ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

На правах рукописи

Леонтьев Владимир Маркович

О СОБИРАТЕЛЬНОМ ПРОЦЕССЕ ДЛЯ ПОЛОЖИТЕЛЬНЫХ СЛОВ СВОБОДНОЙ ГРУППЫ

1.1.5 — математическая логика, алгебра, теория чисел и дискретная математика (физико-математические науки)

Диссертация на соискание ученой степени
кандидата физико-математических наук

Научный руководитель:
доктор физ.-мат. наук
Колесников Сергей Геннадьевич

Красноярск – 2024

Оглавление

Введение

В работе Ф. Холла [16], посвященной теории конечных p-групп, было введено понятие собирательного процесса, суть которого можно описать следующим образом. Пусть W — положительное слово свободной группы $F = F(a_1, \ldots, a_n)$, $n \geqslant 1$, т.е. W не содержит порождающие элементы $a_1, \ldots, a_n$ в отрицательных степенях. Последовательно меняя местами соседние элементы в W с использованием коммутаторов: $QR = RQ[Q, R]$, $Q, R \in F$, собирательный процесс преобразует W к следующему виду:

$$W = q_1^{e_1} \ldots q_j^{e_j} T_j, \quad j \geqslant 1, \tag{1}$$

где $q_1, \ldots, q_j$ — коммутаторы в буквах $a_1, \ldots, a_n$, упорядоченные по возрастанию веса, T_j состоит из коммутаторов веса не меньше, чем $w(q_j)$ (вес q_j), показатели степеней $e_1, \ldots, e_j$ — положительные целые числа.

Результатом применения собирательного процесса к слову $W = (a_1 a_2)^m$, $m \geqslant 1$, стала собирательная формула Ф. Холла [16, теоремы 3.1 и 3.2]:

$$(a_1 a_2)^m = q_1^{e_1} \ldots q_{j(s)}^{e_{j(s)}} \pmod{\Gamma_s(F)}, \quad s \geqslant 2, \tag{2}$$

где $\Gamma_s(F)$ — s-й член нижнего центрального ряда группы F, определяемый следующим образом: $\Gamma_1(F) = F$, $\Gamma_k(F) = [\Gamma_{k-1}(F), F]$, $k \geqslant 2$, и показатели степеней коммутаторов представимы в виде целозначных полиномов от m:

$$e_i(m) = \sum_{k=1}^{w(q_i)} c_k \binom{m}{k} \tag{3}$$

с целыми неотрицательными c_k, не зависящими от m. Для теории p-групп важным оказывается свойство делимости $e_i(p^\alpha)$ на степень простого числа p^α, когда $w(q_i) < p$. Идея доказательства формулы (2) была основана на присвоении вхождениям коммутатора q_i меток (конечных целочисленных последовательностей $(\lambda_1, \ldots, \lambda_{w(q_i)})$). Показатель степени $e_i(m)$, совпадающий с числом меток всех вхождений q_i, оказывался равным количеству элементов $(\lambda_1, \ldots, \lambda_{w(q_i)})$ декартовой степени $\{1, \ldots, m\}^{w(q_i)}$, компоненты которых удовлетворяют определенной системе линейных равенств и неравенств.

В монографии М. Холла [12, теорема 12.3.1], доказательство Ф. Холла было в точности перенесено на слово $W = (a_1 \ldots a_n)^m$, $n \geqslant 1$. Еще большее обобщение было получено в монографии В. Магнуса, А. Карраса, Д. Солитэра [5, теоремы 5.13А и 5.13В], где для произвольного слова W группы F (не обязательно положительного) с использованием аппарата алгебр Ли доказано, что слово W^m, $m \geqslant 1$, представимо в виде:

$$W^m = q_1^{e_1} \ldots q_{j(s)}^{e_{j(s)}} \pmod{\Gamma_s(F)}, \quad s \geqslant 2, \tag{4}$$

где $q_1, \ldots, q_{j(s)}$ — коммутаторы в буквах $a_1, \ldots, a_n$ весов меньше s и e_i делится на m, если m есть степень простого числа p^α и $w(q_i) < p$.

В связи с исследованием нильпотентных произведений циклических групп были получены разные собирательные формулы со свойствами делимости показателей степеней коммутаторов. В работе Р. Струик [20, лемма 4] на основе модификации идеи Ф. Холла была доказана следующая формула:

$$a_1^{m_1} a_2^{m_2} = q_1^{e_1} q_2^{e_2} q_3^{e_3} \ldots q_{j(s)}^{e_{j(s)}} \pmod{\Gamma_s(F)}, \quad s \geqslant 2, \tag{5}$$

где $q_1 = a_2$, $q_2 = a_1$ и

$$e_i = \sum_{k=1}^{w_{a_1}(q_i)} \sum_{t=1}^{w_{a_2}(q_i)} c_{k,t} \binom{m_1}{k} \binom{m_2}{t}, \quad c_{k,t} \in \mathbb{N}_0.$$

Здесь $w_{a_l}(q_i)$ — вес q_i в a_l, $l = 1, 2$. Если m_l, $l = 1, 2$, есть степень простого числа p^α и $1 \leqslant w_{a_l}(q_i) < p$, тогда e_i делится на m_l. Формула (5) была также получена методами из [5] в работе Г. Волдингера [21] при $m_1 = 1$, $m_2 = p$, $s = p+2$ для простого p и в работе Э. Гаглионе [14] при $m_1 = 1$, $m_2 = p^\alpha$, $\alpha \geqslant 1$, $s = p^2+1$ для простого p. С использованием тех же методов в статье Э. Гаглионе и Д. Спеллмана [15, теорема 2.3] доказана упомянутая выше формула для слова $W = (a_1 \ldots a_n)^m$, $n \geqslant 1$.

Рассмотренные выше результаты с разными техниками доказательства приводят к естественному вопросу о существовании универсального метода исследования свойств делимости показателей степеней e_j в собирательных формулах (1) и о возможности получения подобных результатов для других положительных слов. В связи с этим мы ставим следующую задачу.

(A) *Разработать подход к исследованию делимости показателей степеней коммутаторов в собирательных формулах для положительных слов свободной группы, позволяющий единообразно доказать и обобщить известные результаты. В частности, для любых натуральных $n, m, m_1, \ldots, m_n$ в свободной группе с образующими $a_1, \ldots, a_n$ рассмотреть слова $(a_1 \ldots a_n)^m$, $a_1^{m_1} \ldots a_n^{m_n}$ и W^m, где W — произвольное положительное слово, в первом и третьем слове некоторые вхождения букв могут быть удалены.*

Другое направление исследований, связанное с собирательным процессом, заключается в поиске явного вида показателей степеней коммутаторов в собирательной формуле Ф. Холла (2) и, как следствие, получение собирательных формул в явном виде при некоторых ограничениях на группу (ступень разрешимости, нильпотентности группы и т.п.). Рассмотрим группу $G = \langle x, y \rangle$. Известно (см., например, [12]), что при условии $[y, x] \in Z(G)$ формула (2) принимает следующий вид:

$$(xy)^n = x^n y^n [y, x]^{\binom{n}{2}}.$$

Если же $[\Gamma_2(G), \Gamma_2(G)] = 1,\ y \in C_G(\Gamma_2(G))$, получаем формулу

$$(xy)^n = x^n y^n \prod_{i=1}^{n-1} [y, {}_i x]^{\binom{n}{i+1}}.$$

Мы используем краткую запись: $[y, {}_0 x] = y$, $[y, {}_u x] = [[y, {}_{u-1} x], x]$, где $u \in \mathbb{N}$; $[y, {}_u x, {}_v z] = [[y, {}_u x], {}_v z]$, где $u, v \in \mathbb{N}_0$.

Из того факта, что показатель степени коммутатора $[y, {}_i x]$ в собирательной формуле для $(xy)^n$ равен $\binom{n}{i+1}$, следует, что группа простой экспоненты p

удовлетворяет $(p-1)$–му условию Энгеля [12, с. 354]:

$$[y,{}_{p-1}x]=1 \pmod{\Gamma_{p+1}(G)}.$$

Как отмечается в [12, с. 354], данное соотношение было основным при исследовании ослабленной проблемы Бернсайда для групп экспоненты p. Опираясь на него, А. И. Кострикин решил ослабленную проблему Бернсайда для группы экспоненты 5 с двумя образующими.

В работе Ю. Краузе [17] найдены показатели степеней для следующих коммутаторов:

$$\begin{aligned}
[y,{}_ix,{}_jy] \quad &: \quad \sum_{m=0}^{n-1}\binom{m}{i}\binom{m}{j}, \quad \text{где } i\geqslant 1, j\geqslant 0;\\
[[y,x,y],[y,{}_2x]] \quad &: \quad \sum_{m=0}^{n-1} m\left(2\binom{m}{2}+(m+2)\binom{m}{3}\right), \quad \text{где } i\geqslant 1;\\
[[y,{}_ix,{}_jy],[y,x]] \quad &: \quad \sum_{m=0}^{n-1}\binom{m}{i}\left(\binom{m}{2}\binom{m}{j}+\binom{m}{j+1}\right), \quad \begin{matrix}\text{где } i\geqslant 1, j\geqslant 0,\\ \text{и } i\geqslant 2 \text{ при } j=0.\end{matrix}
\end{aligned}$$

Явный вид этих показателей позволил доказать, что группа экспоненты 8 удовлетворяет 14-му условию Энгеля [18].

Собирательная формула Ф. Холла существенно использовалась А. И. Скопиным при исследовании строения нижнего центрального ряда групп бернсайдовского типа примарной экспоненты. В [7] был вычислен отрезок собирательной формулы для $(xy)^8$ по модулю $\Gamma_{10}(G)$, а в [8] установлено, что для любых $x\in G$, $y\in\Gamma_2(G)$ справедливы две следующие формулы:

$$(xy)^n = x^ny^n\prod_{i=1}^{n-1}\prod_{j=0}^{n-1}[y,{}_ix,{}_jy]^{\sum\limits_{k=1}^{n-1}\binom{k}{i}\binom{k}{j}},$$

$$(xy)^n = x^ny^n\prod_{i=1}^{n-1}[y,{}_ix]^{\binom{n}{i+1}}\prod_{m=0}^{n-2}\prod_{i=m+1}^{n-1}[[y,{}_ix],[y,{}_mx]]^{c^n_{mi}}$$

при условии трасметабелевости группы G I типа ($[\Gamma_3(G),\Gamma_3(G)]=1$) и II типа ($[\Gamma_2(G),\Gamma_2(G),\Gamma_2(G)]=1$), соответственно. Было показано, что числа c^n_{mi} удовлетворяют системе соотношений, явные выражения для c^n_{mi} найдены не были.

В работе [9], а также статье А. И. Скопина и Ю. Г. Тетерина [10] был представлен алгоритм построения собирательной формулы Ф. Холла для метабелевых и трансметабелевых групп.

Приведенные результаты использовались, например, в [11] для нахождения ступени нильпотентности и верхней границы порядка максимальной 2-порожденной трансметабелевой группы I типа экспоненты 8. В случае экспоненты 9 верхние границы ступени нильпотентности и порядка группы найдены в статье Ф. А. Иванова и А. И. Скопина [1].

Вычисление в явном виде показателей степеней коммутаторов в собирательной формуле Ф. Холла является, вообще говоря, сложной задачей. Более того, в некоторых случаях, например, при работе с p-группами в формуле для $(xy)^p$ требуется знать показатели степеней по модулю p. В таких условиях крайне полезен холловский вид показателей (3), т.е. выражение $e_i(p)$ через целочисленную линейную комбинацию биномиальных коэффициентов вида $\binom{p}{k}$. Отметим, что из перечисленных выше серий коммутаторов только для $[y, {}_i x]$, $i \geqslant 1$, показатель степени найден в виде (3). В диссертационной работе рассматривается следующая задача.

