \left\langle G, t \;\middle|\; ct\prod_{i=0}^{m}(b_i a_i^t) = 1 \right\rangle, \quad \text{где } m \geqslant 0,\ a_i, b_i \in G \setminus \{1\},\ c \in G. \tag{1}$$

В этом случае мы воспользуемся следующей леммой.

Лемма [K05, лемма 22]. *Если группа G не имеет кручения, а группа $\widetilde{G}$ задана копредставлением* (1), *то существует такое $d \in \{2,3\}$, что*

$$u \equiv \prod_{i=1}^{s} y_i x_i^{t^d} \neq 1 \text{ в } \widetilde{G}$$

для любого натурального s и любых $x_i, y_i \in G$ таких, что $\left|\{i \mid x_i \in \langle a_m \rangle\}\right| + \left|\{i \mid y_i \in \langle b_0 \rangle\}\right| \leqslant 2$ *и* $u \neq 1$ *в* $G * \langle t \rangle_\infty$.

Эта лемма показывает, что элементы $g_1 h_1^{t^d}$ и $h_2^{t^d} g_2$ группы $\widetilde{G}$ порождают свободную подгруппу ранга 2 при любых $g_1, g_2, h_1, h_2 \in G$ таких, что $h_1, h_2, h_1 h_2 \notin \langle a_m \rangle$ и $g_2, g_1, g_2 g_1 \notin \langle b_0 \rangle$. Следовательно, из отсутствия неабелевых свободных подгрупп в $\widetilde{G}$ вытекает, что группа G почти циклическая (либо $|G : \langle a_m \rangle| \leqslant 2$, либо $|G : \langle b_0 \rangle| \leqslant 2$), а значит и циклическая (в силу отсутствия кручения в группе G).

Если группа G циклическая, то группа $\widetilde{G}$ является группой с одним соотношением и по теореме о свободных подгруппах групп с одним соотношением либо содержит неабелеву свободную подгруппу, либо является циклической (чего не может быть при $m \geqslant 0$), либо изоморфна группе $G_{1,k}$. В последнем случае из унимодулярности соотношения w вытекает, что число k обязано быть двойкой, в чём легко убедиться, рассмотрев факторгруппу по коммутанту. Теорема 2 доказана.

3. Доказательство теоремы 3

Пусть слово w имеет вид $w \equiv g_1 t_1 \dots g_n t_n$.

Случай 1: $n = 1$. Ясно, что в этом случае $|T/\langle t_1 \rangle| = \infty$,

$$\widetilde{G} \simeq \begin{cases} G \underset{g_1 = t_1^{-1}}{*} T, & \text{если } g_1 \neq 1 \text{ в } G; \\ G * (T/\langle t_1 \rangle), & \text{если } g_1 = 1 \text{ в } G \end{cases}$$

и утверждение теоремы вытекает из следующих хорошо известных простых фактов:

1. *Свободное произведение с объединённой подгруппой содержит неабелеву свободную подгруппу, если объединяемая подгруппа является собственной в каждом из сомножителей и в одном из сомножителей её индекс больше двух.*
2. *Пусть $\langle a \rangle$ — циклическая нормальная подгруппа группы A. Тогда A содержит неабелеву свободную подгруппу тогда и только тогда, когда такую подгруппу содержит факторгруппа $A/\langle a \rangle$.*

Случай 2: $n > 1$ и группа $\langle t_1, \dots, t_n \rangle$ является циклической (и, следовательно, порождается элементом $t = \prod t_i$ в силу унимодулярности). В этом случае группа $\widetilde{G}$ представляется в виде свободного произведения с объединённой подгруппой:

$$\widetilde{G} \simeq \langle G, t \mid w = 1 \rangle \underset{\langle t \rangle}{*} T.$$

Такое свободное произведение всегда содержит неабелеву свободную подгруппу, поскольку объединяемая подгруппа имеет бесконечный индекс в каждом из сомножителей. Бесконечность индекса подгруппы $\langle t \rangle$ в первом сомножителе следует из теоремы о минимальной сложности, которая, в частности, гарантирует, что $G \cap \langle t \rangle = \{1\}$ при $n > 1$. А то, что $|T : \langle t \rangle| = \infty$, очевидным образом вытекает из унимодулярности слова w и нецикличности группы T.

Случай 3: группа $\langle t_1, \dots, t_n \rangle$ не является циклической. В этом случае без потери общности можно считать, что $T = \langle t_1, \dots, t_n \rangle$.

Положим $t = \prod t_i$. Разложим T в объединение смежных классов:

$$T = \coprod_{x \in T/\langle t \rangle} c_x \langle t \rangle, \quad \text{где } c_1 = 1.$$

Запишем слово w в виде

$$w \equiv t \prod_i g_i^{c_{x_i} t^{k_i}} = 1. \tag{2}$$

Пусть $X_1 = \{x_i\}$ — это множество всех $x \in T/\langle t \rangle$, встречающихся в несократимой записи (2). Заметим, что $|X_1| > 1$, поскольку группа $T = \langle t_1, \dots, t_n \rangle$ не является циклической. В работе [K06] показано, что в группе $\widetilde{G}$ имеет место разложение

$$H_1 = \langle \{G^{c_y} \mid y \in X_1\} \rangle = \underset{y \in X_1}{*} G^{c_y}.$$

Отсюда немедленно следует, что группа $\widetilde{G}$ содержит свободный квадрат группы G, а значит и неабелеву свободную подгруппу.

ГЛАВА 24.
SQ-УНИВЕРСАЛЬНОСТЬ ОТНОСИТЕЛЬНЫХ КОПРЕДСТАВЛЕНИЙ С ОДНИМ СООТНОШЕНИЕМ

1. Введение

Напомним, что группа G называется *SQ-универсальной*, если каждая счётная группа может быть вложена в некоторую факторгруппу группы G. SQ-универсальными являются все неабелевы свободные группы; все группы, раскладывающиеся нетривиальным образом в свободное произведение, кроме бесконечной диэдральной группы $\mathbb{Z}_2 * \mathbb{Z}_2$ (см. [ЛШ80]); многие свободные произведения с объединёнными подгруппами и HNN-расширения ([Ло86], [ЛШ80]); все подгруппы конечного индекса SQ-универсальных групп и все почти SQ-универсальные группы [Neu73]; все неэлементарные гиперболические группы [O95] и даже все (кроме некоторых очевидных исключений) относительно гиперболические группы, в частности, все группы с бесконечным числом концов [AMO07].

Отправной точкой нашего исследования служит следующая теорема.

Теорема Сасердота–Шуппа [SaSc74] (см. также [ЛШ80]). *Группа с одним соотношением и по меньшей мере тремя образующими SQ-универсальна.*

На самом деле имеет место значительно более общий факт.

Теорема Баумслага–Прайда [BaPr78]. *Группа, обладающая копредставлением, в котором число образующих по меньшей мере на два больше числа соотношений, SQ-универсальна. Более того, каждая такая группа является большой в смысле Громова, то есть обладает подгруппой конечного индекса, допускающей эпиморфизм на неабелеву свободную группу.*

Дальнейшим обобщением теоремы Сасердота–Шуппа является следующий результат.

Теорема Штёра–Громова [St83], [Gr83]. *Группа, обладающая копредставлением, в котором число образующих больше числа соотношений и одно из соотношений есть истинная степень, является SQ-универсальной и даже большой в смысле Громова.*[*)]

Дальнейшие результаты на эту тему можно найти, например, в работах [Ed84], [How98], [Bu05], [La05], [OlOs06]. В этой главе мы обобщаем теорему Сасердота–Шуппа в несколько ином направлении.

Пусть G — некоторая группа. Под группой, заданной относительным копредставлением с одним соотношением над группой G, понимается группа

$$\widetilde{G} = \langle G, x_1, x_2, \ldots, x_n \mid w = 1 \rangle \stackrel{\text{опр}}{=} G * F(x_1, x_2, \ldots, x_n) / \langle\langle w \rangle\rangle .$$

Здесь $x_1, \ldots, x_n$ — буквы (не лежащие в G) и w — произвольное слово в алфавите $G \cup \{x_1^{\pm 1}, \ldots, x_n^{\pm 1}\}$ (которое можно трактовать как элемент свободного произведения $G * F(x_1, x_2, \ldots, x_n)$ группы G и свободной группы с базисом $x_1, x_2, \ldots, x_n$). Другими словами, копредставление группы $\widetilde{G}$ получается из копредставления $G = \langle A \mid R \rangle$ группы G добавлением нескольких новых образующих и одного соотношения:

$$\widetilde{G} = \langle A \cup \{x_1, x_2, \ldots, x_n\} \mid R \cup \{w\} \rangle .$$

Теорема 1. *Если G — нетривиальная группа без кручения и $n \geqslant 2$, то группа $\widetilde{G} = \langle G, x_1, x_2, \ldots, x_n \mid w = 1 \rangle$ является SQ-универсальной при любом $w \in G * F(x_1, \ldots, x_n)$.*

Следствие [K06b]. *В условиях теоремы 1 группа $\widetilde{G}$* (как и всякая SQ-универсальная группа) *обладает неабелевыми свободными подгруппами.*

Замечание 1. Нетрудно показать, что группа $\widetilde{G}$ из теоремы 1 уже не обязана быть большой в смысле Громова.

Замечание 2. Разумеется, при $n = 1$ утверждение теоремы 1 перестаёт быть верным (равно как и утверждение теоремы Сасердота–Шуппа перестаёт быть верным для групп с двумя порождающими). Однако некоторыми свойствами, более слабыми, чем SQ-универсальность, группа $\widetilde{G}$ при $n = 1$ всё же обладает. В частности, она нетривиальна [K93], не является неабелевой простой группой (если $w \neq g_1 x_1^{\pm 1} g_2$) [K05], естественное отображение $G \to \widetilde{G}$ несюръективно (если $w \neq g_1 x_1^{\pm 1} g_2$) [CR01]; а в случае, когда сумма показателей степеней при x_1 в

[*)] Под *истинной степенью* мы понимаем элемент свободной группы F вида u^k, где $u \in F$ и $\mathbb{Z} \ni k \geqslant 2$. В частности, единица является истинной степенью, поэтому теорема Штёра–Громова является обобщением теоремы Баумслага–Прайда.

слове w равна ± 1, группа $\widetilde{G}$ всегда (кроме нескольких очевидных исключений) содержит неабелеву свободную подгруппу [K06b].

Теорема 1 говорит об относительных копредставлениях по меньшей мере с двумя дополнительными порождающими, однако важную роль в её доказательстве играет изучение однопорождённых относительных копредставлений

$$\widetilde{G} = \langle G, t \mid w = 1 \rangle \stackrel{\text{опр}}{=} (G * \langle t \rangle_\infty) / \langle\langle w \rangle\rangle, \quad \text{где } w \equiv \prod g_i t^{\varepsilon_i},\ g_i \in G,\ \varepsilon_i \in \{\pm 1\}. \tag{1}$$

Такое копредставление называется *унимодулярным*, если $\sum \varepsilon_i = \pm 1$. Известно, что унимодулярные относительные копредставления обладают многими хорошими свойствами и лучше поддаются изучению (см., например, [K93], [K94], [FeR96], [CR01], [FoR05], [K05], [K06a], [K06b]).

В работе [K06a] было предложено следующее обобщение понятия унимодулярности на так называемые *обобщённые относительные копредставления*

$$\widetilde{G} = \left\langle G * T \;\middle|\; \prod_{i=1}^{n} g_i t_i = 1 \right\rangle \stackrel{\text{опр}}{=} (G * T) \Big/ \left\langle\!\!\left\langle \prod g_i t_i \right\rangle\!\!\right\rangle. \tag{$*$}$$

Здесь T — произвольная (то есть не обязательно циклическая) группа, $g_i \in G$ и $t_i \in T$; слово $\prod\limits_{i=1}^{n} g_i t_i$ мы считаем циклически несократимым.

Обобщённое относительное копредставление $(*)$ над группой G называется *унимодулярным*, если

1) $\prod t_i$ является элементом бесконечного порядка в группе T;
2) циклическая подгруппа $\langle \prod t_i \rangle$ нормальна в T;
3) факторгруппа $T / \langle \prod t_i \rangle$ является группой с сильно однозначным умножением.

Напомним, что группа H называется *группой с однозначным умножением* (или *UP-группой*), если для любых двух её конечных непустых подмножеств $X, Y \subseteq H$ их произведение XY содержит по крайней мере один элемент, раскладывающийся в произведение элемента из X и элемента из Y однозначно.*)

Мы называем группу H *группой с сильно однозначным умножением*, если для любых двух её конечных непустых подмножеств $X, Y \subseteq H$ таких, что $|Y| \geqslant 2$, их произведение XY содержит по крайней мере два однозначно разложимых элемента $x_1 y_1$ и $x_2 y_2$ таких, что $x_1, x_2 \in X,\ y_1, y_2 \in Y$ и $y_1 \neq y_2$.

Насколько мы знаем, все известные примеры UP-групп обладают сильно однозначным умножением. Например, этим свойством обладают все правоупорядочиваемые группы, локально индикабельные группы, диффузные группы в смысле Бовдича.

Теорема 1 легко выводится из следующей теоремы.

Теорема 2. *Пусть обобщённое относительное копредставление $(*)$ над нециклической группой без кручения G унимодулярно и группа T не является циклической. Тогда группа $\widetilde{G}$, заданная копредставлением $(*)$, является SQ-универсальной.*

Для доказательства теоремы 2 мы устанавливаем следующий факт об обычных (необобщённых) унимодулярных относительных копредставлениях:

Теорема 3. *Если $G_1, \ldots, G_l$ — нециклические группы без кручения, $l \geqslant 2$ и относительное копредставление $L = \langle G_1 * \ldots * G_l, t \mid w = 1 \rangle$ над группой $G_1 * \ldots * G_l$ унимодулярно, то группа L является SQ-универсальной. Более того, каждая счётная группа S вкладывается в некоторую факторгруппу L/N, в которой выполняется теорема о свободе, то есть*

$$\langle t, G_{i_1}, \ldots, G_{i_{l-1}} \rangle = \langle t \rangle_\infty * G_{i_1} * \ldots * G_{i_{l-1}} \quad \text{в группе } L/N,$$

если слово w не сопряжено в группе $\langle t \rangle_\infty * G_1 * \ldots * G_l$ никакому элементу подгруппы $\langle t \rangle_\infty * G_{i_1} * \ldots * G_{i_{l-1}}$.

Согласно [K06a] мы говорим, что копредставление (1) является *магнусовым*, если естественное отображение $G \to \widetilde{G}$ инъективно и в группе $\widetilde{G}$ имеет место разложение $\langle H, t \rangle = H * \langle t \rangle_\infty$ (то есть элемент t *трансцендентен* над H в $\widetilde{G}$) для всякого свободного сомножителя H группы G такого, что w не сопряжено в $G * \langle t \rangle_\infty$ с элементами группы $H * \langle t \rangle$.

В работе [K06a] было показано, что каждое унимодулярное копредставление над группой без кручения является магнусовым. Для доказательства основных результатов этой главы нам понадобится более сильное свойство унимодулярных копредставлений.

Мы будем называть копредставление (1) *сильно магнусовым*, если элемент t трансцендентен в $\widetilde{G}$ над каждой подгруппой $H \subseteq G$ такой, что

1) w не сопряжено в $G * \langle t \rangle_\infty$ с элементами группы $H * \langle t \rangle$;
2) каждый коэффициент g_i либо лежит в H, либо трансцендентен над H.

*) Одно время была гипотеза, что всякая группа без кручения является группой с однозначным умножением (обратное, очевидно, верно). Однако выяснилось, что существует контрпример ([P88], [RS87]).

Утверждение 1. *Если копредставление (1) унимодулярно и неединичные коэффициенты g_i имеют бесконечный порядок в группе G, то копредставление (1) сильно магнусово.*

Доказательство утверждения 1 опирается на несколько ранее известных результатов, в частности, на следующую теорему.

Теорема 4. *Пусть $A \underset{C}{*} B$ — свободное произведение групп A и B с объединённой подгруппой C,*

$$v = b_0 a_0 \dots b_m a_m b_{m+1} \in (A \underset{C}{*} B),$$

$m \geqslant 1$, причём каждый коэффициент слова v (кроме, возможно, крайних) трансцендентен над C, то есть $\langle a_i, C\rangle = \langle a_i\rangle_\infty * C$ в группе A для $i = 0, \dots, m$ и $\langle b_i, C\rangle = \langle b_i\rangle_\infty * C$ в группе B для $i = 1, \dots, m$. Тогда для любого автоморфизма φ группы B естественные отображения

$$A \to \left\langle A \underset{C}{*} B \;\middle|\; \{b^v = b^\varphi \mid b \in B\} \right\rangle \leftarrow B$$

инъективны.

Эта теорема была доказана [K94], но не была опубликована. В последнем разделе главы мы приводим доказательство теоремы 4. В отличие от чисто алгебраических рассуждений всех предыдущих разделов, доказательство теоремы 4 имеет геометрическую природу. Другие ранее известные факты, из которых выводится утверждение 1, доказываются в том же духе.

Обозначения, которые мы используем, в целом стандартны. Отметим только, что если $k \in \mathbb{Z}$, x и y — элементы некоторой группы, а φ — гомоморфизм из этой группы в какую-нибудь другую группу, то x^y, x^{ky}, x^{-y}, x^φ, $x^{k\varphi}$ и $x^{-\varphi}$ обозначают $y^{-1}xy$, $y^{-1}x^k y$, $y^{-1}x^{-1}y$, $\varphi(x)$, $\varphi(x^k)$ и $\varphi(x^{-1})$ соответственно; коммутатор $[x, y]$ понимается как $x^{-1}y^{-1}xy$. Если X — подмножество некоторой группы, то $\langle X\rangle$ и $\langle\langle X\rangle\rangle$ означают, соответственно, подгруппу, порождённую множеством X, и нормальную подгруппу, порождённую множеством X. Символом $|X|$ мы обозначаем мощность множества X.

2. Доказательство теоремы 1

Если группа G является циклической, то группа $\widetilde{G}$ является группой с по меньшей мере тремя образующими и одним соотношением. SQ-универсальность таких групп утверждается в теореме Сасердота–Шуппа. В дальнейшем предполагаем, что группа G нециклическая.

Пусть слово w имеет вид $w \equiv g_1 x_{j_1}^{\varepsilon_1} g_2 x_{j_2}^{\varepsilon_2} \dots g_p x_{j_p}^{\varepsilon_p}$ и слово $w' \in F(x_1, \dots, x_n)$ получается из w стиранием коэффициентов: $w' = x_{j_1}^{\varepsilon_1} x_{j_2}^{\varepsilon_2} \dots x_{j_p}^{\varepsilon_p}$.

Случай 1: w' является истинной степенью в свободной группе $F(x_1, \dots, x_n)$. В этом случае группа $\widetilde{G}$ SQ-универсальна, поскольку по теореме Штёра–Громова SQ-универсальна группа с одним соотношением

$$T_1 = \langle x_1, \dots, x_n \mid w' = 1\rangle,$$

которая является гомоморфным образом группы $\widetilde{G}$.

Случай 2: w' не является истинной степенью. Рассмотрим группы

$$T = \langle x_1, \dots, x_n \mid [x_1, w'] = \dots = [x_n, w'] = 1\rangle \quad \text{и} \quad T_1 = \langle x_1, \dots, x_n \mid w' = 1\rangle = T/\langle w'\rangle.$$

Группа T является свободным центральным расширением группы с одним соотношением T_1. Хорошо известно, что если w' не является истинной степенью в свободной группе $F(x_1, \dots, x_n)$, то группа T_1 является локально индикабельной ([Б84]) и, следовательно, группой с сильно однозначным умножением. Элемент w' имеет бесконечный порядок в группе T (см. [ЛШ80]). Таким образом, обобщённое относительное копредставление $\langle G, T \mid w = 1\rangle$ является унимодулярным. Группа T не является циклической, поскольку её факторгруппа по коммутанту является свободной абелевой ранга $n \geqslant 2$. Значит, по теореме 2 группа $\langle G, T \mid w = 1\rangle$ SQ-универсальна. Осталось заметить, что эта группа является гомоморфным образом группы $\widetilde{G}$, а группа, имеющая SQ-универсальный гомоморфный образ, сама, очевидно, является SQ-универсальной.

3. Итерированные свободные произведения с объединёнными подгруппами

В этом разделе мы воспроизводим в несколько более общей ситуации одну конструкцию из [K06a].

Пусть I — некоторое множество и Ω — некоторое семейство подмножеств множества I. Для каждого $i \in I$ рассмотрим некоторую группу G_i, и для каждого $\omega \in \Omega$ рассмотрим некоторую факторгруппу G_ω свободного произведения $\mathop{*}\limits_{i\in\omega} G_i$:

$$G_\omega = \left(\mathop{*}_{i\in\omega} G_i\right) \Big/ N_\omega.$$

Возникает естественный вопрос: при каких условиях естественные отображения

$$\varphi_\omega \colon G_\omega \to G_I \stackrel{\text{опр}}{=} \left(\mathop{*}_{i\in I} G_i\right) \Big/ \left\langle\!\!\left\langle \bigcup_{\omega\in\Omega} N_\omega \right\rangle\!\!\right\rangle$$

инъективны? Или, при каких условиях группу G_I можно трактовать как свободное произведение с объединёнными подгруппами групп G_ω?

Следующее утверждение даёт некоторые достаточные условия для положительного ответа на эти вопросы.

Утверждение 2. *Пусть*

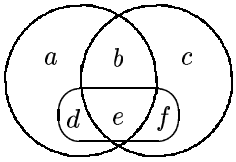
$$N_\omega \cap \mathop{*}_{j\in\omega\setminus\{i\}} G_j = \{1\} \qquad (**)$$

для каждого $\omega \in \Omega$ и каждого $i \in \omega \setminus (\bigcap \Omega)$. Допустим, что, кроме того, для каждого конечного подсемейства $F \subseteq \Omega$ такого, что $|F| \geqslant 2$, найдутся такие элементы $\min, \max \in \bigcup F$, что

1) *элемент* min *содержится ровно в одном множестве $\omega_{\min} \in F$;*
2) *элемент* max *содержится ровно в одном множестве $\omega_{\max} \in F$;*
3) $\omega_{\min} \neq \omega_{\max}$.

Тогда все естественные отображения $\varphi_\omega \colon G_\omega \to G_I$ инъективны.

Пример. Пусть $I = \{a, b, c, d, e, f\}$ и $\Omega = \{\{a, b, d, e\}, \{b, c, e, f\}, \{d, e, f\}\}$.



Соответствующие шесть групп G_i мы обозначим $A, \ldots, F$, а три группы G_ω мы обозначим **ABDE**, **BCEF** и **DEF**. Нетрудно убедиться, что в данном случае условия 1), 2) и 3) выполнены для семейства Ω и каждого его подсемейства, состоящего из двух множеств. Допустим, что выполнено также условие (**). Тогда справедливость утверждения 2 (в данном случае) вытекает из следующего разложения группы G_I в свободное произведение с объединёнными подгруппами:

$$G_I = \left((\mathbf{DEF} * B) \mathop{*}_{B*D*E} \mathbf{ABDE} \right) \mathop{*}_{B*E*F} \mathbf{BCEF}.$$

Для доказательства утверждения в общем случае докажем сперва лемму.

Лемма 1. *Пусть выполнены условия утверждения 2, Ω' — конечное подсемейство семейства Ω, $\omega \in \Omega$ и $\alpha \subseteq \omega \cap (\bigcup \Omega')$ — некоторое собственное подмножество множества ω, лежащее в $\bigcup \Omega'$ и содержащее $\bigcap \Omega$. Тогда естественное отображение*

$$\mathop{*}_{i\in\alpha} G_i \to G_{\Omega'} \stackrel{\text{опр}}{=} \left(\mathop{*}_{i\in\bigcup\Omega'} G_i\right) \Big/ \left\langle\!\!\left\langle \bigcup_{\omega'\in\Omega'} N_{\omega'} \right\rangle\!\!\right\rangle$$

инъективно.

Доказательство.

Случай 1: $\omega \in \Omega'$. Воспользуемся индукцией по мощности семейства Ω'. Если $|\Omega'| = 1$ (то есть $\Omega' = \{\omega\}$), то утверждение леммы верно по условию (**). Допустим, что $|\Omega'| \geqslant 2$. В этом случае в соответствии с условиями 1), 2) и 3) семейство $F = \Omega'$ содержит множество $\omega' \neq \omega$, содержащее элемент $m \in \omega'$, не лежащий в $\bigcup(\Omega' \setminus \{\omega'\})$.

По предположению индукции (применённому к множеству ω' в качестве ω и семейству $\Omega' \setminus \{\omega'\}$ в качестве Ω') группы

$$G_i \text{ с номерами } i \in \beta \stackrel{\text{опр}}{=} \omega' \cap \left(\bigcup(\Omega' \setminus \{\omega'\})\right)$$

свободно порождают своё свободное произведение в группе $G_{\Omega' \setminus \{\omega'\}}$. А по условию $(**)$ те же группы G_i, где $i \in \beta$, свободно порождают своё свободное произведение в группе $G_{\omega'}$ (поскольку ω' содержит элемент m, не лежащий в β). Значит, группа $G_{\Omega'}$ раскладывается в свободное произведение групп $G_{\Omega' \setminus \{\omega'\}}$ и $G_{\omega'}$ с объединённой подгруппой $\underset{i \in \beta}{*} G_i$. При этом интересующие нас группы G_i с номерами $i \in \alpha$ лежат в сомножителе $G_{\Omega' \setminus \{\omega'\}}$. Следовательно, утверждение леммы следует из предположения индукции, применённого к множеству ω и семейству $\Omega' \setminus \{\omega'\}$ в качестве Ω'.

Случай 2: $\omega \notin \Omega'$. Доказательство в этом случае устроено похожим образом. Снова воспользуемся индукцией по мощности семейства Ω'. Если $\Omega' = \varnothing$, то доказывать нечего. Допустим, что $|\Omega'| \geqslant 1$. В этом случае в соответствии с условиями 1), 2) и 3) семейство $F = \Omega' \cup \{\omega\}$ содержит множество $\omega' \neq \omega$, содержащее элемент $m \in \omega'$, не лежащий в $\bigcup(F \setminus \{\omega'\})$ (Рис.1).

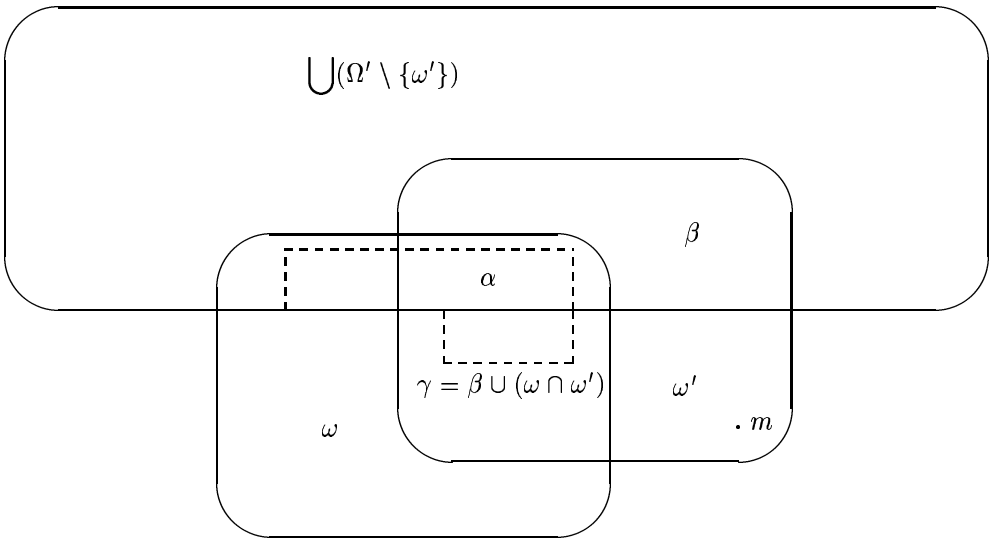


Рис. 1

По предположению индукции (применённому к множеству ω' в качестве ω и семейству $\Omega' \setminus \{\omega'\}$ в качестве Ω') группы

$$G_i \text{ с номерами } i \in \beta \stackrel{\text{опр}}{=} \omega' \cap \left(\bigcup(\Omega' \setminus \{\omega'\})\right)$$

свободно порождают своё свободное произведение в группе $G_{\Omega' \setminus \{\omega'\}}$. Значит, группы

$$G_i \text{ с номерами } i \in \gamma \stackrel{\text{опр}}{=} \beta \cup (\omega \cap \omega') = \omega' \cap \left(\bigcup((\Omega' \cup \omega) \setminus \{\omega'\})\right)$$

свободно порождают своё произведение в группе

$$H = \left(\underset{j \in (\omega \cap \omega') \setminus \beta}{*} G_j\right) * G_{\Omega' \setminus \{\omega'\}}.$$

Но по условию $(**)$ те же группы G_i, где $i \in \gamma$, свободно порождают своё свободное произведение в группе $G_{\omega'}$ (поскольку ω' содержит элемент m, не лежащий в γ). Значит, группа $G_{\Omega'}$ раскладывается в свободное произведение с объединённой подгруппой групп H и $G_{\omega'}$:

$$G_{\Omega'} = H \underset{\langle G_i \,;\, i \in \gamma \rangle}{*} G_{\omega'}.$$

При этом интересующие нас группы G_i с номерами $i \in \alpha$ лежат в сомножителе H. Следовательно, по предположения индукции, применённому к множеству ω и семейству $\Omega' \setminus \{\omega'\}$ в качестве Ω', группы G_i с номерами

$i \in \alpha \cap (\bigcup(\Omega' \setminus \{\omega'\})$ свободно порождают своё свободное произведение в группе $G_{\Omega' \setminus \{\omega'\}}$. Отсюда немедленно вытекает, что группы G_i с номерами $i \in \alpha$ свободно порождают своё свободное произведение в группе H и, следовательно, в группе $G_{\Omega'}$, содержащей, как мы видели, H в качестве подгруппы. Лемма доказана.

Доказательство утверждения 2. Ясно, что утверждение достаточно доказать для конечного семейства Ω мощности большей единицы. Но в этом случае

$$G_I = G_\Omega * \left(\mathop{*}_{i \notin \bigcup \Omega} G_i \right),$$

а группа G_Ω раскладывается в свободное произведение с объединённой подгруппой:

$$G_\Omega = G_{\omega_{\min}} \mathop{*}_{K} G_{\Omega \setminus \{\omega_{\min}\}},$$

где объединяемая группа K является свободным произведением групп G_i с номерами из множества

$$\omega_{\min} \cap \bigcup(\Omega \setminus \{\omega_{\min}\})$$

в силу леммы 1. Поэтому утверждение очевидным образом вытекает из индуктивных соображений.

4. Доказательство теоремы 2. Нерасщепляющийся случай

В этом разделе мы докажем теорему 2 в случае, когда группа $\langle\{t_i\}\rangle \subseteq T$ не является циклической.

Зафиксируем произвольную счётную группу S. Положим $t = \prod t_i$. Разложим T в объединение смежных классов:

$$T = \coprod_{x \in T/\langle t \rangle} c_x \langle t \rangle, \quad \text{где } c_1 = 1.$$

Для каждого $x \in T/\langle t \rangle$ рассмотрим изоморфную копию $G^{(c_x)}$ группы G (подразумевая, что изоморфизм отображает элемент $g \in G$ в элемент $g^{(c_x)} \in G^{(c_x)}$) и запишем соотношение $\prod g_i t_i = 1$ в виде

$$t \prod_i g_i^{c_{x_i} t^{k_i}} = 1. \tag{2}$$

Пусть X_1 — это множество всех $x \in T/\langle t \rangle$, встречающихся в несократимой записи соотношения (2). Заметим, что $|X_1| \geqslant 2$, поскольку в рассматриваемом случае $\langle\{t_i\}\rangle \neq \langle t \rangle$. Положим

$$H_1 = \mathop{*}_{y \in X_1} G^{(c_y)}$$

и рассмотрим унимодулярное относительное копредставление

$$\widetilde{H}_1 = \left\langle H_1, z \;\middle|\; z \prod_i g_i^{(c_{x_i}) z^{k_i}} = 1 \right\rangle$$

над группой H_1. По теореме 3 группа $\widetilde{H}_1$ имеет такую факторгруппу K_1, что

1) группа S вкладывается в K_1;
2) в группе K_1 имеет место разложение

$$\left\langle z, \{G^{(c_y)} \;;\; y \in Y\} \right\rangle = \langle z \rangle_\infty * \left(\mathop{*}_{y \in Y} G_y \right) \tag{3}$$

для каждого собственного подмножества $Y \subset X_1$.

Группа K_1 является факторгруппой группы

$$L_1 = H_1 * \langle z \rangle_\infty = \left(\mathop{*}_{y \in X_1} G^{(c_y)} \right) * \langle z \rangle_\infty$$

по некоторой нормальной подгруппе N_1.

Рассмотрим теперь свободное произведение

$$L = \left(\underset{y \in T/\langle t \rangle}{*} G^{(c_y)} \right) * \langle z \rangle_\infty .$$

Группа T действует справа на группе L автоморфизмами по формулам

$$z^x = z^{\varepsilon_x}, \ \left(g^{(c_y)}\right)^x = g^{(c_{yx})z^l},$$

где $x \in T$, $y \in T/\langle t \rangle$, $\varepsilon_x = \pm 1$ в зависимости от того, коммутирует x с t или нет, а целое число l однозначно определяется из равенства $c_y x = c_{yx} t^l$.

Для каждого $x \in T/\langle t \rangle$ рассмотрим множество $X_x = X_1 x \subseteq T/\langle t \rangle$ и подпроизведение

$$L_x = \left(\underset{y \in X_x}{*} G^{(c_y)} \right) * \langle z \rangle_\infty$$

свободного произведения L. В группе L_x имеется нормальная подгруппа $N_x = N_1^x \overset{\text{опр}}{=} N_1^\chi$, где $\chi \in T$ — это любой представитель элемента $x \in T/\langle t \rangle$.

Покажем, что семейство подпроизведений $\{L_x \mid x \in T/\langle t \rangle\}$ вместе с подгруппами $N_x \lhd L_x$ удовлетворяет условиям утверждения 2. Действительно, условия 1), 2) и 3) этого утверждения непосредственно вытекают из сильной однозначности умножения в группе $T/\langle t \rangle$. Выполнение условия $(**)$ для пары групп $N_1 \lhd L_1$ следует из разложения (3). Выполнение этого условия для других пар $N_x \lhd L_x$ вытекает из того, что группа L_x изоморфна группе L_1; причём изоморфизм (действие элемента $x \in T$) переводит подгруппу N_1 в подгруппу N_x, а каждый из сомножителей $G^{(c_y)}$ группы L_1 в подгруппу $(G^{(c_{yx})})^{z^l}$ группы L_x.

Мы видим, что условия утверждения 2 выполнены. Следовательно, естественные отображения

$$K_x = L_x/N_x \to K \overset{\text{опр}}{=} L \Big/ \left\langle\!\!\left\langle \bigcup_{y \in T/\langle t \rangle} N_y \right\rangle\!\!\right\rangle$$

инъективны.

Группа T действует на K автоморфизмами. Возьмём соответствующее полупрямое произведение $T \leftthreetimes K$ и профакторизуем его по циклической нормальной подгруппе $\langle zt^{-1} \rangle$. Получившаяся группа

$$P = (T \leftthreetimes K)/\langle zt^{-1} \rangle$$

и будет искомой факторгруппой группы $\widetilde{G}$.

Действительно, группа G вкладывается в P в качестве подгруппы: $G = G^{(1)} \subseteq K \subseteq P$. Согласно определению действия, мы имеем $G^{(c_x)} = G^{c_x}$, значит, соотношение группы $\widetilde{H}_1$, выполненное в K, и равенство $t = z$ в группе P дают соотношение (2). То есть группа $P = \langle T, G \rangle$ является факторгруппой группы $\widetilde{G}$, содержащей подгруппу K_1, которая, в свою очередь, содержит произвольную наперёд заданную счётную группу S. Теорема 2 в случае, когда группа $\langle \{t_i\} \rangle$ не является циклической, доказана.

5. Доказательство теоремы 2. Расщепляющийся случай

Докажем теперь теорему 2 в случае, когда группа $\langle \{t_i\} \rangle$ циклическая. Если копредставление $(*)$ имеет вид $\widetilde{G} = \langle G * T \mid t = 1 \rangle$, то группа $\widetilde{G}$ представляет собой свободное произведение двух бесконечных групп G и $T/\langle t \rangle$ и, следовательно, является SQ-универсальной (см. [ЛШ80]). В дальнейшем предполагаем, что копредставление $(*)$ имеет другой вид.

Из условия унимодулярности следует, что $\langle \{t_i\} \rangle = \langle t \rangle_\infty$, где $t = \prod t_i$. Рассмотрим группу R, заданную унимодулярным относительным копредставлением

$$R = \left\langle G, z \;\middle|\; \prod_{i=1}^{n} g_i z^{k_i} = 1 \right\rangle,$$

где показатели k_i определяются из равенств $t_i = t^{k_i}$, при этом $k_i \neq 0$ и $\sum k_i = 1$. Известно, что элемент z имеет бесконечный порядок в группе R и равенство $R = \langle z \rangle$ имеет место только в случае, когда $n = 1$ и $G = \langle g_1 \rangle$ [CR01]. В этом случае теорема в доказательстве не нуждается. В остальных случаях возьмём элемент r группы R, не лежащий в $\langle z \rangle$, но обладающий тем свойством, что $z^{kr} \neq z^l$, если целые числа k и l различны. Нетрудно

сообразить, что такой элемент всегда найдётся. Действительно, для каждого $x \in R$ определим неотрицательное целое число $k(x)$ равенством $\langle z\rangle^x \cap \langle z\rangle = \langle z^{k(x)}\rangle$. Возможны три случая:

1) $k(x) = 0$ для некоторого $x \in R$;
2) $k(x) > 1$ для некоторого $x \in R$;
3) $k(x) = 1$ для всех $x \in R$.

В первом случае мы можем положить $r = x$. В втором случае мы можем положить $r = z^{x^{-1}}$. В случае 3) циклическая подгруппа $\langle z\rangle$ является нормальной в R и не совпадает со своим централизатором (поскольку индекс этого централизатора в R не превосходит двух, а каждая почти циклическая группа без кручения является циклической); в качестве r в этом случае мы можем взять произвольный элемент централизатора z, не лежащий в $\langle z\rangle$.

Выберем также такую бесконечную последовательность элементов $\{t_{ij}\ ;\ i = 1, 2, \ldots,\ j = 1, \ldots, 1000\}$ централизатора элемента t в группе T, что все $t_{ij}^{\pm 1}$ лежат в разных смежных классах по нормальной подгруппе $\langle t\rangle$. Такая последовательность найдётся, поскольку $T/\langle t\rangle$ является нетривиальной группой без кручения и индекс централизатора элемента t в группе T не превосходит двух.

Возьмём произвольную счётную группу $S = \{s_1, s_2, \ldots\}$ и положим $K = R \times S$. Рассмотрим группу

$$L = \left(K \underset{z=t}{*} T\right) \Big/ \left\langle\!\!\left\langle s_i \prod_{j=1}^{1000} r t_{ij}\ ;\ i = 1, 2, \ldots \right\rangle\!\!\right\rangle .$$

Это копредставление группы L удовлетворяет условию малого сокращения $C'(1/100)$ для свободных произведений с объединённой подгруппой (см. [ЛШ80]). Следовательно естественные отображения $S \to K \to L$ инъективны. Для завершения доказательства осталось заметить, что группа L является факторгруппой группы $\widetilde{G} = R \underset{z=t}{*} T$.

6. Доказательство теоремы 3

Лемма 2. *Никакая бесконечная нециклическая группа не может быть объединением конечного числа своих циклических подгрупп.*

Доказательство. Пусть группа G является объединением конечного числа циклических подгрупп. Такая группа, очевидно, обладает следующим свойством:

любые два бесконечных множества $X, Y \subseteq G$ содержат пару коммутирующих элементов $x \in X$, $y \in Y$.

Хорошо известно, что бесконечные группы с таким свойством являются абелевыми.*) Поскольку всякая подгруппа и факторгруппа группы G также является объединением конечного числа своих циклических подгрупп, достаточно показать, что $G \not\cong \mathbb{Z} \oplus \mathbb{Z}_p$. Но в группе $\mathbb{Z} \oplus \mathbb{Z}_p$ имеется бесконечно много максимальных циклических подгрупп: $\langle (1,1)\rangle$, $\langle (p,1)\rangle$, $\langle (p^2,1)\rangle$,...; следовательно, эта группа не может быть объединением конечного числа своих циклических подгрупп.