(B) *В собирательной формуле Ф. Холла для выражения* $(xy)^n$*,* $n \geqslant 1$*, найти в явном холловском виде показатели степеней для двух серий коммутаторов:* $[y, {}_u x, {}_v y]$*, где* $u \geqslant 0$*,* $v \geqslant 0$*, и* $v = 0$ *при* $u = 0$*;* $[[y, {}_u x], [y, {}_v x]]$*, где* $u > v \geqslant 1$*.*

Интерес к указанным сериям коммутаторов вызван, в частности, одним известным вопросом о регулярности конечной p-группы. Напомним, что понятие регулярности введено Ф. Холлом [16] на основе собирательной формулы (2) и суть его заключается в следующем. Конечная p-группа называется *регулярной*, если для любых ее элементов x, y и любого $\alpha \in \mathbb{N}$ существуют такие элементы $c_1, \dots, c_t$ из коммутанта $\langle x, y \rangle'$, что $(xy)^{p^\alpha} = x^{p^\alpha} y^{p^\alpha} c_1^{p^\alpha} \dots c_t^{p^\alpha}$.

В Коуровской тетради Б. Верфрицом была поставлена следующая проблема [19, вопрос 8.3].

(C) *Для целых положительных чисел m, n и простого числа p пусть $P_n(\mathbb{Z}_{p^m})$ — группа всех таких матриц (a_{ij}) над кольцом классов вычетов по модулю p^m, что $a_{ii} \equiv 1 \pmod p$ для всех i и $a_{ij} \equiv 0 \pmod p$ для всех $i > j$. Группа $P_n(\mathbb{Z}_{p^m})$ является конечной p-группой. Для каких m и n она регулярна?*

Из формулы (2) и свойства делимости показателей степеней входящих в нее коммутаторов следует, что любая конечная p-группа ступени нильпотентности $< p$ является регулярной. Согласно работе Ю. И. Мерзлякова [6] группа $P_n(\mathbb{Z}_{p^m})$ имеет ступень нильпотентности $mn - 1$, поэтому при $mn - 1 < p$ она регулярна. В статьях А. В. Ягжева [13] и С. Г. Колесникова [2] для случаев $m = 1$ и $m = 2$, соответственно, доказано, что $P_n(\mathbb{Z}_{p^m})$ регулярна тогда и только тогда, когда ее ступень нильпотентности меньше p. Далее, в [3] установлено, что при $n^2 < p$ группа $P_n(\mathbb{Z}_{p^m})$ регулярна для любого m. Таким образом, ответ на вопрос Б. Верфрица остается неизвестным в следующих случаях:

$$2n - 1 < p \leqslant \min\{mn - 1, n^2\}.$$

В работе [4] показано, что в этих случаях группа $P_n(\mathbb{Z}_{p^m})$ удовлетворяет ряду необходимых условий регулярности из [12, теоремы 12.4.3–12.4.5].

Целью диссертационной работы является получение полного или частичного решения задач **(A)**, **(B)** и **(C)**.

Методы исследования. В работе используются методы комбинаторного анализа, теории групп.

Основные результаты работы.

1. Разработан логико-комбинаторный подход к исследованию делимости показателей степеней коммутаторов, возникающих в собирательных формулах для положительных слов свободной группы.

2. Получены обобщения известных собирательных формул со свойствами делимости показателей степеней коммутаторов, а именно, для любых натуральных $n, m, m_1, \ldots, m_n$ в свободной группе с образующими $a_1, \ldots, a_n$ рас-

смотрены слова $(a_1 \dots a_n)^m$, $a_1^{m_1} \dots a_n^{m_n}$ и W^m, где W — произвольное положительное слово, в первом и третьем слове некоторые вхождения букв могут быть удалены.

3. Представлена параметризация несобранной части собирательной формулы Ф. Холла с помощью функции бинарного веса числа (равной количеству единиц в двоичной записи ее целого неотрицательного аргумента).

4. В собирательной формуле Ф. Холла для выражения $(xy)^n$, $n \geqslant 1$, в явном холловском виде найдены показатели степеней для двух серий коммутаторов: $[y, {}_u x, {}_v y]$, где $u \geqslant 0$, $v \geqslant 0$, и $v = 0$ при $u = 0$; $[[y, {}_u x], [y, {}_v x]]$, где $u > v \geqslant 1$. Как следствие, получены явные собирательные формулы для групп ступени нильпотентности 2, а также для групп с нильпотентным коммутантом ступени 2 и условием перестановочности элемента y с любым элементом коммутанта.

5. Доказана нерегулярность силовской p-подгруппы общей линейной группы $(n \times n)$-матриц над кольцом $\mathbb{Z}_{p^m}$, когда $n \geqslant (p+2)/3$, $m \geqslant 3$ и p — такое простое число, что число $(p+2)/3$ — целое.

Результаты **1** и **2** служат решением поставленной задачи **(A)**. С использованием результата **3** получено полное решение задачи **(B)**, сформулированное в пункте **4**. Результат **5** дает частичный ответ на вопрос **(C)**.

Структура и объем диссертации. Диссертация изложена на 96 страницах, состоит из введения, трех глав и списка литературы, содержащего 36 наименований. Номер определения, теоремы, леммы и др. включает номер главы, параграфа и порядковый номер.

В **главе 1** диссертации представлен подход к исследованию делимости показателей степеней коммутаторов, возникающих в ходе собирательного процесса, примененного к положительному слову свободной группы. В основе подхода лежит идея, реализованная Ф. Холлом в доказательстве формулы (2) и заключающаяся в присваивании вхождениям коммутаторов различных целочисленных последовательностей и, как следствие, равенстве показателя степени коммутатора количеству таких последовательностей.

В **§ 1.1** вводится система базовых понятий и обозначений, рассматриваются основные свойства собирательного процесса. Определяется собирательный процесс, как построение последовательности слов

$$\{W_j \equiv q_1^{e_1} \dots q_j^{e_j} T_j\}_{j \geqslant 0},$$

где W_0 — произвольное положительное слово свободной группы $F(a_1, \dots, a_n)$, $n \geqslant 1$, и слово W_j получено из W_{j-1} путем сбора всех вхождений произвольно выбранного коммутатора q_j в несобранной части T_{j-1}. При этом всем вхождениям коммутаторов в словах присваиваются метки (конечные целочисленные последовательности) следующим образом. Различные вхождения одной буквы a_i, $i = 1, \dots, n$, имеют различные метки одинаковой длины, а вхождениям коммутаторов, возникших в ходе собирательного процесса, присваиваются метки по правилу

$$y(\Lambda_u)x(\Lambda_v) = x(\Lambda_v)y(\Lambda_u)[y, x](\Lambda_u\Lambda_v),$$

где $\Lambda_u\Lambda_v$ — результат конкатенации меток Λ_u и Λ_v.

В **§ 1.2** рассматривается декартово произведение

$$D(q_j) = D(a_{i_1}) \times \dots \times D(a_{i_{w(R)}}), \tag{6}$$

где $D(a_i)$ — множество, содержащее метки всех вхождений a_i, и последовательность букв $a_{i_1}, \dots, a_{i_{w(R)}}$ соответствует бесскобочной записи коммутатора q_j. Поскольку метки всех вхождений q_j содержатся в $D(q_j)$, задается предикат $E_{q_j}^{\Lambda}$, $\Lambda \in D(q_j)$, равный 1 тогда и только тогда, когда Λ есть метка некоторого вхождения q_j. Изучение свойств предиката E_{q_j} оказывается важным для получения информации о показателе степени e_j, поскольку

$$e_j = |\{\Lambda \in D(q_j) \mid E_{q_j}^{\Lambda} = 1\}|. \tag{7}$$

Центральным результатом параграфа является система рекуррентных соотношений (теорема 1.2.2), которая позволяет выразить $E_{q_j}^{\Lambda}$ через операции конъюнкции, дизъюнкции, предикат равенства и предикаты

$$E_{a_i}^{\Lambda}, \quad \Lambda \in D(a_i), \qquad P_{a_i,a_j}^{\Lambda_2\Lambda_2}, \quad \Lambda_1\Lambda_2 \in D(a_i) \times D(a_j), \tag{8}$$

значения которых определяются структурой начального слова W_0. Более точно, $E_{a_i}^{\Lambda} = 1$ тогда и только тогда, когда в W_0 найдется вхождение $a_i(\Lambda)$; $P_{a_i,a_j}^{\Lambda_2\Lambda_2} = 1$ тогда и только тогда, когда в W_0 найдется вхождение $a_i(\Lambda_1)$, предшествующее (расположенное левее) $a_j(\Lambda_2)$. В доказательстве существенно используется установленное соответствие двоичных чисел коммутаторам в несобранной части, что позволяет эффективно описать ее строение и свести вопрос предшествования вхождений коммутаторов к предшествованию двоичных чисел (теорема 1.2.1).

В **§ 1.3** удается найти выражение для мощности

$$|\{\Lambda \in D \mid C(\Lambda) = 1\}|,$$

когда $D = M_1 \times \cdots \times M_r$ — декартово произведение конечных множеств целых чисел, общее пересечение M которых совпадает с одним из них, и отрезок $[\min M, \max M]$ не имеет общих элементов с $M_i \backslash M$, $i = 1, \ldots, r$, а условие $C(\Lambda) = C(\lambda_1, \ldots, \lambda_r)$ выражается L-условием, т.е. формулой, составленной из операций конъюнкции, дизъюнкции и предикатов вида $[\lambda_i = \lambda_j]$, $[\lambda_i = \lambda_j]$, $i = 1, \ldots, r$ (теорема 1.3.1). Найденное выражение будет делиться на $|M|$, когда $|M|$ есть степень простого числа p^{α} и $r < p$.

В **§ 1.4** демонстрируется применение разработанного подхода к исследованию делимости показателей степеней e_j. Суть этого подхода заключается в нахождении разметки для слова W_0, при которой предикаты (8), а следовательно, согласно § 1.2, и предикат E_{q_j} выражаются некоторыми L-условиями, а множество (6) удовлетворяет условиям комбинаторного результата из § 1.3, благодаря которому и будет получено свойство делимости для (7).

В параграфе для любых натуральных $n, m, m_1, \ldots, m_n$ рассмотрены слова $(a_1 \ldots a_n)^m$ (теорема 1.4.1), $a_1^{m_1} \ldots a_n^{m_n}$ (теорема 1.4.2) и W^m (теорема 1.4.3), где W — произвольное положительное слово, в первом и третьем слове некоторые вхождения букв могут быть удалены.

Основные результаты параграфов 1.1, 1.2 и 1.4 опубликованы в работе автора [26], результаты параграфа 1.3 — в работе автора [22].

Глава 2 диссертации посвящена вычислению показателей степеней коммутаторов в собирательной формуле Ф. Холла (2) для выражения $(xy)^n$, $n \geqslant 1$.

В **§ 2.1** представлена параметризация несобранной части формулы Ф. Холла с помощью функции бинарного веса числа $\omega(i)$, равной количеству единиц в двоичной записи целого неотрицательного числа i (теорема 2.1.1). Доказан ряд комбинаторных результатов, связанных с множеством решений i уравнения $\omega(i) = x$, $x \in \mathbb{Z}$, с помощью которых в **§ 2.2** получены в явном холловском виде (3) показатели степеней для двух серий коммутаторов (теоремы 2.2.1 и 2.2.2):

$$[y, {}_u x, {}_v y], \quad \text{где } u \geqslant 0,\ v \geqslant 0, \text{ и } v = 0 \text{ при } u = 0;$$
$$[[y, {}_u x], [y, {}_v x]], \quad \text{где } u > v \geqslant 1.$$

Благодаря холловскому виду для данных показателей степеней были найдены выражения по модулю простого n, в частности, когда вес коммутатора равен n.

Основные результаты параграфа 2.1 опубликованы в совместной работе [24] (в соавторстве с Г. П. Егорычевым и С. Г. Колесниковым), результаты параграфа 2.2 — в работе автора [23].

В **главе 3** диссертации для любых натуральных чисел $n \geqslant (p+2)/3$ и $m \geqslant 3$, где p — такое нечетное простое число, что $(p+2)/3$ — целое, доказана нерегулярность группы $(n \times n)$-матриц

$$\{E + (a_{ij}) \mid a_{ij} \in \mathbb{Z}_{p^m} \text{ при } i > j;\ a_{ij} \in \langle p \rangle \text{ при } i \leqslant j\}, \tag{9}$$

являющейся силовской p-подгруппой общей линейной группы $GL_n(\mathbb{Z}_{p^m})$.

В **§ 3.1** получено необходимое условие регулярности конечной p-группы: для любого целого $j \geqslant 0$ и любых элементов a и b регулярной p-группы G существует элемент $d \in \langle a, b \rangle$ такой, что отрезок собирательной формулы Ф. Холла для $(ab)^p$, содержащий коммутаторы весов $p, p+1, \ldots, p+j$, равен d^p по модулю $\Gamma_{p+j+1}(G)$. С помощью результатов главы 2 полученное равенство удалось записать в явном виде при $j = 0$, когда любой коммутатор, имеющий более двух вхождений b, равен 1, а при весе $\geqslant p$ имеет порядок 1 или p.

В **§ 3.2** найден контрпример к указанному необходимому условию для группы (9) при $n = (p+2)/3$ и $m = 3$:

$$a = E + A, \quad b = E + pB, \qquad \text{где } A = e_{21} + e_{32} + \cdots + e_{n,n-1},\ B = e_{1n},$$

E — единичная матрица, e_{ij} — матрица с единицей на позиции (i, j) и нулями на остальных позициях. Тем самым доказана нерегулярность группы (9) при $n \geqslant (p+2)/3$ и $m \geqslant 3$, поскольку свойство регулярности наследуется подгруппами и факторгруппами (теорема 3.2.1).

Основные результаты параграфов 2.1 и 2.2 опубликованы в совместной работе [25] (в нераздельном соавторстве с С. Г. Колесниковым).

Все основные результаты диссертации являются новыми и опубликованы в работах [22–35]. Статьи [22–26] входят в издания, рекомендованные ВАК для публикации результатов диссертации. Диссертация носит теоретический характер и может быть использована при исследовании проблем комбинаторной теории групп, при изучении проблем бернсайдовского типа, а также для проверки конечных p-групп на регулярность. Кроме того, результаты диссертации могут быть полезны при составлении программ специальных курсов для студентов математических направлений.

Апробация результатов. Основные результаты работы докладывались и обсуждались на следующих семинарах и конференциях.

1. Международная конференция студентов, аспирантов и молодых ученых «Молодежь и наука: Проспект Свободный» (СФУ, г. Красноярск, 2016 г.);

2. Двадцатый Всероссийский конкурс студенческих работ им. Августа Мебиуса (НМУ, г. Москва, 2016 г.);
3. Международная конференция студентов, аспирантов и молодых ученых «Проспект Свободный — 2018» (СФУ, г. Красноярск, 2018 г.);
4. Международная конференция студентов, аспирантов и молодых ученых «Проспект Свободный — 2019» (СФУ, г. Красноярск, 2019 г.);
5. 57-ая Международная научная студенческая конференция МНСК-2019 (НГУ, г. Новосибирск, 2019 г.);
6. Международная конференция студентов, аспирантов и молодых ученых «Проспект Свободный — 2020» (СФУ, г. Красноярск, 2020 г.);
7. Международная конференция математических центров мирового уровня (Образовательный центр Сириус, г. Сочи, 2021 г.);
8. Городской алгебраический семинар им. Д. К. Фаддеева (ПОМИ РАН, г. Санкт-Петербург, 2021 г.);
9. Международная конференция «Мальцевские чтения» (ИМ СО РАН, г. Новосибирск, 2022 г.);
10. Международная конференция по теории групп, посвященная 80-летию В. Д. Мазурова (ИМ СО РАН, НГУ, г. Новосибирск, 2023 г.);
11. Городской алгебраический семинар (СФУ, г. Красноярск, 2024 г.).

Автор искренне благодарит своего научного руководителя Сергея Геннадьевича Колесникова за постановку задач, обсуждение полученных научных результатов и помощь в оформлении текста диссертации. Отдельного упоминания заслуживает д-р физ.-мат. наук Георгий Петрович Егорычев, с которым автор имел честь заниматься исследованиями, связанными с темой диссертации.

Автор выражает благодарность коллективу кафедры алгебры и математической логики Института математики и фундаментальной информатики СФУ за хорошие условия работы над диссертацией.

Исследования по части главы 3, частично главы 2, параграфа 1.3 поддержаны Красноярским математическим центром, финансируемым Минобрнауки РФ (Соглашение 075-02-2024-1429). Основные результаты параграфов 1.1, 1.2 и 1.4 получены при поддержке Российского научного фонда (Проект № 22-21-00733).

Глава 1. Собирательный процесс

В главе 1 диссертации представлен подход к исследованию делимости показателей степеней коммутаторов, возникающих в ходе собирательного процесса, примененного к положительному слову свободной группы.

В § 1.1 вводится система базовых понятий и обозначений, рассматриваются основные свойства собирательного процесса. В § 1.2 доказывается равенство показателя степени коммутатора R и количества элементов множества $D(R)$, удовлетворяющих формуле E_R. Здесь $D(R)$ — множество целочисленных последовательностей конечной длины, определяемое коммутатором R, а E_R — формула, состоящая из операций конъюнкции, дизъюнкции, предиката равенства и предикатов, логические значения которой определяются структурой начального слова, к которому был применен собирательный процесс. Далее, в § 1.3 находится выражение с определенным свойством делимости для искомого количества элементов в случае, когда E_R, иными словами, начальное слово, и $D(R)$ удовлетворяют особым ограничениям. Наконец, в § 1.4 полученные результаты применяются для доказательства собирательных формул со свойствами делимости показателей степеней коммутаторов.

1.1 Базовые понятия и утверждения

Определение 1.1.1. Для букв $a_1, \dots, a_n$, $n \in \mathbb{N}$, определим индуктивно множество *формальных коммутаторов* $\Gamma(a_1, \dots, a_n)$ и функцию *веса* w:

1) $\{a_1, \dots, a_n\} \subset \Gamma(a_1, \dots, a_n)$, $w(a_1) = \dots = w(a_n) = 1$;

2) если $c_1, c_2 \in \Gamma(a_1, \dots, a_n)$, то $[c_1, c_2] \in \Gamma(a_1, \dots, a_n)$ и $w([c_1, c_2]) = w(c_1) + w(c_2)$.

Определение 1.1.2. Конечную последовательность коммутаторов из множества $\Gamma(a_1, \dots, a_n)$ назовем *коммутаторным словом.* Будем говорить, что два коммутаторных слова $c_1 \dots c_m$ и $d_1 \dots d_k$ равны и писать $c_1 \dots c_m \equiv d_1 \dots d_k$ тогда и только тогда, когда они совпадают посимвольно, т.е. равны их длины $m = k$ и $c_i = d_i$ для $i \in \overline{1, m}$.

Пример 1.1.1. Коммутаторные слова длины 1, 2 и 3 соответственно:

$$[a_1, a_2], \qquad a_3[a_1, a_2], \qquad [a_3, [a_1, a_2]]a_3[a_1, a_2].$$

В ходе собирательного процесса удобно работать с коммутаторными словами (последовательностями формальных символов) вместо произведений элементов группы. После завершения собирательного процесса коммутаторные слова уже рассматриваются как элементы свободной группы $F(a_1, \dots, a_n)$, причем $[y, x] = y^{-1}x^{-1}yx$ для любых $x, y \in F(a_1, \dots, a_n)$, т.е. происходит переход от формальных коммутаторов к теоретико-групповым.

Почти всюду ниже в этой главе мы имеем дело только с формальными коммутаторами, поэтому будем опускать прилагательное «формальный» и вместо «формальный коммутатор» писать просто «коммутатор».

Если коммутаторное слово содержит несколько вхождений одного коммутатора, мы должны ясно отличать их друг от друга. Для этого будет естественным использовать следующий инструмент.

Определение 1.1.3. Пусть коммутаторное слово X длины $m \geqslant 1$ содержит вхождение коммутатора R. Поставим в соответствие этому вхождению некоторую конечную целочисленную последовательность и будем называть ее *меткой* вхождения R. Если любые два различные вхождения одного и того же коммутатора в X имеют различные метки одинаковой длины, тогда отображение, которое числу $i \in \overline{1,m}$ ставит в соответствие метку вхождения коммутатора на i-ой позиции, будем называть *разметкой* X.

Если вхождение коммутатора R имеет метку Λ и нам необходимо явно указать на этот факт, мы будет обозначать это вхождение $R(\Lambda)$. Очевидно, любое коммутаторное слово $t_1 \dots t_m$ допускает разметку, например: $t_1(1) \dots t_m(m)$. Далее будем использовать мультипликативную форму записи для операции конкатенации конечных целочисленных последовательностей. Например, если $\Lambda_1 = (1,1,2)$, $\Lambda_2 = (1,2)$, то $\Lambda_1\Lambda_2 = (1,1,2,1,2)$.

Определение 1.1.4. Пусть $X \equiv t_1(\Lambda_1) \dots t_m(\Lambda_m)$ — произвольное коммутаторное слово с некоторой разметкой, в котором существует ровно $e \geqslant 1$ вхождений коммутатора q. *Этапом собирательного процесса*, примененного к X, будем называть преобразование слова X к слову Y по следующим алгоритму. Пусть $t_{i_1}(\Lambda_{i_1}), \dots, t_{i_e}(\Lambda_{i_e})$ — все вхождения q в X, и $1 \leqslant i_1 < \dots < i_e \leqslant n$. Передвигаем $t_{i_1}(\Lambda_{i_1})$ в начало слова, последовательно меняя местами соседние вхождения коммутаторов по правилу

$$y(\Lambda_u)x(\Lambda_v) = x(\Lambda_v)y(\Lambda_u)[y,x](\Lambda_u\Lambda_v).$$

Затем таким же образом передвигаем вхождение $t_{i_2}(\Lambda_{i_2})$, пока оно не окажется непосредственно справа от $t_{i_1}(\Lambda_{i_1})$. Продолжая аналогично, получаем

$$Y \equiv t_{i_1}(\Lambda_{i_1}) \dots t_{i_e}(\Lambda_{i_e}) \prod_{i=1}^{m'} t'_i \equiv q^e T,$$

где слово T включает все коммутаторы из X, кроме q, а также коммутаторы, возникшие при сборе вхождений q. Все вхождения коммутаторов в T помечены.

Определение 1.1.5. Пусть W_0 — произвольное коммутаторное слово с некоторой разметкой, составленное из коммутаторов веса 1. *Собирательным процессом*, примененным к W_0, будем называть построение последовательности коммутаторных слов

$$\left\{W_j \equiv q_1^{e_1} \dots q_j^{e_j} T_j\right\}_{j \geqslant 0} \tag{10}$$

по следующему правилу. Слово W_j, $j \geqslant 1$, получено с помощью j-ого этапа собирательного процесса, примененного к слову T_{j-1}, в ходе которого собирались вхождения произвольно выбранного в T_{j-1} коммутатора q_j. Слова $q_1^{e_1} \dots q_j^{e_j}$ и T_j называем, соответственно, *собранная часть* и *несобранная часть* слова W_j. Начальное слово $W_0 \equiv T_0$ с пустой собранной частью будем считать результатом нулевого этапа собирательного процесса.