Лемма 3. *Пусть $l \geqslant 2$ — натуральное число, $G_1, \ldots, G_l$ — нециклические бесконечные группы,*

$$u_1, \ldots, u_s \in G_1 * \ldots * G_l$$

и S — произвольная счётная группа. Тогда в группе $G_1 * \ldots * G_l$ найдётся такая нормальная подгруппа N, что

1) *группа S вкладывается в $(G_1 * \ldots * G_l)/N$;*
2) *$N \cap \langle u_i, G_{i_1}, \ldots, G_{i_{l-1}}\rangle = \{1\}$ для всех $i \in \{1, \ldots, s\}$ и $i_1, \ldots, i_{l-1} \in \{1, \ldots, l\}$.*

Доказательство. Пусть $U \subseteq G_1 \cup \ldots \cup G_l$ — конечное множество, состоящее из всех коэффициентов всех слов u_i. Из леммы 2 следует, что множество

$$M_k = G_k \setminus \left(\bigcup_{u \in U} \langle u\rangle\right)$$

бесконечно для каждого $k \in \{1, \ldots, l\}$. Рассмотрим счётное множество слов

$$v_i = \prod_{j=1}^{2022} \prod_{k=1}^{l} g_{ijk} \in G_1 * \ldots * G_l,$$

*) Это легко следует теоремы Б. Неймана [Neu76] (ответ на вопрос П. Эрдёша): *группы, в которых любое бесконечное подмножество содержит пару различных коммутирующих элементов, — это в точности группы, у которых индекс центра конечен.*

где $g_{ijk} \in M_k$ и все $g_{ijk}^{\pm 1}$ различны. Пусть $S = \{s_1, s_2, \ldots\}$. Положим

$$H = (G_1 * \ldots * G_l * S) \,/\, \langle\langle v_1 s_1^{-1}, v_2 s_2^{-1}, \ldots \rangle\rangle .$$

Ясно, что указанное копредставление группы H удовлетворяет условию малого сокращения $C'(1/(100l))$ (см. [ЛШ80]), из которого вытекает, что естественное отображение $S \to H$ инъективно, а каждое слово, содержащееся в ядре N естественного эпиморфизма $G_1 * \ldots * G_l \to H$ содержит коэффициенты из каждого из множеств M_k. В частности, $N \cap \langle u_i, G_{i_1}, \ldots, G_{i_{l-1}} \rangle = \{1\}$, что и требовалось.

Докажем теперь теорему 3. Пусть слово w имеет вид $u_1 t^{\varepsilon_1} \ldots u_s t^{\varepsilon_s}$, где $u_i \in G_1 * \ldots * G_l$ и $\varepsilon_i \in \{\pm 1\}$. Заметим, что в группе $G_1 * \ldots * G_l$ каждый неединичный элемент u_i имеет бесконечный порядок и трансцендентен над каждой из подгрупп $G_{i_1} * \ldots * G_{i_k}$, не содержащей этот элемент u_i.

Выберем нормальную подгруппу $N \lhd G_1 * \ldots * G_l$ в соответствии с леммой 3 и положим $G = (G_1 * \ldots * G_l)/N$. По лемме 3 группа G содержит произвольную наперёд заданную счётную группу S и образ каждого неединичного элемента u_i в группе G по-прежнему остаётся элементом бесконечного порядка трансцендентным над каждой из подгрупп $G_{i_1} * \ldots * G_{i_k}$, не содержащей этот элемент u_i. Для завершения доказательства осталось сослаться на утверждение 1.

7. Доказательство утверждения 1

Отметим несколько простых фактов.

Лемма 4. *Пусть $u \in X * Y$ — элемент свободного произведения групп X и Y и Z — подгруппа группы Y, причём элемент u алгебраичен (то есть нетрансцендентен) над $X * Z$. Тогда либо $u \in (X * Z)Y(X * Z)$, либо u имеет вид $x_1 u' x_2$, где $x_1, x_2 \in X * Z$, а элемент $u' \in X * Y$ имеет конечный порядок.*

Доказательство этой элементарной леммы мы оставляем читателю в качестве лёгкого упражнения.

Лемма 5. *Пусть A — нетривиальная подгруппа группы B и $b \in B$. Тогда b трансцендентен над A в том и только том случае, когда*

$$\left\langle \{A^{b^i} \ ; \ i \in \mathbb{Z}\} \right\rangle = \mathop{\ast}_{i \in \mathbb{Z}} A^{b^i}.$$

Доказательство. В одну сторону утверждение очевидно, а в другую сторону следует из того, что, если $u \in A * \langle b \rangle_\infty$ — нетривиальное соотношение между A и b в группе B и $a \in A \setminus \{1\}$, то $[a, u]$ — нетривиальное соотношение между группами A^{b^i}. Лемма 5 доказана.

До конца этого раздела будем предполагать, что подгруппа H группы G удовлетворяет условиям 1) и 2) из определения сильной магнусовости, копредставление (1) является унимодулярным и все неединичные коэффициенты g_i имеют бесконечный порядок в группе G. Будем доказывать, что элемент t трансцендентен над H в группе $\widetilde{G}$.

Лемма 6. *Если*

$$\left\langle \{H^{t^i} \ ; \ i \in \mathbb{Z}\} \right\rangle = \mathop{\ast}_{i \in \mathbb{Z}} H^{t^i} \tag{4}$$

в группе $\widetilde{G}$, то элемент $t \in \widetilde{G}$ является трансцендентным над H.

Доказательство. В случае, когда группа H нетривиальна, утверждение немедленно вытекает из леммы 5. Если же $H = \{1\}$, то утверждается лишь то, что элемент $t \in \widetilde{G}$ имеет бесконечный порядок (если w не сопряжено с $t^{\pm 1}$); в явном виде этот факт отмечен в [CR01]. Лемма 6 доказана.

Положим

$$\overline{H} = \mathop{\ast}_{i \in \mathbb{Z}} H_i, \quad \overline{G} = \overline{H} \mathop{\ast}_{H_0 = H} G,$$

где H_i — это изоморфные копии группы H. Ясно, что $\widetilde{G}$ обладает копредставлением

$$\widetilde{G} \simeq \langle \overline{G}, t \,|\, w(t) = 1, \ \{H_i^t = H_{i+1}; \quad i \in \mathbb{Z}\} \rangle .$$

Передвигая в слове w все буквы $t^{\pm 1}$ влево через коэффициенты, лежащие в H, с помощью соотношений $H_i t^{\pm 1} = t^{\pm 1} H_{i \pm 1}$, мы перепишем копредставление группы $\widetilde{G}$ в виде

$$\widetilde{G} \simeq \left\langle \overline{G}, t \,\middle|\, \prod_{i=1}^{p} \overline{g}_i t^{k_i} = 1, \ \{H_i^t = H_{i+1} \ ; \ i \in \mathbb{Z}\} \right\rangle,$$

где $k_i \in \mathbb{Z} \setminus \{0\}$, $\sum k_i = 1$ и $\overline{g}_i \in \overline{G}$. Причём каждый коэффициент $\overline{g}_i$ имеет вид

$$\overline{g}_i = \prod_{j=1}^{s} \overline{h}_j f_j, \quad \text{где } s \geqslant 1,\ f_j \in \{g_1, g_2, \ldots\} \setminus H,\ \overline{h}_j \in \overline{H} \setminus H \text{ при } j \neq 1,\ \text{а } \overline{h}_1 \in \overline{H}.$$

Здесь f_j, $\overline{h}_j$ и s зависят от i. Заметим, что $f_1, \ldots, f_s$ и $\overline{h}_2, \ldots, \overline{h}_s$ трансцендентны над H в $\overline{G}$.

Если $p = 1$, то есть первое соотношение рассматриваемого копредставления группы $\widetilde{G}$ переписывается в виде

$$t = u, \quad \text{где } u = \overline{g}_1 = \prod_{j=1}^{s} \overline{h}_j f_j \in \overline{G},$$

то всё копредставление переписывается в виде

$$\widetilde{G} \simeq \left\langle \overline{H} \underset{H_0=H}{*} G \;\middle|\; \{H_i^u = H_{i+1}\ ;\ i \in \mathbb{Z}\} \right\rangle.$$

По лемме 6 достаточно доказать инъективность естественного отображения $f\colon \overline{H} \to \widetilde{G}$.

Если $s > 1$, то есть $u \notin \overline{H}G\overline{H}$, то гомоморфизм f является инъективным в силу теоремы 4.

Допустим теперь, что $s = 1$, то есть $u = \overline{h}_1 f_1$, где $\overline{h}_1 \in \overline{H}$, а элемент $f_1 \in G$ трансцендентен над H. В этом случае, вложимость $\overline{H}$ в $\widetilde{G}$ очевидным образом вытекает из разложения

$$\widetilde{G} = G \underset{K=L}{*} (H * \langle t \rangle_\infty),$$

где $G \supseteq K = \langle f_1, H \rangle = \langle f_1 \rangle_\infty * H \simeq L = \left\langle (\overline{h}_1)^{-1} t, H \right\rangle = \left\langle (\overline{h}_1)^{-1} t \right\rangle_\infty * H \subseteq H * \langle t \rangle_\infty$.

Рассмотрим теперь случай, когда $p > 1$. Рассмотрим следующие подгруппы группы $G * \langle t \rangle_\infty$: $G_i = t^{-i} G t^i$, $H_i = t^{-i} H t^i$,

$$\overline{H} = \overset{\infty}{\underset{i=-\infty}{*}} H_i, \quad K^{(m)} = \overset{m}{\underset{i=0}{*}} G_i \quad \text{и} \quad G^{(m)} = \overline{H} \underset{H_0 * \ldots * H_m}{*} K^{(m)}. \tag{5}$$

Рассмотрим все возможные записи соотношения $w = 1$ в виде

$$ct \prod_{i=1}^{n} b_i t^{-1} a_i t = 1, \quad \text{где } a_i, b_i, c \in G^{(m)}. \tag{6}$$

Из всех таких записей выберем те, в которых m минимально, после чего из всех записей с минимальным m выберем запись с наименьшим n. Для такой минимальной записи (6) будем иметь:

1) $n \geqslant 1$ (то есть длина этой записи строго больше единицы);
2) $a_i \notin G^{(m-1)}$ и $b_i \notin (G^{(m-1)})^t$;
3) каждый коэффициент a_i трансцендентен над $G^{(m-1)}$, а каждый коэффициент b_i трансцендентен над $(G^{(m-1)})^t$.

Первое свойство обеспечивается тем, что $p > 1$, значит в записи длины 1 $m > 0$; следовательно, m можно уменьшить, заменив все вхождения элементов группы G_m на фрагменты вида $t^{-1} g t$, где $g \in G_{m-1}$. Второе свойство очевидным образом следует из условий минимальности n и m. Для доказательства свойства 3) надо заметить, что в нормальной форме, соответствующей разложению

$$G^{(m)} = X * Y, \quad \text{где } X = \left(\underset{j \neq m}{*} H_j \right) * G_0 * \ldots G_{m-1} \text{ и } Y = G_m,$$

каждый Y-слог каждого коэффициента a_i лежит в $(H\{f_1, \ldots, f_p\}H)^{t^m}$, и воспользоваться леммой 4, положив $Z = H_m$. Аналогичным образом устанавливается трансцендентность b_i над $(G^{(m-1)})^t$.

Пусть теперь символы H_i и G_i обозначают абстрактные изоморфные копии групп H и G, а группы $\overline{H}$, $K^{(m)}$ и $G^{(m)}$ определены формулами (5). Рассмотрим следующее копредставление группы $\widetilde{G}$:

$$\widetilde{G} = \left\langle G^{(m)}, t \;\middle|\; ct \prod_{i=1}^{n} b_i a_i^t = 1,\ \left\{G_i^t = G_{i+1}\ ;\quad i \in \{0, \ldots m-1\}\right\},\ \left\{H_i^t = H_{i+1}\ ;\quad i \in \mathbb{Z}\right\} \right\rangle. \tag{7}$$

Для завершения доказательства утверждения 1 остаётся только заметить, что свойства 1) и 3) копредставления (7) влекут инъективность естественного отображения $G^{(m)} \to \widetilde{G}$ в силу следующей теоремы.

Теорема ([K93], см. также [Fer96]). *Пусть M и N — изоморфные подгруппы группы L, $\varphi : M \to N$ — изоморфизм, $n \geqslant 1$, $a_1, \ldots, a_n$ — элементы группы L, трансцендентные над M, $b_1, \ldots, b_n$ — элементы группы L, трансцендентные над N, и $c \in L$. Тогда система уравнений*

$$\begin{cases} x^{-1}gx = g^{\varphi}, \quad g \in M, \\ cx\prod\limits_{i=1}^{n} b_i x^{-1} a_i x = 1 \end{cases} \tag{$***$}$$

разрешима над L, то есть естественное отображение $L \to \langle L, x \mid (***)\rangle$ инъективно.

Воспользовавшись этой теоремой для $L = G^{(m)}$ и $M = G^{(m-1)}$, мы получаем, что естественное отображение $\overline{H} \subset G^{(m)} \to \widetilde{G}$ инъективно и элемент $t \in \widetilde{G}$ трансцендентен над H в силу леммы 6.

8. Доказательство теоремы 4

Нам будет удобно переформулировать теорему 4 на языке уравнений над группами. Напомним, что *уравнением над группой G с неизвестным* (или *переменной*) t называют формальное выражение вида

$$g_1 t^{\varepsilon_1} g_2 t^{\varepsilon_2} \ldots g_n t^{\varepsilon_n} = 1, \tag{8}$$

где $g_i \in G$, $\varepsilon_i \in \mathbb{Z}$. Уравнение (8) называют *разрешимым над группой G*, если найдётся бóльшая группа $\widetilde{G}$, содержащая группу G в качестве подгруппы, и элемент $\widetilde{t} \in \widetilde{G}$ (называемый решением уравнения $(*)$) такой, что $g_1\widetilde{t}^{\varepsilon_1} g_2\widetilde{t}^{\varepsilon_2} \ldots g_n\widetilde{t}^{\varepsilon_n} = 1$ в группе $\widetilde{G}$. Аналогичным образом определяется понятие *разрешимости системы уравнений с несколькими неизвестными над группой G*.

Лемма 7. *Пусть $G = A \underset{C}{*} B$ — свободное произведение некоторых групп A и B с объединённой подгруппой C, $v = b_0 a_0 \ldots b_m a_m b_{m+1} \in G$, φ — автоморфизм группы B и*

$$\widehat{G} = \left\langle A \underset{C}{*} B \;\middle|\; \{b^v = b^{\varphi} \mid b \in B\} \right\rangle.$$

Тогда инъективность естественных отображений $A \to \widehat{G} \leftarrow B$ равносильна разрешимости следующей системы уравнений с неизвестными t и x над группой G:

$$\begin{cases} b^{-x} b^{\varphi} = 1 \quad \text{при } b \in B \setminus \{1\} \\ [t, c] = 1 \quad \text{при } c \in C \setminus \{1\} \\ x^{-1} b_0 a_0^t \ldots b_m a_m^t b_{m+1} = 1. \end{cases} \tag{9}$$

Доказательство. Если $\widetilde{t}, \widetilde{x} \in \widetilde{G} \supseteq G$ — решение системы (9), то отображения $a \mapsto a^{\widetilde{t}}$ и $b \mapsto b$ продолжаются до инъективного на A и на B гомоморфизма $\widehat{G} \to \widetilde{G}$.

Наоборот, если естественные отображения $A \to \widehat{G} \leftarrow B$ инъективны, то рассмотрим изоморфную копию

$$\overline{G} = \left\langle \overline{A} \underset{\overline{C}}{*} \overline{B} \;\middle|\; \{\overline{b}^{\overline{v}} = \overline{b}^{\overline{\varphi}} \mid b \in B\} \right\rangle$$

группы $\widehat{G}$. Непосредственно видно, что элементы $\widetilde{t}$ и $\widetilde{x} = b_0 a_0^{\widetilde{t}} \ldots b_m a_m^{\widetilde{t}} b_{m+1} = \overline{v}$ HNN-расширения

$$\left\langle G \underset{B=\overline{B}}{*} \overline{G}, \widetilde{t} \;\middle|\; \{a^{\widetilde{t}} = \overline{a} \;;\; a \in A\} \right\rangle$$

являются решениями системы (9). Лемма 7 доказана.

Эта лемма показывает, что теорема 4 будет вытекать из следующего утверждения:

Теорема 4′. *Пусть G — некоторая группа, содержащая некоторые подгруппы C, B и B^φ, $\varphi\colon B \to B^\varphi$ — изоморфизм, $m \geqslant 1$, $b_i, a_i \in G$, причём элементы $a_0, \ldots, a_m$ и $b_1, \ldots, b_m$ трансцендентны над C. Тогда система уравнений (9) разрешима над группой G.*

Для доказательства теоремы 4′ нам понадобится лемма Хауи, которую мы здесь излагаем для простоты в частном случае, относящемся к системе уравнений (9).

Пусть на ориентированной двумерной сфере имеется карта, углы которой помечены элементами группы G, а рёбра ориентированы (на рисунках на них имеются стрелки) и помечены переменными t и x.

Метка вершины в такой ситуации определяется как произведение меток всех углов при этой вершине, перечисленных по часовой стрелке. Метка вершины является элементом группы G, определённым с точностью до сопряжённости. Например, метка вершины, изображённой на рисунке 2, равна $a_0^{-1}ca_0^2c'$.

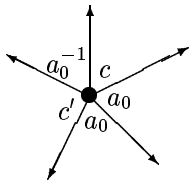


Рис. 2

Чтобы получить *метку грани*, надо обойти её границу против часовой стрелки, выписывая метки всех углов и рёбер этой грани, причём метку ребра надо записывать в минус первой степени, если мы его проходим против стрелки. Метка грани является элементом группы $G * F(t, x)$ (свободного произведения G и свободной группы с базисом $\{t, x\}$), определённым с точностью до циклической перестановки. Например, метка грани, изображённой на рисунке 3 вверху слева, равна $b^{-x}b^\varphi$.

Размеченную таким образом карту мы называем *сферической диаграммой Хауи* (или просто *диаграммой*) над системой уравнений (9), если

1) одна из вершин выделена и называется *внешней*, остальные вершины называются *внутренними*;
2) метка каждой внутренней вершины равна единице в группе G;
3) метка каждой грани равна левой части одного из уравнений системы (9) или слову, обратному к левой части одного из уравнений системы (9); все возможные типы граней изображёны на рисунке 3, на котором буквы b и c означают произвольные неединичные элементы групп B и C соответственно, а рёбра, не помеченные буквой x, считаются помеченными буквой t (на числа, написанные с внешних сторон клеток, пока не следует обращать внимание).

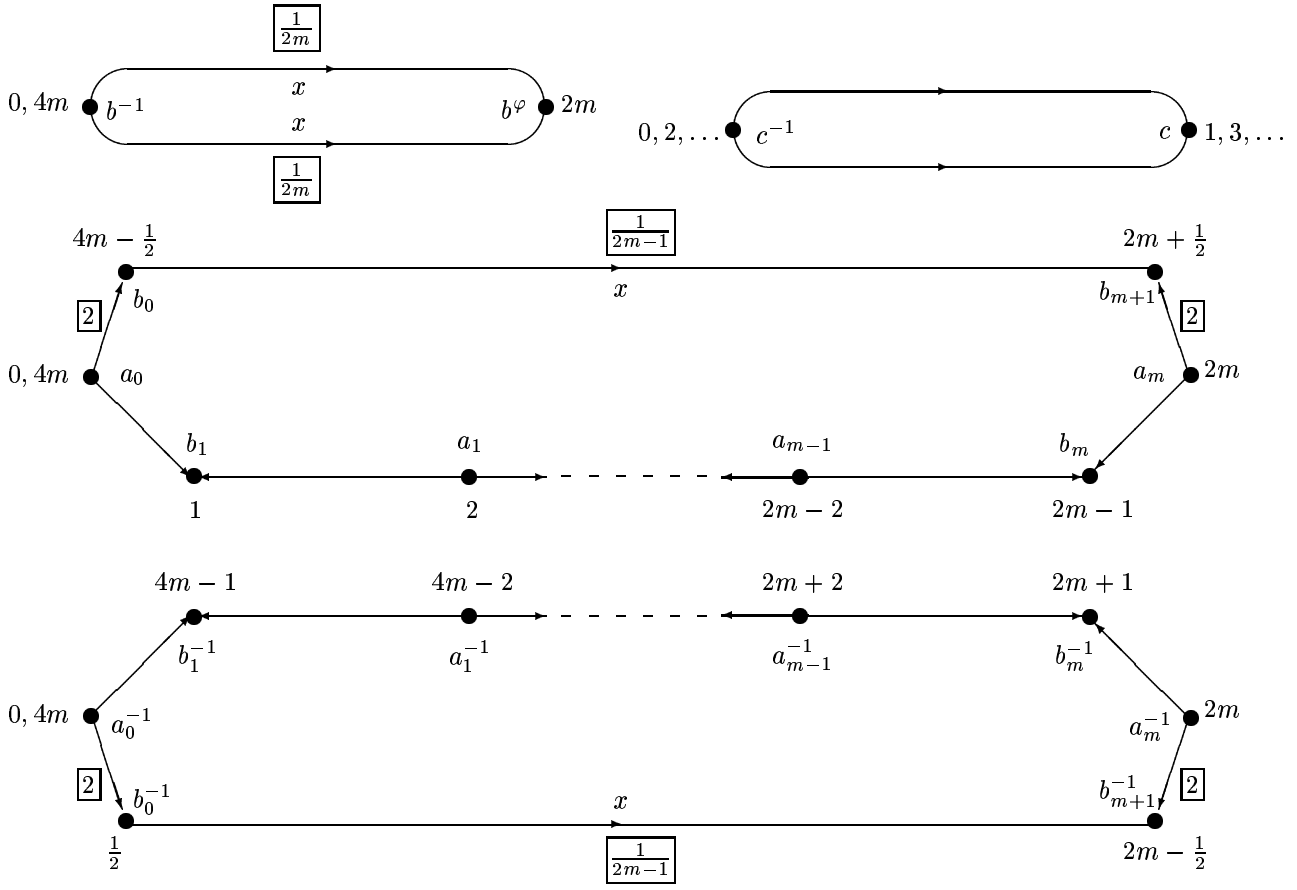


Рис. 3

Диаграмма Хауи называется *приведённой*, если она не содержит такого ребра e, что две грани, его содержащие являются различными, а их метки, написанные начиная с ребра e, взаимнообратны; такая пара клеток с общим ребром называется *сократимой парой*.

Лемма 8 [How83]. *Система уравнений (9) не является разрешимой над группой G тогда и только тогда, когда существует сферическая диаграмма над этой системой, метка внешней вершины которой не равна единице в группе G. Минимальная (по числу клеток) из таких диаграмм является приведённой.*

Назовём диаграмму над системой (9) *сильно приведённой* если она приведена и различные клетки с метками вида $b^{-x}b^{\varphi}$ или $[c, t]$ не имеют общих рёбер.

Лемма 9. *Минимальная (по числу клеток) из всех сферических диаграмм, метка внешней вершины которой не равна единице, является сильно приведённой.*

Доказательство. Действительно, если в какой-то диаграмме пара клеток с метками, например, $b^{-x}b^{\varphi}$ и $(b')^{-x}(b')^{\varphi}$ имеет общее ребро, то либо такая пара клеток есть сократимая пара, либо общее ребро можно стереть, перемножив метки сливающихся при этом углов (рис. 4) и получить диаграмму с меньшим числом клеток и такой же меткой внешней вершины, что означает неминимальность исходной диаграммы и доказывает лемму.

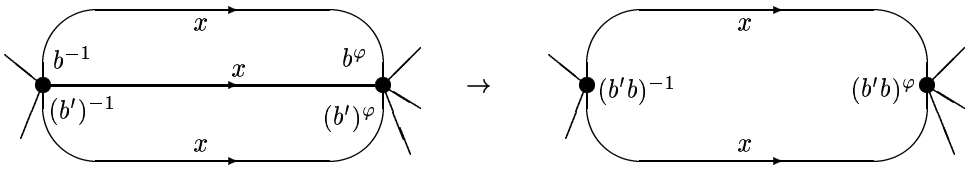


Рис. 4

Представим себе теперь, что по контуру каждой грани D некоторой карты на сфере движется точка (*автомобиль*) α_D. Автомобиль α_D движется непрерывно против часовой стрелки (то есть оставляя внутренность грани D слева) без остановок, разворотов и «бесконечных замедлений», то есть проезжая каждое ребро за конечное время. Такое движение автомобилей мы называем *правильным*.

Если число автомобилей, оказавшихся в момент времени τ в точке p сферы равно кратности этой точки (иными словами, либо во внутренней точке некоторого ребра в момент τ оказываются два автомобиля, либо в вершине кратности k в момент τ оказываются k автомобилей одновременно), то мы говорим, что в точке p в момент τ происходит *полное столкновение*. При этом точка p называется *точкой полного столкновения*. На рисунке 5 изображены полные столкновения на ребре и в вершине кратности три.

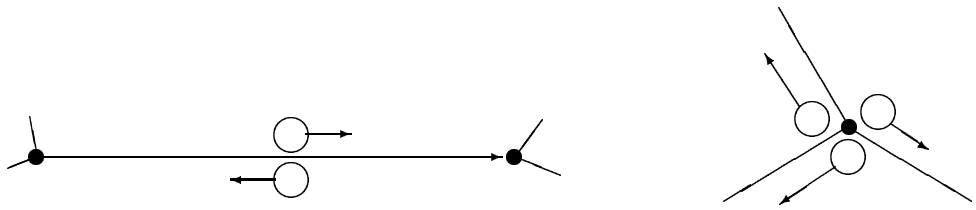


Рис. 5

Лемма 10 [K93] (см. также [FeR96]). *При любом правильном движении на сфере по крайней мере в двух точках происходит полное столкновение.*

Возьмём теперь в качестве карты сферическую диаграмму над копредставлением (9). Рассмотрим следующее правильное движение на этой карте:

а) автомобиль, объезжающий грань с меткой $b^{-x}b^{\varphi}$, движется против часовой стрелки равномерно со скоростью $\frac{1}{2m}$ ребра в единицу времени, проезжая в нулевой момент времени угол с меткой b^{-1};

б) автомобиль, объезжающий грань с меткой $[t,c]$, движется против часовой стрелки равномерно с единичной скоростью (одно ребро в единицу времени), проезжая в нулевой момент времени угол с меткой c^{-1};

в) автомобиль, объезжающий против часовой стрелки грань с меткой $x^{-1}b_0a_0^t\dots b_ma_m^tb_{m+1}$, в нулевой момент времени находится в углу с меткой a_0, далее проезжает $2m$ ребер с меткой t с единичной скоростью и оказывается в момент $2m$ в углу с меткой a_m, следующее ребро с меткой t проезжает со скоростью 2, следующее за ним ребро с меткой x проезжает со скоростью $\frac{1}{2m-1}$, после чего проезжает ребро с меткой t со скоростью 2 и оказывается в момент $4m$ в исходном углу с меткой a_0; далее всё повторяется с периодом $4m$;

г) автомобиль, объезжающий против часовой стрелки грань с меткой $(x^{-1}b_0a_0^t\dots b_ma_m^tb_{m+1})^{-1}$, в нулевой момент времени находится в углу с меткой a_0^{-1}, первое ребро с меткой t проезжает со скоростью 2, следующее за ним ребро с меткой x проезжает со скоростью $\frac{1}{2m-1}$, после чего проезжает ребро с меткой t со скоростью 2, оказывается в момент $2m$ в углу с меткой a_m^{-1}, следующие $2m$ ребер с меткой t проезжает с единичной скоростью и оказывается в момент $4m$ в исходном углу с меткой a_0^{-1}; далее всё повторяется с периодом $4m$.

Это движение является правильным и периодическим с периодом $4m$ (при этом на гранях с меткой $[t,c]$ минимальный период равен двум). На рисунке 3 показано подробное расписание движения на протяжении интервала времени $0 \leqslant \tau \leqslant 4m$, числа в рамочках около рёбер означают скорость автомобиля на этих рёбрах (по умолчанию скорость единичная).

Лемма 11. *При описанном режиме движения на сильно приведённой диаграмме над системой (9) полные столкновения могут происходить только во внешней вершине.*

Доказательство.

Столкновение на ребре с меткой t в момент времени τ означает, что в этот момент направление движения одного из автомобилей совпадает с направлением ребра, а направление движения другого автомобиля противоположно направлению ребра (рис. 5 слева). Но расписание рассматриваемого движения устроено таким образом, что в каждый момент времени τ либо все автомобили, находящиеся на рёбрах с меткой t, едут в направлении ребра (это происходит, когда целая часть τ чётна), либо все автомобили, находящиеся на рёбрах с меткой t, едут в направлении, противоположном направлению ребра (это происходит, когда целая часть τ нечётна).

По аналогичным причинам не может произойти столкновения на ребре с меткой x: на протяжении интервалов времени $[0, 2m] + 4m\mathbb{Z}$ все автомобили, находящиеся на рёбрах с меткой x, едут в направлении ребра, а на протяжении интервалов времени $[2m, 4m] + 4m\mathbb{Z}$ все автомобили, находящиеся на рёбрах с меткой x, едут в направлении, противоположном направлению ребра.

Таким образом, столкновения могут происходить только в вершинах.

Полные столкновения в вершинах, в которых начинается или кончается ребро с меткой x, произойти не могут, поскольку из сильной приведённости диаграммы следует, что каждое ребро с меткой x разделяет клетку с меткой $b^{-x}b^{\varphi}$ и клетку с меткой $(x^{-1}b_0a_0^t \dots b_m a_m^t b_{m+1})^{\pm 1}$ (рис. 6). Это значит, что в начале ребра с меткой x один из автомобилей бывает в моменты $4m\mathbb{Z}$, а другой — в моменты $4m\mathbb{Z} \pm \frac{1}{2}$, то есть полного столкновения не происходит. По аналогичным причинам полного столкновения не происходит в конце ребра с меткой x: один из автомобилей там бывает в моменты $4m\mathbb{Z} + 2m$, а другой — в моменты $4m\mathbb{Z} + 2m \pm \frac{1}{2}$.

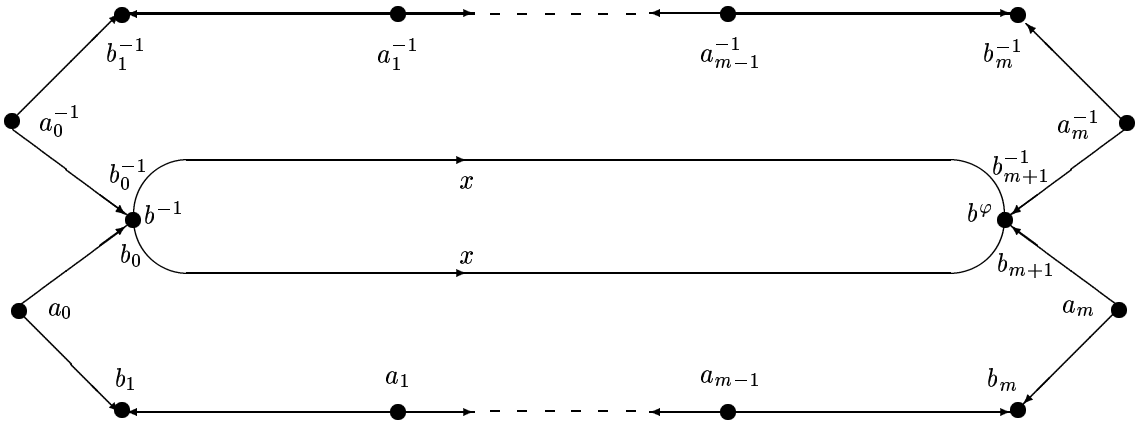


Рис. 6

Полные столкновения во внутренних вершинах, не являющихся началом или концом ребра с меткой x, также происходить не могут. В таких вершинах автомобили появляются только в целые моменты времени τ, причём в каждый такой момент времени τ каждый автомобиль, находящийся в такой вершине, проезжает либо угол с меткой $c \in C \setminus \{1\}$, либо угол с меткой $d \in \{a_0^{\pm 1}, b_1^{\pm 1}, \dots, b_m^{\pm 1}, a_m^{\pm 1}\}$. Причём если один из автомобилей проезжает в момент τ угол с меткой d и одновременно другой автомобиль проезжает угол с меткой d', где $d, d' \in \{a_0^{\pm 1}, b_1^{\pm 1}, \dots, b_m^{\pm 1}, a_m^{\pm 1}\}$, то либо $d' = d$, либо $d' = d^{-1}$.*) Это означает, что метка вершины, в которой в момент τ происходит полное столкновение, имеет вид $\prod z_i$, где $z_i \in \{d, d^{-1}\} \cup C \setminus \{1\}$, причём в силу приведённости диаграммы d и d^{-1} не могут быть соседними в последовательности (z_i), а в силу сильной приведённости диаграммы два элемента из $C \setminus \{1\}$ не могут быть соседними в этой последовательности. Значит, метка $\prod z_i$ вершины полного столкновения не может быть единицей группы G в силу трансцендентности элемента d над группой C. Следовательно, вершина полного столкновения не может быть внутренней вершиной диаграммы. На рисунке 2 показана гипотетическая вершина, в которой происходит полное столкновение в момент $\tau = 0$. Эта вершина не может быть внутренней, поскольку $a_0^{-1}ca_0^2c' \neq 1$ в группе G. Лемма 11 доказана.

Теорема $4'$ легко следует из всего сказанного. Действительно, предположим, что система (9) неразрешима. Тогда по лемме 8 существует диаграмма над этой системой. По лемме 9 эту диаграмму можно считать сильно приведённой. По лемме 11 на этой диаграмме можно задать правильное движение с не более чем одной точкой полного столкновения, что противоречит лемме 10. Тем самым теоремы $4'$ и 4 доказаны.

*) Последний случай возможен лишь при $\tau \in \{0, 2m\} + 4m\mathbb{Z}$, при этом $d = a_0^{\pm 1}$ или $d = a_m^{\pm 1}$. Это позволяет несколько ослабить условия теорем 4 и $4'$, но мы не будем здесь этим заниматься.

ГЛАВА 25.
СТРОЕНИЕ ОТНОСИТЕЛЬНЫХ КОПРЕДСТАВЛЕНИЙ С ОДНИМ СООТНОШЕНИЕМ И ИХ ЦЕНТРЫ

0. Введение

Пусть G — некоторая группа. Под группой, заданной *относительным копредставлением с одним соотношением над группой* G, понимается группа

$$\widehat{G} = \langle G, x_1, x_2, \ldots, x_n \,|\, w = 1 \rangle \stackrel{\text{опр}}{=} G * F(x_1, x_2, \ldots, x_n) / \langle\langle w \rangle\rangle .$$

Здесь $x_1, \ldots, x_n$ — буквы (не лежащие в G) и w — произвольное слово в алфавите $G \cup \{x_1^{\pm 1}, \ldots, x_n^{\pm 1}\}$ (которое можно трактовать как элемент свободного произведения $G * F(x_1, x_2, \ldots, x_n)$ группы G и свободной группы с базисом $x_1, x_2, \ldots, x_n$). Другими словами, копредставление группы $\widehat{G}$ получается из копредставления $G = \langle A \,|\, R \rangle$ группы G добавлением нескольких новых образующих и одного соотношения: $\widehat{G} = \langle A \cup \{x_1, x_2, \ldots, x_n\} \,|\, R \cup \{w\} \rangle$.

Такие группы $\widehat{G}$ являются естественным обобщением групп с одним соотношением и их изучению посвящено множество работ (см., например, [How87], [BoP92], [DuH93], [Met01], [K06b] и литературу цитируемую там). Чтобы получить содержательные результаты приходится накладывать те или иные ограничения на группу G и/или на соотношение w. В этой работе мы накладываем только два ограничения:

(a) группа G не имеет кручения;

(b) слово $w \in G * F(x_1, x_2, \ldots)$ таково, что слово $w' \in F(x_1, x_2, \ldots)$, получающееся из w стиранием коэффициентов, лежащих в G, не является истинной степенью*) в свободной группе $F(x_1, x_2, \ldots)$.

Та же самая ситуация рассматривалась в работах [K06a], [K06b] и [K07], а также в [K93], [FeR96], [CR01], [K05] и [FoR05] в случае $n = 1$.

Центральный результат настоящей работы (теорема 3) показывает, как свести изучение групп $\widehat{G}$ к случаю $n = 1$. Оказывается, что «n-мерная» группа $\widehat{G}$ может быть построена из аналогичных «одномерных» групп при помощи явной конструкции, включающей в себя *итерированные свободные произведения с объединённой подгруппой* (см. раздел 3) и *полупрямые произведения с объединённой подгруппой* (см. раздел 4).

Вероятно, эта структурная теорема (теорема 3) может иметь много приложений, одно из которых мы рассматриваем здесь. А именно, мы изучаем центры групп $\widehat{G}$.

Сначала мы рассматриваем случай $n = 1$, то есть следующую ситуацию. Пусть G — группа без кручения и группа $\widetilde{G}$ получается из группы G добавлением одного образующего и одного *унимодулярного* соотношения, то есть соотношения с единичной суммой показателей при новом образующем:

$$\widetilde{G} = \langle G, t \mid w = 1 \rangle \stackrel{\text{опр}}{=} (G * \langle t \rangle_\infty) / \langle\langle w \rangle\rangle \text{, где } w \equiv g_1 t^{\varepsilon_1} \ldots g_q t^{\varepsilon_q}, \quad g_i \in G, \;\; \varepsilon_i \in \mathbb{Z} \;\; \text{и} \;\; \sum \varepsilon_i = 1.$$

В этом случае, мы говорим, что группа $\widetilde{G}$ задана *унимодулярным относительным копредставлением над группой* G. Известно, что в такой ситуации $\widetilde{G}$ наследует некоторые свойства исходной группы G. В частности:

- абелизации этих групп изоморфны: $G/[G,G] \simeq \widetilde{G}/[\widetilde{G},\widetilde{G}]$;
- группа G вкладывается (естественным образом) в группу $\widetilde{G}$ [K93] (см. также [FeR96]); следовательно, $\widetilde{G}$ нетривиальна, если G нетривиальна, $\widetilde{G}$ неабелева, если G неабелева и т.п.*)
- группа $\widetilde{G}$ (также как и G) не имеет кручения [FoR05];
- группа $\widetilde{G}$ непроста, если G непроста [K05];
- группа $\widetilde{G}$ удовлетворяет альтернативе Титса (то есть либо содержит неабелеву свободную подгруппу, либо является почти разрешимой), если группа G удовлетворяет этой альтернативе [K07].

В этой главе мы устанавливаем ещё одно свойство такого рода:

- центр группы $\widetilde{G}$ либо тривиален, либо изоморфен центру исходной группы G.

Более точно, мы доказываем следующий факт:

---

*) Элемент h группы H мы называем *истинной степенью*, если $h = (h')^k$ для некоторого $h' \in H$ и некоторого целого $k \geqslant 2$. В частности, единица является истинной степенью: $1 = 1^2$.

*) Однако, естественное отображение $G \to \widetilde{G}$ никогда не бывает сюръективным, за исключением случая когда $w \equiv gt$ [CR01].

Теорема 1. *Если группа G не имеет кручения, а слово $w \in G * \langle t \rangle_\infty$ унимодулярно, то центр группы $\widetilde{G} = \langle G, t \mid w = 1 \rangle$ тривиален, за исключением следующих двух случаев:*

1) *$w \equiv gtg'$, где $g, g' \in G$ (при этом $\widetilde{G} \simeq G$), и центр группы G нетривиален;*
2) *G — циклическая группа, и $\widetilde{G}$ — группа с одним соотношением и с нетривиальным центром.*

Группы с одним соотношением, имеющие нетривиальный центр, хорошо изучены ([Mu64], [BaTa68], [Pi74]). Центр каждой такой группы является бесконечной циклической подгруппой (за исключением случая, когда вся группа является свободной абелевой ранга 2, что невозможно нашей ситуации). Простейшим неочевидным примером унимодулярного копредставления с нетривиальным центром является группа кос на трёх нитях $\widetilde{G} = B_3 = \langle g, t \mid gtg = tgt \rangle$, центр которой порождён элементом $(gt)^3$.