Будем использовать следующие обозначения для коммутаторов:

$$[y, {}_0x] = y; \qquad [y, {}_ix] = [[y, {}_{i-1}x], x], \quad i \geqslant 1; \qquad [y, x, z] = [[y, x], z].$$

Пример 1.1.2. Пусть $W_0 \equiv a_1(1)a_2(1)a_1(2)a_2(2)$. Представим возможный вариант собирательного процесса, примененного к слову W_0 (для наглядности несобранные части слов отделены точкой):

$$\begin{aligned}
&W_0 \equiv a_1(1)a_2(1)a_1(2)a_2(2),\\
&W_1 \equiv a_1(1)a_1(2) \cdot a_2(1)[a_2, a_1](1,2)a_2(2),\\
&W_2 \equiv a_1(1)a_1(2)a_2(1)a_2(2) \cdot [a_2, a_1](1,2)[a_2, a_1, a_2](1,2,2),\\
&W_3 \equiv a_1(1)a_1(2)a_2(1)a_2(2)[a_2, a_1](1,2) \cdot [a_2, a_1, a_2](1,2,2),\\
&W_4 \equiv a_1(1)a_1(2)a_2(1)a_2(2)[a_2, a_1](1,2)[a_2, a_1, a_2](1,2,2).
\end{aligned}$$

Собрав коммутаторы в следующем порядке: a_1, a_2, $[a_2, a_1]$, $[a_2, a_1, a_2]$, мы получили слово $W_4 \equiv a_1^2 a_2^2 [a_2, a_1][a_2, a_1, a_2]$ с пустой несобранной частью.

Отметим, что последовательность (10) может быть конечной в двух случаях: мы решили остановить собирательный процесс на некотором этапе, собирательный процесс оборвался на некотором слове W_j, $j \geqslant 1$, несобранная часть которого оказалась пустой.

Любой коммутатор из $\Gamma(a_1, \ldots, a_n)$ можно записать разными способами, например,

$$\Big[\big[[a_2, a_1], a_1\big], a_1\Big] = [a_2, {}_3a_1] = \big[[a_2, a_1], {}_2a_1\big] = \big[[a_2, {}_3a_1], {}_0a_3\big].$$

Далее мы будем придерживаться следующего важного соглашения.

Замечание 1.1.1. *Для любых коммутаторов $Q, R \in \Gamma(a_1, \ldots, a_n)$, мы можем использовать запись $[Q, {}_uR]$ только с максимально возможным значением параметра u, т.е. для любого $S \in \Gamma(a_1, \ldots, a_n)$ имеем $[Q, {}_uR] \neq [S, {}_{u+1}R]$.*

Отметим некоторые очевидные факты о собирательном процессе.

Предложение 1.1.1. *Рассмотрим произвольное слово W_j, $j \geqslant 1$, из последовательности (10). Справедливы следующие утверждения.*

1. *В свободной группе $F(a_1, \ldots, a_n)$ имеет место равенство $W_0 = W_j$. Иными словами, собирательный процесс не изменяет элемент $W_0 \in F(a_1, \ldots, a_n)$.*

2. *Если несобранная часть T_j непуста, тогда любой коммутатор в T_j имеет вид $[R, {}_pq_j]$ для некоторых $R \in \Gamma(a_1, \ldots, a_n)$ и $p \geqslant 0$.*

3. *Любые два вхождения одного коммутатора в T_j имеют различные метки одинаковой длины. Иными словами, метки в T_j образуют разметку слова T_j. Более того, метки не меняются в ходе собирательного процесса.*

4. *Если вхождение $R(\Lambda_u)$ предшествует (находится левее) $Q(\Lambda_v)$ в T_{j-1} и $R \neq q_j$, $Q \neq q_j$, то $R(\Lambda_u)$ предшествует $Q(\Lambda_v)$ в T_j. Иными словами, j-ый этап собирательного процесса не меняет относительное расположение вхождений коммутаторов в T_{j-1}, отличных от q_j.*

Поскольку начальное слово W_0 содержит только коммутаторы $a_1, \ldots, a_n$, справедливо следующее утверждение.

Предложение 1.1.2. *Для любого коммутаторного слова W_j, $j \geqslant 1$, из последовательности (10) несобранная часть T_j не содержит вхождений коммутаторов $q_1, \ldots, q_j$. Как следствие, коммутаторы $q_1, \ldots, q_j$ попарно различны.*

Доказательство. Индукция по номеру этапа собирательного процесса (по номеру слова в последовательности). На первом этапе были собраны все вхождения q_1, при этом возникали только коммутаторы вида $[R, {}_p q_j]$, $p \geqslant 1$. Следовательно, слово W_1 содержит вхождения q_1 только в собранной части.

Предположим, что утверждение выполняется для всех слов в последовательности до $W_j = q_1^{e_1} \ldots q_j^{e_j} T_j$, $j \geqslant 1$, включительно, и несобранная часть T_j оказалась непустой. Докажем утверждение для слова

$$W_{j+1} = q_1^{e_1} \ldots q_k^{e_K} \ldots q_j^{e_j} q_{j+1}^{e_{j+1}} T_{j+1}.$$

Предположим, что q_k имеет вхождение в T_{j+1} для некоторого $k \in \overline{1, j+1}$. Заметим, что $k \neq j+1$, т.к. на этапе $j+1$ все вхождения q_{j+1} в слове T_j были собраны. Далее, на этапе k были собраны все вхождения коммутатора q_k. Из предположения индукции следует, что новые вхождения q_k могли возникнуть только на этапе $j+1$. Следовательно, $q_k = [R, q_{j+1}]$ для некоторого коммутатора R. Напомним, что начальное слово W_0 содержит только элементы $a_1, \ldots, a_n$, поэтому коммутатор $q_k = [R, q_{j+1}]$ возник в ходе собирательного процесса не некотором этапе h, где $h < k < j+1$, т.е. $q_k = [Q, q_h]$ для некоторого Q. Из равенства формальных коммутаторов $[R, q_{j+1}] = [Q, q_h]$ следует, что $q_h = q_{j+1}$. Получаем противоречие с предположением индукции: q_h имеет вхождения как в собранную часть $q_1^{e_1} \ldots q_j^{e_j}$, так и в несобранную часть T_j. $\square$

1.2 Условия существования и предшествования

Пусть W_0 — произвольное коммутаторное слово с некоторой разметкой, содержащее только коммутаторы веса 1: $a_1, \ldots, a_n$, $n \geqslant 1$. Рассмотрим произвольный вариант собирательного процесса

$$\left\{W_j \equiv q_1^{e_1} \ldots q_j^{e_j} T_j\right\}_{j \geqslant 0}. \tag{11}$$

Обозначим через $D(a_k)$, $k \in \overline{1, n}$, произвольное фиксированное множество целочисленных последовательностей одинаковой длины, содержащее все метки вхождений a_k в W_0.

Предположим, что несобранная часть T_m, $m \geqslant 0$ содержит некоторый коммутатор R со следующей бесскобочной записью: $(a_{i_1}, \ldots, a_{i_{w(R)}})$.

Пример 1.2.1. Коммутатор $\Big[\big[a_2, [a_1, a_2]\big], a_4\Big]$ имеет бесскобочную запись (a_2, a_1, a_2, a_4).

Из определения 1.1.4 следует, что метка любого вхождения R в T_m имеет вид

$$\Lambda_1 \ldots \Lambda_{w(R)}, \quad \text{где } \Lambda_1 \in D(a_{i_1}),\ \ldots,\ \Lambda_{w(R)} \in D(a_{i_{w(R)}}).$$

Поскольку различные вхождения R имеют различные метки, число всех вхождений R в T_m равно количеству элементов из декартова произведения $D(a_{i_1}) \times \cdots \times D(a_{i_{w(R)}})$, которые являются метками вхождений R. Обозначим это декартово произведение через $D(R)$.

Определение 1.2.1. Предположим, что некоторая несобранная часть в (11) содержит вхождение коммутатора R. *Условие существования* коммутатора R есть предикат E_R^{Λ}, $\Lambda \in D(R)$, который равен 1 тогда и только тогда, когда существует слово в (11), несобранная часть которого содержит вхождение $R(\Lambda)$.

Определение 1.2.2. Предположим, что некоторая несобранная часть в (11) содержит вхождения коммутаторов R и Q. *Условие предшествования* для коммутаторов R и Q есть предикат $P_{Q,R}^{\Lambda_1\Lambda_2}$, $\Lambda_1\Lambda_2 \in D(Q) \times D(R)$, который равен 1 тогда и только тогда, когда существует слово в (11), в несобранной части которого $Q(\Lambda_1)$ предшествует (находится левее) $R(\Lambda_2)$.

Отметим, что можно определить все значения предиката E_R, рассматривая произвольную несобранную часть T_m, содержащую вхождения R. Иными словами, любая несобранная часть либо не содержит вхождений R, либо содержит все вхождения R, которые когда-либо возникли в ходе собирательного процесса. Действительно, вхождения R возникли на некотором этапе $m_1 \leqslant m$. Из утверждения 3 предложения 1.1.1 следует, что метки вхождений не изменятся на следующих этапах собирательного процесса. Согласно предложению 1.1.2 новые вхождения R никогда не возникнут в несобранных частях. Наконец, вхождения могут «пропасть» только на некотором этапе $m_2 > m \geqslant m_1$, когда все они без исключения будут собраны.

Из рассуждений выше и утверждения 4 предложения 1.1.1 следует, что все значения предиката $P_{Q,R}$ можно определить, рассматривая произвольную несобранную часть, содержащую вхождения R и Q.

Предложение 1.2.1. *Для последовательности (11) имеем равенство*

$$e_j = |\{\Lambda \in D(q_j) \mid E_{q_j}^{\Lambda} = 1\}|.$$

Данное утверждение устанавливает связь между показателем степени коммутатора e_j и его условием существования E_{q_j}. Поэтому, исследуя свойства предиката E_{q_j}, мы получаем информацию о показателе степени e_j.

Определение 1.2.3. Для произвольных коммутаторов R_1, R_2 предикат $R_1 \prec R_2$ равен 1 тогда и только тогда, когда существуют коммутаторы q_i, q_j в (11) такие, что $q_i = R_1$, $q_j = R_2$, $i < j$, т.е., вхождения R_1 были собраны на более раннем этапе, чем вхождения R_2, в ходе собирательного процесса (11).

Пример 1.2.2. Рассмотрим вариант собирательного процесса из примера 1.1.2. Имеют место следующие соотношения:

$$
\begin{aligned}
&D(a_1) = D(a_2) = \{1, 2\};\\
&D([a_2, a_1]) = D(a_2) \times D(a_1) = \{(1,1), (1,2), (2,1), (2,2)\};\\
&D([a_2, a_1, a_2]) = D(a_2) \times D(a_1) \times D(a_2) = \{1, 2\}^3;\\
&E_{a_1}^{\lambda_1} = E_{a_2}^{\lambda_2} = 1,\ P_{a_1,a_2}^{(\lambda_1,\lambda_2)} = (\lambda_1 < \lambda_2) \vee (\lambda_1 = \lambda_2), \quad \text{где } \lambda_1 \in D(a_1),\ \lambda_2 \in D(a_2);\\
&a_1 \prec a_2;\ [a_2, a_1] \prec [a_2, a_1, a_2];\\
&e_3 = \left| \left\{ (\lambda_1, \lambda_2) \in D([a_2, a_1]) \mid E_{[a_2,a_1]}^{(\lambda_1,\lambda_2)} = 1 \right\} \right| = |\{(1,2)\}| = 1.
\end{aligned}
$$

Теорема 1.2.1. *Пусть G — группа, $m \in \mathbb{N}$ и $y, x_1, x_2, \ldots, x_m \in G$. Тогда справедливо следующее тождество:*

$$[y, x_1 x_2 \ldots x_m] = \prod_{i=1}^{2^m-1} [y, {}_{i_1}x_1, {}_{i_2}x_2, \ldots, {}_{i_m}x_m], \tag{12}$$

где $\overline{i_1 i_2 \ldots i_m}$ — m-разрядное двоичное представление индекса i.