В общем случае вычисление чего бы то ни было в группе $\widetilde{G}$ является трудной задачей, поскольку в этой группе не решена (пока) проблема равенства. Например, естественный способ нахождения центра по формуле

$$\text{центр } \widetilde{G} = (\text{централизатор } G) \cap (\text{централизатор } t)$$

не срабатывает — мы не можем вычислить ни одного из этих централизаторов и для вычисления центра приходится использовать некоторый обходной манёвр. На самом деле, доказательство теоремы 1 недлинное (см. раздел 2), однако оно сильно опирается на результаты работы [K05]. Необходимые геометрические понятия мы объясняем в разделе 1.

Далее мы переходим к «многомерному» случаю. На самом деле, мы рассматриваем даже более общую ситуацию. В статье [K06a] было предложено обобщение понятия унимодулярности на случай когда слово w является элементом свободного произведения группы G и произвольной (то есть не обязательно циклической) группы T. В настоящей работе нам понадобиться ещё более общее определение. Слово $w \equiv g_1 t_1 \dots g_q t_q \in G * T$ мы будем называть *обобщённо унимодулярным*, если

1) $\prod t_i \neq 1$, и группа T не имеет кручения;
2) циклическая подгруппа $\langle \prod t_i \rangle$ группы T выделяется свободным сомножителем в некоторой нормальной подгруппе $R = \langle \prod t_i \rangle * S$ группы T;
3) факторгруппа T/R является группой с сильно однозначным умножением.

Напомним, что группа H называется *группой с однозначным умножением* (или *UP-группой*), если для любых двух её конечных непустых подмножеств $X, Y \subseteq H$ их произведение XY содержит по крайней мере один элемент, раскладывающийся в произведение элемента из X и элемента из Y однозначно. Одно время была гипотеза, что всякая группа без кручения является группой с однозначным умножением (обратное, очевидно, верно). Однако выяснилось, что существует контрпример ([P88], [RS87]).

Мы называем группу H *группой с сильно однозначным умножением*, если для любых двух её конечных непустых подмножеств $X, Y \subseteq H$ таких, что $|Y| \geqslant 2$, их произведение XY содержит по крайней мере два однозначно разложимых элемента $x_1 y_1$ и $x_2 y_2$ таких, что $x_1, x_2 \in X$, $y_1, y_2 \in Y$ и $y_1 \neq y_2$.

Насколько мы знаем, все известные примеры UP-групп обладают сильно однозначным умножением. Например, этим свойством обладают все правоупорядочиваемые группы, локально индикабельные группы, диффузные группы в смысле Бовдича.

Основным примером обобщённо унимодулярных копредставлений являются группы вида

$$\widehat{G} = \langle G, x_1, x_2, \dots, x_n \mid w = 1 \rangle,$$

где слово $w \in G * F(x_1, x_2, \dots)$ таково, что слово $w' \in F(x_1, x_2, \dots)$, получающееся из w стиранием коэффициентов, лежащих в G, не является истинной степенью в свободной группе $F(x_1, x_2, \dots)$.

Действительно, пусть слово w имеет вид $w \equiv g_1 x_{j_1}^{\varepsilon_1} g_2 x_{j_2}^{\varepsilon_2} \dots g_q x_{j_q}^{\varepsilon_q}$ и слово $w' \in F(x_1, \dots, x_n)$ получается из w стиранием коэффициентов: $w' = x_{j_1}^{\varepsilon_1} x_{j_2}^{\varepsilon_2} \dots x_{j_q}^{\varepsilon_q}$. Рассмотрим группы

$$T = F(x_1, \dots, x_n) \quad \text{и} \quad T_1 = \langle x_1, \dots, x_n \mid w' = 1 \rangle = T / \langle\langle w' \rangle\rangle .$$

По теореме Бродского [Б84], если w' не является истинной степенью в свободной группе $F(x_1, \dots, x_n)$, то группа T_1 является локально индикабельной и, следовательно, группой с сильно однозначным умножением. По теореме Коэна–Линдона [CoLy63] элемент w' является примитивным элементом свободной подгруппы $\langle\langle w' \rangle\rangle$ группы T. Таким образом, слово w, рассматриваемое как элемент свободного произведения $G * T$, является обобщённо унимодулярным.

В разделе 5 мы доказываем наш основной результат, теорему 3. В качестве следствия этой теоремы о строении в разделе 6 мы получаем следующий факт, обобщающий теорему 1.

Теорема 2. *Пусть G и T — группы без кручения и циклически несократимое слово $w = g_1 t_1 \dots g_q t_q \in G * T$ обобщённо унимодулярно. Тогда*

1) *естественное отображение $G \to \widehat{G} = \langle G, T \mid w = 1\rangle \overset{\text{опр}}{=} (G * T)/\langle\langle w\rangle\rangle$ инъективно;*
2) *если центр группы $\widehat{G}$ нетривиален и группа G нециклическая, то $q = 1$ и либо $t_1 \in Z(T)$ и $\langle g_1\rangle \cap Z(G) \neq 1$* (в этом случае группа $\widehat{G} = G \underset{g_1 = t_1^{-1}}{*} T$ является свободным произведением групп G и T с объединённой циклической подгруппой), *либо группа T является циклической* (в этом случае $T = \langle t_1\rangle$ и $\widehat{G} \simeq G$).

Из этой теоремы легко выводится многомерный аналог теоремы 1:

Следствие 1. *Пусть G — нетривиальная группа без кручения и слово $w \in G * F(x_1, x_2, \dots)$ таково, что слово $w' \in F(x_1, x_2, \dots)$, получающееся из w стиранием коэффициентов, лежащих в G, не является истинной степенью в свободной группе $F(x_1, x_2, \dots)$. Тогда*

1) [K06a] *естественное отображение $G \to \widehat{G} = \langle G, x_1, x_2, \dots, x_n \mid w = 1\rangle$ инъективно;*
2) *если $n \geqslant 2$, то центр группы $\widehat{G}$ тривиален.*

Доказательство. В случае если группа G нециклическая, доказываемое утверждение вытекает из теоремы 2. Если же группа G циклическая, то группа $\widehat{G}$ является группой с одним соотношением и по меньшей мере тремя образующими; тривиальность центра таких групп давно известна [Mu64].

Полученные факты о центре группы $\widehat{G}$ не является, конечно, удивительными. Однако, из них легко выводится гипотеза Кервера–Лауденбаха для групп без кручения [K93], то есть нетривиальность всех групп вида

$$\langle H, t \mid w = 1\rangle\,, \text{ где } H \text{ – нетривиальная группа без кручения, а } w \text{ – произвольное слово в алфавите } H \cup \{t^{\pm 1}\}.$$

Действительно, если группа $\widetilde{H} = \langle H, t \mid w = 1\rangle$ тривиальна, то слово w обязано быть унимодулярным (иначе $\widetilde{H}$ допускает эпиморфизм на нетривиальную циклическую группу). Значит группа $\widehat{H} = \langle H, t, x \mid w = 1\rangle = \widetilde{H} * \langle x\rangle_\infty$ имеет тривиальный центр. Это можно вывести и из теоремы 1 (полагая $G = H * \langle x\rangle_\infty$), и из следствия 1(2) (полагая $G = H$). Тривиальность центра группы $\widehat{H}$ очевидным образом влечёт нетривиальность группы группы $\widetilde{H}$. Таким образом, и теорему 1, и следствие 1(2) можно рассматривать, как усиление основного результата работы [K93].

В работах [Б81] и [Met01] можно найти другие теоремы о центрах относительных копредставлений с одним соотношением. Ещё одно свойство «сильной неабелевости» относительных копредставлений доказано в работе [K06b]: если G — нетривиальная группа без кручения и $n \geqslant 2$, то группа $\langle G, x_1, x_2, \dots, x_n \mid w = 1\rangle$ всегда SQ-универсальна.

Обозначения, которые мы используем, в целом стандартны. Отметим только, что если $k \in \mathbb{Z}$, x и y — элементы некоторой группы, а φ — гомоморфизм из этой группы в какую-нибудь другую группу, то x^y, x^{ky}, x^{-y}, x^φ, $x^{k\varphi}$ и $x^{-\varphi}$ обозначают $y^{-1}xy$, $y^{-1}x^k y$, $y^{-1}x^{-1}y$, $\varphi(x)$, $\varphi(x^k)$ и $\varphi(x^{-1})$ соответственно; коммутатор $[x, y]$ понимается как $x^{-1}y^{-1}xy$. Если X — подмножество некоторой группы, то $\langle X\rangle$, $\langle\langle X\rangle\rangle$ и $C(X)$ означают, соответственно, подгруппу, порождённую множеством X, нормальную подгруппу, порождённую множеством X, и централизатор множества X. Центр группы G обозначается символом $Z(G)$. Символом $|X|$ мы обозначаем мощность множества X. Буквы $\mathbb{Z}$ и $\mathbb{N}$ обозначают множество целых и множество натуральных чисел, соответственно.

1. Диаграммы Хауи

В этом разделе мы напоминаем (следуя [K05]) некоторые факты о диаграммах, введённых в [How83]. Единственным новым результатом этого раздела является лемма 3.

Под поверхностью в этой главе мы всегда понимаем замкнутую двумерную ориентированную поверхность.

Картой M на поверхности S называется конечный набор непрерывных отображений $\{\mu_i\colon D_i \to S\}$, где D_i — двумерный замкнутый ориентированный диск (круг), называемый i-й *гранью* или *клеткой* карты, на границе которого отмечено некоторое конечное непустое множество точек $c_{ij} \in \partial D_i$, называемых *углами* карты. Интервалы e_{ij}, на которые углы делят границу грани, мы называем *прорёбрами* карты. Образы углов $\mu_i(c_{ij})$ и прорёбер $\mu_i(e_{ij})$ называют *вершинами* и *рёбрами* карты соответственно. При этом предполагается, что

1) ограничения отображения μ_i на внутренность грани D_i является гомеоморфным вложением, сохраняющим ориентацию; ограничение μ_i на каждое проребро является гомеоморфным вложением;
2) различные ребра не пересекаются;
3) образы внутренностей разных граней не пересекаются;
4) $\bigcup \mu_i(D_i) = S$.

Карту M мы будем также иногда трактовать как непрерывное отображение $\mathrm{M}\colon \coprod D_i \to S$ из дискретного объединения дисков в поверхность.

Объединение всех вершин и рёбер карты представляет собой граф на поверхности, называемый *одномерным остовом*.

Мы говорим, что угол c является углом при вершине v, если $\mathrm{M}(c) = v$. На множестве всех углов при вершине v имеется естественный циклический порядок; мы называем два угла при вершине v *смежными*, если они являются соседними относительно этого порядка.

Допуская некоторую вольность речи, мы говорим, что точка или подмножество поверхности содержится в грани D_i, если она (оно) лежит в образе μ_i. Аналогично, мы говорим, что грань D_i содержится в некотором подмножестве $X \subseteq S$ поверхности S, если $\mathrm{M}(D_i) \subseteq X$.

На рисунке 1 представлена карта на сфере с пятью гранями: A, B, C, D и E, восемнадцатью углами: a_i, b_i, c_i, d_i и e_i, шестью вершинами, девятью рёбрами и восемнадцатью прорёбрами. Заметим, что число углов всегда равно числу прорёбер и вдвое больше числа рёбер, а величина

$$e(S) \stackrel{\text{опр}}{=} (\textit{число вершин}) - (\textit{число ребер}) + (\textit{число граней})$$

не зависит от выбора карты на поверхности S и называется *эйлеровой характеристикой* этой поверхности. Эйлерова характеристика сферы (единственной поверхности, которая нас на самом деле интересует в этой главе) равна двум.

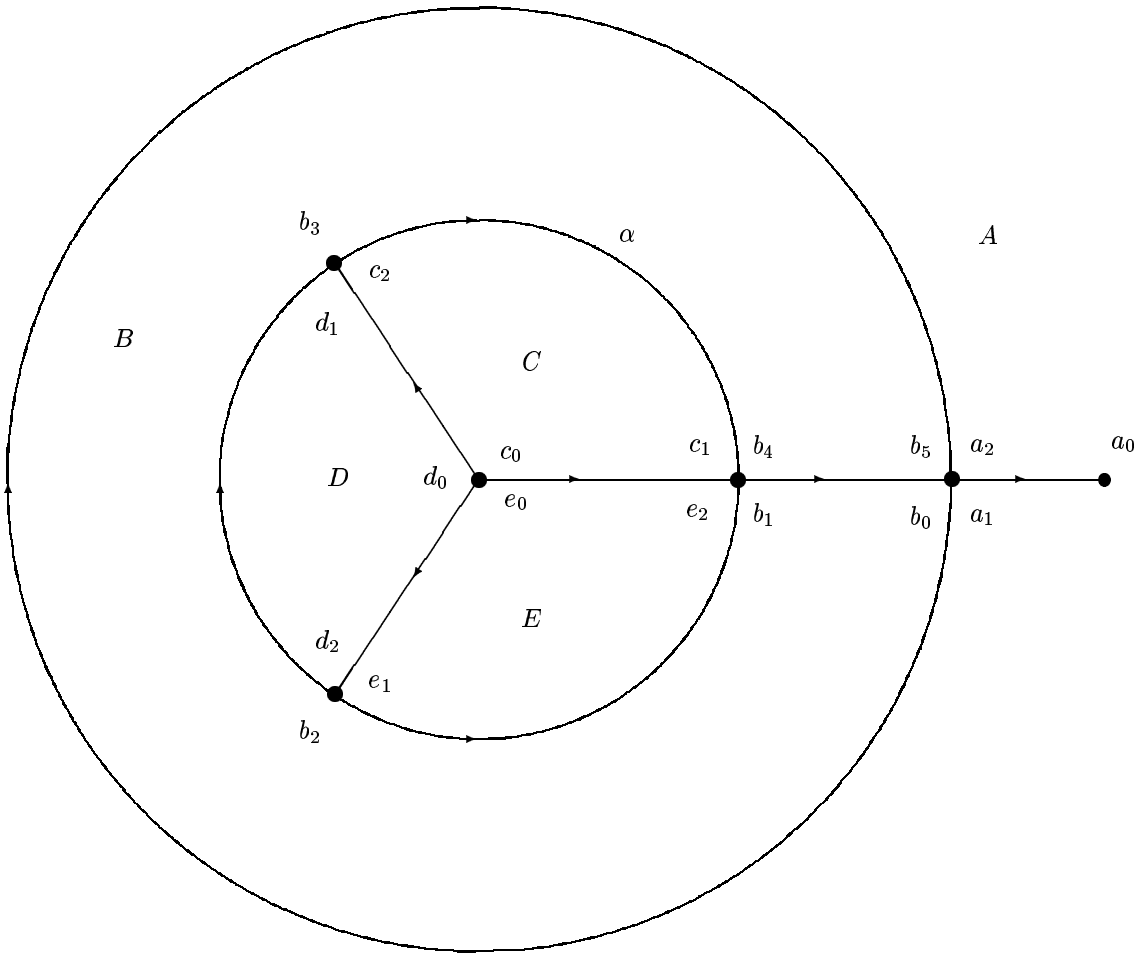


Рис. 1

Пусть имеется карта M на поверхности S, углы которой помечены элементами некоторой группы H, а рёбра ориентированны (на рисунках на них имеются стрелки) и помечены элементами некоторого множества $\{t_1, t_2, \ldots\}$, не пересекающегося с группой H. Метку угла или ребра x будем обозначать $\lambda(x)$.

Метка вершины v в такой ситуации определяется формулой

$$\lambda(v) = \prod_{i=1}^{k} \lambda(c_i),$$

где $c_1, \ldots, c_k$ — это все углы при вершине v, перечисленные по часовой стрелке. Метка вершины является элементом группы H, определённым с точностью до сопряжённости.

Например, метка самой верхней вершины на рисунке 1 есть $\lambda(b_3)\lambda(c_2)\lambda(d_1)$.

Метка грани D определяется формулой

$$\lambda(D) = \prod_{i=1}^{k} \big(\lambda(\mathrm{M}(e_i))\big)^{\varepsilon_i} \lambda(c_i),$$

где $e_1, \ldots, e_k$ и $c_1, \ldots, c_k$ — это все прорёбра и все углы грани D, перечисленные против часовой стрелки, причём концами проребра e_i являются углы c_{i-1} и c_i (индексы по модулю k), а $\varepsilon_i = \pm 1$ в зависимости от того, сохраняет или обращает ориентацию гомеоморфизм $e_i \overset{\mathrm{M}}{\to} \mathrm{M}(e_i)$. Говоря по-простому, чтобы получить метку грани, надо обойти её границу против часовой стрелки, выписывая метки всех встречающихся углов и рёбер, причём метку ребра надо записывать в минус первой степени, если мы его проходим против стрелки.

Метка грани является элементом группы $H * F(t_1, t_2, \ldots)$ (свободного произведения H и свободной группы с базисом $\{t_1, t_2, \ldots\}$), определённым с точностью до циклической перестановки. Более точно, правую часть нашей формулы для $\lambda(D)$ мы называем *меткой грани D, написанной начиная с проребра e_1*.

Например, если на рисунке 1 метки всех рёбер равны t, то метка грани B, написанная начиная с проребра α равна

$$t\lambda(b_4)t\lambda(b_5)t^{-1}\lambda(b_0)t^{-1}\lambda(b_1)t^{-1}\lambda(b_2)t\lambda(b_3).$$

Размеченную таким образом карту мы называем *диаграммой Хауи* (или просто *диаграммой*) над относительным копредставлением

$$K = \langle H, t_1, t_2, \ldots \mid w_1 = 1, w_2 = 1, \ldots \rangle, \qquad (*)$$

если

1) некоторые вершины и некоторые грани выделены и называются *внешними*, остальные вершины и грани называются *внутренними*;
2) метка каждой внутренней грани является циклической перестановкой одного из слов $w_i^{\pm 1}$;
3) метка каждой внутренней вершины равна единице в группе H.

Диаграмма Хауи называется *приведённой*, если она не содержит такого ребра e, что две грани, его содержащие, являются внутренними, эти грани различны, а их метки, написанные начиная с M-прообразов ребра e, взаимнообратны; такая пара клеток с общим ребром называется *сократимой парой*. Например, клетки C и E на рисунке 1 образуют сократимую пару, если $\lambda(c_0) = \lambda(e_0)$, $\lambda(c_1) = \lambda(e_2)$, $\lambda(c_2) = \lambda(e_1)$ и метки всех рёбер равны.

Следующая лемма является аналогом леммы ван Кампена для относительных копредставлений.

Лемма 1 [How83]. *Естественное отображение группы H в группу, заданную относительным копредставлением $(*)$, не является инъективным тогда и только тогда, когда существует сферическая диаграмма над этим копредставлением с единственной внешней вершиной и без внешних граней, причём метка внешней вершины не равна единице в группе H. Минимальная (по числу клеток) из таких диаграмм является приведённой.*
Если это естественное отображение инъективно, то имеет место эквивалентность: образ элемента

$$u \in H * F(t_1, t_2, \ldots) \setminus \{1\}$$

равен единице в группе $(*)$ тогда и только тогда, когда существует сферическая диаграмма над этим копредставлением без внешних вершин и с единственной внешней гранью, метка которой равна u. Минимальная (по числу клеток) из таких диаграмм также является приведённой.

Диаграммы на сфере с единственной внешней гранью и без внешних вершин называют также *дисковыми* диаграммами, границу внешней грани такой диаграммы называют *контуром* диаграммы.

Пусть $\varphi: P \to P^\varphi$ — изоморфизм между двумя подгруппами группы H. Относительное копредставление вида

$$\langle H, t \mid \{p^t = p^\varphi;\ p \in P \setminus \{1\}\}, w_1 = 1,\ w_2 = 1,\ \ldots \rangle \qquad (**)$$

назовём *φ-копредставлением*. Диаграмму над φ-копредставлением $(**)$ назовём *φ-приведённой* если она приведена и различные внутренние клетки, метки которых имеют вид $p^t p^{-\varphi}$, $p \in P$, не имеют общих рёбер.

Лемма 2 [K05]. *Минимальная (по числу клеток) из всех сферических диаграмм над данным φ-копредставлением без внешних граней и с единственной внешней вершиной, метка которой не равна единице, является φ-приведённой. Если таких диаграмм не существует, то минимальная дисковая диаграмма с данной меткой контура является φ-приведённой.* Другими словами, имеет место полный φ-аналог леммы 1.

На рисунке 2 показана идея доказательства этой леммы.

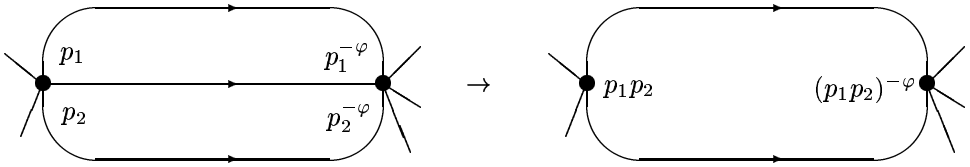


Рис. 2

Относительное копредставление (φ-копредставление), над которым не существует приведённых (соответственно, φ-приведённых) сферических диаграмм с единственной внешней вершиной и без внешних граней, будем называть *асферичными* (соответственно, *φ-асферичными*).

Лемма 3. *Пусть H — группа, слово $v \in H * F(t_1, t_2, \ldots)$ не является истинной степенью в $H * F(t_1, t_2, \ldots)$, а натуральное число l таково, что v^l несопряжено в $H * F(t_1, t_2, \ldots)$ ни с одним из элементов множества $H \cup \{w_i^{\pm 1}\}$ и копредставление*

$$L = \left\langle H, t_1, t_2, \ldots \;\middle|\; v^l = 1, w_1 = 1, w_2 = 1, \ldots \right\rangle,$$

полученное из копредставления $(*)$ добавлением соотношения $v^l = 1$ асферично (или φ-асферично, если исходное копредставление $(*)$ является φ-копредставлением). Тогда

1) *в группе K, заданной копредставлением $(*)$, централизатор элемента v^k совпадает с циклической группой $\langle v \rangle$ при всех натуральных k;*
2) *если группа H нетривиальна, то центр группы K тривиален.*

Доказательство. Первое утверждение доказывается стандартным рассуждением. Во-первых можно считать, что $k = l$, поскольку $C(v^k) \subseteq C(v^{kl})$, а из асферичности копредставления L вытекает асферичность копредставления

$$L_k = \left\langle H, t_1, t_2, \ldots \;\middle|\; v^{kl} = 1, w_1 = 1, w_2 = 1, \ldots \right\rangle$$

при каждом натуральном k (поскольку клетку с меткой w^k можно преобразовать в k клеток с метками w, см. [BoP92]).

Рассмотрим слово u, коммутирующее с v^l в группе K и дисковую диаграмму над копредставлением $(*)$ с меткой контура $[u, v^l]$. Склеим из этой диаграммы кольцо A (добавляя, если надо, клетки, метки которых равны единице в $H * F(t_1, t_2, \ldots)$) метки контуров, которого равны v^l и v^{-l}. Приклеив по этим контурам две новые клетки Γ_+ и Γ_-, мы получим сферическую диаграмму D без внешних вершин и граней над копредставлением L. Эта диаграмма обладает следующими свойствами (рис.3):

а) метка контура грани $\Gamma_\pm$, написанная начиная с некоторой точки $p_\pm \in \partial\Gamma_\pm$ равна $v^{\pm l}$;
б) метки контуров остальных граней лежат в $\{w_i^{\pm 1}\} \cup \{1\}$;
в) точки p_+ и p_- соединены некоторым путём π с меткой u;
г) точка p_+ соединена с некоторой точкой $p'_- \in \partial\Gamma_-$ некоторым путём π', метка которого равна единице в свободном произведении $H * F(t_1, t_2, \ldots)$; при этом метка контура клетки Γ_-, написанная начиная с точки p'_-, имеет вид v^{-l}.

Последнее свойство следует из того, что копредставление L асферично, а в диаграмме D и в диаграммах, которые получаются из неё приведением (уничтожением сократимых пар), клетка Γ_+ может образовать сократимую пару только с клеткой Γ_-.

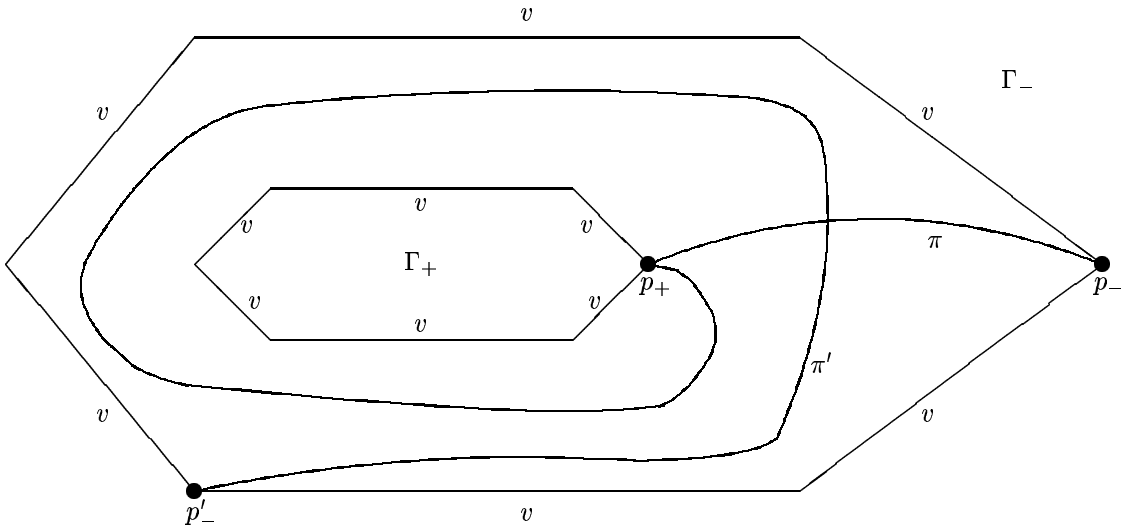


Рис. 3

Из свойств а) и г) и того, что v не является истинной степенью, вытекает, что метка участка σ контура клетки Γ_- между точками p_- и p'_- имеет вид v^i. Осталось заметить, что путь $\pi\sigma$ гомотопен в кольце $A = D \setminus \{\Gamma_\pm\}$ некоторому пути вида $\pi'\delta^j$, где δ — путь с меткой v^{-l} вокруг клетки Γ_-, начинающийся и кончающийся в p'_-. Из этой гомотопности вытекает, что метка u пути π равна в группе K слову v^{-lj-i}, что доказывает первое утверждение леммы.

Докажем второе утверждение. По утверждению 1) центр группы K обязан содержаться в циклической группе $\langle v\rangle$. Применяя ещё раз утверждение 1) к гипотетическому центральному элементу вида v^k, мы получаем, что $K = \langle v\rangle$. Значит, $v^{ks} = h$ для некоторых $s \in \mathbb{N}$ и $h \in H$, что противоречит (φ-)асферичности копредставления L.

2. Доказательство теоремы 1

В работе [K05] показано, что группа $\widetilde{G}$ всегда (кроме некоторых очевидных исключений) задаётся относительным (φ-)копредставлением, которое (φ-)асферично и остаётся таковым при наложении некоторого дополнительного соотношения. В силу леммы 3 это влечёт справедливость теоремы 1. Более точно, доказательство распадается на два случая.

Случай 1: слово w имеет вид $ct\prod_{i=0}^{m}(b_i a_i^t) = 1$, где $c, a_i, b_i \in G$ (то есть сложность слова w не превосходит единицы в терминологии [FoR05]).

Лемма 4 ([K05], лемма 23). *Если G — группа без кручения и $m \geqslant 0$, то найдётся такое $d \in \{2,3\}$, что копредставление*

$$\left\langle G, t \;\middle|\; ct\prod_{i=0}^{m}(b_i a_i^t) = 1,\ (a^{t^d} b)^4 = 1 \right\rangle$$

асферично для любых элементов $a, b \in G$ таких, что $a^2 \notin \langle a_m\rangle$ и $b^2 \notin \langle b_0\rangle$.

Если $G^2 \stackrel{\text{опр}}{=} \{g^2\ ;\ g \in G\} \not\subseteq \langle a_m\rangle$ и $G^2 \not\subseteq \langle b_0\rangle$, то утверждение теоремы 1 вытекает из лемм 3 и 4. Для завершения доказательства осталось сослаться на следующий простой факт, который мы оставляем читателю в качестве упражнения.

Лемма 5. *Если G — группа без кручения и $\langle G^2\rangle$ — циклическая группа, то и сама группа G является циклической.*

Случай 2: слово w не сопряжено слову вида $ct\prod_{i=0}^{m}(b_i a_i^t) = 1$ (то есть сложность слова w больше единицы в терминологии [FoR05]).

В этом случае утверждение теоремы 1 непосредственно вытекает из леммы 3 и следующих двух лемм.

Лемма 6 ([K05], лемма 2; смотрите также [K93], [Fer96]). *Группа $\widetilde{G}$ обладает относительным копредставлением вида*

$$\widetilde{G} \simeq \left\langle H, t \;\middle|\; \{p^t = p^\varphi,\ p \in P \setminus \{1\}\},\ ct\prod_{i=0}^{m}(b_i a_i^t) = 1 \right\rangle, \tag{1}$$

где $a_i, b_i, c \in H$, P и P^φ — изоморфные подгруппы группы H, $\varphi\colon P \to P^\varphi$ — изоморфизм между ними. При этом группы H, P и P^φ являются свободным произведением конечного числа изоморфных копий группы G. Если слово w не сопряжено в $G * \langle t\rangle_\infty$ слову вида $ct\prod_{i=0}^{m}(b_i a_i^t)$, то группы P и P^φ нетривиальны.

Лемма 7 ([K05], лемма 10). *Если G — нециклическая группа без кручения и $P \neq \{1\}$ в копредставлении* (1)*, то существуют такие элементы $a, b \in H$, что копредставление*

$$\widetilde{G}\Big/\Big\langle\Big\langle a^{t^2} b\Big\rangle\Big\rangle \simeq \left\langle H, t \;\middle|\; \{p^t = p^\varphi,\ p \in P \setminus \{1\}\},\ ct\prod_{i=0}^{m}(b_i a_i^t) = 1,\ a^{t^2} b = 1 \right\rangle,$$

полученное из копредставления (1) *добавлением соотношения $a^{t^2} b = 1$, φ-асферично.*

Теорема 1 доказана. Оставшаяся часть главы посвящена изучению обобщённых унимодулярных копредставлений.

3. Свободные итерированные произведения с объединёнными подгруппами

Этот раздел представляет собой расширенный вариант аналогичного раздела работы [K06b].

Пусть $\{M_j\,;\,j\in J\}$ — некоторое семейство групп. Определим группу M_J, *[строгое] свободное итерированное произведение с объединёнными подгруппами (СИПСОП)* групп M_j, индуктивно:

– если $J=\varnothing$, то положим $M_J=\{1\}$;

– если J — конечное непустое множество, то [строгим] СИПСОПом семейства групп $\{M_j\,;\,j\in J\}$ мы называем всякое свободное произведение с объединёнными подгруппами вида

$$M_J = M_{j_0} \underset{H=H^\varphi}{*} M_{J\setminus\{j_0\}},$$

где j_0 — некоторый элемент множества J, $M_{J\setminus\{j_0\}}$ — [строгий] СИПСОП семейства групп $\{M_j\,;\,j\in J\setminus\{j_0\}\}$, а $\varphi: H\to H^\varphi$ — некоторый изоморфизм между [собственной] подгруппой $H\subseteq M_{j_0}$ и некоторой подгруппой $H^\varphi\subseteq M_{J\setminus\{j_0\}}$;

– если множество J бесконечно, то [строгим] СИПСОПом семейства групп $\{M_j\,;\,j\in J\}$ мы называем прямой предел

$$M_J=\lim\{M_K;\ K\text{ — конечное подмножество множества }J\},$$

где M_K — [строгий] СИПСОП семейства групп $\{M_j\,;\,j\in K\}$; причём для каждой пары конечных подмножеств $K\subset K'\subset J$ имеется гомоморфизм $M_K\to M_{K'}$ тождественный на группах M_j, где $j\in K$, и прямой предел берётся относительно этого семейства гомоморфизмов.

Замечание. В определение строгого СИПСОПа мы требуем, чтобы объединяемая подгруппа H была собственной только в одном из сомножителей — в M_{j_0}. Поэтому всякая нетривиальная группа G может быть разложена в строгий СИПСОП: $G=\{1\}*G$ (а тривиальная группа является строгим СИПСОПом пустого семейства групп). Аналогично, если группа G является объединением некоторой строго возрастающей цепочки своих подгрупп, $G=\bigcup G_i$, где $G_1\subset G_2\subset\ldots$, то группа G раскладывается в строгий СИПСОП групп G_i.

Пусть I — некоторое множество и Ω — некоторое семейство подмножеств множества I. Для каждого $i\in I$ рассмотрим некоторую группу G_i, и для каждого $\omega\in\Omega$ рассмотрим некоторую факторгруппу G_ω свободного произведения $\underset{i\in\omega}{*} G_i$:

$$G_\omega=\left(\underset{i\in\omega}{*} G_i\right)\Big/N_\omega.$$

Возникает естественный вопрос: при каких условиях естественные отображения

$$\varphi_\omega\colon G_\omega\to G_I\overset{\text{опр}}{=}\left(\underset{i\in I}{*} G_i\right)\Big/\left\langle\!\!\left\langle\bigcup_{\omega\in\Omega}N_\omega\right\rangle\!\!\right\rangle$$

инъективны? Или, при каких условиях группа G_I является свободным итерированным произведением с объединёнными подгруппами групп G_ω?

Следующее утверждение даёт некоторые достаточные условия для положительного ответа на эти вопросы.

Утверждение 1. *Пусть*

$$N_\omega\cap\left(\underset{j\in\omega\setminus\{i\}}{*} G_j\right)=\{1\}\qquad(***)$$

для каждого $\omega\in\Omega$ и каждого $i\in\omega\setminus(\bigcap\Omega)$. Допустим, что, кроме того, для каждого конечного подсемейства $F\subseteq\Omega$ такого, что $|F|\geqslant 2$, найдутся такие элементы $\min,\max\in\bigcup F$, *что*

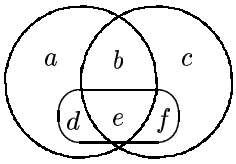
1) *элемент* min *содержится ровно в одном множестве $\omega_{\min}\in F$;*
2) *элемент* max *содержится ровно в одном множестве $\omega_{\max}\in F$;*
3) $\omega_{\min}\neq\omega_{\max}$.

Тогда все естественные отображения $\varphi_\omega\colon G_\omega\to G_I$ инъективны и группа G_I является итерированным свободным произведением с объединёнными подгруппами групп G_ω. Если, кроме того,

$$\left(\underset{j\in\omega\setminus\{i\}}{*} G_j\right)N_\omega\not\supseteq G_i$$

для каждого $\omega \in \Omega$ и каждого $i \in \omega \setminus (\bigcap \Omega)$, то свободное итерированное произведение с объединёнными подгруппами является строгим.

Пример. Пусть $I = \{a, b, c, d, e, f\}$ и $\Omega = \{\{a, b, d, e\}, \{b, c, e, f\}, \{d, e, f\}\}$.



Соответствующие шесть групп G_i мы обозначим $A, \ldots, F$, а три группы G_ω мы обозначим **ABDE**, **BCEF** и **DEF**. Нетрудно убедиться, что в данном случае условия 1), 2) и 3) выполнены для семейства Ω и каждого его подсемейства, состоящего из двух множеств. Допустим, что выполнено также условие (***). Тогда справедливость утверждения 1 (в данном случае) вытекает из следующего разложения группы G_I в свободное произведение с объединёнными подгруппами:

$$G_I = \Big((\mathbf{DEF} * B) \underset{B*D*E}{*} \mathbf{ABDE} \Big) \underset{B*E*F}{*} \mathbf{BCEF}.$$

Для доказательства утверждения в общем случае докажем сперва лемму.

Лемма 8 ([K06b] лемма 1). *Пусть выполнены условия утверждения 1, Ω' — конечное подсемейство семейства Ω, $\omega \in \Omega$ и $\alpha \subseteq \omega \cap (\bigcup \Omega')$ — некоторое собственное подмножество множества ω, лежащее в $\bigcup \Omega'$ и содержащее $\bigcap \Omega$. Тогда естественное отображение*

$$\underset{i\in\alpha}{*} G_i \to G_{\Omega'} \overset{\text{опр}}{=} \left(\underset{i\in\bigcup \Omega'}{*} G_i \right) \Big/ \left\langle\!\!\left\langle \bigcup_{\omega'\in\Omega'} N_{\omega'} \right\rangle\!\!\right\rangle$$

инъективно.

Доказательство.
Случай 1: $\omega \in \Omega'$. Воспользуемся индукцией по мощности семейства Ω'. Если $|\Omega'| = 1$ (то есть $\Omega' = \{\omega\}$), то утверждение леммы верно по условию (***). Допустим, что $|\Omega'| \geqslant 2$. В этом случае в соответствии с условиями 1), 2) и 3) семейство $F = \Omega'$ содержит множество $\omega' \neq \omega$, содержащее элемент $m \in \omega'$, не лежащий в $\bigcup(\Omega' \setminus \{\omega'\})$.

По предположению индукции (применённому к множеству ω' в качестве ω и семейству $\Omega' \setminus \{\omega'\}$ в качестве Ω') группы

$$G_i \text{ с номерами } i \in \beta \overset{\text{опр}}{=} \omega' \cap \Big(\bigcup (\Omega' \setminus \{\omega'\}) \Big)$$

свободно порождают своё свободное произведение в группе $G_{\Omega'\setminus\{\omega'\}}$. А по условию (***) те же группы G_i, где $i \in \beta$, свободно порождают своё свободное произведение в группе $G_{\omega'}$ (поскольку ω' содержит элемент m, не лежащий в β). Значит, группа $G_{\Omega'}$ раскладывается в свободное произведение групп $G_{\Omega'\setminus\{\omega'\}}$ и $G_{\omega'}$ с объединённой подгруппой $\underset{i\in\beta}{*} G_i$. При этом интересующие нас группы G_i с номерами $i \in \alpha$ лежат в сомножителе $G_{\Omega'\setminus\{\omega'\}}$. Следовательно, утверждение леммы следует из предположения индукции, применённого к множеству ω и семейству $\Omega' \setminus \{\omega'\}$ в качестве Ω'.
Случай 2: $\omega \notin \Omega'$. Доказательство в этом случае устроено похожим образом. Снова воспользуемся индукцией по мощности семейства Ω'. Если $\Omega' = \varnothing$, то доказывать нечего. Допустим, что $|\Omega'| \geqslant 1$. В этом случае в соответствии с условиями 1), 2) и 3) семейство $F = \Omega' \cup \{\omega\}$ содержит множество $\omega' \neq \omega$, содержащее элемент $m \in \omega'$, не лежащий в $\bigcup(F \setminus \{\omega'\})$ (рис.4).

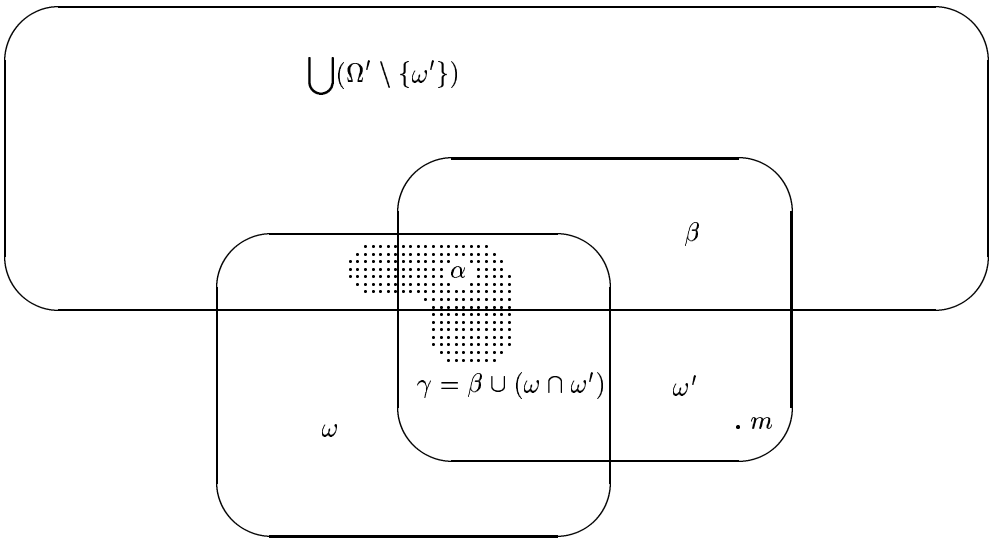


Рис. 4

По предположению индукции (применённому к множеству ω' в качестве ω и семейству $\Omega' \setminus \{\omega'\}$ в качестве Ω') группы

$$G_i \text{ с номерами } i \in \beta \stackrel{\text{опр}}{=} \omega' \cap \left(\bigcup(\Omega' \setminus \{\omega'\})\right)$$

свободно порождают своё свободное произведение в группе $G_{\Omega' \setminus \{\omega'\}}$. Значит, группы

$$G_i \text{ с номерами } i \in \gamma \stackrel{\text{опр}}{=} \beta \cup (\omega \cap \omega') = \omega' \cap \left(\bigcup((\Omega' \cup \omega) \setminus \{\omega'\})\right)$$

свободно порождают своё произведение в группе

$$H = \left(\mathop{*}_{j \in (\omega \cap \omega') \setminus \beta} G_j \right) * G_{\Omega' \setminus \{\omega'\}}.$$

Но по условию (***) те же группы G_i, где $i \in \gamma$, свободно порождают своё свободное произведение в группе $G_{\omega'}$ (поскольку ω' содержит элемент m, не лежащий в γ). Значит, группа $G_{\Omega'}$ раскладывается в свободное произведение с объединённой подгруппой групп H и $G_{\omega'}$:

$$G_{\Omega'} = H \mathop{*}_{\langle G_i \ ; \ i \in \gamma \rangle} G_{\omega'}.$$

При этом интересующие нас группы G_i с номерами $i \in \alpha$ лежат в сомножителе H. Следовательно, по предположения индукции, применённому к множеству ω и семейству $\Omega' \setminus \{\omega'\}$ в качестве Ω', группы G_i с номерами $i \in \alpha \cap (\bigcup(\Omega' \setminus \{\omega'\})$ свободно порождают своё свободное произведение в группе $G_{\Omega' \setminus \{\omega'\}}$. Отсюда немедленно вытекает, что группы G_i с номерами $i \in \alpha$ свободно порождают своё свободное произведение в группе H и, следовательно, в группе $G_{\Omega'}$, содержащей, как мы видели, H в качестве подгруппы. Лемма доказана.

Доказательство утверждения 1. Ясно, что утверждение достаточно доказать для конечного семейства Ω мощности большей единицы. Но в этом случае

$$G_I = G_\Omega * \left(\mathop{*}_{i \notin \bigcup \Omega} G_i \right),$$

а группа G_Ω раскладывается в свободное произведение с объединённой подгруппой:

$$G_\Omega = G_{\omega_{\min}} \mathop{*}_{K} G_{\Omega \setminus \{\omega_{\min}\}},$$

где объединяемая группа K является свободным произведением групп G_i с номерами из множества

$$\omega_{\min} \cap \bigcup(\Omega \setminus \{\omega_{\min}\})$$

в силу леммы 8. Поэтому утверждение очевидным образом вытекает из индуктивных соображений.

Далее нам понадобится одно свойство итерированных свободных произведений с объединёнными подгруппами.

Утверждение 2. *Пусть группа M_J является строгим итерированным свободным произведением с объединёнными подгруппами конечно порождённых групп M_j, где $j \in J$. Тогда*

1) *в группе M_J все подгруппы M_j, где $j \in J$, попарно различны;*
2) *если элемент $h \in M$ переставляет группы M_j, то есть для каждого $j \in J$ найдётся такое $k \in J$, что $M_j^h = M_k$, то h лежит в одной из групп M_i, где $i \in J$; в частности, каждый центральный элемент группы M содержится в центре одной из групп M_i.*

Доказательство. Докажем первое утверждение. Допустим, что $M_i = M_k$, где i и k — различные элементы множества J. В силу конечной порождённости группы M_i равенство $M_i = M_k$ выполняется в одном из СИПСОПов M_P конечного числа групп, пределом которых является группа M_J. Здесь P — некоторое конечное множество, содержащее i и k. Далее доказываем индукцией по мощности множества P. Группа M_P раскладывается в свободное произведение с объединённой подгруппой

$$M_P = M_{p_0} \underset{H}{*} M_{P\setminus\{p_0\}}.$$

Подгруппа H является собственной подгруппой в M_{p_0} по определению строгого СИПСОПа. Поэтому M_{p_0} не может совпадать ни с одной из подгрупп группы $M_{P\setminus\{p_0\}}$. В частности, $i \neq p_0 \neq k$. Но тогда равенство $M_i = M_k$ выполняется уже в группе $M_{P\setminus\{p_0\}}$. Ссылка на предположение индукции завершает доказательство первого утверждения.

Второе утверждение доказывается аналогично. Пусть $h \in \langle M_{j_1}, \ldots, M_{j_l}\rangle$. Рассмотрим равенства

$$M_{j_1}^h = M_{k_1}, \ldots, M_{j_l}^h = M_{k_l}.$$

В силу конечной порождённости групп M_j эти равенства выполняются в одном из СИПСОПов M_P конечного числа групп, пределом которых является группа M_J. Здесь P — некоторое конечное множество, содержащее $j_1, \ldots, j_l$ и $k_1, \ldots, k_l$. Далее доказываем индукцией по мощности множества P. Группа M_P раскладывается в свободное произведение с объединённой подгруппой

$$M_P = M_{p_0} \underset{H}{*} M_{P\setminus\{p_0\}}.$$

Подгруппа H является собственной подгруппой в M_{p_0} по определению строгого СИПСОПа. Кроме того, мы можем считать также, что H является собственной подгруппой в $M_{P\setminus\{p_0\}}$, поскольку в противном случае элемент h будет содержаться в M_{p_0} и доказывать будет нечего.

Если $p_0 \notin \{j_1, \ldots, j_l, k_1, \ldots, k_l\}$, то $h \in M_{P\setminus\{p_0\}}$, интересующие нас равенства выполняются уже в группе $M_{P\setminus\{p_0\}}$ и утверждение можно считать доказанным по предположению индукции.

Если же $p_0 = j_i$, то группа $(M_{p_0})^h$ либо будет содержаться в сомножителе $M_{P\setminus\{p_0\}}$, либо будет совпадать с M_{p_0} (в зависимости от того равны k_i и j_i, или нет). Из стандартных свойств свободного произведения с объединённой подгруппой вытекает, что первый случай невозможен, а второй случай возможен лишь при $h \in M_{p_0}$.

Случай $p_0 = k_i$ рассматривается аналогичным образом: в рассуждении из предыдущего абзаца надо h заменить на h^{-1}. Утверждение 2 доказано.

Замечание. Можно показать, что в этом утверждение нельзя отбросить ни требование строгости СИПСОПа, ни требование конечной порождённости сомножителей.

4. Полупрямые произведения с объединёнными подгруппами

Пусть группа A действует на группе B автоморфизмами $\varphi\colon A \to \operatorname{Aut} B$, а $N \lhd A$ и $N^\psi \subseteq B$ — изоморфные подгруппы групп A и B, причём N нормальна в A и изоморфизм $\psi\colon N \to N^\psi$ *согласован с действием* φ, то есть

$$(n^a)^\psi = (n^\psi)^{a^\varphi} \quad \text{и} \quad b^{n^\varphi} = b^{n^\psi} \quad \text{для всех } a \in A,\ b \in B \text{ и } n \in N.$$

Рассмотрим полупрямое произведение $A \leftthreetimes B$, отвечающее действию φ, то есть группу, состоящую из формальных произведений ab, умножаемых по правилу $(ab)(a_1b_1) = (aa_1)(b^{a_1^\varphi}b_1)$. Элементы вида $nn^{-\psi}$, где $n \in N$, составляют подгруппу полупрямого произведения $A \leftthreetimes B$:

$$(nn^{-\psi})(n_1n_1^{-\psi}) = (nn_1)((n^{-\psi})^{n_1^\varphi}n_1^{-\psi}) = (nn_1)((n^{-\psi})^{n_1^\psi}n_1^{-\psi}) = (nn_1)((n^{-1})^{n_1}n_1^{-1})^\psi = (nn_1)(nn_1)^{-\psi};$$
$$(nn^{-\psi})^{-1} = n^\psi n^{-1} = n^{-1}(n^\psi)^{n^{-\varphi}} = n^{-1}(n^\psi)^{n^{-\psi}} = n^{-1}(n^{n^{-1}})^\psi = n^{-1}n^\psi.$$

Причём эта подгруппа нормальна:

$$(nn^{-\psi})^a = n^a(n^{-\psi})^{a^\varphi} = n^a(n^{-a})^\psi = n^a(n^a)^{-\psi};$$
$$(nn^{-\psi})^b = b^{-1}(nn^{-\psi})b = nb^{-n^\varphi}n^{-\psi}b = nb^{-n^\psi}n^{-\psi}b = nn^{-\psi}.$$

Полупрямым произведением групп B и A (относительно действия φ) с объединёнными (посредством изоморфизма ψ) подгруппами N и N^ψ мы называем факторгруппу

$$A \underset{N=N^\psi}{\leftthreetimes} B \stackrel{\text{опр}}{=} (A \leftthreetimes B)/\{nn^{-\psi}\ ;\ n \in N\}.$$

Ясно, что эта группа содержит A и B в качестве подгрупп, является их произведением, причём подгруппа B нормальна и $A \cap B = N$.

5. Строение группы $\widehat{G}$

Пусть G и T — группы без кручения и $w = g_1t_1 \dots g_qt_q \in G * T$ — циклически несократимое обобщённо унимодулярное слово, то есть

$$\prod t_i = t \in \langle t \rangle_\infty * S = R \triangleleft T \quad \text{и } T/R \text{ — группа с сильно однозначным умножением.}$$

Мы изучаем группу

$$\widehat{G} = \langle G, T \mid w = 1 \rangle \stackrel{\text{опр}}{=} (G * T) \Big/ \left\langle\!\!\left\langle \prod g_it_i \right\rangle\!\!\right\rangle.$$

Опишем сначала основную идею нашего подхода. Группа $G*T$ раскладывается в полупрямое произведение с объединёнными подгруппами:

$$G * T = T \underset{R}{\leftthreetimes} \langle\!\langle G, R \rangle\!\rangle.$$

Нормальное замыкание $\langle\!\langle G, R \rangle\!\rangle$ подгруппы $G * R$ в группе $G * T$ можно представить, в свою очередь, как свободное произведение

$$\langle\!\langle G, R \rangle\!\rangle = \left(\underset{y \in T/R}{*} G^y \right) * S * \langle t \rangle_\infty.$$

При этом

$$w \in L_1 = \left(\underset{y \in X_1}{*} G^y \right) * S * \langle t \rangle_\infty, \quad \text{где } X_1 \text{ — некоторое конечное подмножество группы } T/R.$$

Группу $\langle\!\langle G, R \rangle\!\rangle$ можно рассматривать как СИПСОП групп L_1^x, где $x \in T/R$. Условие обобщённой унимодулярности гарантирует, что подобное разложение сохранится после факторизации по нормальному замыканию слова w. Дело в том, что факторгруппа группы L_1^x по нормальному замыканию слова w^x задаётся (обычным) унимодулярным относительным копредставлением над группой

$$H_x = \left(\underset{y \in xX_1}{*} G^y \right) * S.$$

Перейдём теперь к подробному изложению. Разложим T в объединение смежных классов по подгруппе R:

$$T = \coprod_{x \in T/R} c_xR, \quad \text{где } c_1 = 1.$$

Запишем соотношение $\prod t_ig_i = 1$ в виде

$$t \prod_{i=1}^{q} g_i^{c_{x_i}r_i} = 1, \tag{2}$$

где $r_i \in R$, $x_i = t_it_{i+1} \dots t_qR$ и $c_{x_i}r_i = t_it_{i+1} \dots t_q$. Пусть X_1 — это множество всех $x_i \in T/R$, встречающихся в соотношении (2). Для каждого $x \in T/R$ рассмотрим изоморфную копию $G^{(c_x)}$ группы G (подразумевая, что

изоморфизм отображает элемент $g \in G$ в элемент $g^{(c_x)} \in G^{(c_x)}$). Возьмём также изоморфную копию $\overline{R} = \langle \overline{t} \rangle_\infty * \overline{S}$ группы $R = \langle t \rangle_\infty * S$. Положим

$$H_1 = \overline{S} * \left(\mathop{*}_{y \in X_1} G^{(c_y)} \right)$$

и рассмотрим унимодулярное относительное копредставление

$$\widetilde{H}_1 = \left\langle H_1, \overline{t} \,\middle|\, \overline{t} \prod_i \left(g_i{}^{(c_{x_i})} \right)^{\overline{r}_i} = 1 \right\rangle$$

над группой H_1. Группа $\widetilde{H}_1$ является факторгруппой группы

$$L_1 = H_1 * \langle \overline{t} \rangle_\infty = \overline{R} * \left(\mathop{*}_{y \in X_1} G^{(c_y)} \right)$$

по нормальной подгруппе $N_1 = \left\langle\!\left\langle \overline{t} \prod g_i{}^{(c_{x_i})^{\overline{r}_i}} \right\rangle\!\right\rangle$. Рассмотрим теперь свободное произведение

$$L = \overline{R} * \left(\mathop{*}_{y \in T/R} G^{(c_y)} \right)$$

и правое действие $\varphi \colon T \to \operatorname{Aut} L$ группы T на L:

$$(\overline{r})^{x^\varphi} = \overline{r^x}, \quad \left(g^{(c_y)} \right)^{x^\varphi} = \left(g^{(c_{yx})} \right)^{\overline{a}}, \tag{3}$$

где $x \in T$, $y \in T/R$, а элемент $a \in R$ однозначно определяется из равенства $c_y x = c_{yx} a$.

Для каждого $x \in T/R$ положим

$$X_x = X_1 x \subseteq T/R, \quad H_x = \overline{S} * \left(\mathop{*}_{y \in X_x} G^{(c_y)} \right), \quad L_x = L_1^{\chi^\varphi} = H_x * \langle \overline{t} \rangle_\infty = \overline{R} * \left(\mathop{*}_{y \in X_x} G^{(c_y)} \right),$$

$$N_x = N_1^{\chi^\varphi} \lhd L_x, \quad \widetilde{H}_x = L_x / N_x,$$

где $\chi \in T$ — это любой представитель элемента $x \in T/R$.

Утверждение 3. *Группы $\widetilde{H}_x$ обладают следующими свойствами:*

1) *все они изоморфны между собой, изоморфизм $\widetilde{H}_1 \to \widetilde{H}_x$ действует так: $\overline{t} \mapsto \overline{t^{c_x}}$, $\overline{s} \mapsto \overline{s^{c_x}}$, $g^{(c_y)} \mapsto \left(g^{(c_{yx})} \right)^{\overline{r}}$, где элемент $r \in R$ однозначно определяется из равенства $c_y c_x = c_{yx} r$;*
2) *группа $\widetilde{H}_x$ задаётся унимодулярным относительным копредставлением над группой, изоморфной H_1 и представляющей собой свободное произведение группы S и p изоморфных копий группы G, где число $p = |X_x| = |X_1|$ равно числу различных смежных классов в наборе*

$$R,\ t_2 t_3 \dots t_q R,\ t_3 t_4 \dots t_q R,\ \dots,\ t_q R;$$

3) *в группе $\widetilde{H}_x$ имеет место разложение*

$$\left\langle \overline{R}, \{ G^{(c_y)} \ ;\ y \in Y \} \right\rangle = \overline{R} * \left(\mathop{*}_{y \in Y} G_y \right) \tag{4}$$

для каждого собственного подмножества $Y \subset X_x$; в частности, естественное отображение $\overline{R} \to \widetilde{H}_x$ инъективно, если $w \notin T$;

4) *естественные отображения*

$$\widetilde{H}_x = L_x / N_x \to K \stackrel{\text{опр}}{=} L \Big/ \left\langle\!\!\left\langle \bigcup_{y \in T/R} N_y \right\rangle\!\!\right\rangle$$

инъективны и группа K является итерированным свободным произведением с объединёнными подгруппами семейства групп $\{ \widetilde{H}_x \ ;\ x \in T/R \}$;

5) *СИПСОП K является строгим, если группа G не является циклической.*

Доказательство.

1) Указанное отображение представляет собой действие φ элемента c_x на L. Это отображение переводит группу L_1 в группу L_x. При этом подгруппа $N_1 \lhd L_1$ переходит в подгруппу $N_x \lhd L_x$, что влечёт изоморфность факторгрупп $\widetilde{H}_1 = L_1/N_1$ и $\widetilde{H}_x = L_x/N_x$.
2) Для группы $\widetilde{H}_1$ это верно по определению. Выполнение этого свойства для группы $\widetilde{H}_x$ следует из изоморфизма $\widetilde{H}_1 \to \widetilde{H}_x$, указанного в пункте 1).
3) Для группы $\widetilde{H}_1$ это свойство немедленно вытекает из следующей леммы.

Лемма 9 ([K06a], лемма 1). *Пусть группа H не имеет кручения, $P \subseteq H$ — свободный сомножитель группы H, слово $v \in H * \langle z \rangle_\infty$ унимодулярно и не сопряжено в $H * \langle z \rangle_\infty$ с элементами подгруппы $P * \langle z \rangle_\infty$.*
Тогда $\langle\langle v \rangle\rangle \cap (P * \langle z \rangle_\infty) = \{1\}$. Другими словами, элемент z трансцендентен над P в группе $\widetilde{H} = \langle H, z \mid v = 1 \rangle$.

Для других групп $\widetilde{H}_x$ это свойство следует из изоморфизма $\widetilde{H}_1 \to \widetilde{H}_x$, указанного в пункте 1).

4) Покажем, что семейство подпроизведений $\{L_x \mid x \in T/R\}$ свободного произведения L вместе с подгруппами $N_x \lhd L_x$ удовлетворяет условиям утверждения 1. Действительно, условия 1), 2) и 3) этого утверждения непосредственно вытекают из сильной однозначности умножения в группе T/R. Условие (***) следует из разложения (4). Таким образом, доказываемое свойство вытекает из утверждения 1.
5) Согласно утверждению 1, достаточно показать, что для каждого $x \in T/R$ и каждого $y \in X_x$ в группе $\widetilde{H}_x$ мы имеем $G^{(c_y)} \not\subseteq \langle \overline{R}, \{G^{(c_z)}; z \in X_x \setminus \{y\}\}\rangle$. В силу изоморфизма $\widetilde{H}_x \simeq \widetilde{H}_1$ мы можем без ограничения общности положить $x = 1$ и доказывать невозможность включения

$$G^{(c_y)} \subseteq \left\langle \overline{R}, \{G^{(c_z)}; z \in X_1 \setminus \{y\}\} \right\rangle \quad \text{в группе} \quad \widetilde{H}_1 = \left\langle H_1, \overline{t} \,\middle|\, \overline{t} \prod_i \left(g_i^{(c_{x_i})}\right)^{\overline{r}_i} = 1 \right\rangle. \tag{5}$$

Рассмотрим факторгруппу $U = \widetilde{H}_1 / \langle\langle \overline{S}, \{G^{(c_z)}; z \in X_1 \setminus \{y\}\} \rangle\rangle$. Группа U задаётся унимодулярным относительным копредставлением над группой $G^{(c_y)}$, поэтому естественное отображение $G^{(c_y)} \to U$ инъективно [K93]. Следовательно, включение (5) означало бы, что группа $G^{(c_y)}$, изоморфная группе G, лежит внутри циклической подгруппы $\langle \overline{t} \rangle$ группы U; то есть, группа G является циклической вопреки условию. Утверждение 3 полностью доказано.

Действие φ группы T на L очевидным образом опускается до действия на K, которое мы обозначим той же буквой $\varphi\colon T \to \operatorname{Aut} K$. Это действие согласовано с изоморфизмом $T \supseteq R \simeq \overline{R} \subseteq K$. Действительно, из формул (3) мы видим, что

$$(\overline{r})^{x^\varphi} = \overline{(r^x)} \quad \text{и} \quad \left(g^{(c_y)}\right)^{r^\varphi} = \left(g^{(c_y)}\right)^{\overline{r}} \quad \text{для всех } x \in T,\ y \in T/R \text{ и } r \in R.$$

Теорема 3. *Полупрямое произведение с объединёнными подгруппами $P = T \underset{R=\overline{R}}{\leftthreetimes} K$, соответствующее действию φ и изоморфизму $r \mapsto \overline{r}$, изоморфно группе $\widehat{G}$. Изоморфизм $P \to \widehat{G}$ тождественен на T, переводит подгруппу $G^{(1)} \subseteq P$ в подгруппу $G \subseteq \widehat{G}$ и подгруппу $K \lhd P$ в подгруппу $\langle\langle G, S \rangle\rangle = \langle\langle G, R \rangle\rangle \lhd \widehat{G}$.*

Доказательство. Группа G вкладывается в P в качестве подгруппы: $G = G^{(1)} \subseteq K \subseteq P$. Согласно определению действия, мы имеем $G^{(c_x)} = G^{c_x}$, значит, соотношение группы $\widetilde{H}_1$, выполненное в K, и равенство $R = \overline{R}$ в группе P дают соотношение (2). То есть отображение, действующее по правилу $G \ni g \mapsto g^{(1)} \in G^{(1)}$ и $T \ni x \mapsto x$, является гомоморфизмом из группы $\widehat{G}$ в P. Обратный гомоморфизм имеет вид $G^{(c_x)} \ni g^{(c_x)} \mapsto g^{c_x}$ и $T \ni x \mapsto x$.

Замечание. Из теоремы 3 и утверждения 3 (свойство 3) следует, что естественное отображение $T \to \widehat{G}$ инъективно, если $w \notin T$. В случае, когда T – свободная группа, этот факт был впервые получен С. В. Ивановым геометрическими методами (неопубликовано).

6. Доказательство теоремы 2

Первое утверждение теоремы непосредственно вытекает из теоремы 3. Докажем второе утверждение. Рассмотрим циклически несократимое обобщённо унимодулярное слово $w = g_1 t_1 \dots g_q t_q$ и положим $t = t_1 t_2 \dots t_q$. В силу теоремы 1 мы можем без ограничения общности предполагать, что группа T не является циклической.

Случай 1: $q = 1$ и $g_1 = 1$. В этом случае центр группы $\widehat{G} \simeq G * (T/\langle\langle t \rangle\rangle)$ тривиален, если $\langle\langle t \rangle\rangle \neq T$. Если же $\langle\langle t \rangle\rangle = T$, то $R = T$, $S = \{1\}$ (см. определение унимодулярности) и $T = R = \langle t \rangle * S = \langle t \rangle$, что противоречит предположению о нецикличности группы T.

Случай 2: $q = 1$ и $g_1 \neq 1$. В этом случае $T \neq \langle t \rangle$ (поскольку по условию группа T не является циклической),

$$\widehat{G} \simeq G \underset{g_1 = t^{-1}}{*} T$$

и утверждение теоремы вытекает из следующего хорошо известного простого факта (см., например, [ЛШ80]):

Лемма 10. *Центр свободного произведения с объединённой подгруппой, которая является собственной в каждом из сомножителей, совпадает с пересечением центров сомножителей.*

Случай 3: $q > 1$ и группа $\langle t_1, \ldots, t_q \rangle$ является циклической (и, следовательно, порождается элементом $t = \prod t_i$ в силу унимодулярности). В этом случае группа $\widehat{G}$ представляется в виде свободного произведения с объединённой подгруппой:

$$\widehat{G} \simeq \langle G, t \mid w = 1 \rangle \underset{\langle t \rangle}{*} T.$$

В силу леммы 10 центр группы $\widehat{G}$ может быть нетривиальным только в случае, когда центр группы

$$\widetilde{G} = \langle G, t \mid w = 1 \rangle$$

нетривиально пересекается с $\langle t \rangle$. По теореме 1 нетривиальность центра группы $\widetilde{G}$ означает, что группа G является циклической, что противоречит условию доказываемой теоремы.

Случай 4: группа $\langle t_1, \ldots, t_q \rangle$ не является циклической. В этом случае без потери общности можно считать, что $T = \langle t_1, \ldots, t_q \rangle$. Мы предполагаем, что группа G не является циклической и хотим доказать, что центр группы $\widehat{G}$ тривиален.

Во-первых отметим, что утверждение достаточно доказать для конечно порождённой группы G. Действительно, группа $\widehat{G}$ раскладывается в свободное произведение с объединёнными подгруппами

$$\widehat{G} = G \underset{\langle g_1, \ldots, g_q \rangle}{*} \langle \langle g_1, \ldots, g_q \rangle * T \mid g_1 t_1 \ldots g_q t_q = 1 \rangle .$$

Если $G \neq \langle g_1, \ldots, g_q \rangle$, то из этого разложения вытекает (по лемме 10), что центр группы $\widehat{G}$ содержится в G. С другой стороны, воспользуемся разложением $\widehat{G} = T \underset{R=\overline{R}}{\leftthreetimes} K$ из теоремы 3. В соответствие с описанием группы K (см. раздел 5), группа G содержится в подгруппе H_1 группы K, представляющей собой свободное произведение группы S и нескольких копий группы G:

$$G = G^{(1)} \subseteq H_1 = \overline{S} * \underset{y \in X_1}{*} G^{(c_y)} \subset K.$$

Центр группы H_1 может быть нетривиальным лишь в случае, когда $S = \{1\}$ и $|X_1| = 1$. Это означает (по утверждению 3), что $T = R = \langle t \rangle$, то есть группа T является циклической вопреки предположению.

В дальнейшем считаем, что G является конечно порождённой нециклической группой и $q \geqslant 2$. Нам требуется доказать, что центр группы $\widehat{G}$ тривиален. Снова воспользуемся теоремой 3. Пусть fy — центральный элемент группы $\widehat{G} = T \underset{R=\overline{R}}{\leftthreetimes} K$, где $y \in T$ и $f \in K$. Согласно утверждению 3 группа K является строгим итерированным свободным произведением с объединёнными подгруппами семейства групп $\{\widetilde{H}_x \,;\, x \in T/R\}$. Элемент $f \in K$ переставляет сомножители:

$$\widetilde{H}_x^f = \widetilde{H}_x^{y^{-1}} = \widetilde{H}_{xy^{-1}}.$$

Следовательно, $f \in \widetilde{H}_z$ для некоторого $z \in T/R$ (по утверждению 2). Центральность элемента fy теперь означает, что

$$\widetilde{H}_z = \widetilde{H}_z^{fy} = \widetilde{H}_z^{y} = \widetilde{H}_{zy}.$$

Согласно утверждению 2 такое равенство может выполняться лишь при $z = zy \in T/R$. Отсюда мы получаем, что $y \in R$ и $fy \in Z(K)$. Снова воспользовавшись утверждением 2, мы видим, что $fy \in Z(\widetilde{H}_z)$ при некотором $z \in T/R$. Для завершения доказательства остаётся вспомнить, что согласно теореме 1 центр группы $\widetilde{H}_z \simeq \widetilde{H}_1$ может быть нетривиальным лишь в случае когда группа H_1 является циклической, что противоречит предположению о нецикличности группы $G \simeq G^{(1)} \subseteq H_1$.

ГЛАВА 26.
ОТНОСИТЕЛЬНАЯ ГИПЕРБОЛИЧНОСТЬ И БЛИЗКИЕ СВОЙСТВА ОТНОСИТЕЛЬНЫХ КОПРЕДСТАВЛЕНИЙ С ОДНИМ ДОПОЛНИТЕЛЬНЫМ ОБРАЗУЮЩИМ И ОДНИМ СООТНОШЕНИЕМ, ЯВЛЯЮЩИМСЯ ИСТИННОЙ СТЕПЕНЬЮ УНИМОДУЛЯРНОГО СЛОВА

1. Введение

Пусть G — группа без кручения и группа $\widehat{G}$ получается из группы G добавлением одного образующего и одного *унимодулярного* соотношения, то есть соотношения с единичной суммой показателей при новом образующем:

$$\widehat{G} = \langle G, t \mid w = 1\rangle \stackrel{\text{опр}}{=} (G * \langle t\rangle_\infty)/\langle\langle w\rangle\rangle\,, \text{ где } w \equiv g_1 t^{\varepsilon_1} \dots g_n t^{\varepsilon_n},\quad g_i \in G,\ \varepsilon_i \in \mathbb{Z} \text{ и } \sum \varepsilon_i = 1.$$

Известно, что на такие *унимодулярные относительные копредставления с одним соотношением* распространяется значительная часть теории групп с одним соотношением В частности:

- группа G вкладывается (естественным образом) в группу $\widehat{G}$ [K93] (см. также [FeR96]);*)
- группа $\widehat{G}$ не имеет кручения [FoR05];
- группа $\widehat{G}$ непроста, если она не совпадает с G [K05];
- группа $\widehat{G}$ почти всегда (кроме нескольких известных исключений) содержит неабелеву свободную подгруппу [K07];
- группа $\widehat{G}$ SQ-универсальна, если группа G нетривиальным образом раскладывается в свободное произведение [K06b];
- центр группы $\widehat{G}$ почти всегда тривиален (кроме нескольких известных исключений) [K09].

Некоторые обобщения этих результатов на относительные копредставления, содержащие более одного добавленного порождающего, можно найти в работах [K09], [K07], [K06a] и [K06b].

Хорошо известно, что группы с одним соотношением, являющимся истинной степенью, больше похожи на свободные группы, чем произвольные группы с одним соотношением. Одним из выражений этого эффекта является теорема Ньюмана [New68] (см. также [ЛШ80]), утверждающая (если её переформулировать на современном языке), что группы с одним соотношением, являющимся истинной степенью, гиперболичны. Частичным обобщением этой теоремы на случай относительных копредставлений является следующая недавно опубликованная теорема.

Теорема Ле Тхи Жанг [Le09]. *Если группа G не имеет кручения, слово $w \in G * \langle t\rangle_\infty$ унимодулярно и $k \geqslant 2$, то группа*

$$\widetilde{G} = \langle G, t \,\big|\, w^k = 1\rangle \stackrel{\text{опр}}{=} G * \langle t\rangle_\infty \,/\, \langle\langle w^k\rangle\rangle \qquad (*)$$

относительно гиперболична (в смысле Осина) *относительно G, то есть копредставление $(*)$ удовлетворяет линейному изопериметрическому неравенству: существует константа $C > 0$ такая, что любое слово u в алфавите $G \cup \{t^{\pm 1}\}$, равное единице в $\widetilde{G}$, разлагается в группе $G * \langle t\rangle_\infty$ в произведение не более чем $C|u|$ слов, сопряжённых с $w^{\pm k}$.*

Здесь и далее символ $|u|$ обозначает число букв $t^{\pm 1}$ в слове u.

Относительно гиперболические группы обладают многими хорошими свойствами. Например, они являются SQ-универсальными (кроме некоторых очевидных исключений) [AMO07], в них разрешима проблем равенства (если она разрешима в подгруппах, относительно которых эти группы гиперболичны) [Far98], проблема сопряжённости (при некоторых естественных ограничениях) [Bum04] и многие другие алгоритмические проблемы. Подробнее с относительно гиперболическими группами можно познакомиться по книге [Os06].

Оказывается, что условие отсутствия кручения в теореме Ле Тхи Жанг можно заменить на отсутствие лишь элементов порядка два (или просто убрать, если $k \geqslant 3$). Следующая теорема является пока единственным результатом об унимодулярных относительных копредставлениях, в котором условие отсутствия кручения удаётся заменить на условия отсутствия элементов маленьких порядков.

*) Однако, естественное отображение $G \to \widehat{G}$ никогда не бывает сюръективным, за исключением случая когда $w \equiv gt$ [CR01].

Теорема. *Если слово $w \in G * \langle t \rangle_\infty$ унимодулярно и $k \geqslant 2$, то группа $\widetilde{G}$, заданная относительным копредставлением $(*)$, содержит G в качестве подгруппы (вложенной естественным образом),*[*)] *причём $\langle G, G^t \rangle = G * G^t$ в $\widetilde{G}$.*
Если при этом группа G не содержит инволюций или $k \geqslant 3$, то $\widetilde{G}$ относительно гиперболична относительно подгруппы G.

Пример 1 [Le09]. Группа $\widetilde{G} = \langle g, t \mid g^3 = 1, [g,t]^3 = 1 \rangle$ не является гиперболической (в частности, она не является относительно гиперболической относительно своей конечной подгруппы $G = \langle g \rangle_3$), так как её подгруппа $\langle a^t a, a a^t \rangle$ является свободной абелевой группой ранга два. Этот пример показывает, что условие унимодулярности в теореме нельзя отбросить.

Пример 2. Группа Баумслага–Солитэра $\widetilde{G} = \langle g, t \mid t^g = t^2 \rangle$ не является гиперболической (в частности, она не является относительно гиперболической относительно своей циклической подгруппы $G = \langle g \rangle$), так как централизатор элемента t является нециклической локально циклической группой $\left\langle t^{g^{-1}}, t^{g^{-2}}, \ldots \right\rangle$. Этот пример показывает, что условие $k \geqslant 2$ в теореме нельзя отбросить.

Вопрос. *Можно ли отбросить условие отсутствия инволюций при $k = 2$ в теореме?*
Предположительный ответ: нет.

Применяя упомянутые выше известные факты об относительно гиперболических группах, мы получаем, например, такое следствие.

Следствие 1. *Пусть слово w унимодулярно и либо $k \geqslant 3$, либо $k \geqslant 2$ и группа G не имеет инволюций. Тогда*
1) *если группа G нетривиальна, то группа $\widetilde{G}$ SQ-универсальна, то есть любая счётная группа вложима в некоторую факторгруппу группы $\widetilde{G}$.*
2) *в группе $\widetilde{G}$ разрешимы проблемы равенства и сопряжённости, если соответствующие проблемы разрешимы в группе G и она конечно порождена.*

Доказательство. Второе утверждение немедленно вытекает из нашей теоремы и результатов Фарба [Far98] и Бумагиной [Bum04], упомянутых выше.

Чтобы доказать первое утверждение, достаточно сослаться на упомянутую выше теорему Аржанцевой–Минасяна–Осина [AMO07], которая утверждает, что группа, относительно гиперболическая относительно своей собственной подгруппы, либо SQ-универсальна, либо почти циклическая.

То что группа $\widetilde{G}$ относительно гиперболична относительно G утверждается в теореме. То, что G является собственной подгруппой $\widetilde{G}$, следует из того, $\widetilde{G}/\langle\langle G \rangle\rangle = \langle t \mid t^k = 1 \rangle$ является циклической группой порядка $k \geqslant 2$. Наконец, то, что группа $\widetilde{G}$ не является почти циклической вытекает из того, что согласно теореме группа $\widetilde{G}$ содержит свободный квадрат группы G. А свободный квадрат группы порядка большего чем два (в частности, всякой нетривиальной группы без инволюций) не является, как известно, почти циклической группой. Оставшийся случай $G \simeq \mathbb{Z}_2$ и $k \geqslant 3$ покрывается теоремой Баумслага–Моргана–Шалена [BMS87], из которой следует, что в этом случае $\widetilde{G}$ содержит неабелеву свободную подгруппу и потому не является почти циклической.

Следствие 2. *Если слово w унимодулярно, $G \neq \{1\}$ и $k \geqslant 2$, то группа $\widetilde{G}$ содержит неабелеву свободную подгруппу, кроме случая, когда G состоит из двух элементов, $k = 2$ и слово w сопряжено в $G * \langle t \rangle_\infty$ слову вида gt, где $g \in G$ (в этом случае группа $\widetilde{G}$ является бесконечной диэдральной).*

Доказательство. Согласно теореме группа $\widetilde{G}$ содержит свободный квадрат группы G, который содержит неабелеву свободную группу, кроме случая, когда $G \simeq \mathbb{Z}_2$. Если при этом $k \geqslant 3$, то наличие неабелевой свободной подгруппы вытекает из следствия 1. Если же $k = 2$, то обобщённая треугольная группа $\widetilde{G} = \langle g, t \mid g^2 = w^2 = 1 \rangle$ попадает под действие теоремы Хауи [How98], описывающей обобщённые треугольные группы такого (в частности) вида без свободных подгрупп.

Замечание. Наше доказательство показывает также, что относительное копредставление $(*)$ асферично (если слово w унимодулярно и $k \geqslant 2$). В частности, это означает (см. [FoR05]), что каждая конечная подгруппа группы $\widetilde{G}$ сопряжена либо подгруппе исходной группы G, либо подгруппе циклической группы $\langle w \rangle$.

Если не предполагать унимодулярность слова w из копредставления $(*)$, а предположить лишь, что w не сопряжено с элементами из G в $G * \langle t \rangle_\infty$, то известно, например, следующее:

– группа G естественным образом вложена в $\widetilde{G}$, если либо G локально индикабельна [Б84], либо G циклическая и $k \geqslant 2$ [BMS87], [Boy88], либо $k \geqslant 4$ [How90], либо $k \geqslant 3$ и группа G без инволюций [DuH92];

*) Другими словами, *уравнение вида $(w(t))^k = 1$, где $k \geqslant 2$, а слово $w(t) \in G * \langle t \rangle_\infty$ унимодулярно разрешимо над любой группой G, то есть найдётся группа H, содержащая G в качестве подгруппы, и такой элемент $h \in H$, что $w(h) = 1$ в H.*

– группа $\widetilde{G}$ относительно гиперболична относительно G, если либо G локально индикабельна и $k \geqslant 2$ [DuH91], либо G без инволюций и $k \geqslant 4$ [DuH93].

Обзор результатов по относительным копредставлениям с одним соотношением, являющимся истинной степенью, можно найти в [DuH93] и в [FiR99].

Наш подход к доказательству теоремы, так же как подход Ле Тхи Жанг, основан на использовании одного стандартного алгебраического трюка (параграф 2) и геометрической техники: диаграмм Хауи (параграф 4) и столкновений автомобилей (параграфы 6 и 7). Разница состоит в том, что тест столкновений мы используем совместно с весовым тестом, то есть комбинаторной формулой Гаусса–Боне (параграф 3). На самом деле большую часть теоремы удаётся доказать (в параграфе 5) без использования «автомобильной техники». Автомобили нам нужны только для доказательства относительной гиперболичности при $k = 2$ и отсутствии инволюций (параграф 8).

Обозначения, которые мы используем, в целом стандартны. Отметим только, что если $k \in \mathbb{Z}$, x и y — элементы некоторой группы, а φ — гомоморфизм из этой группы в какую-нибудь другую группу, то x^y, x^{ky}, x^{-y}, x^φ, $x^{k\varphi}$ и $x^{-\varphi}$ обозначают $y^{-1}xy$, $y^{-1}x^ky$, $y^{-1}x^{-1}y$, $\varphi(x)$, $\varphi(x^k)$ и $\varphi(x^{-1})$ соответственно. Если X — подмножество некоторой группы, то $\langle X\rangle$ и $\langle\langle X\rangle\rangle$ означают, соответственно, подгруппу, порождённую множеством X, и нормальную подгруппу, порождённую множеством X. Буквы $\mathbb{Z}$, $\mathbb{N}$ и $\mathbb{R}$ обозначают множество целых, натуральных и вещественных чисел, соответственно. Символ $\widetilde{G}$ будет всегда обозначать группу, заданную копредставлением $(*)$.

2. Алгебраическая лемма

Следующая лемма представляет собой нетрудное обобщение леммы 2.1 из [Le09]. Аналогичный трюк с заменой копредставления был использован в [K93] и потом во многих других работах (см., например, [КП95], [CG95], [CG00], [CR01], [FeR96], [FeR98], [FoR05], [K05], [K06b], [K07] и [K09]). Геометрическую интерпретацию этого приёма можно найти в [FoR05].

Лемма 1. *Если слово $w = g_1t^{\varepsilon_1}\dots g_nt^{\varepsilon_n}$ унимодулярно, циклически несократимо и $n > 1$, то тогда группа $\widetilde{G}$ обладает относительным копредставлением вида*

$$\widetilde{G} = \left\langle H, t \;\middle|\; \{p^t = p^\varphi, p \in P \setminus \{1\}\}, \left(ct\prod_{i=0}^{m}(b_ia_i^t)\right)^k = 1\right\rangle, \tag{1}$$

где $a_i, b_i, c \in H$, P и P^φ — изоморфные подгруппы группы H и $\varphi\colon P \to P^\varphi$ — изоморфизм между ними. При этом

1) *$m \geqslant 0$ (то есть произведение в формуле (1) непустое);*
2) *$a_i \notin P$, а $b_i \notin P^\varphi$;*
3) *$\langle P, a_i\rangle = P * \langle a_i'\rangle$ и $\langle P^\varphi, b_i\rangle = P^\varphi * \langle b_i'\rangle$ в H, где $a_i' \in Pa_i$, $b_i' \in P^\varphi b_i$;*
4) *группы H, P и P^φ являются свободным произведением конечного числа изоморфных копий группы G: $H = G^{(0)} * \dots * G^{(s)}$, $P = G^{(0)} * \dots * G^{(s-1)}$ и $P^\varphi = G^{(1)} * \dots * G^{(s)}$, где $s \geqslant 0$ (при $s = 0$ группы P и P^φ тривиальны), а изоморфизм φ представляет собой сдвиг: $\left(G^{(i)}\right)^\varphi = G^{(i+1)}$.*

Доказательство. Сначала покажем, что у группы $\widetilde{G}$ имеется по крайней мере одно копредставление вида (1), удовлетворяющее условию 4). Поскольку $\sum\varepsilon_i = 1$, слово w можно записать в виде

$$w = \left(\prod g_i^{t^{k_i}}\right)t.$$

Сопрягая, если надо, w при помощи t, мы можем считать, что $k_i \geqslant 0$. Полагая $g^{(i)} = g^{t^i}$ для $g \in G$, $G^{(i)} = G^{t^i}$, $s = \max k_i$ и $c = \prod g_i^{(k_i)}$, мы видим, что $\widetilde{G}$ обладает копредставлением

$$\widetilde{G} \simeq \left\langle G^{(0)} * \dots * G^{(s)}, t \;\middle|\; \left\{\left(g^{(i)}\right)^t = g^{(i+1)},\ i = 0,\dots,s-1,\ g \in G\right\},\ (ct)^k = 1\right\rangle,$$

то есть копредставлением вида (1) (с $m = -1$), удовлетворяющим условию 4).