Доказательство. Индукцией по m докажем эквивалентное тождество:

$$y x_1 x_2 \ldots x_m = x_1 x_2 \ldots x_m y \prod_{i=1}^{2^m-1} [y, {}_{i_1}x_1, {}_{i_2}x_2, \ldots, {}_{i_m}x_m]. \tag{13}$$

Для $m = 1$ тождество примет вид $y x_1 = x_1 y [y, x_1]$. Рассмотрим произведение $y x_1 x_2 \ldots x_m x_{m+1}$. Используя предположение индукции, получаем

$$
\begin{aligned}
(y x_1 \ldots x_m) x_{m+1} &= x_1 \ldots x_m y \left(\prod_{i=1}^{2^m-1} [y, {}_{i_1}x_1, \ldots, {}_{i_m}x_m] \right) x_{m+1}\\
&= x_1 \ldots x_{m+1} \prod_{i=0}^{2^m-1} [y, {}_{i_1}x_1, \ldots, {}_{i_m}x_m, {}_0x_{m+1}][y, {}_{i_1}x_1, \ldots, {}_{i_m}x_m, {}_1x_{m+1}],
\end{aligned}
$$

где $\overline{i_1 \ldots i_m 0}$ и $\overline{i_1 \ldots i_m 1}$ являются двоичными представлениями чисел $2i$ и $2i+1$, соответственно. Таким образом, имеем равенство

$$(y x_1 \ldots x_m) x_{m+1} = x_1 \ldots x_{m+1} \prod_{i=0}^{2^{m+1}-1} [y, {}_{i_1}x_1, \ldots, {}_{i_m}x_m, {}_{i_{m+1}}x_{m+1}],$$

где $\overline{i_1 \ldots i_{m+1}}$ — двоичное представление индекса i. □

Пример 1.2.3. При $m = 2$ тождество (12) принимает вид хорошо известной формулы (см., например, [12]):

$$[y, x_1 x_2] = [y, {}_0x_1, {}_1x_2][y, {}_1x_1, {}_0x_2][y, {}_1x_1, {}_1x_2] = [y, x_2][y, x_1][y, x_1, x_2].$$

Доказанная теорема позволяет выразить факт предшествования для двух вхождений коммутаторов в терминах предшествования для двух двоичных чисел.

Мы обозначаем через $\vee$ и $\wedge$ дизъюнкцию и конъюнкцию соответственно. Символ $\wedge$ обычно будет опускаться для экономии места. Например, мы пишем $AB \vee C$ вместо $(A \wedge B) \vee C$.

Обозначим через $\omega(i)$ количество единиц в двоичной записи целого неотрицательного числа i.

Предложение 1.2.2. *Пусть $N, M \in \overline{1, 2^m - 1}$, $\omega(N) = u$, $\omega(M) = v$, где $u, v, m \geqslant 1$. Предположим, что в последовательностях $(j_1, \ldots, j_u)$ и $(k_1, \ldots, k_v)$ элементы j_s, $s \in \overline{1, u}$, и k_l, $l \in \overline{1, v}$ равны номерам позиций s-ой единицы и l-ой единицы в двоичных записях N и M соответственно (отсчитываем единицы и номера позиций слева направо, начиная с 1). Тогда*

$$N < M \;\Leftrightarrow\; (u < v) \bigwedge_{t=1}^{u} (j_t = k_t) \vee \bigvee_{t=1}^{\min\{u,v\}} (k_t < j_t) \bigwedge_{h=1}^{t-1} (j_h = k_h).$$

Следствие 1.2.1. *Пусть $F(Q, R)$ — свободная группа и коммутаторное слово*

$$W_0 \equiv Q(\Lambda_0) R(\Lambda_1) \ldots R(\Lambda_m), \quad m \in \mathbb{N}, \tag{14}$$

имеет произвольную разметку с некоторыми множествами $D(Q)$ и $D(R)$. Если на первом этапе собирательного процесса мы соберем вхождения R, тогда получим коммутаторное слово

$$W_1 \equiv R(\Lambda_1) \ldots R(\Lambda_m) \cdot Q(\Lambda_0) \prod_{i=1}^{2^m-1} [Q, {}_{\omega(i)}R](\phi(i)), \tag{15}$$

где $\phi(i) = \Lambda_0\Lambda_{j_1}\dots\Lambda_{j_{\omega(i)}}$ *и* j_s, $s \in \overline{1,\omega(i)}$ *есть номер позиции* s*-ой единицы в двоичном представлении индекса* i *(отсчитываем единицы и номера позиций слева направо, начиная с 1). Более того, для любых* $u, v \in \mathbb{N}$ *имеем*

$$E^{\Lambda_0^1\Lambda_1^1\dots\Lambda_u^1}_{[Q,{}_uR]} = E^{\Lambda_0^1}_{Q} \bigwedge_{k=1}^{u-1} P^{\Lambda_k^1\Lambda_{k+1}^1}_{R,R},$$

$$P^{\Lambda_0^1\dots\Lambda_u^1\Lambda_0^2\dots\Lambda_v^2}_{[Q,{}_uR],[Q,{}_vR]}$$

$$= E^{\Lambda_0^1\dots\Lambda_u^1}_{[Q,{}_uR]} E^{\Lambda_0^2\dots\Lambda_v^2}_{[Q,{}_vR]} \left((u < v) \bigwedge_{k=1}^{u} (\Lambda_k^2 = \Lambda_k^1) \vee \bigvee_{k=1}^{\min\{u,v\}} P^{\Lambda_k^2\Lambda_k^1}_{R,R} \bigwedge_{h=1}^{k-1} (\Lambda_h^2 = \Lambda_h^1) \right),$$

где $\Lambda_0^1, \Lambda_0^2 \in D(Q)$*,* $\Lambda_1^1, \dots, \Lambda_u^1, \Lambda_1^2, \dots, \Lambda_v^2 \in D(R)$*.*

Доказательство. Первое утверждение следствия непосредственно вытекает из тождества (13).

Рассмотрим произведение по i в (15). Любое m-разрядное двоичное число однозначно задается позициями единиц в своей двоичной записи. Следовательно, ϕ является биективным отображением множества $\{1, \dots, 2^m - 1\}$ на

$$\{\Lambda_0\Lambda_{j_1}\dots\Lambda_{j_s} \mid s \geqslant 1,\ 1 \leqslant j_1 < \dots < j_s \leqslant m\}.$$

Любые две целочисленные последовательности

$$\Lambda_0\Lambda_{j_1}\dots\Lambda_{j_u} \in D([Q,{}_uR]) = D(Q) \times D(R)^u,$$
$$\Lambda_0\Lambda_{k_1}\dots\Lambda_{k_v} \in D([Q,{}_vR]) = D(Q) \times D(R)^v$$

являются метками некоторых вхождений коммутаторов $[Q,{}_uR]$ и $[Q,{}_vR]$ в (15), соответственно, тогда и только тогда, когда $\Lambda_0\Lambda_{j_1}\dots\Lambda_{j_u} = \phi(i_1)$, $\Lambda_0\Lambda_{k_1}\dots\Lambda_{k_v} = \phi(i_2)$ для некоторых i_1, i_2. Иными словами, должны выполняться следующие условия:

$$\bigwedge_{t=1}^{u-1} (j_t < j_{t+1}), \quad \bigwedge_{t=1}^{v-1} (k_t < k_{t+1}).$$

Если при этом вхождение $[Q, {}_uR]$ должно предшествовать вхождению $[Q, {}_vR]$, то мы получаем условие $i_1 < i_2$. Согласно предложению 1.2.2, оно эквивалентно

$$\bigwedge_{t=1}^{u-1}(j_t < j_{t+1}) \bigwedge_{t=1}^{v-1}(k_t < k_{t+1})$$
$$\wedge \left((u < v) \bigwedge_{t=1}^{u}(j_t = k_t) \vee \bigvee_{t=1}^{\min\{u,v\}} (k_t < j_t) \bigwedge_{h=1}^{t-1}(j_h = k_h) \right).$$

Отметим, что

$$j_t < j_{t+1} \Leftrightarrow P_{R,R}^{\Lambda_{j_t}\Lambda_{j_{t+1}}}, \quad k_t < k_{t+1} \Leftrightarrow P_{R,R}^{\Lambda_{k_t}\Lambda_{k_{t+1}}},$$
$$j_t = k_t \Leftrightarrow \Lambda_{j_t} = \Lambda_{k_t}, \quad k_t < j_t \Leftrightarrow P_{R,R}^{\Lambda_{k_t}\Lambda_{j_t}}.$$

Таким образом, для любых $\Lambda_0^1, \Lambda_0^2 \in D(Q)$, $\Lambda_1^1, \ldots, \Lambda_u^1, \Lambda_1^2, \ldots, \Lambda_v^2 \in D(R)$ справедливы равенства:

$$E_{[Q,{}_uR]}^{\Lambda_0^1\Lambda_1^1\ldots\Lambda_u^1} = E_Q^{\Lambda_0^1} \bigwedge_{k=1}^{u} E_R^{\Lambda_k^1} \bigwedge_{k=1}^{u-1} P_{R,R}^{\Lambda_k^1\Lambda_{k+1}^1} = E_Q^{\Lambda_0^1} \bigwedge_{k=1}^{u-1} P_{R,R}^{\Lambda_k^1\Lambda_{k+1}^1},$$

$$P_{[Q,{}_uR],[Q,{}_vR]}^{\Lambda_0^1\ldots\Lambda_u^1\Lambda_0^2\ldots\Lambda_v^2}$$
$$= E_{[Q,{}_uR]}^{\Lambda_0^1\ldots\Lambda_u^1} E_{[Q,{}_vR]}^{\Lambda_0^2\ldots\Lambda_v^2} \left((u < v) \bigwedge_{k=1}^{u}(\Lambda_k^2 = \Lambda_k^1) \vee \bigvee_{k=1}^{\min\{u,v\}} P_{R,R}^{\Lambda_k^2\Lambda_k^1} \bigwedge_{h=1}^{k-1}(\Lambda_h^2 = \Lambda_h^1) \right).$$

□

Следствие 1.2.2. *Пусть существует $e \geqslant 1$ вхождений коммутатора R в следующее коммутаторное слово с произвольной разметкой:*

$$X \equiv \prod_{k=1}^{m} t_k(\Lambda_k).$$

После одного этапа собирательного процесса мы получим слово

$$Y \equiv R^e \prod_{\substack{k=1 \\ t_k \neq R}}^{m} t_k(\Lambda_k)\Omega_k, \quad \text{где} \;\; \Omega_k \equiv \prod_{i=1}^{2^{m_k}-1} [t_k, {}_{\omega(i)}R](\phi_k(i)),$$

m_k — число вхождений R, находящихся правее $t_k(\Lambda_k)$ в слове X, метка $\phi_k(i)$ определена согласно предыдущей теореме.

Далее Ω_k будем называть *ω-произведением с начальным элементом* $t_k(\Lambda_k)$.

Теорема 1.2.2. *Пусть $\{W_j\}_{j\geqslant 0}$ — произвольный вариант собирательного процесса. Тогда имеют место следующие рекуррентные соотношения (если левая часть соотношения определена для $\{W_j\}_{j\geqslant 0}$):*

$$E^{\Lambda_0^1\dots\Lambda_u^1}_{[Q_1,\,_uR_1]} = P^{\Lambda_0^1\Lambda_1^1}_{Q_1,R_1}\bigwedge_{k=1}^{u-1} P^{\Lambda_k^1\Lambda_{k+1}^1}_{R_1,R_1}, \quad u\geqslant 1; \tag{16}$$

$P^{\Lambda_0^1\dots\Lambda_u^1\Lambda_0^2\dots\Lambda_v^2}_{[Q_1,\,_uR_1],[Q_2,\,_vR_2]}$ *равен*

$$E^{\Lambda_0^1\dots\Lambda_u^1}_{[Q_1,\,_uR_1]}E^{\Lambda_0^2\dots\Lambda_v^2}_{[Q_2,\,_vR_2]}F, \qquad \text{если } u+v\geqslant 1,\ R_1=R_2,\ Q_1=Q_2; \tag{17a}$$

$$E^{\Lambda_0^1\dots\Lambda_u^1}_{[Q_1,\,_uR_1]}E^{\Lambda_0^2\dots\Lambda_v^2}_{[Q_2,\,_vR_2]}P^{\Lambda_0^1\Lambda_0^2}_{Q_1,Q_2}, \qquad \begin{array}{l}\text{если } u+v\geqslant 1,\ R_1=R_2,\ Q_1\neq Q_2,\\ u=0\Rightarrow w(Q_1)=1,\ v=0\Rightarrow w(Q_2)=1;\end{array} \tag{17b}$$

$$E^{\Lambda_0^1\dots\Lambda_u^1}_{[Q_1,\,_uR_1]}E^{\Lambda_0^2\dots\Lambda_v^2}_{[Q_2,\,_vR_2]}P^{\Lambda_0^1\dots\Lambda_u^1\Lambda_0^2}_{[Q_1,\,_uR_1],Q_2}, \ \text{если } u,v\geqslant 1, \quad R_1\prec R_2; \tag{17c}$$

$$E^{\Lambda_0^1\dots\Lambda_u^1}_{[Q_1,\,_uR_1]}E^{\Lambda_0^2\dots\Lambda_v^2}_{[Q_2,\,_vR_2]}P^{\Lambda_0^1\Lambda_0^2\dots\Lambda_v^2}_{Q_1,[Q_2,\,_vR_2]}, \ \text{если } u,v\geqslant 1, \quad R_2\prec R_1; \tag{17d}$$

где $[Q_1,\,_uR_1]\neq Q_2$ *для* $u\geqslant 1$ *и* $[Q_2,\,_vR_2]\neq Q_1$ *для* $v\geqslant 1$,

$$\Lambda_0^1\in D(Q_1),\ \Lambda_0^2\in D(Q_2),\ \Lambda_1^1,\dots,\Lambda_u^1\in D(R_1),\ \Lambda_1^2,\dots,\Lambda_v^2\in D(R_2),$$

$$F = P^{\Lambda_0^1\Lambda_0^2}_{Q_1,Q_2}\vee(\Lambda_0^1=\Lambda_0^2)\Bigg((u<v)\bigwedge_{k=1}^{u}(\Lambda_k^2=\Lambda_k^1)\vee\bigvee_{k=1}^{\min\{u,v\}}P^{\Lambda_k^2\Lambda_k^1}_{R_1,R_2}\bigwedge_{h=1}^{k-1}(\Lambda_h^2=\Lambda_h^1)\Bigg).$$

Доказательство. Соотношения (16) и (17a). Пусть $u,v\geqslant 1$. Поскольку условие существования $E_{[Q_1,\,_uR_1]}$ определено для $\{W_j\}_{j\geqslant 0}$, существуют вхождения коммутатора $[Q_1,\,_uR_1]$ в некоторую несобранную часть T_m. Следовательно, они возникли в ходе l-ого этапа собирательного процесса, $l\in\overline{1,m}$, когда собирались вхождения коммутатора R_1. Рассмотрим схематичную запись коммутаторного слова T_{l-1}, где выделим два вхождения Q_1 (хотя бы одно такое вхождение существует):

$$T_{l-1} = \dots Q_1(\Lambda_1)\dots Q_1(\Lambda_2)\dots.$$

Из следствия 1.2.2 заключаем, что T_l имеет следующий вид:

$$T_l = \dots Q_1(\Lambda_1)\Omega_{Q_1(\Lambda_1)}\dots Q_1(\Lambda_2)\Omega_{Q_1(\Lambda_2)}\dots,$$

где $\Omega_{Q_1(\Lambda_1)}$, $\Omega_{Q_1(\Lambda_2)}$ являются ω-произведениями с соответствующими начальными элементами.

Пусть $\Lambda_0^1 \in D(Q_1)$, $\Lambda_1^1, \ldots, \Lambda_u^1 \in D(R_1)$ и $P_{Q_1,R_1}^{\Lambda_0^1\Lambda_1^1} = 1$. Тогда согласно следствию 1.2.1 вхождение $[Q_1, {}_uR_1](\Lambda_0^1 \ldots \Lambda_u^1)$ присутствует в ω-произведении с начальным элементом $Q_1(\Lambda_0^1)$ тогда и только тогда, когда

$$E_{Q_1}^{\Lambda_0^1} \bigwedge_{k=1}^{u-1} P_{R_1,R_1}^{\Lambda_k^1\Lambda_{k+1}^1} = 1.$$

Таким образом, имеем

$$E_{[Q_1,{}_uR_1]}^{\Lambda_0^1\ldots\Lambda_u^1} = P_{Q_1,R_1}^{\Lambda_0^1\Lambda_1^1} E_{Q_1}^{\Lambda_0^1} \bigwedge_{k=1}^{u-1} P_{R_1,R_1}^{\Lambda_k^1\Lambda_{k+1}^1} = P_{Q_1,R_1}^{\Lambda_0^1\Lambda_1^1} \bigwedge_{k=1}^{u-1} P_{R_1,R_1}^{\Lambda_k^1\Lambda_{k+1}^1}.$$

Далее, коммутаторы вида $[Q_1, {}_tR_1]$, $t \geqslant 1$, имеют вхождения только в ω-произведениях. Более того, метка любого вхождения в ω-произведение начинается с Λ_1, если начальный элемент равен $Q_1(\Lambda_1)$, с Λ_2, если начальный элемент равен $Q_1(\Lambda_2)$, и т.д. Значит, для произвольных вхождений $[Q_1, {}_uR_1](\Lambda_0^1 \ldots \Lambda_u^1)$ и $[Q_1, {}_vR_1](\Lambda_0^2 \ldots \Lambda_v^2)$ существует две альтернативы: они находятся в одном ω-произведении (т.е. $\Lambda_0^1 = \Lambda_0^2$) либо в разных. Во втором случае условие предшествования $P_{[Q_1,{}_uR_1],[Q_1,{}_vR_1]}^{\Lambda_0^1\ldots\Lambda_u^1\Lambda_0^2\ldots\Lambda_v^2}$ эквивалентно предшествованию соответствующих ω-произведений, т.е. начальных элементов $Q_1(\Lambda_0^1)$ и $Q_1(\Lambda_0^2)$. В первом же случае мы используем рекуррентное соотношение из следствия 1.2.1. Таким образом, имеем

$$P_{[Q_1,{}_uR_1],[Q_1,{}_vR_1]}^{\Lambda_0^1\ldots\Lambda_u^1\Lambda_0^2\ldots\Lambda_v^2} = E_{[Q_1,{}_uR_1]}^{\Lambda_0^1\ldots\Lambda_u^1} E_{[Q_1,{}_vR_1]}^{\Lambda_0^2\ldots\Lambda_v^2} F.$$

Нетрудно показать, что полученное соотношение справедливо, когда либо $u = 0$, либо $v = 0$. Действительно, поскольку Q_1 не имеет вхождений в ω-произведениях, для любых вхождений $[Q_1, {}_uR_1](\Lambda_0^1 \ldots \Lambda_u^1)$ и $[Q_1, {}_vR_1](\Lambda_0^2 \ldots \Lambda_v^2)$ имеем

$$P_{[Q_1,{}_uR_1],[Q_1,{}_vR_1]}^{\Lambda_0^1\ldots\Lambda_u^1\Lambda_0^2\ldots\Lambda_v^2} \Leftrightarrow \begin{cases} P_{Q_1,Q_1}^{\Lambda_0^1\Lambda_0^2} \vee (\Lambda_0^1 = \Lambda_0^2), & \text{если } u = 0, v \neq 0; \\ P_{Q_1,Q_1}^{\Lambda_0^1\Lambda_0^2}, & \text{если } u \neq 0, v = 0. \end{cases}$$

Соотношение (17b). Пусть $u, v \geqslant 1$. Как и в предыдущем случае, вхождения коммутаторов $[Q_1, {}_uR_1]$ и $[Q_2, {}_vR_1]$ возникли в ходе одного и того же этапа собирательного процесса. Однако вхождения $[Q_1, {}_uR_1]$ находятся в ω-произведении с начальным элементом $Q_1(\Lambda)$, $\Lambda \in D(Q_1)$, а вхождения $[Q_2, {}_vR_1]$ находятся в ω-произведении с начальным элементом $Q_2(\Lambda)$, $\Lambda \in D(Q_2)$. Как указано выше, предшествование ω-произведений эквивалентно предшествованию соответствующих начальных элементов. Таким образом, получаем

$$P^{\Lambda_0^1 \dots \Lambda_u^1 \Lambda_0^2 \dots \Lambda_v^2}_{[Q_1, {}_uR_1], [Q_2, {}_vR_1]} = E^{\Lambda_0^1 \dots \Lambda_u^1}_{[Q_1, {}_uR_1]} E^{\Lambda_0^2 \dots \Lambda_v^2}_{[Q_2, {}_vR_1]} P^{\Lambda_0^1 \Lambda_0^2}_{Q_1, Q_2}.$$

Теперь пусть $u = 0$ и $w(Q_1) = 1$. Коммутатор Q_1 имеет вхождения в начальное слово $W_0 \equiv T_0$. Следовательно, Q_1 и Q_2 имеют вхождения в одной несобранной части на этапе сбора R_1, в ходе которого возникали вхождения $[Q_2, {}_vR_1]$. Здесь мы имеем дело с предшествованием начального элемента и ω-произведения, что эквивалентно предшествованию соответствующих начальных элементов. Поскольку $Q_1 \neq Q_2$, получаем

$$P^{\Lambda_0^1 \Lambda_0^2 \dots \Lambda_v^2}_{Q_1, [Q_2, {}_vR_1]} = E^{\Lambda_0^1}_{Q_1} E^{\Lambda_0^2 \dots \Lambda_v^2}_{[Q_2, {}_vR_1]} P^{\Lambda_0^1 \Lambda_0^2}_{Q_1, Q_2}.$$

Для случая, когда $v = 0$, $w(Q_2) = 1$, рассуждения аналогичны.