Теперь из всех копредставлений вида (1) группы $\widetilde{G}$, удовлетворяющих условию 4), выберем те, в которых s минимально, а из всех копредставлений с минимальным s выберем то, в котором m минимально. Полученное копредставление (1) будет искомым.

Действительно, если $m < 0$ (то есть $w = ct$, где $c \in H$), то $s = 0$, так как в противном случае мы могли бы уменьшить s, заменив в слове c все вхождения $g^{(s)}$ на $(g^{(s-1)})^t$. Но условия $m < 0$ и $s = 0$ означают, что исходное слово w имеет вид $w = ct$, $c \in G$, что противоречит тому, что $n > 1$. Таким образом условие 1) выполнено.

Условие 2) выполнено, поскольку в противном случае мы могли бы в копредставлении (1) заменить подслово $t^{-1}a_it$, где $a_i \in P$ (или подслово tb_it^{-1}, где $b_i \in P^\varphi$), на a_i^φ (соответственно, на $b_i^{\varphi^{-1}}$), уменьшив тем самым m (не увеличив при этом s).

Условия 3) следует из условий 2) и 4) в силу следующего простого факта, доказательство которого мы оставляем читателю в качестве упражнения.

Если $u \in A * B$, то $\langle A, u\rangle = A * \langle u'\rangle$ для некоторого $u' \in Au$.

Лемма доказана.

Следствие. *Если для некоторого i в группе H имеет место равенство вида $a_i^{n_1}p_1 \dots a_i^{n_s}p_s = 1$ или вида $b_i^{n_1}p_1^\varphi \dots b_i^{n_s}p_s^\varphi = 1$, где $s \geqslant 1$, $n_j \in \mathbb{Z} \setminus \{0\}$, $p_j \in P$ и $p_j \neq 1$ при $j \neq s$, то минимальный порядок неединичного элемента группы G не превосходит $\max\limits_{k<l} \left|\sum\limits_{j=k}^{l} n_j\right|$.*

Доказательство. Это немедленно вытекает из утверждений 4), 3) и 2) леммы 1.

3. Карты и весовой тест

Под поверхностью в этой главе мы всегда понимаем замкнутую двумерную ориентированную поверхность.

Картой M на поверхности S называется конечный набор непрерывных отображений $\{\mu_i\colon D_i \to S\}$, где D_i — двумерный замкнутый ориентированный диск (круг), называемый i-й *гранью* или *клеткой* карты, на границе которого отмечено некоторое конечное непустое множество точек $c_{ij} \in \partial D_i$, называемых *углами* карты. Интервалы e_{ij}, на которые углы делят границу грани, мы называем *прорёбрами* карты. Образы углов $\mu_i(c_{ij})$ и прорёбер $\mu_i(e_{ij})$ называют *вершинами* и *рёбрами* карты соответственно. При этом предполагается, что

1) ограничения отображения μ_i на внутренность грани D_i является гомеоморфным вложением, сохраняющим ориентацию; ограничение μ_i на каждое проребро является гомеоморфным вложением;
2) различные ребра не пересекаются;
3) образы внутренностей разных граней не пересекаются;
4) $\bigcup \mu_i(D_i) = S$.

Карту M мы будем также иногда трактовать как непрерывное отображение $\mathrm{M}\colon \coprod D_i \to S$ из дискретного объединения дисков в поверхность.

Объединение всех вершин и рёбер карты представляет собой граф на поверхности, называемый *одномерным остовом*.

Мы говорим, что угол c является углом при вершине v, если $\mathrm{M}(c) = v$. На множестве всех углов при вершине v имеется естественный циклический порядок; мы называем два угла при вершине v *смежными*, если они являются соседними относительно этого порядка.

Допуская некоторую вольность речи, мы говорим, что точка или подмножество поверхности содержится в грани D_i, если она (оно) лежит в образе μ_i. Аналогично, мы говорим, что грань D_i содержится в некотором подмножестве $X \subseteq S$ поверхности S, если $\mathrm{M}(D_i) \subseteq X$.

На рисунке 1 представлена карта на сфере с десятью гранями: A, B, C, D, E, F, G, H, I и K, тридцатью двумя углами, восемью вершинами, шестнадцатью рёбрами и тридцатью двумя прорёбрами. Заметим, что число углов всегда равно числу прорёбер и вдвое больше числа рёбер, а величина

$$\chi(S) \stackrel{\text{опр}}{=} (\textit{число вершин}) - (\textit{число ребер}) + (\textit{число граней})$$

не зависит от выбора карты на поверхности S и называется *эйлеровой характеристикой* этой поверхности. Эйлерова характеристика сферы (единственной поверхности, которая нас на самом деле интересует в этой главе) равна двум.

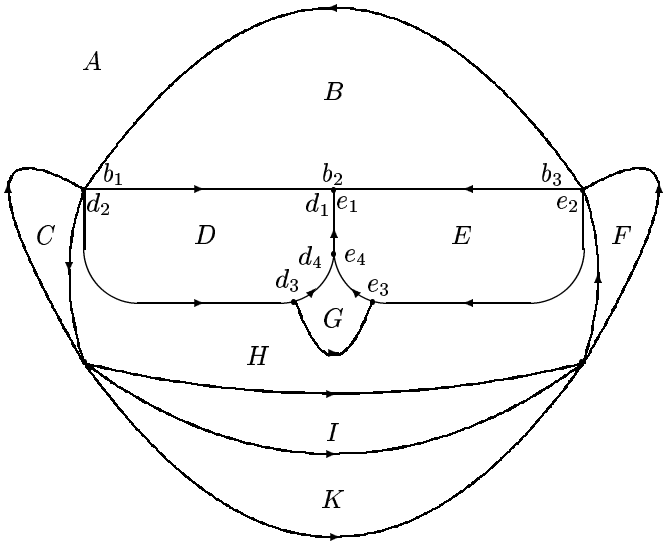


Рис. 1

Нам понадобится также следующее простое, но полезное утверждение, называемое иногда комбинаторной формулой Гаусса–Боне.

Весовой тест [Ger87], [Pri88], см. также [MCW02]. *Если каждому углу c некоторой карты на поверхности S поставлено в соответствие число $\nu(c)$* (которое мы будем называть *весом* или *величиной угла* c), *то*

$$\sum_v K(v) + \sum_D K(D) + \sum_e K(e) = 2\chi(S).$$

Здесь суммирования распространяются на все вершины v и все клетки D рассматриваемой карты, а величины $K(v)$, $K(D)$ и $K(e)$ называемые кривизнами соответствующей вершины, клетки и ребра определяются так:

$$K(v) \stackrel{\text{опр}}{=} 2 - \sum_c \nu(c), \qquad K(D) \stackrel{\text{опр}}{=} 2 - \sum_c (1 - \nu(c)), \qquad K(e) \stackrel{\text{опр}}{=} 0,$$

где первая сумма распространяется на все углы при вершине v, а вторая — на все углы клетки D.

4. Диаграммы Хауи

Пусть имеется карта M на поверхности S, углы которой помечены элементами некоторой группы H, а рёбра ориентированы (на рисунках на них имеются стрелки) и помечены элементами некоторого множества $\{t_1, t_2, \ldots\}$, не пересекающегося с группой H. Метку угла или ребра x будем обозначать $\lambda(x)$.

Метка вершины v в такой ситуации определяется формулой

$$\lambda(v) = \prod_{i=1}^{k} \lambda(c_i),$$

где $c_1, \ldots, c_k$ — это все углы при вершине v, перечисленные по часовой стрелке. Метка вершины является элементом группы H, определённым с точностью до сопряжённости. Например, метка одной из вершины на рисунке 1 есть $\lambda(b_2)\lambda(e_1)\lambda(d_1)$.

Метка грани D определяется формулой

$$\lambda(D) = \prod_{i=1}^{k} \big(\lambda(\mathrm{M}(e_i))\big)^{\varepsilon_i} \lambda(c_i),$$

где $e_1, \ldots, e_k$ и $c_1, \ldots, c_k$ — это все прорёбра и все углы грани D, перечисленные против часовой стрелки, причём концами проребра e_i являются углы c_{i-1} и c_i (индексы по модулю k), а $\varepsilon_i = \pm 1$ в зависимости от того,

сохраняет или обращает ориентацию гомеоморфизм $e_i \xrightarrow{\mathrm{M}} \mathrm{M}(e_i)$. Говоря по-простому, чтобы получить метку грани, надо обойти её границу против часовой стрелки, выписывая метки всех встречающихся углов и рёбер, причём метку ребра надо записывать в минус первой степени, если мы его проходим против стрелки.

Метка грани является элементом группы $H * F(t_1, t_2, \ldots)$ (свободного произведения H и свободной группы с базисом $\{t_1, t_2, \ldots\}$), определённым с точностью до циклической перестановки.

Например, если на рисунке 1 метки всех рёбер равны t, то метка грани B равна $t\lambda(b_1)t\lambda(b_2)t^{-1}\lambda(b_3)$.

Размеченную таким образом карту мы называем *диаграммой Хауи* (или просто *диаграммой*) над относительным копредставлением

$$K = \langle H, t_1, t_2, \ldots \mid w_1 = 1, w_2 = 1, \ldots \rangle\,, \qquad (**)$$

если

1) некоторые вершины и некоторые грани выделены и называются *внешними*, остальные вершины и грани называются *внутренними*;
2) метка каждой внутренней грани является циклической перестановкой одного из слов $w_i^{\pm 1}$;
3) метка каждой внутренней вершины равна единице в группе H.

На рисунке 4 изображены все возможные внутренние грани для диаграммы Хауи над копредставлением (1).

Диаграмма Хауи называется *приведённой*, если она не содержит такого ребра e, что две грани, его содержащие, являются внутренними, эти грани различны и метка одной из этих граней, если её написать начиная с метки ребра e, обратна метки другой грани, если её написать заканчивая меткой ребра e; такая пара клеток с общим ребром называется *сократимой парой*. Например, клетки D и E на рисунке 1 образуют сократимую пару, если $\lambda(d_i) = (\lambda(e_i))^{-1}$ и метки всех рёбер равны.

Следующая лемма является аналогом леммы ван Кампена для относительных копредставлений.

Лемма 2 [How83]. *Естественное отображение группы H в группу, заданную относительным копредставлением (**), не является инъективным тогда и только тогда, когда существует сферическая диаграмма над этим копредставлением с единственной внешней вершиной и без внешних граней, причём метка внешней вершины не равна единице в группе H. Минимальная (по числу клеток) из таких диаграмм является приведённой. Если это естественное отображение инъективно, то имеет место эквивалентность: образ элемента $u \in H * F(t_1, t_2, \ldots) \setminus \{1\}$ равен единице в группе (**) тогда и только тогда, когда существует сферическая диаграмма над этим копредставлением без внешних вершин и с единственной внешней гранью, метка которой равна u. Минимальная (по числу клеток) из таких диаграмм также является приведённой.*

Диаграммы на сфере с единственной внешней гранью и без внешних вершин называют также *дисковыми* диаграммами, границу внешней грани такой диаграммы называют *контуром* диаграммы.

Пусть $\varphi\colon P \to P^\varphi$ — изоморфизм между двумя подгруппами группы H. Относительное копредставление вида

$$\left\langle H, t \mid \{p^t = p^\varphi;\ p \in P \setminus \{1\}\}, w_1 = 1,\ w_2 = 1,\ \ldots \right\rangle \qquad (***)$$

назовём *φ-копредставлением*. Диаграмму над φ-копредставлением (***) назовём *φ-приведённой* если она приведена и различные внутренние клетки, метки которых имеют вид $p^t p^{-\varphi}$, $p \in P$, не имеют общих рёбер.

Лемма 3 [K05]. *Минимальная (по числу клеток) из всех сферических диаграмм над данным φ-копредставлением без внешних граней и с единственной внешней вершиной, метка которой не равна единице, является φ-приведённой. Если таких диаграмм не существует, то минимальная дисковая диаграмма с данной меткой контура является φ-приведённой.* Другими словами, имеет место полный φ-аналог леммы 2.

На рисунке 2 показана идея доказательства этой леммы.

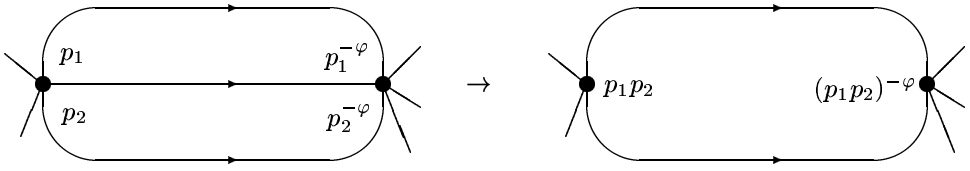


Рис. 2

Относительное копредставление (φ-копредставление), над которым не существует приведённых (соответственно, φ-приведённых) сферических диаграмм с единственной внешней вершиной и без внешних граней, называют *асферичными* (соответственно, *φ-асферичными*).

Пусть имеется карта на поверхности, ребра которой ориентированы (например, диаграмма Хауи). На такой карте бывает 4 сорта углов: $(++)$, $(--)$, $(+-)$ и $(-+)$ (рис. 3).

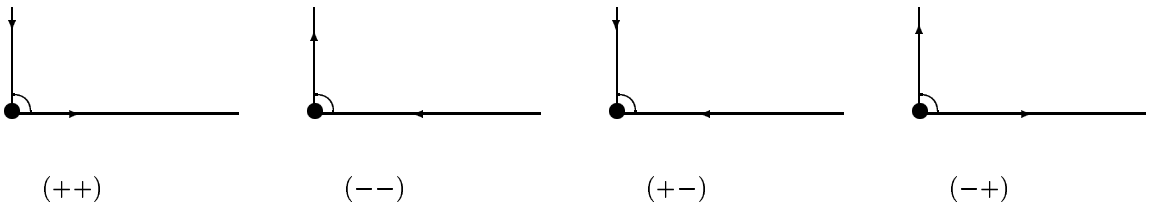


Рис. 3

Следующую лемму мы не доказываем ввиду ее очевидности.

Лемма 4. *При обходе против часовой стрелки углов при любой вершине v углы типа $(++)$ и $(--)$ чередуются. Если же при вершине v углов типа $(++)$ нет, или, что то же самое, углов типа $(--)$ нет, то либо все углы при v имеют тип $(+-)$ (в этом случае вершина v называется стоком), либо все углы при v имеют тип $(-+)$ (в этом случае вершина v называется источником).*

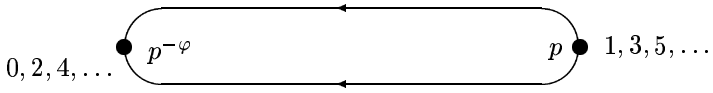


Рис. 4а

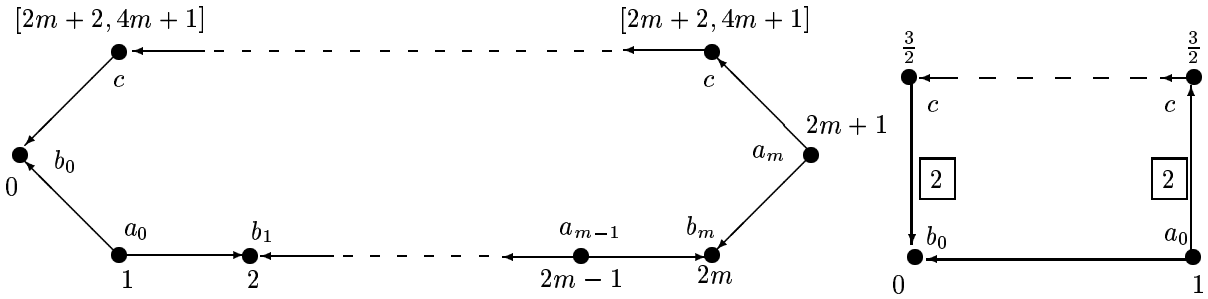


Рис. 4б

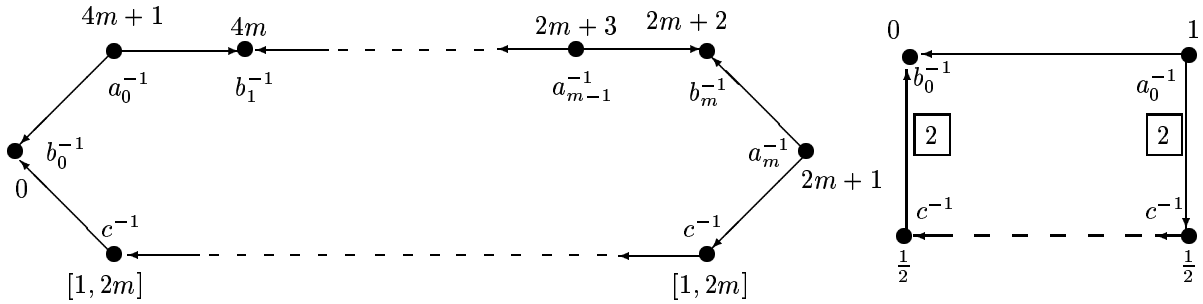


Рис. 4в

5. Доказательство большей части теоремы

В этом параграфе мы докажем все утверждения теоремы, кроме относительной гиперболичности при $k = 2$.

Если слово w сопряжено слову gt, то группа $\widetilde{G}$ представляет собой свободное произведение группы G на циклическую группу порядка k и все утверждения теоремы очевидны. Если же в слове w буквы $t^{\pm 1}$ встречаются более одного раза, то по лемме 1 группа $\widetilde{G}$ задаётся копредставлением (1).

Рассмотрим φ-приведённую сферическую диаграмму Хауи над копредставлением (1) без внешних граней и с единственной внешней вершиной, либо без внешних вершин и с единственной внешней гранью. Грани с метками вида $p^{-\varphi}p^t$, будем называть *двуугольниками*, остальные внутренние грани будем называть *большими гранями*.

Вершины и рёбра, лежащие на границе внешней грани будем называть *граничными*. Внешнюю вершину, если она есть, также будем для единообразия называть граничной.

Назовём двуугольник *особым*, если обе соседние с ним грани внутренние и один из его углов (называемый в дальнейшем *положительным*) является смежным с углами типа $(++)$ и $(--)$ (рис.5). Отметим, что второй угол особого двуугольника (называемый в дальнейшем *отрицательным*), при этом автоматически несмежен с углами типа типа $(++)$ и $(--)$.

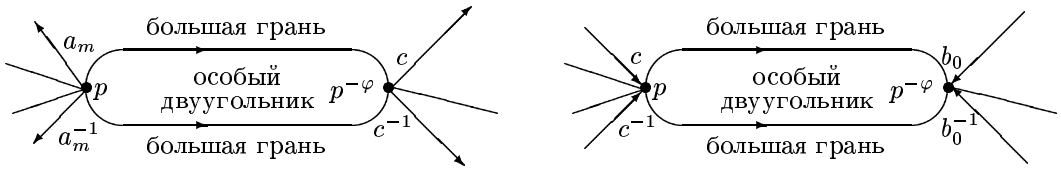


Рис. 5

Припишем каждому углу γ диаграммы вес $\nu(\gamma)$ по следующему правилу:

$$\nu(\gamma) = \begin{cases} 0, & \text{если } \gamma \text{ — угол неособого двуугольника} \\ & \text{или угол типа } (++) \text{ или } (--) \text{ внутренней грани (метка такого угла равна } c^{\pm 1}); \\ -1, & \text{если } \gamma \text{ — отрицательный угол особого двуугольника;} \\ 1 & \text{в остальных случаях.} \end{cases}$$

Посчитаем теперь кривизны вершин и граней в соответствии с весовым тестом (см. параграф 3). Для граней мы имеем:

$$K(\text{двуугольник}) = 0, \quad K(\text{большая грань}) = 2 - k, \quad K(\text{внешняя грань}) = 2.$$

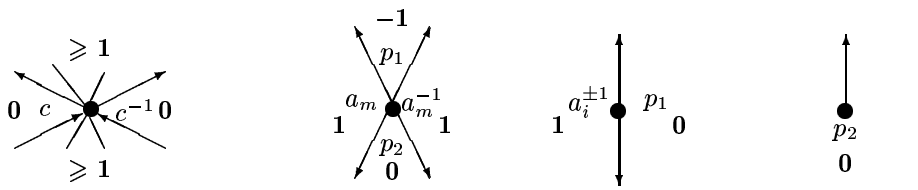
Для вершин v ситуация такая:

$$K(v) = 2 + n - l - \mathbf{p} - x, \tag{2}$$

где l — число углов типа $(+-)$ и $(-+)$ больших граней, $\mathbf{p}$ — число положительных углов особых двуугольников, n — число отрицательных углов особых двуугольников и x — число углов внешней грани (все углы при вершине v).

Каждый отрицательный угол особого двуугольника соседствует с двумя углами типа $(+-)$ или $(-+)$ больших граней (по определению специального двуугольника), причём никакой угол типа $(+-)$ или $(-+)$ не может соседствовать с двумя отрицательными углами (так как иначе соответствующая большая грань имела бы и угол типа $(++)$, и угол типа $(--)$, что невозможно). Поэтому $l \geqslant 2n$.

Отметим ещё, что углы типа $(++)$ и $(--)$ при негранничной вершине чередуются (по лемме 4) и не могут быть соседними (иначе диаграмма не была бы приведённой), между ними обязательно есть угол веса 1 (либо угол типа $(+-)$ или $(-+)$ большой грани, либо положительный угол особого двуугольника). С учётом предыдущего замечания об отрицательных углах это означает, что сумма весов углов, расположенных между углами типа $(++)$ и $(--)$ при обходе по часовой стрелке вокруг вершины v не меньше единицы (рис. 6, слева). Значит, негранничная вершина с положительной кривизной обязана быть источником или стоком и в такой вершине $\mathbf{p} = 0$, причём либо $n = 1$ и $l = 2$, либо $n = 0$ и $l = 1$, либо $n = 0$ и $l = 0$ ($n < 2$, так как иначе формула (2) и неравенство $l \geqslant 2n$, упомянутое выше, дали бы неположительную кривизну). Смотрите рис. 6, жирными цифрами показаны величины углов.



$n = 1, l = 2$ $\quad n = 0, l = 1$ $\quad n = 0, l = 0$

$K(v) \leqslant 0$ $\quad K(v) = 1$ $\quad K(v) = 1$ $\quad K(v) = 2$

Рис. 6

Первый случай ($n = 1$ и $l = 2$) в неграничной вершине невозможен, поскольку метка такой вершины, то есть произведение меток углов, равно $a_m^{-1} p_1 a_m p_2$ (если вершина — источник) или $b_0^{-1} p_1^{\varphi} b_0 p_2^{\varphi}$ (если вершина — сток), где p_1 и p_2 лежат в P и не равны единице (в силу приведённости диаграммы) и, следовательно, метка вершины не равна единице по следствию из леммы 1, то есть такая вершина не может быть внутренней. Второй и третий случаи ($n = 0$ и $l \in \{0, 1\}$) в неграничной вершине невозможны примерно по той же причине: они означали бы равенство $a_i^{\pm 1} p_1 = 1$, $b_i^{\pm 1} p_1^{\varphi} = 1$, $p_2 = 1$ или $p_2^{\varphi} = 1$, где $p_1 \in P \ni p_2 \neq 1$.

В итоге мы получаем, что кривизна любой неграничной вершины v неположительна. Кривизны внутренних граней также неположительны (при $k \geqslant 2$), кривизны граничных вершины не превосходят двойки (это следует из формулы (2) и того, что $l \geqslant 2n$), а суммарная кривизна должна быть четвёркой в соответствии с весовым тестом.

Это означает, что, во-первых, диаграмм без внешних граней и с единственной внешней вершиной не бывает, то есть естественное отображение $H \to \widetilde{G}$ (и, тем более, естественное отображение $G \to \widetilde{G}$) инъективно по лемме 2; а во-вторых, если внешняя грань одна, внешних вершин нет и $k \geqslant 3$, то число внутренних больших граней ограничено линейной функцией от периметра внешней грани:

$$2 \cdot (\text{периметр внешней грани}) - (k-2) \cdot (\text{число больших внутренних граней}) + 2 \geqslant 4.$$

Нетрудно сообразить, что такое изопериметрическое неравенство для копредставления (1) влечёт обычное линейное изопериметрическое неравенство для копредставления $(*)$ (см. [Le09]), то есть относительную гиперболичность группы $\widetilde{G}$ при $k \geqslant 3$. Для полноты картины мы приведём доказательство этого факта.

Утверждение 1. *Предположим, что некоторое слово $u \in G * \langle t \rangle_{\infty}$ равно единице в группе $\widetilde{G}$, то есть представляется в виде произведения*

$$u = v_1 \dots v_p w_1 \dots w_s,$$

где v_i сопряжены в $H * \langle t \rangle_{\infty}$ словам вида $p^{-t} p^{\varphi}$ ($p \in P$), а w_i сопряжены в $H * \langle t \rangle_{\infty}$ словам вида $\left(ct \prod_{i=0}^{m} (b_i a_i^t) \right)^{\pm k}$ (в терминологии леммы 1, где группа G отождествляется с $G^{(0)}$). Тогда слово u представляется в виде произведения s слов, каждое из которых сопряжено в $G * \langle t \rangle_{\infty}$ слову $w^{\pm k}$.

Менее формально, любое изопериметрическое неравенство для копредставления (1), в котором учитываются только длинные соотношения (только большие клетки), влечёт точно такое же изопериметрическое неравенство для копредставления $(*)$.

Доказательство. В группе $\langle H, t \,|\, \{p^t = p^{\varphi} \,;\, p \in P\} \rangle$ (которая изоморфна группе $G * \langle t \rangle_{\infty}$) каждое из слов v_i равно единице, а каждое из слов w_i сопряжено слову $w^{\pm k}$ (так как слово $ct \prod_{i=0}^{m} (b_i a_i^t)$ равно циклической перестановке слова w по построению), что и требовалось.

Вернёмся к доказательству теоремы и покажем, что $\langle G, G^t \rangle = G * G^t$ в группе $\widetilde{G}$. Если $H \neq G$, то есть $P \neq \{1\}$, то есть $s > 0$ в лемме 1, то доказывать нечего, так как уже доказано, что естественное отображение $H = G * G^t * \ldots \to \widetilde{G}$ инъективно.

Осталось рассмотреть случай $H = G$ (то есть $P = \{1\}$). Предположим, что $u \in G * G^t$ — несократимое непустое слово, представляющее единицу группы $\widetilde{G}$. По лемме 2 слово u является меткой внешней грани некоторой φ-приведённой сферической диаграммы над копредставлением $(*)$ (оно же копредставление (1) в рассматриваемом случае) без внешних вершин и с единственной внешней гранью. Поскольку двуугольники отсутствуют, а на внешней грани нет углов типа $(++)$ и $(--)$, кривизна каждой граничной вершины неположительна. Суммарная кривизна всех граней и вершин должна быть четвёркой, но единственное положительное слагаемое в этой сумме равно двойке (кривизна внешней грани). Это противоречие с весовым тестом завершает доказательство теоремы, за исключением утверждения об относительной гиперболичности при $k = 2$.

Замечание. Наше рассуждение доказывает также φ-асферичность копредставления (1) (если $k \geqslant 2$), а отсюда стандартным образом (см. [FoR05]) получается асферичность копредставления $(*)$.

Оставшаяся часть главы посвящена доказательству относительной гиперболичности в случае $k = 2$.

6. Движения

Все определения и утверждения этого параграфа мы позаимствовали из работы [K05].

Пусть на замкнутой ориентированной поверхности S имеется карта M, некоторые из углов которой помечены и называются *остановочными углами*.

Автомобилем, объезжающим грань D этой карты, называют непрерывное локально неубывающее*) отображение из ориентированной окружности R (*окружности времени*) в границу ∂D грани D такое, что прообраз каждой точки, не являющейся остановочным углом, дискретен.

Говоря по-простому, автомобиль объезжает границу своей грани против часовой стрелки (внутренность грани остается слева от автомобиля), не разворачиваясь, а останавливаться ему разрешается только в остановочных углах. При этом движение периодично.

Мы говорим, что автомобиль α находится в углу $c \in \partial D$ в момент времени $t \in R$ если $\alpha(t) = c$, кроме того, мы говорим, что в момент времени $t \in R$ автомобиль α *находится* в точке $p \in S$, если $\mu(\alpha(t)) = p$. Если число автомобилей, оказавшихся в момент времени t в точке p одномерного остова поверхности, S равно кратности этой точки (иными словами $\bigcup \alpha_i(t) \supseteq M^{-1}(p)$), то мы говорим, что в точке p в момент t происходит *полное столкновение*. При этом точка p называется *точкой полного столкновения*. Точки полного столкновения, лежащие на ребрах, мы называем просто *точками столкновения*.

Кратным движением периода T с разделёнными остановками на карте M называется набор автомобилей $\alpha_{D,j}\colon R \to \partial D$, где $j = 1, \ldots, d_D$, такой что

1) $d_D \geqslant 1$ (то есть каждую грань объезжает по крайней мере один автомобиль);
2) в каждой вершине v, при которой имеется хотя бы один остановочный угол, остановки разделены в следующем смысле: пусть $c_1, \ldots, c_k$ — это все остановочные углы при вершине v, занумерованные против часовой стрелки; требуется, чтобы для каждого i в углах c_i и c_{i+1} (индексы по модулю k) автомобили никогда не находились одновременно (в частности, это условие означает, что $k \geqslant 2$);
3) $\alpha_{D,j}(t+T) = \alpha_{D,j+1}(t)$ для любого $t \in R$ и $j = \{1, ..., d_D\}$ (здесь индексы берутся по модулю d_D, а сложение точек окружности R производится естественным образом: $R = \mathbb{R}/l\mathbb{Z}$);
4) существует такое разбиение каждой из окружностей ∂D на d_D дуг (с непересекающимися внутренностями), что на протяжении интервала времени $[0, T]$ каждый автомобиль $\alpha_{D,j}$ движется по j-й дуге.

Тест столкновений [K05], [K97]. *Для любого кратного движения с разделёнными остановками на карте* M *на поверхности S имеет место равенство*

$$\sum_v K'(v) + \sum_e K'(e) + \sum_D K'(D) = \chi(S),$$

где суммы распространяются на все вершины v, рёбра e и грани D карты M.
Здесь $K'(D) = 1 - d_D$, величина $K'(e)$ есть число точек столкновения на ребре e (не считая концов), а $K'(v) = 1$, если в вершине v происходит полное столкновение, в противном случае $K'(v)$ будет целым неположительным числом (точное определение которого можно найти в [K05]).

В этой главе поверхностью всегда будет сфера, её эйлерова характеристика равна 2.

---

*) Мы называем непрерывное отображение ориентированной окружности X в ориентированную окружность Y *локально неубывающим*, если прообраз всякого интервала $U \subset Y$ есть объединение интервалов, ограничение α на каждый из которых является неубывающей функцией (в обычном смысле, как отображение одного ориентированного интервала в другой).

7. Стандартное кратное движение

В этом параграфе мы определим некоторое конкретное кратное движение на диаграммах Хауи над копредставлением (1). Наше определение почти в точности повторяет определение из [Le09]. Аналогичный режим движения рассматривался и в [K05].

Назовём *стандартным* следующее движение на диаграмме Хауи над копредставлением (1):

а) внутреннюю грань с меткой $p^{-\varphi}p^t$ объезжает один автомобиль; он едет против часовой стрелки равномерно с единичной скоростью (одно ребро в единицу времени), проезжая в нулевой момент времени угол типа $(+-)$ (рис. 4а);

б) внутреннюю грань с меткой $\left(ct\prod_{i=0}^{m} b_i a_i^t\right)^k$ объезжают k автомобилей; при $m>0$ они стоят на протяжении промежутков времени $[2m+2,4m+1]+(4m+2)\mathbb{Z}$ в углах типа $(++)$ (с меткой c), а остальное время они едут против часовой стрелки равномерно с единичной скоростью; при $m=0$ эти автомобили едут без остановок, двигаясь по направлению ребра со скоростью 2, а против направления ребра — со скоростью 1, и находясь в углу типа $(+-)$ (с меткой b_0) в нулевой момент времени (рисунок 4б);

в) внутреннюю грань с меткой $\left(ct\prod_{i=0}^{m} b_i a_i^t\right)^{-k}$ объезжают тоже k автомобилей; при $m>0$ они стоят на протяжении промежутков времени $[1,2m]+(4m+2)\mathbb{Z}$ в углах типа $(--)$ (с меткой c^{-1}), а остальное время едут против часовой стрелки равномерно с единичной скоростью; при $m=0$ эти автомобили едут без остановок, двигаясь против направления ребра со скоростью 2, а по направлению ребра — со скоростью 1, и находясь в углу типа $(+-)$ (с меткой b_0^{-1}) в нулевой момент времени (рисунок 4в);

г) внешнюю грань объезжает один автомобиль; он двигается с периодом $4m+2$, в нулевой момент времени он находится в какой-то вершине, на протяжении интервала времени $[0,\frac{1}{4}]$ он (быстро) объезжает против часовой стрелки всю границу внешней грани, кроме последнего ребра; а оставшееся время он (медленно) едет по этому ребру.

Стандартное движение является периодическим с периодом $4m+2$ (при этом на гранях с меткой $p^{-\varphi}p^t$ минимальный период равен двум). На рисунке 4 показано подробное расписание движения автомобилей, объезжающих внутренние клетки, на протяжении интервала времени $[0,4m+2)$, числа в рамочках около рёбер означают скорость автомобиля на этих рёбрах (по умолчанию скорость единичная).

Лемма 5 (ср. [Le09], [K05]). *Предположим, что у диаграммы Хауи над копредставлением (1) имеется не более чем одна внешняя грань. Тогда стандартное движение является движением с разделенными остановками. Полные столкновения, которые происходят не на границе внешней грани, могут происходить только в вершинах, являющихся стоком или источником, и только в целые моменты времени. На каждом ребре границы внешней грани имеется не более $k(2m+1)$ точек полного столкновения.*

Доказательство. Объявим остановочными углами все углы типа $(++)$ и $(--)$. Из расписания движения видно, что автомобили никогда не бывают одновременно в углах типа $(++)$ и $(--)$: в углах типа $(--)$ автомобили, объезжающие внутренние грани, бывают только в первую половину периода, а в углах типа $(++)$ — во вторую половину, а автомобиль, объезжающий внешнюю грань, в такие моменты вообще находится не в углу. Из этого и из леммы 4 следует, что стандартное движение является движением с разделенными остановками. Столкновение на ребре разделяющем внутренние клетки в момент времени t означает, что в этот момент направление движения одного из автомобилей совпадает с направлением ребра, а направление движения другого автомобиля противоположно направлению ребра. Но расписание стандартного движения устроено так, что в каждый момент времени t либо все автомобили, объезжающие внутренние грани и находящиеся на ребрах, едут по направлению ребра (это происходит, когда целая часть t нечетна), либо все автомобили, объезжающие внутренние грани и находящиеся на ребрах, едут в направлении, противоположном направлению ребра (это происходит, когда целая часть t четна). Заметим также, что из определения кратного движения следует, что обгонов не бывает. Значит, столкновения могут происходить только в вершинах; из условия разделенности остановок следует, что вершины, в которых происходят полные столкновения, не могут иметь остановочных углов и, следовательно, являются источниками или стоками. В таких вершинах автомобили, объезжающие внутренние грани, появляются только в целые моменты времени.

Автомобиль β, объезжающий внешнюю грань, на каждом ребре e имеет возможность столкнуться не более чем с k автомобилями. За период $[0;4m+2)$ автомобиль β на на каждом ребре появится лишь один раз, а каждый из автомобилей, проезжающих это ребро в противоположном направлении, — не более $2m+1$ раза (эта величина достигается на двуугольнике). Следовательно, за период на каждом ребре границы внешней грани произойдёт не более $k(2m+1)$ столкновения. Эта сильно завышенная оценка завершает доказательство.

8. Завершение доказательства теоремы

В этом параграфе мы завершаем доказательство теоремы, то есть доказываем, что группа $\widetilde{G}$ относительно гиперболична относительно G, если G не содержит инволюций и $k = 2$ (впрочем, приводимое ниже доказательство годиться для любого $k \geqslant 2$).

Если слово w сопряжено слову gt, то группа $\widetilde{G}$ представляет собой свободное произведение группы G на циклическую группу порядка k и доказывать нечего. Если же в слове w буквы $t^{\pm 1}$ встречаются более одного раза, то по лемме 1 группа $\widetilde{G}$ задаётся копредставлением (1).

Рассмотрим φ-приведённую сферическую диаграмму Хауи над копредставлением (1) без внешних вершин и с единственной внешней гранью. Как и в параграфе 5 достаточно показать, что такие диаграммы удовлетворяет линейному изопериметрическому неравенству, то есть число больших внутренних граней ограниченно некоторой линейной функцией от периметра внешней грани.

Припишем всем углам диаграммы веса так же, как в параграфе 5. Напомним, что при таком распределении весов кривизны внутренних вершин неположительны. При этом кривизна внутренней вершины в соответствии с формулой (2) может быть нулевой только в следующих случаях:

а) $p > 0$ (и, следовательно, вершина не является ни источником, ни стоком);
б) $p = 0$, $n = 0$, $l = 2$;
в) $p = 0$, $n = 1$, $l = 3$;
г) $p = 0$, $n = 2$, $l = 4$ (рис. 7).

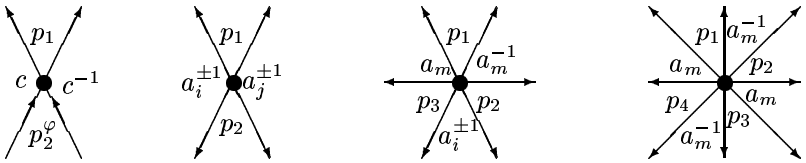


Рис. 7

Заметим, что ни в одном из случаев а), б), в), г) в вершине v не может произойти полного столкновения при стандартном движении (параграф 7). Действительно, в силу леммы 5 вершина полного столкновения должна быть источником или стоком, поэтому в случае а) нет полного столкновения. Полное столкновение в случае б), когда вершина v является, например, источником, означало бы в соответствии с расписанием движения, что оба угла больших граней при этой вершине имеют метки $a_i^{\pm 1}$ с одним и тем же индексом i, а произведение всех меток углов равно единице в группе G, чего не может быть в силу приведённости диаграммы, отсутствия инволюций и следствия из леммы 1. По тем же причинам полных столкновений не может быть в случаях в) и г): в этих случаях все углы больших граней должны иметь метку $a_m^{\pm 1}$, если вершина — источник, или $b_0^{\pm 1}$, если вершина — сток.

Заметим ещё что при стандартном определении движения (параграф 7) мы имеем:

$$K'(\text{двуугольник}) = 0,\ K'(\text{большая грань}) = 1-k,\ K'(\text{неграничное ребро}) = 0,\ K'(\text{граничное ребро}) \leqslant k(2m+1),$$

где величина K' определена в параграфе 4 (тест столкновений). Последние два неравенства следуют из леммы 5.

Определим *комбинированную кривизну* вершины, грани или ребра формулой

$$K_\Sigma(\cdot) \stackrel{\text{опр}}{=} K(\cdot) + K'(\cdot).$$

Ясно, что мы имеем неравенство $K_\Sigma(v) \leqslant 0$ для любой внутренней вершины v, поскольку $K(v)$ либо целое отрицательное число, либо ноль, но в последнем случае, как мы видели, в вершине v нет полного столкновения и, следовательно, $K'(v) \leqslant 0$.

Осталось заметить, что для любого неграничного ребра e и любой внутренней большой грани Γ

$$K_\Sigma(e) = K'(e) = 0 \text{ и } \quad K_\Sigma(\Gamma) = K(\Gamma) + K'(\Gamma) = 2 - k + (1 - k) \leqslant -1 \text{ при } k \geqslant 2.$$

Комбинированная кривизна граничных рёбер ограничена некоторой константой (зависящей только от k и m) по лемме 5. Комбинированная кривизна граничных вершин не превосходит, очевидно, тройки (так как $K(v) \leqslant 2$, как отмечалось в параграфе 5). Комбинированная кривизна внешней грани равна двум. С другой стороны, сумма комбинированных кривизн всех вершин, рёбер и граней в соответствии с весовым тестом и тестом столкновений должна быть $4 + 2$.

Это означает, что число внутренних больших граней ограничено линейной функцией от периметра внешней грани:

$$(D + 3) \cdot (\text{периметр внешней грани}) - (\text{число больших внутренних граней}) + 2 \geqslant 4 + 2,$$

где $D = k(2m + 1)$ — константа из леммы 5 (но это очень завышенная оценка). Это изопериметрическое неравенство завершает доказательство (в силу утверждения 1).

Другие применения комбинированного теста, а также описание всех возможных тестов (в некотором точном смысле) можно найти в [K97].

ГЛАВА 27.
АВТОМОРФИЗМЫ И ИЗОМОРФИЗМЫ ГРУПП И АЛГЕБР ШЕВАЛЛЕ

0. Введение

Пусть Φ — приведённая неприводимая система корней, R — ассоциативная коммутативное кольцо с единицей, $G(\Phi, R)$ — соответствующего присоединённая группа Шевалле и $E(\Phi, R)$ — её элементарная подгруппа (смотрите раздел 5).

Имеется много результатов (смотрите, например, [Wat80], [Пет82], [ГМи83], [HO'M89], [Абе93], [Che00], [Бун07] и литературу, там цитируемую*)), утверждающих, что при некоторых условиях все автоморфизмы групп Шевалле (или похожих групп) стандартны в том или ином смысле (зависящем того, что автору удалось доказать). В этой главе мы используем наиболее универсальное и естественное определение стандартности, предложенное А. Е. Залесским [Зал83]: автоморфизм присоединённой группы Шевалле называется *стандартным*, если он индуцирован автоморфизмом соответствующей алгебры Ли. Более точно, это означает следующее. Группы $E(\Phi, R)$ и $G(\Phi, R)$ вкладываются естественным образом в группу автоморфизмов соответствующей алгебры Ли $L(\Phi, R)$ над R. Немного менее очевидно, что (при некоторых условиях, смотрите раздел 5) обе группы нормальны в $\mathrm{Aut}_R L(\Phi, R)$ и даже в большей группе $\mathrm{Aut}_{\mathbb{Z}} L(\Phi, R) = \mathrm{Aut}_{\mathbb{Z}} R \leftthreetimes \mathrm{Aut}_R L(\Phi, R)$, состоящей из автоморфизмов этой алгебры, рассматриваемой как кольцо Ли. Таким образом, каждый автоморфизм $f \in \mathrm{Aut}_{\mathbb{Z}} L(\Phi, R)$ кольца Ли индуцирует автоморфизм $f' \colon g \mapsto fgf^{-1}$ групп Шевалле $G(\Phi, R)$ и $E(\Phi, R)$. Основными результатами этой главы являются следующие теоремы.

Теорема об автоморфизмах. *Для любой приведённой неприводимой системы корней Φ ранга $\geqslant 2$ существует такое целое число m, что для любого ассоциативного коммутативного кольца R без аддитивного кручения, с единицей и $\frac{1}{m}$ все автоморфизмы группы Шевалле $G(\Phi, R)$ и её элементарной подгруппы $E(\Phi, R)$ стандартны; группы $\mathrm{Aut}_{\mathbb{Z}} L(\Phi, R)$, $\mathrm{Aut}_{\mathbb{Z}} R \leftthreetimes \mathrm{Aut}_R L(\Phi, R)$, $\mathrm{Aut}\, G(\Phi, R)$ и $\mathrm{Aut}\, E(\Phi, R)$ изоморфны; отображение $\mathrm{Aut}_{\mathbb{Z}} L(\Phi, R) \ni f \mapsto f' \in \mathrm{Aut}\, G(\Phi, R)$ является изоморфизмом; аналогичное отображение*

$$\mathrm{Aut}_{\mathbb{Z}} L(\Phi, R) \to \mathrm{Aut}\, E(\Phi, R)$$

также является изоморфизмом.

Теорема об изоморфизмах. *Для любой приведённой неприводимой системы корней Φ ранга $\geqslant 2$ существует такое целое число m, что для любых ассоциативных коммутативных колец R и R' без аддитивного кручения, с единицей и $\frac{1}{m}$ имеются естественные взаимно однозначные соответствия между следующими тремя множествами:*

$$\{\text{групповые изоморфизмы } G(\Phi, R) \to G(\Phi, R')\}, \quad \{\text{групповые изоморфизмы } E(\Phi, R) \to E(\Phi, R')\}$$
$$\text{и} \quad \{\text{изоморфизмы колец Ли } L(\Phi, R) \to L(\Phi, R')\},$$

то есть каждый групповой изоморфизм $G(\Phi, R) \to G(\Phi, R')$ отображает $E(\Phi, R)$ на $E(\Phi, R')$; каждый групповой изоморфизм $E(\Phi, R) \to E(\Phi, R')$ продолжается единственным образом до изоморфизма $G(\Phi, R) \to G(\Phi, R')$; каждый кольцевой изоморфизм $f \colon L(\Phi, R) \to L(\Phi, R')$ индуцирует групповой изоморфизм

$$\mathrm{Aut}_{\mathbb{Z}} L(\Phi, R) \supseteq G(\Phi, R) \to G(\Phi, R') \subseteq \mathrm{Aut}_{\mathbb{Z}} L(\Phi, R')$$

по формуле $\varphi \mapsto f\varphi f^{-1}$; каждый групповой изоморфизм $G(\Phi, R) \to G(\Phi, R')$ индуцируется таким образом единственным кольцевым изоморфизмом.

Каждый кольцевой изоморфизм

$$f \colon L(\Phi, R) \to L(\Phi, R')$$

является полулинейным, то есть $f(rx) = \alpha(r) f(x)$ для некоторого кольцевого изоморфизма $\alpha \colon R \to R'$, однозначно определённого отображением f.

В частности, эти теоремы позволяют описать автоморфизмы всех групп Шевалле ранга большего единицы над любыми коммутативными алгебрами над полем рациональных чисел. Похожие результаты были получены Ю Ченом [Che95], [Che96] (смотрите также [Che00]), но при дополнительном условии, что кольцо R является алгеброй над $\mathbb{Q}$ без делителей нуля.

Идея описания автоморфизмов линейных групп путём перехода к соответствующим алгебрам Ли была впервые предложена и применена В. М. Левчуком [Лев83] и Е. И. Зельмановым [Зел85]. Мы используем ту же самую общую идею, но в остальном наш подход сильно отличается.

*) К сожалению, некоторые интересные работы по этой теме (например, [Абе93]) содержат ошибки.

Наши теоремы сводят задачу нахождения автоморфизмов/изоморфизмов групп Шевалле к более лёгкой аналогичной задаче об алгебрах Шевалле. Автоморфизмы алгебр Шевалле явно описаны в разделе 7. Каждый автоморфизм алгебры $L(\Phi, R)$ является композицией внутреннего автоморфизма (то есть сопряжения элементом группы $G(\Phi, R)$) и автоморфизмов, индуцированных симметриями соответствующей диаграммы Дынкина.

Наши доказательства совсем не содержат вычислений и используют лишь немногие свойства групп Шевалле. Таким образом, этот подход может работать в более общей ситуации. *Элементарной групповой схемой* E мы называем подгруппу группы $\mathbf{SL}_n(\mathbb{Z}[z_1, z_2, \ldots])$, порождённую некоторыми матрицами $\{x_i(z_j)\ ;\ i \in I,\ j = 1, 2, \ldots\}$. Для элементарной групповой схемы E символ $E(R)$ обозначает подгруппу группы $\mathbf{SL}_n(R)$, состоящую из всех матриц вида $a(r_1, r_2, \ldots)$, где $a \in E$ и $r_j \in R$. Группу $E(R)$ мы называем n-мерной R-*группой*. Понятно, что группа $E(R)$ порождается матрицами $\{x_i(r)\ ;\ i \in I,\ r \in R\}$. Прежде всего нас будут интересовать R-группы $E(R)$, обладающие следующими свойствами:

(EX) *Экспоненциальность*: $x_i(z_1)x_i(z_2) = x_i(z_1 + z_2)$ для всех $i \in I$.

(AL) *Алгебраичность*: $E(R[t])$ является нормальной подгруппой некоторой линейной алгебраической группы $G \subseteq \mathbf{SL}_n(R[t])$ определённой полиномиальными уравнениями с целыми коэффициентами. Группа $E(R[t])$ является нормальным замыканием своей подгруппы $E(R)$.

(PC_S) *Сопряжённость степеней*: две матрицы x_i и x_i^s сопряжены в $E(R)$ для каждого $i \in I$ и каждого $s \in S$, где $S \subseteq \mathbb{Z}$ — некоторое множество целых чисел.

Пример. В разделе 5 мы покажем, что при выполнении условий основных теорем присоединённая элементарная группа Шевалле $E(\Phi, R)$ обладает свойствами (EX), (AL) и (PC_S), где $S = \mathbb{Z} \cap \{a^2\ ;\ a \in R^*\}$.

1. Теорема о нулях

Напомним, что идеал называется *радикальным*, если соответствующее факторкольцо не содержит ненулевых нильпотентных элементов. Нам понадобится следующая формулировка теоремы Гильберта о нулях.

Теорема о нулях. *Пусть* $g, f_1, \ldots, f_l \in \mathbb{Z}[y_1, \ldots, y_m]$ *— некоторые многочлены и квазитождество*

$$\forall r_1, \ldots, r_l \in R \quad f_1(r_1, \ldots) = 0\ \&\ \ldots\ \&\ f_l(r_1, \ldots) = 0 \implies g(r_1, \ldots) = 0$$

выполняется для $R = \mathbb{C}$. *Тогда существует натуральное число* b *такое, что квазитождество*

$$\forall r_1, \ldots, r_l \in R \quad f_1(r_1, \ldots) = 0\ \&\ \ldots\ \&\ f_l(r_1, \ldots) = 0 \implies (g(r_1, \ldots))^b = 0$$

выполняется для любого ассоциативного коммутативного кольца R *с единицей и без аддитивного кручения. Если идеал кольца* $\mathbb{Z}[y_1, \ldots, y_m]$, *порождённый многочленами* $f_1, \ldots, f_l$, *является радикальным, то можно положить* $b = 1$.

2. Унипотентность

Матрица A называется *унипотентной*, если $A - 1$ — нильпотентная матрица. Назовём автоморфизм R-группы $E(R)$ *унипотентным*, если он отображает все $x_i(r)$ в унипотентные матрицы. Будем говорить, что автоморфизм φ является m-*унипотентным*, если $(\varphi(x_i(r)) - 1)^m = 0$ для всех $i \in I$ и $r \in R$.

Утверждение 1. *Если ассоциативное коммутативное кольцо* R *с единицей не имеет аддитивного кручения, то для любых целых* $n \geqslant 1$, $p \geqslant 2$ *и* $d \geqslant 1$ *существуют такие натуральные числа* q *и* m, *что любой автоморфизм* n-*мерной* R-*группы со свойством* ($\mathrm{PC}_{\{p, q^d\}}$) *является* m-*унипотентным.*

Доказательство. Если R-группа обладает свойством ($\mathrm{PC}_{\{p,q^d\}}$), то для любого автоморфизма φ матрицы $\varphi(x_i(r))$, $\varphi(x_i(r))^p$ и $\varphi(x_i(r))^{q^d}$ сопряжены. Таким образом, утверждение 1 вытекает из следующей леммы.

Лемма 1. *Для любых целых* $n \geqslant 1$, $p \geqslant 2$ *и* $d \geqslant 1$ *существуют такие натуральные числа* q *и* m, *что если характеристические многочлены матриц* $A, A^p, A^{q^d} \in \mathbf{SL}_n(R)$ *над ассоциативным коммутативным кольцом* R *с единицей и без аддитивного кручения совпадают, то* $(A - 1)^m = 0$.

Доказательство. Предположим для начала, что $R = \mathbb{C}$. Тогда, три указанные матрицы имеют одинаковые наборы собственных значений и возведение в степень p является перестановкой этих собственных значений. Следовательно, для любого собственного значения λ

$$\lambda^{p^{n!}-1} = 1 \quad \text{и, по тем же причинам,} \quad \lambda^{q^{dn!}-1} = 1.$$

Ясно, что из этих равенств следует, что $\lambda = 1$, если взять, например, $q = p^{n!} - 1$ (в этом случае $p^{n!} - 1$ и $q^{dn!} - 1$ взаимно просты). Итак, утверждение доказано для $R = \mathbb{C}$.

Условие

$$\det A = 1 \text{ и характеристические многочлены матриц } A,\ A^p \text{ и } A^{q^d} \text{ совпадают} \qquad (*)$$

является системой полиномиальных уравнений с целыми коэффициентами на элементы матрицы A. Каждый комплексный корень $B \in M_n(\mathbb{C})$ этой системы является унипотентной матрицей (если число q выбрано как выше). По теореме о нулях, это означает, что если матрица A над R удовлетворяет условию $(*)$, то каждый элемент c_{ij} матрицы $C = (A-1)^n$ удовлетворяет уравнению $c_{ij}^b = 0$ для некоторого целого b. Следовательно, $C^{bn^2} = (A-1)^{bn^3} = 0$. Лемма 1 и утверждение 1 доказаны.

3. Кривые

Рассмотрим некоторую R-группу $E(R)$ и назовём группу $E(R[t])$ *группой кривых на группе* $E(R)$.

Ясно, что для любой кривой $g(t) \in E(R[t])$ и любого многочлена $f(t) \in R[t]$ кривая $\mathrm{REP}_f(g) \overset{\text{опр}}{=} g(f(t))$ также принадлежит группе $E(R[t])$. Кривую $g(f(t))$ мы будем называть *репараметризацией кривой* g *с помощью многочлена* f. Отображение $\mathrm{REP}_f\colon E(R[t]) \to E(R[t])$ является эндоморфизмом группы кривых.

Стандартные вычисления

$$(1 + tX + t^2Y + o(t^2))^{-1} = 1 - (tX + t^2Y) + (tX + t^2Y)^2 + o(t^2) = 1 - tX + t^2(X^2 - Y) + o(t^2),$$

$$\begin{aligned}
&[(1 + tX_1 + t^2Y_1 + o(t^2)), (1 + tX_2 + t^2Y_2 + o(t^2))] = \\
&= (1 + tX_1 + t^2Y_1 + o(t^2))(1 + tX_2 + t^2Y_2 + o(t^2))(1 + tX_1 + t^2Y_1 + o(t^2))^{-1}(1 + tX_2 + t^2Y_2 + o(t^2))^{-1} = \\
&= 1 + t^2(Y_1 + Y_2 - Y_1 - Y_2 + X_1^2 + X_2^2 + X_1X_2 - X_1^2 - X_1X_2 - X_2X_1 - X_2^2 + X_1X_2) + o(t^2) = \\
&= 1 + t^2(X_1X_2 - X_2X_1) + o(t^2)
\end{aligned}$$

доказывают стандартную формулу:

$$[(1 + tX_1 + o(t)), (1 + tX_2 + o(t))] = \mathrm{REP}_{t^2}(1 + t[\![X_1, X_2]\!] + o(t)) + o(t^2), \qquad (1)$$

где $[x, y] \overset{\text{опр}}{=} xyx^{-1}y^{-1}$ — групповой коммутатор и $[\![x, y]\!] \overset{\text{опр}}{=} xy - yx$ — кольцевой коммутатор.

4. Непрерывность и гладкость

Множество матриц $T(E(R)) = \{X \in M_n(R) \mid 1 + tX + t^2Y \in E(R[t]) \text{ для некоторого } Y \in M_n(R[t])\}$ назовём *касательным модулем* R-группы $E(R)$. Ясно, что это множество является $R[E(R)]$-модулем, то есть оно замкнуто относительно

- сложения: $(1 + tX + o(t))(1 + tY + o(t)) = 1 + t(X + Y) + o(t)$;
- умножения на скаляры: $\mathrm{REP}_{rt}(1 + tX + o(t)) = 1 + tXr + o(t)$;
- действия группы $E(R)$: $g(1 + tX + o(t))g^{-1} = (1 + tgXg^{-1} + o(t))$ (В дальнейшем, мы используем обозначение $g \circ X \overset{\text{опр}}{=} gXg^{-1}$).

Если касательный модуль является алгеброй Ли, то есть если он замкнут относительно кольцевого коммутатора $[\![A, B]\!] = AB - BA$, мы называем этот модуль *касательной алгеброй*. Назовём n-мерную R-группу $E(R)$ *присоединённой*, если $T(E(R))$ является алгеброй Ли, изоморфной как $R[E(R)]$-модуль модулю R^n (с естественным действием группы $E(R)$).

Автоморфизм φ группы $E(R)$ назовём *квазинепрерывным*, если он может быть продолжен до автоморфизма $\widetilde{\varphi}$ группы кривых, коммутирующего со всеми целочисленными репараметризациями:

$$\widetilde{\varphi}(\mathrm{REP}_f(g)) = \mathrm{REP}_f(\widetilde{\varphi}(g))$$

для всех $g \in E(R[t])$ и всех $f \in \mathbb{Z}[t]$. Автоморфизм φ назовём *непрерывным*, если он является квазинепрерывным, автоморфизм $\widetilde{\varphi}$ квазинепрерывен, автоморфизм $\widetilde{\widetilde{\varphi}}$ квазинепрерывен и так далее (бесконечно много раз).

Положим $E_k(R) \overset{\text{опр}}{=} E(R[t]) \cap (1 + t^k M_n(R[t]))$. Так как $\ker \mathrm{REP}_0 = E_1(R)$, мы имеем равенство

$$\widetilde{\varphi}(E_1(R)) = E_1(R)$$

для любого непрерывного автоморфизма φ. Непрерывный автоморфизм φ назовём *гладким* (дважды дифференцируемым), если $\widetilde{\varphi}(E_k(R)) = E_k(R)$ для $k = 1, 2, 3$. Заметим, что непрерывность [гладкость] автоморфизма влечёт непрерывность [гладкость] обратного автоморфизма. В разделе 5 мы покажем, что любой непрерывный автоморфизм группы Шевалле является гладким (при некоторых условиях).

Утверждение 2. *Каждый гладкий автоморфизм φ группы $E(R)$ индуцирует автоморфизм $d\varphi$ (дифференциал автоморфизма φ) касательного модуля, рассматриваемого как абелева группа. При этом*

$$\widetilde{\varphi}(1+tX+o(t))=1+td\varphi(X)+o(t) \quad \textit{и} \quad d\varphi(g\circ X)=\varphi(g)\circ d\varphi(X) \quad \textit{для всех } g\in E(R) \textit{ и } X\in T(E(R));$$

если $T(E(R))$ является алгеброй Ли, то $d\varphi$ является автоморфизмом этой алгебры, рассматриваемой как кольцо Ли.

Доказательство. Если $X\in T(E(R))$, то $1+tX+t^2Y\in E(R[t])$ для некоторого $Y\in M_n(R[t])$ и

$$\widetilde{\varphi}(1+tX+t^2Y)=1+tZ+o(t)$$

для некоторого $Z\in M_n(R)$ (в силу инвариантности подгруппы $E_1(R)$). Положим $d\varphi(X)=Z$. Это определение корректно, поскольку автоморфизм $\widetilde{\varphi}$ оставляет инвариантной подгруппу $E_2(R)$. Биективность отображения $d\varphi$ следует из гладкости автоморфизма φ^{-1}. Равенства

$$\begin{array}{rcl}\widetilde{\varphi}((1+tX+o(t))(1+tY+o(t))) & = & \widetilde{\varphi}(1+t(X+Y)+o(t))=1+td\varphi(X+Y)+o(t)\\ \qquad\qquad || & & \\ \widetilde{\varphi}(1+tX+o(t))\widetilde{\varphi}(1+tY+o(t)) & = & (1+td\varphi(X)+o(t))(1+td\varphi(Y)+o(t))=1+t(d\varphi(X)+d\varphi(Y))+o(t)\end{array}$$

показывают, что $d\varphi$ является эндоморфизмом аддитивной группы. Аналогичные рассуждения

$$\begin{array}{rcl}\widetilde{\varphi}(g(1+tX+o(t))g^{-1}) & = & \widetilde{\varphi}(1+tgXg^{-1}+o(t))=1+td\varphi(gXg^{-1})+o(t)\\ \qquad\qquad || & & \\ \varphi(g)\widetilde{\varphi}(1+tX+o(t))\varphi(g)^{-1} & = & \varphi(g)(1+td\varphi(X)+o(t))\varphi(g)^{-1}=1+t\varphi(g)d\varphi(X)\varphi(g)^{-1}+o(t)\end{array}$$

доказывают равенство $d\varphi(g\circ X)=\varphi(g)\circ d\varphi(X)$.

Автоморфизм $\widetilde{\varphi}$ коммутирует с целочисленными репараметризациями, оставляет инвариантной подгруппу $E_3(R)$ и, следовательно, отображает равенство (1) в

$$[\widetilde{\varphi}(1+tX_1+o(t)),\widetilde{\varphi}(1+tX_2+o(t))]=\mathrm{REP}_{t^2}\widetilde{\varphi}(1+t[\![X_1,X_2]\!]+o(t))+o(t^2).$$

Значит,

$$[(1+td\varphi(X_1)+o(t)),(1+td\varphi(X_2)+o(t))]=\mathrm{REP}_{t^2}(1+td\varphi([\![X_1,X_2]\!])+o(t))+o(t^2).$$

Применяя формулу (1) к левой части, мы получаем

$$\begin{array}{rl}\mathrm{REP}_{t^2}(1+t[\![d\varphi(X_1),d\varphi(X_2)]\!]+o(t))+o(t^2)=[(1+td\varphi(X_1)+o(t)),(1+td\varphi(X_2)+o(t))]= & \\ =\mathrm{REP}_{t^2}(1+td\varphi([\![X_1,X_2]\!])+o(t))+o(t^2). & \end{array}$$

Таким образом, $[\![d\varphi(X_1),d\varphi(X_2)]\!]=d\varphi([\![X_1,X_2]\!])$. Это показывает, что $d\varphi$ является эндоморфизмом касательной алгебры и завершает доказательство.

Если группа $E(R)$ присоединённая, то она вкладывается естественным образом в группу автоморфизмов $\mathrm{Aut}_{\mathbb{Z}}T(E(R))$ её касательной алгебры, рассматриваемой как кольцо Ли.

Утверждение 3. *Любой гладкий автоморфизм присоединённой R-группы $E(R)$ является стандартным, то есть имеет вид $\varphi(g)=\alpha g\alpha^{-1}$, где α — некоторый автоморфизм кольца Ли $T(E(R))$, нормализующий подгруппу $E(R)$.*

Доказательство. Это непосредственно вытекает из утверждения 2, мы можем взять $\alpha=d\varphi$.

Утверждение 4. *Пусть коммутативное ассоциативное кольцо R с единицей и $\frac{1}{q!}$ не имеет аддитивного кручения, R-группа $E(R)$ обладает свойствами* (EX) *и* (AL), *φ и φ^{-1} являются взаимно обратными q-унипотентными автоморфизмами группы $E(R)$. Тогда эти автоморфизмы непрерывны.*

Доказательство. Рассмотрим матрицу $a(t) \in E(R[t])$. Ясно, что $a(r) \in E(R)$ для любого $r \in R$. Докажем, что

$$\textit{матрица } \varphi(a(k)) \textit{ полиномиально зависит от числа } k \in \mathbb{Z},$$

то есть существует матрица $b_a(t) \in \mathbf{SL}_n(R[t])$ такая, что $\varphi(a(k)) = b_a(k)$ для всех $k \in \mathbb{Z}$. (Отметим, что отсутствие аддитивного кручения влечёт единственность такой матрицы $b_a(t)$.)

Действительно, достаточно доказать этот факт для матрицы $a(t) = x_i(rt^l)$, поскольку эти матрицы порождают группу $E(R[t])$. Итак,

$$\varphi(x_i(rk^l)) = (\varphi(x_i(r)))^{k^l} \quad \text{по свойству (EX).}$$

Но матрица $(\varphi(x_i(r)))^m$ полиномиально зависит от m, так как матрица $\varphi(x_i(r))$ унипотентна:

$$(\varphi(x_i(r)))^m = (1+A)^m = 1 + mA + \frac{m(m-1)}{2}A^2 + \ldots + \frac{m(m-1)\ldots(m-q+1)}{q!}A^q.$$

Таким образом, мы можем продолжить автоморфизм φ на группу $E(R[t])$, полагая $\widetilde{\varphi}(a(t)) \stackrel{\text{опр}}{=} b_a(t)$.

Докажем, что $\widetilde{\varphi}(a(t)) = b_a(t)$ принадлежит группе $E(R[t])$. Для каждого целого k матрица $b_a(k)$ принадлежит группе $E(R)$ и, следовательно, принадлежит группе G, определённой целочисленными полиномиальными уравнениями (смотрите свойство (AL)). Следовательно, матрица $b_a(t)$ удовлетворяет тем же уравнениями. Таким образом, $b_a(t) \in G$ и мы имеем

$$\begin{array}{ccccccc}
E(R)=\widetilde{\varphi}(E(R)) & \subseteq & E(R[t]) & & E(R[t]) = \langle\langle E(R)\rangle\rangle_{E(R[t])} \subseteq & \langle\langle E(R)\rangle\rangle_G & \supseteq \langle\langle E(R)\rangle\rangle_{\widetilde{\varphi}(E(R[t]))} = \widetilde{\varphi}(E(R[t])) \\
\cap\vert & & \cap\vert & \text{и} & & \Vert & \text{(по свойству (AL))} \\
\widetilde{\varphi}(E(R[t])) & \subseteq & G & & & E(R[t]), &
\end{array}$$

где $\langle\langle X\rangle\rangle_H$ обозначает нормальное замыкание множества X в группе H. Таким образом, $\widetilde{\varphi}(E(R[t])) \subseteq E(R[t])$.

Автоморфизм φ^{-1} также может быть продолжен на группу кривых и $\widetilde{\varphi}(\widetilde{\varphi^{-1}})(a(k)) = (\widetilde{\varphi^{-1}})\widetilde{\varphi}(a(k)) = a(k)$ для любого $k \in \mathbb{Z}$ и любой матрицы $a(t) \in E(R[t])$. Отсюда следуют равенства $\widetilde{\varphi}(\widetilde{\varphi^{-1}})(a(t)) = (\widetilde{\varphi^{-1}})\widetilde{\varphi}(a(t)) = a(t)$ (поскольку кольцо R не имеет аддитивного кручения) и биективность отображения $\widetilde{\varphi}$.

По построению автоморфизм $\widetilde{\varphi}$ коммутирует с целочисленными репараметризациями, то есть φ квазинепрерывен. Ясно, что автоморфизм $\widetilde{\varphi}$ также является q-унипотентным и, следовательно, квазинепрерывным. Таким образом, очевидная индукция завершает доказательство непрерывности автоморфизма φ.

5. Группы Шевалле

Пусть Φ — приведённая неприводимая система корней, $L(\Phi)$ — соответствующая простая комплексная алгебра Ли. Алгебра $L(\Phi)$ имеет такой базис (*базис Шевалле*) $h_1, h_2, \ldots, x_1, x_2, \ldots$, что все структурные константы являются целыми и матрицы операторов $(\operatorname{ad} x_i)^k/k!$ целочисленны и нильпотентны для всех $k \in \mathbb{N}$. *Алгеброй Шевалле* $L(\Phi, R)$ называют алгебру Ли над кольцом R с такими же структурными константами.

Пусть $N(\Phi) = \operatorname{Aut}_{\mathbb{C}} L(\Phi)$ — группа автоморфизмов алгебры $L(\Phi)$ и $G(\Phi) = (\operatorname{Aut}_{\mathbb{C}} L(\Phi))^\circ$ — связная компонента единицы этой группы. Алгебраические группы $G(\Phi) \subseteq N(\Phi) \subseteq \mathbf{GL}(L(\Phi)) \subset \mathbf{SL}_n(\mathbb{C})$ определены над $\mathbb{Z}$. Пусть R — ассоциативное коммутативное кольцо с единицей и $N(\Phi, R)$ и $G(\Phi, R)$ — группы R-рациональных точек групп $N(\Phi)$ и $G(\Phi)$, то есть подгруппы в $\mathbf{SL}_n(R)$ (где $n = 1+\dim L(\Phi)$), определённые теми же целочисленными полиномиальными уравнениями, что группы $N(\Phi)$ и $G(\Phi)$ соответственно (в базисе Шевалле). Отметим, что $N(\Phi, R) = \operatorname{Aut}_R L(\Phi, R)$, поскольку свойство быть автоморфизмом может быть записано системой целочисленных полиномиальными уравнений (зависящих от структурных констант). Группа $G(\Phi, R)$ называется (*присоединённой*) *группой Шевалле*. Группу $E(\Phi, R) \subseteq G(\Phi, R)$, порождённую матрицами $x_i(r) = \exp(\operatorname{ad} r x_i)$, где $r \in R$, называют *элементарной подгруппой* группы Шевалле $G(\Phi, R)$.

Пример. Для системы корней A_l мы имеем $L(A_l) = \mathbf{sl}_{l+1}(\mathbb{C})$ — алгебра Ли, состоящая из всех матриц с нулевым следом, $L(A_l, R) = \mathbf{sl}_{l+1}(R)$, $G(A_l, R) = \mathbf{PGL}_{l+1}(R)$ и $E(A_l, R) = \mathbf{PE}_{l+1}(R)$ — подгруппа группы $\mathbf{PGL}_{l+1}(R)$, порождённая образами трансвекций $1 + rE_{ij}$, где $i \neq j$ и $r \in R$. (Отметим, что для некоторых колец таким образом определённая группа $\mathbf{PGL}_{l+1}(R)$ может быть больше, чем факторгруппа полной линейной группы $\mathbf{GL}_{l+1}(R)$ по её центру.)

В следующей лемме мы собрали некоторые (вероятно) известные свойства групп и алгебр Шевалле.

Лемма 2. *Пусть Φ — приведённая неприводимая система корней ранга $\geqslant 2$ и R — ассоциативное коммутативное кольцо без аддитивного кручения, с единицей и $\frac{1}{6}$. Тогда*

(i) *группа $E(\Phi, R)$ является R-группой со свойствами* (EX) *и* (PC_S), *где $S = \mathbb{Z} \cap \{a^2 \ ; \ a \in R^*\}$;*

(ii) *для каждой подгруппы H группы $G(\Phi, R)$, нормализуемой группой $E(\Phi, R)$, существует единственный идеал J кольца R такой, что H содержится в $G(\Phi, R) \cap (1 + M_n(J))$ и содержит нормальное замыкание $\langle\langle \{x_i(r) \ ; \ r \in J\} \rangle\rangle_{E(\Phi,R)}$ множества $\{x_i(r) \ ; \ r \in J\}$;*

(iii) *$E(\Phi, R)$ является автоморфно допустимой (то есть характеристической) подгруппой группы $G(\Phi, R)$;*

(iv) *$E(\Phi, R)$ обладает свойством* (AL);

(v) $\mathrm{Aut}_{\mathbb{Z}} L(\Phi, R) \simeq \mathrm{Aut}_{\mathbb{Z}} R \leftthreetimes \mathrm{Aut}_R L(\Phi, R)$;

(vi) *в группе $\mathrm{Aut}_{\mathbb{Z}} L(\Phi, R)$ подгруппы $G(\Phi, R)$ и $E(\Phi, R)$ нормальны и их централизаторы тривиальны.*

Доказательство.

(i) Свойство (EX) вытекает прямо из определения. Соотношение Стейнберга R5, $h_i(s)x_i(r)h_i(s)^{-1} = x_i(s^2 r)$ (смотрите, например, [VPl96]), где $r \in R$, $s \in R^*$ и $h_i(s) \in E(\Phi, R)$ суть некоторые специальные матрицы, доказывает свойство (PC_S).

(ii) Принимая во внимание тривиальность центра группы $G(\Phi, R)$ в присоединённом случае [AHu88], мы видим, что (ii) является слегка ослабленной формулировкой известной теоремы об описании подгрупп группы Шевалле, нормализуемых элементарной подгруппой, [Vas86] (смотрите также [ASu76], [Abe89], [Гол97], [CKe99], [ВГН06]).

(iii) Это также доказано Васерштейном в работе [Vas86]. Отметим, что в работе [HaV03] фактически доказана эндоморфная допустимость элементарных подгрупп групп Шевалле.

(iv) Нормальность группы $E(\Phi, R[t])$ в линейной алгебраической группе $G(\Phi, R[t])$, определённой полиномиальными уравнениями с целыми коэффициентами, непосредственно следует из (iii).
Равенство $\langle\langle E(\Phi, R) \rangle\rangle_{E(\Phi,R[t])} = E(\Phi, R[t])$ следует из (ii). Действительно, пусть $H = \langle\langle E(\Phi, R) \rangle\rangle_{E(\Phi,R[t])}$. Включение $E(\Phi, R) \subseteq H \subseteq G(\Phi, R[t]) \cap (1 + M_n(J))$ влечёт равенство $J = R[t]$. Следовательно,

$$E(\Phi, R[t]) = \langle\langle \{x_i(f) \ ; \ f \in R[t]\} \rangle\rangle_{E(\Phi,R[t])} = \langle\langle \{x_i(f) \ ; \ f \in J\} \rangle\rangle_{E(\Phi,R[t])} \subseteq H$$

и $H = E(\Phi, R[t])$.

(v) Пусть U — алгебра $L(\Phi, R)$, рассматриваемая как левый модуль над собой. Тогда

$$\mathrm{End}_{L(\Phi,R)} U = R, \quad \text{то есть все эндоморфизмы пропорциональны тождественному.} \qquad (**)$$

Действительно, это верно для $R = \mathbb{C}$, поскольку алгебра $L(\Phi, \mathbb{C})$ проста. Следовательно, условие (**) выполняется для любого кольца R без аддитивного кручения, поскольку оба условия на матрицу, задавать эндоморфизм модуля U и быть скалярной матрицей, являются системами линейных уравнений с целыми коэффициентами.
Отметим, что условие (**) останется справедливым, если рассматривать U как модуль над кольцом Ли $L(\Phi, R)$, то есть каждый эндоморфизм f модуля U обязан быть R-линейным. Действительно, для любого $u \in U$ существуют $y_i \in L(\Phi, R)$ и $u_i \in U$ такие, что $u = \sum (\mathrm{ad}\, y_i)(u_i)$, поскольку $L(\Phi, R) = [L(\Phi, R), L(\Phi, R)]$. Следовательно,

$$ru = \sum (\mathrm{ad}\, r y_i)(u_i) \quad \text{и} \quad f(ru) = f\left(\sum (\mathrm{ad}\, r y_i)(u_i)\right) = \sum (\mathrm{ad}\, r y_i) f(u_i) = r \sum (\mathrm{ad}\, y_i) f(u_i) = r f(u).$$

Теперь возьмём некоторый автоморфизм φ кольца $L(\Phi, R)$ и рассмотрим алгебру $L(\Phi, R)$ как $L(\Phi, R)$-модуль U_φ относительно действия $(y, u) \mapsto (\mathrm{ad}\, \varphi(y))u$. Ясно, что отображение $u \mapsto \varphi(u)$ является изоморфизмом модулей U и U_φ над кольцом Ли $L(\Phi, R)$. Этот изоморфизм индуцирует изоморфизм колец эндоморфизмов $R = \mathrm{End}_{L(\Phi,R)} U \xrightarrow{\alpha_\varphi} \mathrm{End}_{L(\Phi,R)} U_\varphi = R$. Мы имеем гомоморфизм $\mathrm{Aut}_{\mathbb{Z}} L(\Phi, R) \to \mathrm{Aut}_{\mathbb{Z}} R$, $\varphi \mapsto \alpha_\varphi$, ядром которого является группа $\mathrm{Aut}_R L(\Phi, R)$. Правый обратный гомоморфизм $\mathrm{Aut}_{\mathbb{Z}} R \to \mathrm{Aut}_{\mathbb{Z}} L(\Phi, R)$ отображает $\alpha \in \mathrm{Aut}_{\mathbb{Z}} R$ в очевидный автоморфизм кольца Ли $L(\Phi, R) = L(\Phi, \mathbb{Z}) \otimes R$, индуцированный автоморфизмом α. Таким образом, мы получаем требуемое разложение группы $\mathrm{Aut}_{\mathbb{Z}} L(\Phi, R)$ в полупрямое произведение.

(vi) **Нормальность.** В силу (iii), достаточно доказать нормальность подгруппы $G(\Phi, R)$. В случае $R = \mathbb{C}$ это свойство хорошо известно, смотрите, например, [BO88]. Пусть $F_N(y_{ij}) = 0$ и $F_G(y_{ij}) = 0$ — системы полиномиальных уравнений с целыми коэффициентами, определяющие группы $N(\Phi, R) = \mathrm{Aut}_R L(\Phi, R)$ и $G(\Phi, R)$ (эти системы не зависят от R). Будем считать, что идеалы кольца $\mathbb{Z}[y_{11}, y_{12}, \ldots, y_{nn}]$, порождённые наборами многочленов $F_N(y_{ij})$ и $F_G(y_{ij})$, радикальны. Для $R = \mathbb{C}$ мы имеем квазитождество

$$F_G(Y) = 0 \ \& \ F_N(Z) = 0 \implies F_G(ZYZ^{-1}) = 0. \qquad (2)$$

Так как идеал кольца $\mathbb{Z}[y_{11}, y_{12}, \dots, y_{nn}, z_{11}, z_{12}, \dots, z_{nn}]$, порождённый многочленами $F_G(Y)$ и $F_N(Z)$, является радикальным, теорема о нулях влечёт, что квазитождество (2) выполняется для все колец R без аддитивного кручения. Таким образом, $G(\Phi, R)$ является нормальной подгруппой группы $N(\Phi, R)$.

Централизаторы. Для $R = \mathbb{C}$ централизатор множества $\{x_i(1)\}$ в $\mathrm{Aut}_R L(\Phi, R)$ тривиален. Следовательно, то же самое верно для любого кольца R без аддитивного кручения (по теореме о нулях). Таким образом, централизатор множества $\{x_i(1)\}$ в группе $\mathrm{Aut}_{\mathbb{Z}} L(\Phi, R) = (\mathrm{Aut}_{\mathbb{Z}} R) \leftthreetimes \mathrm{Aut}_R L(\Phi, R)$ совпадает с $\mathrm{Aut}_{\mathbb{Z}} R$. С другой стороны, каждый нетривиальный кольцевой автоморфизм $\alpha \in \mathrm{Aut}_{\mathbb{Z}} R$ индуцирует нетривиальный автоморфизм $x_i(r) \mapsto x_i(\alpha(r))$ группы $E(\Phi, R)$. Следовательно, централизатор группы $E(\Phi, R)$ в группе $\mathrm{Aut}_{\mathbb{Z}} L(\Phi, R)$ тривиален и лемма 2 доказана.

Утверждение 5. *Пусть Φ — приведённая неприводимая система корней ранга $\geqslant 2$ и R — ассоциативное коммутативное кольцо без аддитивного кручения, с единицей и $\frac{1}{6}$. Тогда любая ретракция $\pi\colon E(\Phi, R[t]) \to E(\Phi, R)$ (то есть такой гомоморфизм, что $\pi^2 = \pi$) имеет вид $E(\Phi, R[t]) \ni a(t) \mapsto a(r) \in E(\Phi, R)$ для некоторого $r \in R$. Другими словами, $\pi = \mathrm{REP}_r$.*

Доказательство. Согласно лемме 2 (ii),

$$\langle\!\langle \{x_i(f) \ ; \ f \in J\} \rangle\!\rangle_{E(\Phi, R[t])} \subseteq \ker \pi \subseteq E(\Phi, R[t]) \cap (1 + M_n(J)) \quad \text{для некоторого идеала } J \text{ of } R[t].$$

Правое включение и равенство $E(\Phi, R[t]) = E(\Phi, R) \leftthreetimes \ker \pi$ показывают, что $t - r \in J$ для некоторого $r \in R$; левое включение и равенство $E(\Phi, R) \cap \ker \pi = \{1\}$ показывают, что $J = (t - r)R[t]$. Следовательно,

$$\ker \pi = E(\Phi, R[t]) \cap (1 + M_n(J))$$

и $\pi = \mathrm{REP}_r$.