Соотношения (17c) и (17d). Предположим, что вхождения R_1 были собраны на более раннем этапе, чем R_2. Согласно условию теоремы должна существовать несобранная часть, содержащая вхождения как $[Q_1, {}_uR_1]$, так и $[Q_2, {}_vR_2]$. Следовательно, на этапе сбора R_2 соответствующая несобранная часть содержит как $[Q_1, {}_uR_1]$, так и Q_2. Поскольку $[Q_1, {}_uR_1] \neq Q_2$, мы используем рассуждения из предыдущего случая и получаем

$$P^{\Lambda_0^1 \dots \Lambda_u^1 \Lambda_0^2 \dots \Lambda_v^2}_{[Q_1, {}_uR_1], [Q_2, {}_vR_2]} = E^{\Lambda_0^1 \dots \Lambda_u^1}_{[Q_1, {}_uR_1]} E^{\Lambda_0^2 \dots \Lambda_v^2}_{[Q_2, {}_vR_2]} P^{\Lambda_0^1 \dots \Lambda_u^1 \Lambda_0^2}_{[Q_1, {}_uR_1], Q_2}.$$

Если вхождения R_2 были собраны на более раннем этапе, чем R_1, рассуждения аналогичны. $\square$

Пример 1.2.4. Рассмотрим вариант собирательного процесса из примера 1.1.2 и выразим условие существования

$$E^{(\lambda_1,\lambda_2,\lambda_3)}_{[[a_2,a_1],a_2]}, \quad (\lambda_1,\lambda_2) \in D([a_2,a_1]) = D(a_2)\times D(a_1),\ \lambda_3 \in D(a_2),$$

через $E_{a_1}, E_{a_2}, P_{a_1,a_2}, P_{a_2,a_1}, P_{a_1,a_1}, P_{a_2,a_2}$.

$$\begin{aligned}
E^{(\lambda_1,\lambda_2,\lambda_3)}_{[[a_2,a_1],a_2]} &= P^{(\lambda_1,\lambda_2,\lambda_3)}_{[a_2,a_1],a_2} && \begin{array}{l}\text{используем (16) при } u=1,\\ Q_1=[a_2,a_1],\ R_1=a_2\end{array}\\
&= E^{(\lambda_1,\lambda_2)}_{[a_2,a_1]} E^{(\lambda_3)}_{a_2} P^{(\lambda_1\lambda_3)}_{a_2,a_2} && \begin{array}{l}\text{используем (17a) при } u=1,\ v=0,\\ Q_1=Q_2=a_2,\ R_1=a_1\end{array}\\
&= P^{(\lambda_1,\lambda_2)}_{a_2,a_1} E^{(\lambda_3)}_{a_2} P^{(\lambda_1\lambda_3)}_{a_2,a_2} && \begin{array}{l}\text{используем (16) при } u=1,\\ Q_1=a_2,\ R_1=a_1\end{array}.
\end{aligned}$$

Используя информацию из примера 1.2.2, получаем

$$E^{(\lambda_1,\lambda_2,\lambda_3)}_{[[a_2,a_1],a_2]} = (\lambda_1<\lambda_2)(\lambda_1<\lambda_3), \quad (\lambda_1,\lambda_2,\lambda_3)\in\{1,2\}^3.$$

Единственный случай, когда $E^{(\lambda_1,\lambda_2,\lambda_3)}_{[[a_2,a_1],a_2]} = 1$, — это $(\lambda_1,\lambda_2,\lambda_3)=(1,2,2)$.

Следствие 1.2.3. *Пусть коммутатор $R\in\Gamma(a_1,\ldots,a_n)$ возник в ходе некоторого варианта собирательного процесса $\{W_j\}_{j\geqslant 0}$. Тогда условие существования E_R выражается формулой, содержащей не более чем операции $\vee$ и $\wedge$, предикаты E_{a_i}, P_{a_i,a_j}, $i,j\in\overline{1,n}$, и отношение равенства $=$ на $\mathbb{Z}$.*

Доказательство. Сначала покажем, что для любого предиката

$$E_Q, \quad w(Q)\geqslant 2; \qquad P_{Q,R}, \quad w(Q)+w(R)\geqslant 3;$$

существует подходящее рекуррентное соотношение из предыдущей теоремы. Любой формальный коммутатор Q, $w(Q)\geqslant 2$, может быть записан как $[Q_1,{}_uR_1]$, $u\geqslant 1$. Следовательно, мы используем соотношение (16) для условия существования E_Q.

Рассмотрим условие предшествования $P_{Q,R}$. Предположим, что $w(R)=1$, и запишем Q как $[Q_1,{}_uR_1]$, $u\geqslant 1$. Если $Q_1\neq R$, то используем соотношение (17b). Если $Q_1=R$, то записываем $[Q_1,{}_uR_1]$, R как $[Q_1,{}_uR_1]$, $[Q_1,{}_0R_1]$ соответственно и используем (17a). В случае $w(Q)=1$ рассуждения аналогичные.

Пусть $w(Q), w(R) \geqslant 2$. Тогда Q и R могут быть записаны как $[Q_1, {}_u R_1]$, $u \geqslant 1$, и $[Q_2, {}_v R_2]$, $v \geqslant 1$ соответственно. Если $Q_1 \neq [Q_2, {}_v R_2]$ и $Q_2 \neq [Q_1, {}_u R_1]$, то мы применяем для $P_{Q,R}$ одно из соотношений (17). Если же $Q_1 = [Q_2, {}_v R_2]$, то мы представляем $[Q_1, {}_u R_1]$ и $[Q_2, {}_v R_2]$ в виде $[Q_1, {}_u R_1]$ и $[Q_1, {}_0 R_1]$ соответственно и используем (17a). Рассуждения аналогичны, если $Q_2 = [Q_1, {}_u R_1]$.

Таким образом, используя рекуррентные соотношения из предыдущей теоремы конечное число раз, мы выражаем E_R через формулу, содержащую не более чем операции $\vee$ и $\wedge$, предикаты E_{a_i}, P_{a_i,a_j}, $i, j \in \overline{1,n}$, и отношение равенства $\Lambda_u = \Lambda_v$. Остается заметить, что для любых целочилсенных последовательностей одинаковой длины $\Lambda_u = (\lambda_{i_1}, \ldots, \lambda_{i_s})$, $\Lambda_v = (\lambda_{j_1}, \ldots, \lambda_{j_s})$ отношение $\Lambda_u = \Lambda_v$ может быть записано в терминах равенства на множестве $\mathbb{Z}$:

$$\bigwedge_{k=1}^{s} (\lambda_{i_k} = \lambda_{j_k}).$$

$\square$

Напомним, что согласно предложению 1.2.1 показатель степени коммутатора R равен мощности множества

$$\{(\lambda_1, \ldots, \lambda_r) \in D(R) \mid E_R^{(\lambda_1,\ldots,\lambda_r)} = 1\}.$$

Согласно доказанному следствию, если предикаты E_{a_i}, P_{a_i,a_j} выражаются формулами, содержащими не более чем операции $\vee$ и $\wedge$ и предикаты вида $[\lambda_i < \lambda_j]$, $[\lambda_i = \lambda_j]$, то таковой будет и формула $E_R^{(\lambda_1,\ldots,\lambda_r)}$. В следующем параграфе будет найдено выражение со свойством делимости для мощности множества

$$\{(\Lambda \in D \mid C(\Lambda) = 1\},$$

когда D — декартово произведение конечных множеств целых чисел, удовлетворяющих определенным ограничениям, а формула $C(\Lambda)$ имеет строение, как описано выше.

1.3 Комбинаторный анализ L-условий

Определение 1.3.1. Обозначим через L множество всех формул алгебры высказываний, в которых каждая пропозициональная переменная заменена на предикатные символы $[\lambda_i < \lambda_j]$ или $[\lambda_i = \lambda_j]$, где $i, j \in \mathbb{N}$.

Определение 1.3.2. Произвольный элемент $C \in L$ будем называть *L-условием* ранга r, $r \in \mathbb{N}$, если формула C содержит в своей записи хотя бы один из следующих предикатных символов: $[\lambda_i < \lambda_r]$, $[\lambda_r < \lambda_i]$, $[\lambda_i = \lambda_r]$, $[\lambda_r = \lambda_i]$, $i \in \mathbb{N}$, и не содержит предикатных символов $[\lambda_i < \lambda_j]$ и $[\lambda_i = \lambda_j]$, где $i > r$ или $j > r$. Логические константы 0 и 1 будем называть L-условиями ранга ноль.

Пример 1.3.1. L-условия рангов 1, 2 и 3, соответственно:

$$\neg[\lambda_1 = \lambda_1] \to [\lambda_1 < \lambda_1]; \quad ([\lambda_1 = \lambda_1] \wedge [\lambda_2 = \lambda_2]) \oplus 1; \quad [\lambda_2 = \lambda_3] \leftrightarrow [\lambda_3 = \lambda_2].$$

Символ $\oplus$ обозначает сложение по модулю 2.

Пусть M — произвольное непустое множество с введенными на нем отношениями равенства «$=_1$» и строгого линейного порядка «$<_1$». Тогда любое L-условие C ранга не выше r можно интерпретировать как r-местный предикат на любом непустом декартовом произведении $M_1 \times \cdots \times M_r \subseteq M \times \cdots \times M$. При этом двуместные предикатные символы $[\lambda_i < \lambda_j]$ и $[\lambda_i = \lambda_j]$, $i, j \in \overline{1, r}$, определяются очевидным образом:

$$[\lambda_i = \lambda_j]\Big|_{\substack{\lambda_i = \lambda_i^* \\ \lambda_j = \lambda_j^*}} = \begin{cases} 1, \text{если } \lambda_i^* =_1 \lambda_j^*, \\ 0, \text{иначе.} \end{cases} \qquad [\lambda_i < \lambda_j]\Big|_{\substack{\lambda_i = \lambda_i^* \\ \lambda_j = \lambda_j^*}} = \begin{cases} 1, \text{если } \lambda_i^* <_1 \lambda_j^*, \\ 0, \text{иначе.} \end{cases}$$

Далее будем говорить, что набор элементов $(\lambda_1^*, \ldots, \lambda_r^*) \in M_1 \times \cdots \times M_r$ удовлетворяет L-условию C, если $C(\lambda_1^*, \ldots, \lambda_r^*) = 1$, т.е. набор $(\lambda_1^*, \ldots, \lambda_r^*)$ реализует истинное значение предиката $C = C(\lambda_1, \ldots, \lambda_r)$.

Пример 1.3.2. L-условие $A(\lambda_1, \lambda_2) = [\lambda_1 < \lambda_2]$ на множестве натуральных чисел $\{1, 2\}^2$ принимает следующие значения:

$$A(1,1) = A(2,1) = A(2,2) = 0, \quad A(1,2) = 1.$$

Отсюда можем заключить, что L-условие A тождественно ложно на $\{1\}^2$ и не является таковым на множестве $\{1, 2\}^2$.

Предложение 1.3.1. *Пусть M и N — произвольные линейно упорядоченные множества, причем M не менее чем счетно. Если некоторое L-условие ранга не выше r тождественно истинно на множестве M^r, то оно тождественно истинно на N^r.*

Доказательство. Зафиксируем произвольный набор $(\lambda_1^*, \dots, \lambda_r^*) \in N^r$ со значениями компонент: $v_1 < \dots < v_s$, где $1 \leqslant s \leqslant r$, и покажем, что $C(\lambda_1^*, \dots, \lambda_r^*) = 1$. Поскольку M бесконечно и любые два конечных линейно упорядоченных множества одинаковой мощности изоморфны, можем построить инъективное отображение $f : \{v_1, \dots, v_s\} \to M$, сохраняющее линейный порядок. Поэтому, положив

$$\lambda_i^{**} = f(v_j) \Leftrightarrow \lambda_i^* = v_j, \quad i \in \overline{1, r},$$

будем иметь для $i, j \in \overline{1, r}$ следующие равенства:

$$[\lambda_i = \lambda_j]\Big|_{\substack{\lambda_i = \lambda_i^* \\ \lambda_j = \lambda_j^*}} = [\lambda_i = \lambda_j]\Big|_{\substack{\lambda_i = \lambda_i^{**} \\ \lambda_j = \lambda_j^{**}}}; \quad [\lambda_i < \lambda_j]\Big|_{\substack{\lambda_i = \lambda_i^* \\ \lambda_j = \lambda_j^*}} = [\lambda_i < \lambda_j]\Big|_{\substack{\lambda_i = \lambda_i^{**} \\ \lambda_j = \lambda_j^{**}}}.$$

Таким образом, $C(\lambda_1^*, \dots, \lambda_r^*) = C(\lambda_1^{**}, \dots, \lambda_r^{**}) = 1$. □

Определение 1.3.3. Будем говорить, что два L-условия C_1 и C_2 *эквивалентны*, и писать $C_1 \sim C_2$, если для любого линейно упорядоченного множества M L-условие $C_1 \leftrightarrow C_2$ тождественно истинно на M^r. Ввиду предложения 1.3.1 достаточно проверить тождественную истинность, например, при $M = \mathbb{N}$.