Таким образом, мы имеем естественное взаимно однозначное соответствие между кольцом R и множеством ретракций. Ясно, что кольцевая структура на R также может быть описана в терминах ретракций и целочисленных репараметризаций:

$$\begin{aligned} \mathrm{REP}_{r+r'}\colon E(\Phi, R[t]) &\xrightarrow{t \to t+t'} E(\Phi, R[t, t']) \xrightarrow[t' \to r']{t \to r} E(\Phi, R), \\ \mathrm{REP}_{rr'}\colon E(\Phi, R[t]) &\xrightarrow{t \to tt'} E(\Phi, R[t, t']) \xrightarrow[t' \to r']{t \to r} E(\Phi, R). \end{aligned} \tag{3}$$

Из утверждения 5 и этих формул следует, что любой непрерывный автоморфизм $\varphi \in \mathrm{Aut}\, E(\Phi, R)$ индуцирует кольцевой автоморфизм $\widehat{\varphi} \in \mathrm{Aut}_{\mathbb{Z}} R$ по формуле $\varphi \mathrm{REP}_r \widetilde{\varphi}^{-1} = \mathrm{REP}_{\widehat{\varphi}(r)}$:

$$\begin{array}{ccc} E(\Phi, R[t]) & \xrightarrow{\widetilde{\varphi}} & E(\Phi, R[t]) \\ \downarrow \mathrm{REP}_r & & \downarrow \mathrm{REP}_{\widehat{\varphi}(r)} \\ E(\Phi, R) & \xrightarrow{\varphi} & E(\Phi, R). \end{array}$$

Каждому идеалу $J \lhd R$ соответствуют две нормальные подгруппы группы $E(\Phi, R)$, а именно,

$$E(J)_{\max} \stackrel{\text{опр}}{=} E(\Phi, R) \cap (1 + M_n(J))$$

и

$$E(J)_{\min} \stackrel{\text{опр}}{=} \langle\!\langle \{x_i(r) \ ; \ r \in J\} \rangle\!\rangle_{E(\Phi, R)}.$$

Лемма 3. *Пусть Φ — приведённая неприводимая система корней ранга $\geqslant 2$ и R — ассоциативное коммутативное кольцо без аддитивного кручения, с единицей и $\frac{1}{6}$. Тогда $\varphi(E(J)_{\min}) = E(\widehat{\varphi}(J))_{\min}$ и $\varphi(E(J)_{\max}) = E(\widehat{\varphi}(J))_{\max}$ для любого нерерывного автоморфизма φ группы $E(\Phi, R)$.*

Доказательство. Ясно, что достаточно определить $E(J)_{\min}$ и $E(J)_{\max}$ в терминах ретракций. Подгруппа $E_1(\Phi, R) \stackrel{\text{опр}}{=} E(\Phi, R[t]) \cap (1 + tM_n(R[t]))$ может быть определена как $E_1(\Phi, R) = \ker \mathrm{REP}_0$ (следовательно, эта подгруппа является $\widetilde{\varphi}$-инвариантной). Далее,

$$E(J)_{\min} = \langle\!\langle \{\mathrm{REP}_r(a(t)) \ ; \ r \in J, \ a(t) \in E_1(\Phi, R)\} \rangle\!\rangle_{E(\Phi, R)}.$$

Включение $\supseteq$ вытекает из равенства $E_1(R) = \langle\!\langle \{x_i(rt^k) \ ; \ i \in I, \ r \in R, \ k = 1, 2 \dots\} \rangle\!\rangle_{E(\Phi, R[t])}$, справедливого для любой R-группы со свойством (EX).

$$E(J)_{\max} = \begin{array}{l} \text{(единственная) максимальная подгруппа среди всех нормальных подгрупп } H \\ \text{таких, что } E(J)_{\min} \subseteq H \text{ и } E(J')_{\min} \not\subseteq H \text{ для любого идеала } J' \not\subseteq J. \end{array}$$

Корректность этого определения $E(J)_{\max}$ следует из леммы 2 (ii) и равенства $E(J_1 + J_2)_{\min} = E(J_1)_{\min} \cdot E(J_2)_{\min}$.

Лемма 4. *Пусть Φ — приведённая неприводимая система корней ранга $\geqslant 2$ и R — ассоциативное коммутативное кольцо без аддитивного кручения, с единицей и $\frac{1}{6}$. Тогда любой непрерывный автоморфизм φ группы $E(\Phi, R)$ является гладким.*

Доказательство. Мы должны доказать, что подгруппы $E_k(\Phi, R) \overset{\text{опр}}{=} E(\Phi, R[t]) \cap (1 + t^k M_n(R[t]))$ являются $\widetilde{\varphi}$-инвариантными. Это верно для $k = 1$, поскольку $E_1(\Phi, R) = \ker \mathrm{REP}_0$. С другой стороны,

$$E_1(\Phi, R) = E(tR[t])_{\max}.$$

Следовательно, идеал

$$tR[t] \lhd R[t]$$

является $\widehat{\widetilde{\varphi}}$-инвариантным по лемме 3. Значит, идеал $(tR[t])^k$ также $\widehat{\widetilde{\varphi}}$-инвариантен и подгруппа

$$E_k(\Phi, R) = E((tR[t])^k)_{\max}$$

инвариантна относительно $\widetilde{\varphi}$.

Утверждение 6. *Касательный модуль группы Шевалле совпадает с соответствующей алгеброй Ли: $T(E(\Phi, R)) = L(\Phi, R)$.*

Доказательство. Пусть $X \in T(E(\Phi, R))$, то есть $1 + tX + o(t) \in E(\Phi, R[t])$. Выразим этот элемент через порождающие:

$$1 + tX + o(t) = \prod_j x_{i_j}(r_j t^{k_j}) \tag{4}$$

Можно считать, что $k_j \in \{0, 1\}$. Подстановка $t = 0$ показывает что

$$\prod_j{}' x_{i_j}(r_j) = 1. \quad \text{где штрих означает, что произведение берётся по всем } j \text{ таким, что } k_j = 0.$$

Следовательно, выражение (4) может быть переписано в виде

$$1 + tX + o(t) = \prod_l g_l x_{i_l}(r_l t) g_l^{-1}, \quad \text{где } g_l \in E(\Phi, R).$$

Значит, $X = \sum g_l \circ r_l x_{i_l} \in L(\Phi, R)$ и $T(E(\Phi, R)) \subseteq L(\Phi, R)$.

Докажем теперь обратное включение. Ясно, что $T(E(\Phi, R))$ содержит нильпотентную часть $\{x_i\}$ базиса Шевалле: $x_i(t) = \exp(tx_i) = 1 + tx_i + o(t)$. Остальные базисные вектора h_i также содержатся в $T(E(\Phi, R))$, поскольку $h_i = x_i(1) \circ x_{-i} + x_i - x_{-i}$ (смотрите, например, [Bor70]). Утверждение доказано.

В частности, утверждение 6 показывает, что каждая присоединённая группа Шевалле является присоединённой в смысле раздела 4.

6. Доказательство основных теорем

Автоморфизмы группы $E(\Phi, R)$. По лемме 2 (vi) мы имеем естественный инъективный гомоморфизм $\Pi\colon \mathrm{Aut}_{\mathbb{Z}} L(\Phi, R) \to \mathrm{Aut}\, E(\Phi, R)$. По утверждению 1 и лемме 2 (i) каждый автоморфизм группы $E(\Phi, R)$ унипотентен (при подходящем выборе числа m) и, следовательно, непрерывен (по утверждению 4 и лемме 2 (i) и (iv)) и гладок (по лемме 4). Значит, отображение Π сюръективно по утверждениям 3 и 6. Таким образом, $\mathrm{Aut}\, E(\Phi, R) \simeq \mathrm{Aut}_{\mathbb{Z}} L(\Phi, R) \simeq \mathrm{Aut}_{\mathbb{Z}} R \leftthreetimes \mathrm{Aut}_R L(\Phi, R)$ (второй изоморфизм следует из леммы 2 (v)).

Автоморфизмы группы $G(\Phi, R)$ такие же как у $E(\Phi, R)$. Действительно, каждый автоморфизм группы $E(\Phi, R)$ стандартен и, следовательно, может быть продолжен до автоморфизма группы $G(\Phi, R)$ по лемме 2 (vi). Таким образом, естественное отображение $\mathrm{Aut}\, G(\Phi, R) \to \mathrm{Aut}\, E(\Phi, R)$ сюръективно (и корректно определено по лемме 2 (iii)). Инъективность этого отображения вытекает из леммы 2 (vi) и следующего общего факта.

Лемма 5. *Если A — автоморфно допустимая подгруппа группы B и централизатор подгруппы A в B тривиален, то естественное отображение $\rho\colon \mathrm{Aut}\, B \to \mathrm{Aut}\, A$ инъективно.*

Доказательство. Для любых $\varphi \in \ker \rho$, $a \in A$, и $b \in B$, мы имеем

$$bab^{-1} = \varphi(bab^{-1}) = \varphi(b)\varphi(a)\varphi(b^{-1}) = \varphi(b)a\varphi(b^{-1}).$$

Следовательно, $b^{-1}\varphi(b)$ коммутирует с A. Значит, $b = \varphi(b)$ для любого $b \in B$. Теорема об автоморфизмах доказана.

Теорема об изоморфизмах является простым следствием теоремы об автоморфизмах. Каждый изоморфизм групп Шевалле $\sigma\colon G(\Phi, R) \to G(\Phi, R')$ индуцирует автоморфизм φ_σ группы $G(\Phi, R \times R')$, поскольку этой группа раскладывается в прямое произведение $G(\Phi, R) \times G(\Phi, R')$ и мы можем положить $\varphi_\sigma(g, g') = (\sigma^{-1}(g'), \sigma(g))$. Стандартность автоморфизма φ_σ означает, что σ индуцирован изоморфизмом соответствующих колец Ли. Аналогичным образом доказывается утверждение об элементарных подгруппах.

7. Автоморфизмы алгебр Шевалле

Напомним, что *внутренним автоморфизмом* алгебры Шевалле $L(\Phi, R)$ называют сопряжение $x \mapsto gxg^{-1}$ элементом g группы Шевалле $G(\Phi, R)$. Ясно, что внутренние автоморфизмы образуют группу, изоморфную группе $G(\Phi, R)$.

Пусть $\Delta = \{\delta_1, \ldots, \delta_d\}$ — группа симметрий диаграммы Дынкина системы Φ (число d может быть 1, 2 или 6, в зависимости от Φ) и пусть $R = R_1 \oplus \ldots \oplus R_d$ — (возможно тривиальное) разложение кольца R в прямую сумму идеалов. Пусть $f_i \in \mathrm{Aut}_{R_i} L(\Phi, R_i)$ — автоморфизм, индуцированный симметрией δ_i (смотрите [BO88]). Автоморфизм f алгебры $L(\Phi, R) = L(\Phi, R_1) \oplus \ldots \oplus L(\Phi, R_d)$, отображающий $x_1 + \ldots + x_d$ в $f_1(x_1) + \ldots + f_d(x_d)$, где $x_i \in L(\Phi, R_i)$, мы называем *диаграммным автоморфизмом* алгебры $L(\Phi, R)$. Ясно, что диаграммные автоморфизмы образуют группу, изоморфную подгруппе

$$D(\Phi, R) = \left\{ \sum e_i \delta_i \;\mid\; e_i \in R,\ e_i^2 = e_i,\ e_i e_j = 0 \text{ для } i \neq j,\ \sum e_i = 1 \right\}$$

группы единиц групповой алгебры $R\Delta$.

Теорема 1. *Пусть R — ассоциативное коммутативное кольцо без аддитивного кручения, с единицей и $\frac{1}{6}$ и пусть Φ — приведённая неприводимая система корней. Тогда любой автоморфизм f R-алгебры Ли $L(\Phi, R)$ единственным образом раскладывается в композицию диаграммного и внутреннего автоморфизма,*

$$\mathrm{Aut}_R L(\Phi, R) \simeq D(\Phi, R) \leftthreetimes G(\Phi, R).$$

Доказательство. Пусть n — размерность алгебры Ли $L(\Phi)$. Рассмотрим идеал J кольца $\mathbb{Z}[x_{11}, x_{12}, \ldots, x_{nn}]$, определяющий группу $\mathrm{Aut}_{\mathbb{C}} L(\Phi)$. Идеал J раскладывается в произведение $J = J_1 J_2 \ldots J_d$ простых идеалов J_i, отвечающих неприводимым (= связным) компонентам $h_i G(\Phi)$ группы $\mathrm{Aut}_{\mathbb{C}} L(\Phi)$, где h_i — целочисленные матрицы диаграммных автоморфизмов. Рассмотрим матрицу $A = (a_{pq}) \in \mathrm{Aut}_R L(\Phi, R)$. Тогда $f(a_{pq}) = 0$ для $f \in J$. Положим $I_i = \{f(a_{pq})\ ;\ f \in J_i\} \lhd R$. Тогда

(i) $\prod I_i = \{0\}$;

(ii) $I_i + I_j = R$ для $i \neq j$ (в противном случае мы рассмотрим факторкольцо по максимальному идеалу $M \supseteq I_i + I_j$ и получим, матрицу A_M, лежащую в пересечении двух неприводимых компонент группы $\mathrm{Aut}_{R/M} L(\Phi, R/M)$, но это пересечение пусто, поскольку R/M — поле).

Условия (i) и (ii) означают, что кольцо R раскладывается в прямую сумму $R = \bigoplus R/I_i$ [Bou61, Ch.2 §1, Утверждение 5]. Итак, $A = \sum A_{I_i}$ и элементы матрицы $A_{I_i} \in M_n(R/I_i)$ удовлетворяют уравнениям $f(a_{pq}) = 0$ для $f \in I_i$. Следовательно, $A_{I_i} = h_i g_i \in h_i G(\Phi, R/I_i)$ и $A = (\sum e_i h_i)(\sum g_i)$, где e_i — единица кольца R/I_i. Это завершает доказательство.

Другой подход к описанию автоморфизмов алгебр Шевалле был предложен в статье [Pia02].

ГЛАВА 28.
ЧИСЛО НЕРЕШЕНИЙ УРАВНЕНИЯ В ГРУППЕ И НЕТОПОЛОГИЗИРУЕМЫЕ ГРУППЫ БЕЗ КРУЧЕНИЯ

1. Введение

Основная теорема. *Существует такая конечно порождённая группа без кручения H и такое уравнение $w(x) = 1$ (где $w(x) \in H * \langle x \rangle_\infty$) над ней, что решениями этого уравнения являются все элементы группы H, кроме одного:*

$$\{h \in H \mid w(h) \neq 1\} = \{1\}. \tag{1}$$

Замечание. Из теоремы Лёвенгейма–Сколема следует, что слова «конечно порождённая» в основной теореме могут быть заменены на слова «произвольной бесконечной мощности» (вместе с группой H требуемым свойством обладают, например, любые её ультрастепени, и их подгруппы, содержащие диагональ).

Поскольку множество решений любого уравнения замкнуто в любой отделимой групповой топологии, мы получаем ответ на вопрос П. И. Кирку [НЗТА85, вопрос 1.4]:

Следствие. *Существует нетривиальная счётная нетопологизируемая группа без кручения.*

Отметим, что, согласно теореме Маркова [М46], дополнение до единицы во всякой счётной нетопологизируемой группе должно разлагаться в объединение множеств решений конечного числа систем уравнений. В известных примерах бесконечных счётных нетопологизируемых групп эти разложения выглядят так:

$$G \setminus \{g_1, \dots, g_n\} = \bigcup_{i=1}^{n-1} \{g \in G \mid g^n = g_i\} \quad \text{(пример Ольшанского}^{**}\text{ [О80], [О89] и его модификации [МО98]);}$$

$$G \setminus \{g_1, \dots, g_{2n}\} = \{g \in G \mid [g, a]^n = 1\} \quad \text{(примеры из [Т04]).}$$

Здесь g_i и a — некоторые фиксированные элементы соответствующей группы G, а число n в обоих случаях является большим (по меньшей мере 665) и нечётным. Разложение (1) представляется максимально простым. Отметим однако, что уравнение $w(x) = 1$, построенное при доказательстве основной теоремы, является гораздо более замысловатым (см. формулы $(**)$ и $(*)$), чем уравнения $x^n = a$ и $[x, a]^n = 1$, фигурирующие в ранее известных примерах счётных нетопологизируемых групп. Отметим ещё, что пример Ольшанского и его модификации является периодическим (при этом примеры Морриса и Образцова [МО98] являются квазициклическими); примеры из [Т04] имеют кручение, но периодическими не являются, более того, в [Т04] показано, что любая счётная группа может быть вложена в один из таких примеров.

Естественно задать вопрос, какие значения могут принимать мощность множества решений уравнения в группе и мощность дополнения до этого множества? Из основной теоремы нетрудно вывести такой факт:

Теорема 1. *Для любых двух кардиналов* $\mathbf{s}$ *и* $\mathbf{n}$*, по крайней мере один из которых бесконечен, найдётся такая группа G (мощности $\mathbf{s} + \mathbf{n}$) и такое уравнение $u(x) = 1$ над ней, что ровно* $\mathbf{s}$ *элементов группы G являются решениями этого уравнения и ровно* $\mathbf{n}$ *элементов группы G не являются решениями этого уравнения.*

Замечание. Условие бесконечности одного из кардиналов здесь существенно. Например, нетрудно сообразить, что в группе порядка три число решений никакого уравнения не может быть равно двум.

** Пример Ольшанского является факторгруппой по центральной подгруппе группы, построенной Адяном [Адян71].

2. Подход Ольшанского к построению групп с заданными свойствами

Градуированным копредставлением мы называем групповое копредставление $G(\infty) = \langle \mathcal{A} \mid \mathcal{R} \rangle$, на множестве определяющих соотношений которого задана фильтрация

$$\mathcal{R} = \bigcup_{i=0}^{\infty} \mathcal{R}_i, \quad \varnothing = \mathcal{R}_0 \subseteq \mathcal{R}_1 \subseteq \dots.$$

Соотношения из $\mathcal{R}_i \setminus \mathcal{R}_{i-1}$ мы называем *соотношениями ранга* i, а копредставление $\langle \mathcal{A} \mid \mathcal{R}_i \rangle$ мы обозначаем $G(i)$ и рассматриваем как градуированное копредставление (полагая $\mathcal{R}_j = \mathcal{R}_i$ при $j > i$).

В соответствии с [O89], мы говорим, что градуированное копредставление $G(\infty)$ без периодических соотношений удовлетворяет *условию* R (с параметрами α, h, d и n), если, для каждого i, найдётся такое множество $\mathcal{X}_i \subseteq F$ слов (называемых *периодами ранга* i), что

1) длина каждого слова из $\mathcal{X}_i$ равна i и никакое слово из $\mathcal{X}_i$ не сопряжено в $G(i-1)$ степени слова меньшей длины;
2) различные слова из $\mathcal{X}_i$ не сопряжены между собой и не сопряжены к обратным друг другу в $G(i-1)$;
3) каждое соотношение $R \in \mathcal{R}_i \setminus \mathcal{R}_{i-1}$ имеет вид

$$R \equiv \prod_{k=1}^{h} (T_k A^{n_k}), \text{ где } A \in \mathcal{X}_i,$$

причём выполнены условия:

R1. $n_k \geqslant n$.

R2. $|n_i|/|n_j| \leqslant 1 + \frac{1}{2}h^{-1}$.

R3. никакое из слов T_k не равно в $G(i-1)$ слову меньшей длины и $|T_k| < di$.

R4. $T_k \notin \langle A \rangle$ в группе $G(i-1)$.

R5. Слово R не является истинной степенью в свободной группе и, если $V \equiv A^{n_s - 1} \prod_{k=s}^{s+l} (T_k A^{n_k})$ — циклическое подслово в R, $l \geqslant \alpha^{-1} - 4$ и VV_1, VV_2 — циклические сдвиги слова R, то $V_1 \equiv V_2$;

R6. Пусть $V \equiv A^{m_1} T_k A^{n_k} \dots T_{k+l} A^{m_2}$ — подслово циклического сдвига соотношения R, где $l \geqslant \alpha^{-1} - 2$, а $V' \equiv A^{m_1'} T_{k'}' A^{n_k'} \dots T_{k'+l}' A^{m_2'}$ — подслово циклического сдвига соотношения $(R')^{\pm 1}$ с тем же периодом A, причём знаки показателей m_1 и m_1', n_k и n_k', …, m_2 и m_2' совпадают. Пусть V и V' графически разлагаются в произведения $V_0 \dots V_l$ и $V_0' \dots V_l'$, где $V_0 \equiv A^{m_1} T_k A^{c_1}$, $V_1 \equiv A^{b_1} T_{k+1} A^{c_2}$, …, $V_l \equiv A^{b_l} T_{k+l} A^{m_2}$, $V_0' \equiv A^{m_1'} T_{k'}' A^{c_1'}$, $V_1' \equiv A^{b_1'} T_{k'+1}' A^{c_2'}$, …, $V_l \equiv A^{b_l'} T_{k'+l}' A^{m_2'}$; причём в группе $G(i-1)$ имеют место равенства $V_j = V_j'$ при $j = 0, \dots, l$. Тогда $R' \equiv R$, $V' \equiv V$ и V не является подсловом циклического слова R^{-1}.

В книге [O89] можно найти много полезных свойств копредставлений с условием R. Упомянем некоторые из этих свойств.

Лемма 1. *Пусть градуированное копредставление $G(\infty)$ удовлетворяют условию* R *для достаточно маленького числа α и достаточно больших чисел h, d и n ($1 \ll \alpha^{-1} \ll h \ll d \ll n$). Тогда*

1) *абелевы подгруппы группы $G(\infty)$ являются циклическими;*
2) *группа $G(\infty)$ не имеет кручения;*
3) *если элементы X и Y сопряжены в $G(\infty)$, то найдётся такой элемент $Z \in G(\infty)$, что $X = ZYZ^{-1}$ и $|Z| \leqslant (\frac{1}{2} + \alpha)(|X| + |Y|)$;*
4) *если A, B и C — неединичные элементы группы $G(\infty)$ и X — такой элемент, что $X^{-1}AXB$ и C сопряжены в $G(\infty)$, то в двойном смежном классе $\langle A \rangle X \langle B \rangle$ найдётся элемент X' длины меньшей, чем $(\frac{1}{2} + \alpha)(|A| + |B| + |C|) + \left[\frac{1}{2}|A|\right] + \left[\frac{1}{2}|B|\right]$* (здесь квадратные скобки обозначают целую часть числа);
5) если слово X равно единице в $G(\infty)$, то $X = 1$ в группе $\left\langle \mathcal{A} \;\middle|\; \{R \in \mathcal{R} \mid |R| < (1-\alpha)^{-1}|X|\} \right\rangle$.
6) если элементы X и ZXZ^{-1} коммутируют в $G(\infty)$, то X и Z коммутируют в $G(\infty)$.

Доказательство. Все эти свойства доказаны в [O89]: первое утверждение является одним из утверждений теоремы 26.5; второе утверждение является частным случаем леммы 25.2; третье утверждение представляет собой лемму 25.4; четвёртое утверждение есть перевод на алгебраический язык несколько ослабленной формулировки леммы 22.2 о разрезах диаграмм на сфере с тремя дырами; пятое утверждение есть перевод на алгебраический язык леммы 23.16; а шестое утверждение совпадает леммой 25.14.

3. Конструкция группы H

Зафиксируем достаточно большое чётное число h и целое число $n \gg h$. В качестве алфавита $\mathcal{A}$ возьмём множество букв $\{a, b, c_1, c_2, \ldots, c_h\}$. Свободную группу с базисом $\mathcal{A}$ обозначим буквой F.

Положим $\mathcal{R}_0 = \mathcal{R}_1 = \mathcal{R}_2 = \varnothing$. Далее, при $i > 2$, предполагая, что копредставление $G(i-1) = \langle \mathcal{A} \mid \mathcal{R}_{i-1} \rangle$ уже определено, определим копредставление $G(i) = \langle \mathcal{A} \mid \mathcal{R}_i \rangle$. В качестве периодов ранга i возьмём некоторое множество слов $\mathcal{X}_i \subset F$ длины i, удовлетворяющее условиям

1) никакое слово из $\mathcal{X}_i$ не сопряжено в $G(i-1)$ слову меньшей длины;
2) различные слова из $\mathcal{X}_i$ не сопряжены между собой и не сопряжены к обратным друг другу в группе $G(i-1)$;
3) каждое слово из $\mathcal{X}_i$ равно ab в $G(i-1)/([G(i-1), G(i-1)]\,\langle c_1 c_2 \ldots c_h \rangle)$;
4) множество $\mathcal{X}_i$ максимально среди всех множеств, удовлетворяющих условиям 1), 2) и 3).

Определим множество $\mathcal{Y}_{i,j,Z} \subseteq F$, где $j = 1, \ldots, h$, $Z \in G(i-1)$, как множество всех минимальных (то есть не равных словам меньшей длины) в $G(i-1)$ слов длины меньшей чем di, представляющих в $G(i-1)$ элемент $Z c_j Z^{-1}$. Положим

$$\mathcal{R}_i = \mathcal{R}_{i-1} \cup \mathcal{T}_i,$$

где $\mathcal{T}_i$ есть максимальное множество попарно несопряжённых в $G(i-1)$ слов вида

$$R = R_{A,Z} = \prod_{j=1}^{h} \left(T_j A^{(-1)^j n} \right), \quad \text{где } A \in \mathcal{X}_i,\ T_j \in \mathcal{Y}_{i,j,Z},\ Z \in G(i-1).$$

Лемма 2. *Градуированное копредставление*

$$H = G(\infty) = \langle \mathcal{A} \mid \mathcal{R} \rangle, \quad \text{где } \mathcal{R} = \bigcup_{i=0}^{\infty} \mathcal{R}_i,$$

удовлетворяет условию R.

Доказательство. Заметим, что по модулю коммутанта каждое из соотношений нашего копредставления имеет вид $c_1 c_2 \ldots c_h$, $T_j = c_j$, а каждый период имеет вид $ab(c_1 \ldots c_h)^k$; поэтому периоды не являются истинными степенями и условия 1), 2), R1, R2 и R3 выполнены по построению. Условие R4 очевидным образом выполнено даже по модулю коммутанта.

Поскольку, как известно, длинные общие подслова двух слов вида A^n обязаны быть согласованными, из невыполнения условия R5 следовало бы, что либо одно из слов T_j лежит в $\langle A \rangle$, либо два слова T_j с разными номерами j лежат в одном и том же двойном смежном классе по $\langle A \rangle$; ни то, ни другое очевидным образом невозможно даже по модулю коммутанта.

Предположим, что условие R6 не выполнено. Мы имеем равенство вида $T_j^{\pm 1} A^p = A^s T_{j'}'$ в $G(i-1)$. Рассматривая это равенство по модулю коммутанта, мы приходим к выводу, что $j = j'$, $p = s$ и $\pm 1 = 1$. Вспоминая, что $T_j = Z c_j Z^{-1}$ и $T_j' = Z' c_j (Z')^{-1}$ в группе $G(i-1)$, мы видим, что c_j коммутирует с $Z^{-1} A^p Z'$ в группе $G(i-1)$. Поскольку по индукции мы можем считать, что копредставление $G(i-1)$ удовлетворяет условию R, то есть, в частности, коммутировать в $G(i-1)$ могут только степени одного и того же элемента (по лемме 1), а c_j не являются истинными степенями (даже по модулю коммутанта), мы получаем равенство вида $Z^{-1} A^p Z' = c_j^k$. Но то, что условие R6 не выполнено для $G(i)$, означает, что подобные равенства выполняются в $G(i-1)$ для многих номеров j. А рассматривая два таких равенства

$$Z^{-1} A^p Z' = c_j^k \quad \text{и} \quad Z^{-1} A^{p_1} Z' = c_{j_1}^{k_1}$$

при $j \neq j_1$ по модулю коммутанта, мы приходим к выводу, что $k = 0$, то есть $Z' \in \langle A \rangle Z$ и слова R и R' представляют сопряжённые элементы группы $G(i-1)$, что по построению означает $R \equiv R'$.

4. Доказательство основной теоремы

Лемма 3. *Для каждого элемента g коммутанта группы H и слова A, сопряжённого в H элементу $g^{-1}agb$, найдётся такое слово Z длины не большей $\frac{1}{3}d|A|$, что $Z^{-1}AZ = g^{-1}agb$ в H.*

Доказательство. Согласно утверждению 4) леммы 1, $|a^p g b^r| < |A| + 2$ для некоторых целых p и r (здесь и далее речь идёт о длинах элементов в $H = G(\infty)$). Но рассмотрев элемент $a^p g b^r$ по модулю коммутанта, мы видим, что $|a^p g b^r| \geqslant |p| + |r|$ и, следовательно,

$$|g| \leqslant |p| + |r| + |a^p g b^r| \leqslant 2|a^p g b^r| < 2|A| + 4 \quad \text{и} \quad |g^{-1}agb| < 4|A| + 10.$$

Из последнего неравенства по утверждению 3) леммы 1 вытекает, что найдётся такой элемент Z, что

$$Z^{-1}AZ = g^{-1}agb$$

и

$$|Z| \leqslant |A| + |g^{-1}agb| < 5|A| + 10 < \frac{1}{3}d|A|$$

(последнее неравенство обеспечивается тем, что $d \gg 1$).

Рассмотрим уравнение

$$v(x) = 1, \quad \text{где } v(x) \equiv \prod_{j=1}^{h} \left(c_j (x^{-1}axb)^{(-1)^j n}\right) \in H * \langle x \rangle_\infty , \tag{$*$}$$

над группой H.

Лемма 4. *В группе H всякий неединичный элемент коммутанта является решением уравнения $(*)$, а единица не является решением этого уравнения.*

Доказательство. То, что $v(1) \neq 1$, вытекает из утверждения 5) леммы 1, поскольку $v(1) \neq 1$ в свободной группе, а длина каждого определяющего соотношения R группы H не меньше, чем $3(n - d - 2)h$, и

$$\frac{|v(1)|}{|R|} \leqslant \frac{2n+1}{3(n-d-2)} < 1 - \alpha \quad \text{при } \alpha < \frac{1}{3} \text{ и } n \gg d.$$

Покажем теперь, что всякий неединичный элемент g коммутанта группы H является решением уравнения $(*)$. Пусть $u \in F$ — слово минимальной длины, представляющее элемент, сопряжённый к $g^{-1}agb$.

Если $|u| \leqslant 2$, то $u = ab$ или $u = ba$ (в чём легко убедиться рассматривая u по модулю коммутанта). При этом, в соответствии с утверждением 4) леммы 1, u сопряжено с элементом вида $\widetilde{g}^{-1}a\widetilde{g}b$, где $\widetilde{g} \in \langle a \rangle g \langle b \rangle$ и $|\widetilde{g}| < 3$. Рассматривая $\widetilde{g}$ по модулю коммутанта, мы видим, что

$$\widetilde{g} \text{ есть } \text{ либо } 1, \text{ либо } a^{\pm 1}, \text{ либо } b^{\pm 1}, \text{ либо } a^{\pm 1}b^{\pm 1}, \text{ либо } b^{\pm 1}a^{\pm 1}.$$

Первые 4 случая невозможны, поскольку они означают, что $g \in \langle a \rangle \langle b \rangle \cap [H, H] = \{1\}$. А в том, что равенство $\widetilde{g} = b^{\pm 1}a^{\pm 1}$ невозможно, легко убедиться рассматривая соотношение $\widetilde{g}^{-1}a\widetilde{g}b \sim u \sim ab$ по модулю нормальной подгруппы $\langle\langle c_1, \ldots, c_h \rangle\rangle$, порождённой $\{c_1, \ldots, c_h\}$, так как $G(\infty)/\langle\langle c_1, \ldots, c_h \rangle\rangle$ есть свободная группа с базисом $\{a, b\}$.

Мы показали, что $|u| > 2$. Но в таком случае, u сопряжено с некоторым периодом A ранга $|u|$ (по определению множества $\mathcal{X}_{|u|}$). По лемме 3, $Z^{-1}AZ = g^{-1}agb$ для некоторого слова Z длины не большей, чем $\frac{1}{3}d|A|$. Следовательно, для каждого $j = 1, \ldots, h$, некоторое минимальное слово T_j, представляющее в $G(|u| - 1)$ элемент Zc_jZ^{-1}, имеет длину меньшую, чем $d|A|$, и, стало быть, по построению, слово

$$\prod_{j=1}^{h} \left(T_j A^{(-1)^j n}\right)$$

сопряжено к одному из определяющих соотношений группы $G(|u|)$, что и доказывает лемму.

Лемма 5. *Множество решений уравнения*

$$[c_1 v([a,x])c_1^{-1}, v([b,x])] = 1 \qquad (**)$$

над H есть $H \setminus \{1\}$.

Доказательство. Поскольку a не является истинной степенью (по модулю коммутанта), согласно лемме 1, $[a,g] \neq 1$ при $g \notin \langle a \rangle$. Следовательно, по лемме 4, все элементы группы H, не лежащие в $\langle a \rangle$, являются решениями уравнения $(**)$. По тем же причинам все элементы группы H, не лежащие в $\langle b \rangle$, являются решениями уравнения $(**)$. Но $\langle a \rangle \cap \langle b \rangle = \{1\}$, в чём легко убедиться, опять рассмотрев факторгруппу по коммутанту.

Осталось доказать, что единица не является решением уравнения $(**)$. Предположив противное, мы бы имели $[c_1 v(1) c_1^{-1}, v(1)] = 1$. По утверждению 6) леммы 1, это означает, что $[c_1, v(1)] = 1$. Последнее равенство в свою очередь означает, что $v(1) \in \langle c_1 \rangle$ (по лемме 1 и поскольку c_1 не является истинной степенью (по модулю коммутанта)). Рассматривая равенство $v(1) = c_1^k$ по модулю коммутанта, мы приходим к выводу, что $k = 0$ и $v(1) = 1$, что противоречит лемме 4.

Лемма 5 доказана, а вместе с ней доказана и основная теорема, поскольку, согласно лемме 1, группа H не имеет кручения.

5. Доказательство теоремы 1

Если $\mathbf{n} = 0$, $\mathbf{s} = 0$ или $\mathbf{s} = 1$, то «уравнения» $1 = 1$, $g = 1$ (где g — нетривиальный элемент группы) и $x = 1$ над группой подходящей мощности очевидным образом обладают нужными свойствами.

Если $1 < \mathbf{s} \leqslant \mathbf{n}$, то в качестве группы G можно взять свободное произведение произвольной абелевой группы A мощности $\mathbf{s}$ и произвольной группы B мощности $\mathbf{n}$. Нетрудно сообразить, что решениями уравнения $xa = ax$, где $a \in A \setminus \{1\}$, будут все элементы группы A и только они. Таким образом, число решений будет равно $\mathbf{s}$, а число нерешений будет равно $\mathbf{n}$ (поскольку кардинал $\mathbf{n}$ бесконечен и не меньше, чем $\mathbf{s}$).

Если $\mathbf{s} > \mathbf{n} > 0$, то в качестве группы G можно взять прямое произведение группы H мощности $\mathbf{s}$, существование которой утверждается в основной теореме и в замечании после неё, и произвольной группы K мощности $\mathbf{n}$. В качестве уравнения следует взять уравнение $w(x) = 1$ из основной теоремы. Поскольку построенное при доказательстве основной теоремы уравнение $(**)$ имеет нулевую сумму показателей при x, множеством его решений в группе $G = H \times K$ будет $(H \setminus \{1\}) \times K$, а множеством его нерешений будет $\{1\} \times K$, что и влечёт утверждение теоремы.

ЗАКЛЮЧЕНИЕ

Получены новые результаты, относящиеся
- в основном к теории групп (и конечных, и бесконечных),
- а также (в некоторой степени) к теории колец и конечных полей,
- к универсальным алгебрам
- и графам.

Осталось много открытых вопросов, заслуживающих дальнейшего изучения (смотрите соответствующие главы).

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

[Абе93] Э. Абе, Автоморфизмы групп Шевалле над коммутативными кольцами, Алгебра и Анализ., 5:2 (1993), 74-90.

[Адян71] С. И. Адян, О некоторых группах без кручения, Изв. АН СССР, сер. матем., 35:3 (1971), 459-468.

[Адян75] С. И. Адян, Проблема Бернсайда и тождества в группах. М.: Наука, 1975.

[Б81] С. Д. Бродский, Аномальные произведения локально индикабельных групп, в сборнике Алгебраические системы. Ивановскии государственный университет. Иваново. 1981. 51-77.

[Б84] С. Д. Бродский, Уравнения над группами и группы с одним определяющим соотношением, Сиб. матем. ж., 25:2 (1984), 84-103.

[БаОл75] Ю. А. Бахтурин , А. Ю. Ольшанский, Тождественные соотношения в конечных кольцах Ли, Матем. сб., 96(138):4 (1975), 543-559.

[БаОл88] Ю.А. Бахтурин, А.Ю. Ольшанский, Тождества, Алгебра-2, Итоги науки и техн., Сер. Соврем. пробл. мат. Фундам. направления, 18, ВИНИТИ, М., 1988, 117-240.

[БеК03] В.В. Беляев, М. Кузуджуоглу, Локально конечные едва транзитивные группы, Алгебра и Логика, 42:3 (2003), 261-270.

[Бело99] А. Я. Белов, О нешпехтовых многообразиях, Фундамент. и прикл. матем., 5:1 (1999), 47-66.

[Бо72] А. Борель, Линейные алгебраические группы, М.: Мир, 1972.

[Бун07] Е. И. Бунина, Автоморфизмы элементарных присоединённых групп Шевалле типов A_l, D_l, E_l над локальными кольцами с 1/2, Алгебра и логика, 48:4 (2009), 443-470. См. также arXiv:math/0702046.

[ВГН06] Н. А. Вавилов, М. Р. Гаврилович, С. И. Николенко, Строение групп Шевалле: доказательство из книги, Зап. Научн. Сем. С-Петерб. Отд. Мат. Инст. Акад. Наук СССР., 330:13 (2006) 36-76.

[ВО88] Э. Б. Винберг, А. Л. Онищик, Семинар по группам Ли и алгебраическим группам, М., Наука 1988.

[ВаЗе89] А. Я. Вайс, Е. И. Зельманов, Теорема Кемера для конечно порожденных йордановых алгебр, Изв. вузов. Сер. матем., 6 (1989), 63-72.

[Вас13] А. Н. Васильев, Казахстанская республиканская олимпиада по математике. 2013. Заключительный этап. 9 класс. Задача 4. `http://matol.kz/olympiads/151`

[Вас14] А. Н. Васильев, Девятая студенческая олимпиада по алгебре в МГУ. 2014. Задача 3. `http://halgebra.math.msu.su/Olympiad/`

[Вд00] Е. П. Вдовин, Большие нормальные нильпотентные подгруппы конечных групп, Сибирский математический журнал, 41:2 (2000), 304-310.

[Ви49] А. А. Виноградов, О свободном произведении упорядоченных групп, Матем. сб., 25(67):1 (1949), 163-168.

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

[ГКП18] Н. Л. Гордеев, Б. Э. Кунявский, Е. Б. Плоткин, Геометрия вербальных уравнений в простых алгебраических группах над специальными полями, УМН, 73:5(443) (2018), 3-52.
См. также arXiv:1808.02303.

[ГШ64] Е. С. Голод, И. Р. Шафаревич, О башне полей классов, Изв. АН СССР. Сер. матем., 28:2 (1964), 261-272.

[Гол97] И. З. Голубчик, Группы лиевского типа над PI-кольцами, Фунд. и Прикл. Мат., 3:2 (1997) 399-424.

[ГМи83] И. З. Голубчик, А. В. Михалёв, Изоморфизмы унитарных групп над ассоциативными кольцами, Зап. Научн. Сем. Ленингр. Отд. Мат. Инст. Акад. Наук СССР., 132 (1983), 97-109.

[Гриш99] А. В. Гришин, Примеры не конечной базируемости T-пространств и T-идеалов в характеристике 2, Фундамент. и прикл. матем., 5:1 (1999), 101-118.

[Зайц78] М. В. Зайцев, О конечной базируемости многообразий алгебр Ли, Матем. сб., 106(148) (1978), 499-506.

[Зал83] А. Е. Залесский, Линейные группы. Итоги науки и техн. ВИНИТИ. Алгебра. Топология. Геометрия. 1983. 135-182.

[Зел85] Е. И. Зельманов, Изоморфизмы линейных групп над ассоциативным кольцом, Сибирск. матем. журн., 26:4 (1985), 49-67.

[Ива13] А. В. Иванищук, Из опыта учебно-исследовательской деятельности учащихся в лицее 1511 при МИФИ, в книге *Сгибнев А. И. Исследовательские задачи для начинающих. Москва: МЦНМО, 2013.* (Доступна здесь: `http://www.mccme.ru/free-books/`)

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

[Кеме87] А. Р. Кемер, Конечная базируемость тождеств ассоциативных алгебр, Алгебра и логика, 26:5 (1987), 597-641.

[Крас90] А. Н. Красильников, О конечности базиса тождеств групп с нильпотентным коммутантом, Изв. АН СССР. Сер. матем., 54:6 (1990), 1181-1195.

[Кур62] А. Г. Курош, Лекции по общей алгебре. М.: Физ.-мат. лит., 1962.

[Кур67] А. Г. Курош, Теория групп. М.: Наука, 1967.

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

[Латы73] В. Н. Латышев, О некоторых многообразиях ассоциативных алгебр, Изв. АН СССР. Сер. матем., 37:5 (1973), 1010-1037.

[Лев83] В. М. Левчук Связи унитреугольной группы с некоторыми кольцами. II. Группы автоморфизмов, Сибирск. матем. журн., 24:4 (1983) 543-557.

[Ло86] К. И. Лоссов, SQ-универсальность свободных произведений с конечными объединёнными подгруппами, Сиб. матем. ж., 27:6 (1986), 128-139.

[Льво73] И. В. Львов, О многообразиях ассоциативных колец, I, Алгебра и логика, 12 (1973), 269-297.

[М46] А. А. Марков, О безусловно замкнутых множествах, Мат. сборник, 18:1(1946), 3-28.

[МКС74] В. Магнус, А. Каррас, Д. Солитэр, Комбинаторная теория групп. М.: Наука, 1974.

[МаХ07] Н. Ю. Макаренко, Е. И. Хухро, Большие характеристические подгруппы, удовлетворяющие полилинейным коммутаторным тождествам, ДАН, 412:5 (2007), 594-596.

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

[Маль40] А. И. Мальцев, Об изоморфном представлении бесконечных групп матрицами, Матем. сб., 8(50):3 (1940), 405-422.

[Мо69] Д. И. Молдаванский, Об одной теореме Магнуса, Уч. зап. Ивановск. гос. пед. ин-та, 44 (1969), 26-28.

[НЗТА85] Нерешённые задачи топологической алгебры. (ред. В.И.Арнаутов, А.В.Архангельский, П.И.Кирку, А.В.Михалёв, Ю.Н. Мухин, И.В.Протасов, М.М.Чобан), Кишинёв: Штиинца, 1985.

[Нейм69] Х. Нейман, Многообразия групп. М.: Мир, 1969.

[Нос16] Г. А. Носков, Доказательство Минеева-Дикса HN-гипотезы и характеристика Эйлера-Пуанкаре, Мат. заметки, 99:3 (2016), 376-383.

[О70] А. Ю. Ольшанский, О проблеме конечного базиса тождеств в группах, Изв. АН СССР. Сер. матем., 34:2 (1970), 376-384.

[О80] А. Ю. Ольшанский, Замечание о счётной нетопологизируемой группе, Вестн. МГУ: мат., мех., 1980:3 (1980), 103-103.

[О89] А. Ю. Ольшанский, Геометрия определяющих соотношений в группах. М.: Наука, 1989.

[О95] А. Ю. Ольшанский, SQ-универсальность гиперболических групп, Мат. Сборник, 186:8 (1995), 119-132.

[ОА91] В. А. Артамонов, В. Н. Салий, Л. А. Скорняков, Л. Н. Шеврин, Е. Г. Шульгейфер, Общая алгебра, 2, М.: Наука, 1991.

[Пет82] В. М. Петечук, Автоморфизмы матричных групп над коммутативными кольцами, Мат. Сб., 117:4 (1982), 534-547.

[Ром77] Н. С. Романовский, Свободные подгруппы в конечно-определенных группах, Алгебра и логика, 16:1 (1977), 88-97.

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

[Стру95] С. П. Струнков, К теории уравнений на конечных группах, Изв. РАН., Сер. матем., 59:6 (1995), 171-180.

[Т04] А. В. Трофимов, Теорема вложения в нетопологизируемую группу, Вестн. МГУ: мат., мех., 2007:1 (2007), 7-13.

[Шем78] Л. А. Шеметков, Формации конечных групп. М.: Наука, 1978.

[Щиго99] В. В. Щиголев, Примеры бесконечно базируемых Т-идеалов, Фундамент. и прикл. матем., 5:1 (1999), 307-312.

[ACNT13] T. Asai, N. Chigira, T. Niwasaki, Yu. Takegahara, On a theorem of P. Hall, Journal of Group Theory, 16:1 (2013), 69-80.

[AHu88] E. Abe, J. Hurley, Centers of Chevalley groups over commutative rings, Comm. Algebra, 16:1 (1988), 57-74.

[AMO07] G. Arzhantseva, A. Minasyan, D. Osin, The SQ-universality and residual properties of relatively hyperbolic groups, Journal of Algebra, 315:1 (2007), 165-177. См. также arXiv:math.GR/0601590.

[AMS14] Y. Antolín, A. Martino, I. Schwabrow, Kurosh rank of intersections of subgroups of free products of right-orderable groups, Mathematical Research Letters, 21:4 (2014), 649-661. См. также arXiv:1109.0233.

[ASS15] V. Araújo, P. V. Silva, M. Sykiotis, Finiteness results for subgroups of finite extensions, J. Algebra, 423 (2015), 592-614. См. также arXiv:1402.0401.

[AST13] A. Arikan, H. Smith, N. Trabelsi, On certain application of the Khukhro-Makarenko theorem, Glasgow Math. J., 55(2013), 275-283.

[ASu76] E. Abe, K. Suzuki, On normal subgroups of Chevalley groups over commutative rings, Tôhoku Math. J., 28:1 (1976), 185-198.

[Abe89] E. Abe, Normal subgroups of Chevalley groups over commutative rings, Contemp. Math., 83 (1989), 1-117.

[AmV11] A. Amit, U. Vishne, Characters and solutions to equations in finite groups, J. Algebra Its Appl., 10:4 (2011), 675-686.

[And16] R. Andreev, A translation of "Verallgemeinerung des Sylow'schen Satzes" by F. G. Frobenius, arXiv:1608.08813.

[AsTa01] T. Asai, Yu. Takegahara, $|\mathrm{Hom}(A,G)|$, IV, J. Algebra, 246 (2001), 543-563.

[AsYo93] T. Asai, T. Yoshida, $|\mathrm{Hom}(A,G)|$, II, J. Algebra, 160 (1993), 273-285.

[BGGT12] E. Breuillard, B.Green, R. Guralnick, T. Tao, Strongly dense free subgroups of semisimple algebraic groups, Israel Journal of Mathematics, 192:1 (2012), 347-379. См. также arXiv:1010.4259.

[BMRe99] G. Baumslag, A. Myasnikov, V. Remeslennikov, Algebraic geometry over groups I. Algebraic sets and ideal theory, J. Algebra., 219 (1999), 16-79.

[BMRo97] G. Baumslag, A. Myasnikov, V. Roman'kov, Two theorems about equationally Noetherian groups, J. Algebra., 194 (1997), 654-664.

[BMS87] G. Baumslag, J. W. Morgan, P. B. Shalen, Generalized triangle groups, Math. Proc. Camb. Phil. Soc., 102 (1987), 25-31.

[BaPr78] B. Baumslag, S. Pride, Groups with two more generators than relators, J. London Math. Soc., 17 (1978), 425-426.

[BaTa68] G. Baumslag, T. Taylor, The centre of groups with one defining relator, Math. Ann., 175 (1968), 315-319.

[BoP92] W.A. Bogley, S. J. Pride, Aspherical relative presentations, Proc. Edinburgh Math. Soc. II, 35:1, (1992), 1-39.

[Bog18] O. Bogopolski, Equations in acylindrically hyperbolic groups and verbal closedness, arXiv:1805.08071.

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

[Bor70] A. Borel, Properties and linear representations of Chevalley groups. In Semin. Algebr. Groups related Finite Groups Princeton 1968/69, Lect. Notes Math. 131, A1-A55 (1970).

[Bou61] N. Bourbaki, Éléments de Mathématique. Algèbre commutative. Chapitres 1 et 2. Paris: Hermann. 1961.

[Boy88] S. Boyer, On proper powers in free products and Dehn surgery, J. Pure Appl. Algebra, 51:3 (1988), 217-229.

[Bra69] R. Brauer, On A Theorem of Frobenius, The American Mathematical Monthly, 76:1 (1969), 12-15.

[BrNa04] B. Bruno, F. Napolitani, A note on nilpotent-by-Černikov groups, Glasgow Math. J., 46 (2004), 211-215.

[BrTh88] K. Brown, J. Thévenaz, A generalization of Sylow's third theorem, J. Algebra, 115 (1988), 414-430.

[Bro00] K. S. Brown, The coset poset and probabilistic zeta function of a finite group, J. Algebra, 225 (2000), 989-1012.

[Bum04] I. Bumagina, The conjugacy problem for relatively hyperbolic groups, Algebraic & Geometric Topology, 4 (2004), 1013-1040. См. также arXiv:math/0308171.

[Bu05] J. O. Button, Large mapping tori of free group endomorphisms, arXiv:math.GR/0511715.

[But08] J. O. Button, Largeness of LERF and 1-relator groups, arXiv:0803.3805, 2008.

[Ch18] L. Chen, Spectral gap of scl in free products, Proc. Amer. Math. Soc., 146:7 (2018), 3143-3151. См. также arXiv:1611.07936.

[C02] A. Clifford, A class of exponent sum two equations over groups, Glasgow Math. J., 44 (2002) 201-207.

[C03] A. Clifford, Nonamenable type K equations over groups, Glasgow Math. J., 45 (2003), 389-400.

[CCE91] J. A. Comerford, L. P. Comerford, C. C. Edmunds, Powers asproducts of commutators, Comm. Algebra, 19 (1991), 675-684.

[CER94] L. P. Comerford, C. C. Edmunds, G. Rosenberger, Commutators as powers in free products of groups, Proc. Amer. Math. Soc., 122 (1994), 47-52.

[CG00] A. Clifford, R. Z. Goldstein, Equations with torsion-free coefficients, Proc. Edinburgh Math. Soc., 43:2 (2000), 295-307.

[CG95] A. Clifford, R. Z. Goldstein, Tesselations of S^2 and equations over torsion-free groups, Proc. Edinburgh Math. Soc., 38 (1995), 485-493.

[CKe99] D. L. Costa, G. E. Keller, On the normal subgroups of $G_2(A)$, Trans. Amer. Math. Soc., 351:12 (1999), 5051-5088.

[CR01] M. M. Cohen, C. Rourke, The surjectivity problem for one-generator, one-relator extensions of torsion-free groups, Geometry & Topology, 5 (2001), 127-142. См. также arXiv:math.GR/0009101..

[ChD89] A. Chermak, A. Delgado, A measuring argument for finite group. Proc. Amer. Math. Soc., 107 (1989), 907-914.

[Che00] Yu Chen, Isomorphisms of Chevalley groups over algebras, J. Algebra, 226:2 (2000) 719-741.

[Che95] Yu Chen, Automorphisms of simple Chevalley groups over $\mathbb{Q}$-algebras, ,Tôhoku Math. J., 47:1 (1995), 81-97.

[Che96] Yu Chen, Isomorphisms of adjoint Chevalley groups over integral domains, Trans. Amer. Math. Soc., 348:2 (1996), 521-541.

[CoLy63] D. E. Cohen, R. C. Lyndon, Free bases for normal subgroups of free groups, Trans. Amer. Math. Soc., 108 (1963), 528-537.

[Coll10] D. J. Collins, Generating Sequences of Finite Groups. Senior Thesis. Cornell University Mathematics Department, 2010. (Доступно здесь: `http://www.math.cornell.edu/m/sites/default/files/imported/Research/SeniorTheses/2010/collinsThesis.pdf`)

[Corn13] Y. Cornulier (http://mathoverflow.net/users/14094/yves-cornulier), Large abelian characteristic subgroups in abelian-by-countable groups, URL (version: 2013-12-15): http://mathoverflow.net/q/151889

[Cull81] M. Culler, Using surfaces to solve equations in free groups, Topology, 20 (1981), 133-145.

[D12] W. Dicks, Simplified Mineyev, `https://mat.uab.cat/~dicks/pub.html`.

[dGT18a] F. de Giovanni, M. Trombetti, A note on large characteristic subgroups. Communications in Algebra, 46:11 (2018), 4654-4662.

[dGT18b] F. de Giovanni, M. Trombetti, Large characteristic subgroups with modular subgroup lattice, Archiv der Mathematik, 111:2 (2018), 123-128.

[dGT19a] F. de Giovanni, M. Trombetti, Large characteristic subgroups in which normality is a transitive relation, Atti Accad. Naz. Lincei Cl. Sci. Fis. Mat. Natur. 30 (2019), 255-268.

[dGT19b] F. de Giovanni, M. Trombetti, Large characteristic subgroups and abstract group classes, Quaestiones Mathematicae (to appear).

[DuH91] A. J. Duncan, J. Howie, The genus problem for one-relator products of locally indicable groups, Math. Z., 208 (1991), 225-237.

[DuH92] A. J. Duncan, J. Howie, Weinbaum's conjecture on unique subwords of nonperiodic words, Proc. Amer. Math. Soc., 115 (1992), 947-954.

[DuH93] A. J. Duncan, J. Howie, One-relator products with high-powered relator, in: Geometric group theory (G.A.Niblo, M.A.Roller, eds.), 48-74, Cambridge Univ. Press, Cambridge (1993).

[DŠ20] W. Dicks, Z. Šunić, Orders on trees and free products of left-ordered groups, Canadian Mathematical Bulletin, 63:2 (2020), 335-347. См. также arXiv:1405.1676.

[Ed84] M. Edjvet, Groups with balanced presentations, Arch. Math., 42:4 (1984), 311-313.

[EH91] M. Edjvet, J. Howie, The solution of length four equations over groups, Trans. Amer. Math. Soc., 326 (1991), 345-369.

[EdJu00] M. Edjvet, A. Juhász, Equations of length 4 and one-relator products, Math. Proc. Cambridge Phil. Soc., 129:2 (2000), 217-230.

[Er12] M. Ershov, Golod-Shafarevich groups: a survey, Int. J. Algebra Comput. 22:5 (2012), 1230001. См. также arXiv:1206.0490.

[Far98] B. Farb, Relatively hyperbolic groups, GAFA, 8 (1998), 810-840.

[FeR96] R. Fenn, C. Rourke, Klyachko's methods and the solution of equations over torsion-free groups, L'Enseignment Mathématique, 42 (1996), 49-74.

[FeR98] R. Fenn, C. Rourke, Characterisation of a class of equations with solution over torsion-free groups, from "The Epstein Birthday Schrift", (I. Rivin, C. Rourke and C. Series, editors), Geometry and Topology Monographs., 1 (1998), 159-166.

[FeTh63] W. Feit, J. G. Thompson, Solvability of groups of odd order, Pacific J. Math., 13 (1963), 755-1029.

[FiR99] B. Fine, G. Rosenberger, Algebraic generalizations of discrete groups. A path to combinatorial group theory through one-relator products. Monographs and Textbooks in Pure and Applied Math. 223. Marcel Dekker, Inc., New York, 1999.

[FoR05] M. Forester and C. Rourke, Diagrams and the second homotopy group, Comm. Anal. Geom., 13 (2005), 801-820. См. также arXiv:math.AT/0306088.

[Fr14] J. Friedman, Sheaves on graphs, their homological invariants, and a proof of the Hanna Neumann conjecture. With an appendix by Warren Dicks, Mem. Amer. Math. Soc. 233:1100 (2014). См. также arXiv:1105.0129.

[Fr18] E. Frolova, Khukhro-Makarenko type theorems for algebras, arXiv:1804.00268.

[Frob95] F. G. Frobenius, Verallgemeinerung des Sylow'schen Satzes, Sitzungsberichte der Königl. Preuß. Akad. der Wissenschaften (Berlin) (1895), 981-993.

[Frob03] F. G. Frobenius, Über einen Fundamentalsatz der Gruppentheorie, Sitzungsberichte der Königl. Preuß. Akad. der Wissenschaften (Berlin) (1903), 987-991.

[GR62] M. Gerstenhaber, O.S. Rothaus, The solution of sets of equations in groups, Proc. Nat. Acad. Sci. USA, 48:9 (1962), 1531-1533.

[GRV12] C. Gordon, F. Rodriguez-Villegas, On the divisibility of $\#\mathrm{Hom}(\Gamma, G)$ by $|G|$, J. Algebra, 350:1 (2012), 300-307. См. также arXiv:1105.6066.

[Ger87] S. M. Gersten, Reducible diagrams and equations over groups. InEssays in group theory, 15-73. Springer, New York-Berlin, 1987.

[Gr83] M. Gromov, Volume and bounded cohomology, Inst. Hautes Etudes Sci. Publ. Math., 1982:56 (1983), 5-99.

[GuKr03] C. K. Gupta, A. N. Krasilnikov, The finite basis question for varieties of groups - Some recent results, Illinois Journal of Mathematics, 47:1-2 (2003), 273.

[HIÖ89] T. Hawkes, I. M. Isaacs, M. Özaydin, On the Möbius function of a finite group, Rocky Mountain J. Math., 19:4 (1989), 1003-1034

[HO'M89] A. J. Hahn, O. T. O'Meara, The classical groups and K-theory. Springer. Berlin et al. 1989.

[HW16] J. Helfer, D. T. Wise, Counting cycles in labeled graphs: the nonpositive immersion property for one-relator groups, International Mathematics Research Notices 2016:9 (2016), 2813-2827.

[HaV03] R. Hazrat, N. Vavilov, K_1 of Chevalley groups are nilpotent, J. Pure Appl. Algebra, 179 (2003), 99-116.

[Hall36a] P. Hall, The Eulerian functions of a group, Quart. J. Math. Oxford Ser., 7 (1936), 134-151.

[Hall36b] P. Hall, On a theorem of Frobenius, Proc. London Math. Soc. 40 (1936), 468-501.

[Higg56] P. J. Higgins, Groups with multiple operators, Proc. London Math. Soc. (3) 6 (1956), 366-416.

[How81] J. Howie, On pairs of 2-complexes and systems of equations over groups, J. Reine Angew Math., 1981:324 (1981), 165-174.

[How83] J. Howie, The solution of length three equations over groups, Proc. Edinburgh Math. Soc., 26 (1983), 89-96.

[How87] J. Howie, How to generalize one-relator group theory, in: Combinatorial group theory and topology (S.M. Gersten and J.R. Stallings, eds.), 53-78, Ann. of Math. Stud., 111, Princeton Univ. Press, (1987).

[How90] J. Howie, The quotient of a free product of groups by a single high-powered relator. II. Fourth powers, Proc. London Math. Soc., 61 (1990), 33-62.

[How91] J. Howie, The quotient of a free product of groups by a single high-powered relator. III: The word problem, Proc. Lond. Math. Soc., 62:3 (1991), 590-606.

[How98] J. Howie, Free subgroups in groups of small deficiency, J. Group Theory, 1:1 (1998), 95-112.

[Is08] I. M. Isaacs, Finite group theory, GSM 92, American Math. Soc., Providence RI, 2008.

[Isaa70] I. M. Isaacs, Systems of equations and generalized characters in groups, Canad. J. Math., 22 (1970), 1040-1046.

[Iv17] S. V. Ivanov, Intersecting free subgroups in free products of left ordered groups, Journal of Group Theory, 20:4 (2017), 807-821. См. также arXiv:1607.03010.

[Iwa82] S. Iwasaki, A note on the nth roots ratio of a subgroup of a finite group, J. Algebra, 78:2 (1982), 460-474.

[JZ17] A. Jaikin-Zapirain, Approximation by subgroups of finite index and the Hanna Neumann conjecture, Duke Mathematical Journal, 166:10 (2017), 1955-1987.

[Juhá03] Juhász A. On the solvability of a class of equations over groups, Math. Proc. Cambridge Phil. Soc., 135:2 (2003), 211-217.

[KPS73] A. Karrass, A. Pietrowski, D. Solitar, Finitely generated groups with a free subgroup of finite index, J. Austral. Math. Soc., 16 (1973), 458-466.

[KT84] C. Kratzer, J. Thévenaz, Fonction de Möbius d'un groupe fini et anneau de Burnside, Commentarii Mathematici Helvetici, 59:1 (1984), 425-438.

[KhV12] O. Kharlampovich, A. Vdovina, Linear estimates for solutions of quadratic equations in free groups, International Journal of Algebra and Computation, 22:01 (2012), 1250004. См. также arXiv:1107.2843.

[KhM07a] E. I. Khukhro, N. Yu. Makarenko, Large characteristic subgroups satisfying multilinear commutator identities, J. London Math. Soc., 75:3 (2007), 635-646.

[KhM07b] E. I. Khukhro, N. Yu. Makarenko, Characteristic nilpotent subgroups of bounded co-rank and automorphically-invariant ideals of bounded codimension in Lie algebras, Quart. J. Math., 58 (2007), 229-247.

[KhM08] E. I. Khukhro, N. Yu. Makarenko, Automorphically-invariant ideals satisfying multilinear identities, and group-theoretic applications, J. Algebra, 320:4 (2008), 1723-1740.

[KhM14] B. Khoussainov, A. Miasnikov, Finitely presented expansions of groups, semigroups, and algebras, Trans. Amer. Math. Soc. 366 (2014), 1455-1474.

[Ki18] K. Kishore, Representation variety of surface groups, Proc. Amer. Math. Soc. 146 (2018), 953-959. См. также arXiv:1702.05981.

[Kras09] A. N. Krasilnikov, A non-finitely based variety of groups which is finitely based as a torsion-free variety, Journal of Group Theory, 12:5 (2009), 735-743.

[Kruse73] R. L. Kruse, Identities satisfied by a finite ring, J. Algebra, 26 (1973), 298-318.

[Ku83] R. S. Kulkarni, An extension of a theorem of Kurosh and applications to Fuchsian groups, Michigan Mathematical Journal, 30:3 (1983), 259-272.

[Kula38] A. Kulakoff, Einige Bemerkungen zur Arbeit: "On a theorem of Frobenius" von P. Hall, Матем. сб., 3(45):2 (1938), 403-405.

[LL13] M. Larsen, A. Lubotzky, Representation varieties of Fuchsian groups, From Fourier analysis and number theory to radon transforms and geometry, 375-397, Dev. Math., 28, Springer, New York, 2013. См. также arXiv:1203.3408.

[LM11] S. Liriano, S. Majewicz, Algebro-geometric invariants of groups (the dimension sequence of representation variety), Int. J. Algebra Comput., 21:4 (2011), 595-614.

[LS05] M. Liebeck, A. Shalev, Fuchsian groups, finite simple groups and representation varieties, Inventiones mathematicae 159:2 (2005), 317-367.

[LT18] D. D. Long, M. B. Thistlethwaite, The dimension of the Hitchin component for triangle groups, Geometriae Dedicata (to appear).

[La05] M. Lackenby, Expanders, rank and graphs of groups, Israel Journal of Mathematics, 146:1 (2005), 357-370. См. также arXiv:math/0403127.

[Lang02] S. Lang, Algebra. New York, Berlin, Heidelberg: Springer-Verlag, 2002.

[Le09] Le Thi Giang, The relative hyperbolicity of one-relator relative presentations, Journal of Group Theory, 12:6 (2009), 949-959. См. также arXiv:0807.2487.

[Le62] F. Levin, Solutions of equations over groups, Bull. Amer. Math. Soc., 68:6 (1962), 603-604.

[Lee02] D. Lee, On certain C-test words for free groups, J. Algebra, 247 (2002), 509-540.

[Ly80] R.C. Lyndon, Equations in groups, Bol. Soc. Bras. Math., 11:1 (1980), 79-102.

[MCW02] J. P. McCammond, D. T. Wise, Fans and ladders in small cancellation theory, Proc. London Math. Soc. (3), 84:3 (2002), 599-644.

[MO10] J. Martín-Morales, A. M. Oller-Marcén, On the number of irreducible components of the representation variety of a family of one-relator groups, Internat. J. Algebra Comput. 20:1 (2010), 77-87. См. также arXiv:0805.4716.

[MO11] A. Myasnikov, D. Osin. Algorithmically finite groups, J. Pure Appl. Algebra 215:11 (2011), 2789-2796. См. также arXiv:1012.1653.

[MO98] S. A. Morris, V. N. Obraztsov, Nondiscrete topological groups with many discrete subgroups, Topology Appl., 84 (1998), 105-120.

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

[MSh12] N. Yu. Makarenko, P. Shumyatsky, Characteristic subgroups in locally finite groups, J. Algebra, 352:1 (2012), 354-360.

[Ma32] W. Magnus, Das Identitätsproblem für Gruppen mit einer definierenden Relation, Math. Ann., 106 (1932), 295-307.

[Mag30] W. Magnus, Über diskontinuierliche Gruppen mit einer definierenden Relation (Der Freiheitssatz), J. Reine Angew Math., 163 (1930) 141-165.

[Mas84] R.C. Mason, Diophantine Equations over Function Fields, London Mathematical Society Lecture Note Series 96, Cambridge, England: Cambridge University Press, 1984.

[Mazh17] A. M. Mazhuga, On free decompositions of verbally closed subgroups of free products of finite groups, Journal of Group Theory, 20:5, 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.

[Met01] V. Metaftsis, On the structure of one-relator products of locally indicable groups with centre, J. Pure Appl. Algebra, 161:3 (2001), 309-325.

[Mi12a] I. Mineyev, Submultiplicativity and the Hanna Neumann conjecture, Ann. Math., 175 (2012), 393-414.

[Mi12b] I. Mineyev, Groups, graphs, and the Hanna Neumann conjecture, J. Topol. Anal., 4:1 (2012), 1-12.

[Mu64] K. Murasugi, The center of a group with a single defining relation, Math.Ann., 155 (1964), 246-251.

[Neu54] B. H. Neumann, Groups covered by permutable subsets, J. London Math. Soc., s1-29:2 (1954), 236-248.

[Neu76] B. H. Neumann, A problem of Paul Erdős on groups, J. Austral. Math. Soc. Ser. A., 21:4 (1976), 467-472.

[Neu73] P. M. Neumann, The SQ-universality of some finitely presented groups, J. Austral. Math. Soc., 16 (1973), 1-6.

[New68] B. B. Newman, Some results on one-relator groups, Bull. Amer. Math. Soc., 74 (1968) 568-571.

[New85] M. Newman, A note on Fuchsian groups, Illinois J. Math., 29:4 (1985), 682-686.
[OaPo64] S. Oates, M. B. Powell, Identical relations in finite groups, J. Algebra 1 (1964), 11-39.
[OlOs06] A. Yu. Olshanskii, D. V. Osin, Large groups and their periodic quotients, Proceedings of the American Mathematical Society, 136:3 (2008), 753-759. См. также arXiv:math/0601589.
[Os06] Osin D.V. Relatively hyperbolic groups: Intrinsic geometry, algebraic properties, and algorithmic problems. Memoirs Amer. Math. Soc. 179:843 (2006). См. также arXiv:math/0404040.
[P88] S. D. Promyslow, A simple example of a torsion free nonunique product group, Bull. London Math. Soc., 20 (1988), 302-304.
[PSz02] K. Podoski, B. Szegedy, Bounds in groups with finite abelian coverings or with finite derived groups, J. Group Theory, 5:4 (2002), 443-452.
[Pi74] A. Pietrowski, The isomorphism problem for one-relator groups with non-trivial centre, Math.Z., 136 (1974), 95-106.
[Pia02] A. Pianzola, Automorphisms of toroidal Lie algebras their central quotients, J. Algebra and Appl., 1:1 (2002), 113-121.
[Pri88] S. J. Pride, Star-complexes, and the dependence problems for hyperbolic complexes, Glasgow Math. J., 30:2 (1988), 155-170.
[RBCh96] A. S. Rapinchuk, V. V. Benyash-Krivetz, V. I. Chernousov, Representation varieties of the fundamental groups of compact orientable surfaces, Israel Journal of Mathematics, 93:1 (1996), 29-71.
[RS87] E. Rips, Y. Segev, Torsion free groups without unique product property, J. Algebra, 108 (1987), 116-126.
[Rom12] V. A. Roman'kov, Equations over groups, Groups Complexity Cryptology, 4:2 (2012), 191-239.
[Ry25] S. Ryley, The Ladies' Diary, 122 (1825), 35.
[SaAs07] J. Sato, T. Asai, On the n-th roots of a double coset of a finite group, J. School Sci. Eng., Kinki Univ., 43 (2007), 1-4.
[SaSc74] G. S. Sacerdote, P. E. Schupp, SQ-universality in HNN groups and one relator groups, J. London Math. Soc., 7 (1974), 733-740.
[Sch59] M. P. Schützenberger, Sur l'equation $a^{2+n} = b^{2+m}c^{2+p}$ dans un groupe libre, C. R. Acad. Sci. Paris Sér. I Math., 248 (1959), 2435-2436.
[Sehg62] S. K. Sehgal, On P. Hall's generalisation of a theorem of Frobenius, Proc. Glasgow Math. Assoc., 5 (1962), 97-100.
[Ser77] J.-P. Serre. Arbres, amalgames, SL_2, Rédigé avec la collaboration de Hyman Bass. Astérisque, No. 46. Sociéte Mathématique de France, Paris, 1977. (English translation: Trees. Springer-Verlag, 1980).
[Sil86] Silverman J. H. The Arithmetic of Elliptic Curves. New York: Springer-Verlag, 1986.
[Sny00] Snyder N. An alternate proof of Mason's theorem, Elem. Math., 55:3 (2000), 93-94.
[Solo69] L. Solomon, The solution of equations in groups, Arch. Math., 20:3 (1969), 241-247.
[Speht52] W. Specht, Gesetze in Ringen. I, Math. Z., 52 (1950), 557-589.
[Sta71] J. Stallings, Group theory and three-dimensional manifolds, Yale Math. Monographs (1971).
[Sta87] J. R. Stallings, A graph-theoretic lemma and group embeddings, Combinatorial group theory and topology (eds. S. M. Gersten, J. R. Stallings). Annals of Mathematical Studies. 111. 1987. 145-155.
[Sto81] W. W. Stothers, Polynomial identities and hauptmoduln, Quarterly J. Math., 32:3 (1981), 349-370.
[Str80] A. Strojnowski, A note on u.p. groups, Comm. Algebra, 8 (1980), 231-234.
[Stö83] Stöhr R. Groups with one more generator than relators, Math. Z., 182:1 (1983), 45-47.
[VPl96] N. Vavilov, E. Plotkin, Chevalley groups over commutative rings. I: Elementary calculations, Acta Appl. Math., 45:1 (1996), 73-113.
[Vas86] L. N. Vaserstein, On normal subgroups of Chevalley groups over commutative rings, Tôhoku Math. J., 36:5 (1986), 219-230.
[Wag67] K. Wagner, Fastplättbare Graphen, J. Combinatorial Theory, 3 (1967), 326-365.
[Wat80] W. C. Waterhouse, Automorphisms of $\mathbf{GL}_n(\mathbb{R})$, Proc. Amer. Math. Soc., 79:3 (1980) 347-351.
[Wils09] R. A. Wilson, The Finite Simple Groups. Graduate Texts in Mathematics. Springer. 2009.
[Wise01] D. T. Wise, The residual finiteness of positive one-relator groups, Comment. Math. Helv., 76 (2001), 314-338.
[Yosh93] T. Yoshida, $|\mathrm{Hom}(A, G)|$, Journal of Algebra, 156:1 (1993), 125-156.
[Za14] A. Zakharov, On the rank of the intersection of free subgroups in virtually free groups, J. Algebra, 418 (2014), 29-43. См. также arXiv:1301.3115.
[ZS18] G. L. Zhou, Z. W. Sun, On sums and products in a field, arXiv:1807.01181.

РАБОТЫ АВТОРА ПО ТЕМЕ ДИССЕРТАЦИИ

Статьи в рецензируемых научных изданиях, рекомендованных для защиты в диссертационном совете МГУ по специальности

[БК21] Е. К. Брусянская, А. А. Клячко, О числе эпи-, моно- и гомоморфизмов групп, Известия РАН. Сер. мат., 86:2 (2022), 25-33. См. также arXiv:2012.03123.

[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.

[KL21] A. A. Klyachko, N. M. Luneva, Invariant systems of representatives, or The cost of symmetry, Discrete Mathematics, 344:6 (2021), 112361. См. также arXiv:1908.03315.

[KP20] A. A. Klyachko, A. N. Ponfilenko, Intersections of subgroups in virtually free groups and virtually free products, Bull. Austral. Math. Soc., 101:2 (2020), 266-271. См. также arXiv:1904.07350.

[KR20] A. A. Klyachko, M. A. Ryabtseva, The dimension of solution sets to systems of equations in algebraic groups, Israel Journal of Mathematics, 237:1 (2020), 141-154. См. также arXiv:1903.05236.

[BKV19] E. K. Brusyanskaya, A. A. Klyachko, A. V. Vasil'ev, What do Frobenius's, Solomon's, and Iwasaki's theorems on divisibility in groups have in common?, Pacific Journal of Mathematics, 302:2 (2019), 437-452. См. также arXiv:1806.08870.

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

[KM18] А. А. Клячко, А. М. Мажуга, Вербально замкнутые почти свободные подгруппы, Мат. сборник, 209:6 (2018), 75-82. См. также arXiv:1702.07761.

[IK18] I. V. Ivanov, A. A. Klyachko, Quasiperiodic and mixed commutator factorizations in free products of groups, Bull. London Math. Soc., 50:5 (2018), 832-844. См. также arXiv:1702.01379.

[KM17] A. A. Klyachko, A. A. Mkrtchyan, Strange divisibility in groups and rings, Archiv der Mathematik, 108:5 (2017), 441-451. См. также arXiv:1506.08967.

[KV16] A. A. Klyachko, A. N. Vassiliev, Balanced factorizations, American Mathematical Monthly, 123:10 (2016), 989-1000. См. также arXiv:1506.01571.

[KMo15] А. А. Клячко, А. К. Монгуш, Финитно аппроксимируемые алгоритмически конечные группы, их подгруппы и прямые произведения, Мат. заметки, 98:3 (2015), 372-377. См. также arXiv:1402.0887.

[KMi15] A. A. Klyachko, M. V. Milentyeva, Large and symmetric: The Khukhro–Makarenko theorem on laws — without laws, Journal of Algebra, 424 (2015), 222-241. См. также arXiv:1309.0571.

[KM14] A. A. Klyachko, A. A. Mkrtchyan, How many tuples of group elements have a given property? With an appendix by Dmitrii V. Trushin, International Journal of Algebra and Computation, 24:4 (2014), 413-428. См. также arXiv::1205.2824.

[KM12] A. A. Klyachko, E. V. Menshova, The identities of additive binary arithmetics, Electronic Journal of Combinatorics, 19:1 (2012), #P40. См. также arXiv:1102.5555.

[БК12] Д. В. Баранов, А. А.Клячко, Экономное присоединение квадратных корней к группам, Сибирский мат. журнал, 53:2 (2012), 250-257. См. также arXiv:1101.3019.

[KL12] A. A. Klyachko, D. E. Lurye, Relative hyperbolicity and similar properties of one-generator one-relator relative presentations with powered unimodular relator, Journal of Pure and Applied Algebra, 216:3 (2012), 524-534. См. также arXiv:1010.4220.

[KhKMM09] E. I. Khukhro, A. A. Klyachko, N. Yu. Makarenko, Yu. B. Melnikova, Automorphism invariance and identities, Bull. London Math. Soc., 41:5 (2009), 804-816. См. также arXiv:0812.1359.

[KM09] А. А. Клячко, Ю. Б. Мельникова, Короткое доказательство теоремы Макаренко–Хухро о больших характеристических подгруппах с тождеством, Мат. сборник, 200:5 (2009), 33-36. См. также arXiv:0805.2747.

[K10] A. A. Klyachko, Automorphisms and isomorphisms of Chevalley groups and algebras, Journal of Algebra, 324:10 (2010), 2608-2619. См. также arXiv:0708.2256.

[K09] A. A. Klyachko, The structure of one-relator relative presentations and their centres, Journal of Group Theory, 12:6 (2009), 923-947. См. также arXiv:math.GR/0701308.

[K06б] А. А. Клячко, SQ-универсальность относительных копредставлений с одним соотношением, Мат. сборник, 197:10 (2006), 87-108. См. также arXiv:math.GR/0603468.

[K07] А. А. Клячко, Свободные подгруппы относительных копредставлений с одним соотношением, Алгебра и логика, 46:3 (2007), 290-298. См. также arXiv:math.GR/0510582.

[KT05] A. A. Klyachko, A. V. Trofimov, The number of non-solutions of an equation in a group, Journal of Group Theory, 8:6 (2005), 747-754. См. также arXiv:math.GR/0411156.

[K05] А. А. Клячко, Гипотеза Кервера–Лауденбаха и копредставления простых групп, Алгебра и логика, 44:4 (2005), 399-437. См. также arXiv:math.GR/0409146.

[K06a] А. А. Клячко, Как обобщить известные результаты об уравнениях над группами, Мат. заметки, 79:3 (2006), 409-419. См. также arXiv:math.GR/0406382.

Другие работы автора по теме диссертации

[KZ21] A. A. Klyachko, A. O. Zakharov, An analogue of the strengthened Hanna Neumann conjecture for virtually free groups and virtually free products, Michigan Mathematical Journal (в печати). См. также arXiv:2106.05821.

[KMO21]* A. A. Klyachko, V. Yu. Miroshnichenko, A. Yu. Olshanskii, Finite and nilpotent strongly verbally closed groups, Journal of Algebra and Its Applications (в печати). См. также arXiv:2109.12397.

[DK21]* N. S. Dergacheva, A. A. Klyachko, Small non-Leighton two-complexes, arXiv:2108.01398.

[BeK20]* V. Yu. Bereznyuk, A. A. Klyachko, Commutator length of powers in free products of groups, Proc. Edinburgh Math. Soc., 65:1 (2022), 102-119. См. также arXiv:2008.02861.

[KT17]* A. A. Klyachko, A. B. Thom, New topological methods to solve equations over groups, Algebraic and Geometric Topology, 17:1 (2017), 331-353. См. также arXiv:1509.01376.

[КМП17] А. А. Клячко, А. М. Мажуга, А. Н. Понфиленко, Уравновешенные разложения на множители в некоторых алгебрах, Мат. просвещение, 21 (2017), 136-144. См. также arXiv:1607.01957.

[FK12]* E. V. Frenkel, A. A. Klyachko, Commutators cannot be proper powers in metric small-cancellation torsion-free groups, arXiv:1210.7908.

[KOO13]* A. A. Klyachko, A. Yu. Olshanskii, D. V. Osin, On topologizable and non-topologizable groups, Topology and its Applications, 160:16 (2013), 2104-2120. См. также arXiv:1210.7895.

[IK01]* S. V. Ivanov, A. A. Klyachko, The asphericity and Freiheitssatz for certain lot-presentations of groups, International Journal of Algebra and Computation, 11:3 (2001), 291-300.

[KS01]* A. A. Klyachko, O. V. Sipacheva, Topological solvability of equations over groups, Communications in Algebra, 29:9 (2001), 4249-4265.

[IK00]* S. V. Ivanov, A. A. Klyachko, Solving equations of length at most six over torsion-free groups, Journal of Group Theory, 3:3 (2000), 329-337.

[K99]* A. A. Klyachko, Equations over groups, quasivarieties, and a residual property of a free group, Journal of Group Theory, 2:3 (1999), 319-327.

[K97]* A. A. Klyachko, Asphericity tests, International Journal of Algebra and Computation, 7:4 (1997), 415-431.

[КП95]* А. А. Клячко, М. И. Прищепов, Метод спуска для уравнений над группами, Вестник Московского университета. Серия 1: Математика. Механика, 4 (1995), 90-93.

[K94]* А. А. Клячко, Гипотеза Кервера–Лауденбаха и уравнения над группами, Дисс. ... к.ф.-м.н., М.: МГУ, 1994.

[K93]* A. A. Klyachko, A funny property of sphere and equations over groups, Communications in Algebra, 21:7 (1993), 2555-2575.

Результаты из работ, помеченных звёздочкой, не вошли в диссертацию, хотя и соответствуют по теме.