Пример 1.3.3. Справедливы следующие отношения L-условий:

$$[\lambda_1 = \lambda_2] \vee [\lambda_3 < \lambda_4] \sim [\lambda_3 < \lambda_4] \vee [\lambda_1 = \lambda_2], \quad [\lambda_1 = \lambda_2] \sim [\lambda_1 = \lambda_2] \wedge [\lambda_3 = \lambda_3].$$

Пусть C_1 и C_2 — два эквивалентных L-условия рангов r и s, соответственно, $r \leqslant s$. Из определения 1.3.3 ясно, что $C_1(\lambda_1^*, \ldots, \lambda_s^*) = C_2(\lambda_1^*, \ldots, \lambda_s^*)$ для любых элементов $\lambda_1^*, \ldots, \lambda_s^*$ произвольного линейно упорядоченного множества. Более того, справедливо правило замены: если A есть подформула L-условия C, и $A \sim B$, то замена A на B в C приведет к L-условию эквивалентному C.

Отметим также, что не все эквивалентости L-условий можно получить по правилу замены или путем использования свойств логических операций (коммутативность дизъюнкции и т.п.).

Предложение 1.3.2. *Для любых натуральных $i, j, k \in \mathbb{N}$ справедливы следующие отношения L-условий:*

$$[\lambda_i = \lambda_i] \sim 1; \tag{18}$$

$$[\lambda_i = \lambda_j] \sim [\lambda_j = \lambda_i]; \tag{19}$$

$$[\lambda_i = \lambda_j] \wedge [\lambda_j = \lambda_k] \sim [\lambda_i = \lambda_j] \wedge [\lambda_j = \lambda_k] \wedge [\lambda_i = \lambda_k]; \tag{20}$$

$$[\lambda_i < \lambda_j] \wedge [\lambda_j < \lambda_k] \sim [\lambda_i < \lambda_j] \wedge [\lambda_j < \lambda_k] \wedge [\lambda_i < \lambda_k]; \tag{21}$$

$$[\lambda_i < \lambda_j] \oplus [\lambda_j < \lambda_i] \oplus [\lambda_i = \lambda_j] \oplus ([\lambda_i < \lambda_j] \wedge [\lambda_j < \lambda_i] \wedge [\lambda_i = \lambda_j]) \sim 1. \tag{22}$$

Кроме того, из (18)-(22) следуют эквивалентности:

$$[\lambda_i < \lambda_i] \sim 0; \tag{23}$$

$$[\lambda_i < \lambda_j] \wedge [\lambda_j < \lambda_i] \sim 0; \tag{24}$$

$$\neg[\lambda_i = \lambda_j] \sim [\lambda_i < \lambda_j] \vee [\lambda_j < \lambda_i]; \tag{25}$$

$$\neg[\lambda_i < \lambda_j] \sim [\lambda_j < \lambda_i] \vee [\lambda_j = \lambda_i]. \tag{26}$$

Доказательство. Отношения (18)-(20) следуют из аксиом равенства: рефлексивности, симметричности и транзитивности, соответственно. А из аксиом транзитивности и трихотомии строгого линейного порядка следуют отношения (21) и (22), соответственно. Напомним, что любое отношение со свойствами транзитивности и трихотомии является антирефлексивным и асимметричным.

Выведем из (18)-(22) отношения (23) и (24) при помощи логических преобразований и правила замены. Используем (22) при $j = i$, затем (18):

$$\begin{aligned}
[\lambda_i < \lambda_i] &\sim [\lambda_i < \lambda_i] \wedge 1 \\
&\sim [\lambda_i < \lambda_i] \wedge \Big([\lambda_i = \lambda_i] \oplus ([\lambda_i < \lambda_i] \wedge [\lambda_i = \lambda_i])\Big) \\
&\sim [\lambda_i < \lambda_i] \wedge (1 \oplus [\lambda_i < \lambda_i]) \\
&\sim [\lambda_i < \lambda_i] \oplus [\lambda_i < \lambda_i] \sim 0.
\end{aligned}$$

Из (21) при $k = i$ и (23) следует

$$[\lambda_i < \lambda_j] \wedge [\lambda_j < \lambda_i] \sim [\lambda_i < \lambda_j] \wedge [\lambda_j < \lambda_i] \wedge [\lambda_i < \lambda_i] \sim 0.$$

Нетрудно вывести отношения (25) и (26) по аналогии с предыдущими, используя (22) и (24). $\square$

Из отношений (25) и (26) следует

Предложение 1.3.3. *В каждом классе эквивалентности множества всех L-условий можно выбрать формулу, записанную в ДНФ без операции отрицания.*

Заметим, что для любого L-условия можно найти эквивалентное ему L-условие большего ранга. Обратное, вообще говоря, неверно.

Пусть $M_1 \times \cdots \times M_r$ — декартово произведение произвольных непустых подмножеств некоторого линейно упорядоченного множества. Покажем, что множество $M_1 \times \cdots \times M_r$ можно разбить на попарно непересекающиеся классы таким образом, что для любого L-условия C либо все элементы произвольного класса удовлетворяют C, либо ни один из них. Вычислив мощности этих классов, мы найдем выражение для количества элементов $M_1 \times \cdots \times M_r$, удовлетворяющих произвольному L-условию.

Пусть $v_1 < \cdots < v_t$ — все различные значения компонент произвольного набора $(\lambda_1, \ldots, \lambda_r) \in M_1 \times \cdots \times M_r$, $1 \leqslant t \leqslant r$. Положим $I_k = \{i \mid \lambda_i = v_k\}$ для

k от 1 до t. Тогда набор $(I_1, \dots, I_t)$ есть упорядоченное разбиение множества индексов $\{1, \dots, r\}$, т.е.

$$\{1, \dots, r\} = I_1 \cup \dots \cup I_t, \quad I_i \cap I_j = \varnothing \Leftrightarrow i \neq j.$$

Таким образом, любому набору из $M_1 \times \dots \times M_r$ соответствует единственное упорядоченное разбиение $\{1, \dots, r\}$, откуда вытекает утверждение следующей леммы.

Лемма 1.3.1. *Декартово произведение $M_1 \times \dots \times M_r$, составленное из непустых подмножеств произвольного линейно упорядоченного множества, представимо в виде объединения попарно непересекающихся классов:*

$$M_1 \times \dots \times M_r = \bigcup_{t=1}^{r} \bigcup_{\substack{I_1 \cup \ldots \cup I_t = \{1,\ldots,r\} \\ I_i \cap I_j = \varnothing \Leftrightarrow i \neq j}} \left\langle {M_1 \times \dots \times M_r \atop (I_1,\ldots,I_t)} \right\rangle,$$

где класс $\left\langle {M_1 \times \dots \times M_r \atop (I_1,\ldots,I_t)} \right\rangle$ состоит из всех наборов $(\lambda_1, \dots, \lambda_r)$, удовлетворяющих условиям:

$$\begin{cases} (\lambda_1, \dots, \lambda_r) \in M_1 \times \dots \times M_r; \\ \lambda_i = \lambda_j \Leftrightarrow \exists k \, (i \in I_k) \wedge (j \in I_k); \\ \lambda_i < \lambda_j \Leftrightarrow \exists p \, \exists q \, (i \in I_p) \wedge (j \in I_q) \wedge (p < q). \end{cases}$$

Пример 1.3.4. Пусть декартово произведение $M_1 \times M_2$ составлено из подмножеств целых чисел $M_1 = \{0, 1, 2\}$ и $M_2 = \{0, 1, 2, 3\}$. Имеют место равенства:

$$\left\langle {M_1 \times M_2 \atop (\{1,2\})} \right\rangle = \{(0,0), (1,1), (2,2)\};$$
$$\left\langle {M_1 \times M_2 \atop (\{1\},\{2\})} \right\rangle = \{(0,1), (0,2), (0,3), (1,2), (1,3), (2,3)\};$$
$$\left\langle {M_1 \times M_2 \atop (\{2\},\{1\})} \right\rangle = \{(1,0), (2,0), (2,1)\}.$$

Лемма 1.3.2. *Пусть C — произвольное L-условие ранга не выше r. Тогда для любого упорядоченного разбиения $(I_1, \dots, I_t)$ множества $\{1, \dots, r\}$ либо каждый элемент класса $\left\langle {M_1 \times \dots \times M_r \atop (I_1,\ldots,I_t)} \right\rangle$ удовлетворяет C, либо ни один из них.*

Доказательство. Для L-условий ранга 0 утверждение леммы очевидно. Далее положим ранг C больше нуля. По определению $\left\langle{M_1\times\dots\times M_r \atop (I_1,\dots,I_t)}\right\rangle$ все наборы $(\lambda_1,\dots,\lambda_r)$ из этого класса удовлетворяют фиксированному упорядочению компонент $\lambda_1,\dots,\lambda_r$. Поэтому мы можем построить L-условие ранга r, соответствующее этому упорядочению, следующим образом:

$$K = \bigwedge_{\substack{1\leqslant i\leqslant r\\ 1\leqslant j\leqslant r}} K_{ij}, \quad K_{ij} = \begin{cases} [\lambda_i < \lambda_j], \text{ если } \lambda_i < \lambda_j; \\ [\lambda_i = \lambda_j], \text{ если } \lambda_i = \lambda_j; \\ 1, \text{ если } \lambda_i > \lambda_j. \end{cases}$$

Далее, ввиду предложения 1.3.3 условие C можно привести к ДНФ вида

$$C \sim \bigvee_{i=1}^{s} (C_{i1} \wedge \dots \wedge C_{ik_i}),$$

где C_{uv} — предикаты типа $[\lambda_i < \lambda_j]$ или $[\lambda_i = \lambda_j]$. Предположим, что в классе $\left\langle{M_1\times\dots\times M_r \atop (I_1,\dots,I_t)}\right\rangle$ нашелся набор $(\lambda_1^*,\dots,\lambda_r^*)$, удовлетворяющий условию C. Тогда $(\lambda_1^*,\dots,\lambda_r^*)$ удовлетворяет каждому конъюнкту некоторого дизъюнкта $C_{j1} \wedge \dots \wedge C_{jk_j}$. Значит, каждый предикат из $C_{j1},\dots,C_{jk_j}$ обязательно встретится в K. Таким образом, любой набор из класса $\left\langle{M_1\times\dots\times M_r \atop (I_1,\dots,I_t)}\right\rangle$ удовлетворяет дизъюнкту $C_{j1} \wedge \dots \wedge C_{jk_j}$, а следовательно, условию C. □

Лемма 1.3.3. *Пусть* $\{N_i\}_{i=1}^t$ *— семейство конечных непустых подмножеств некоторого линейно упорядоченного множества. Если*

$$N = N_1 \cap \dots \cap N_t \neq \varnothing; \qquad [\min N, \max N] \cap (N_i \backslash N) = \varnothing, \quad i \in \overline{1,t},$$

то мощность множества

$$V = \{(v_1,\dots,v_t) \in N_1 \times \dots \times N_t \mid v_1 < \dots < v_t\}$$

равна

$$\binom{|N|}{t} + b_{t-1}\binom{|N|}{t-1} + \dots + b_1\binom{|N|}{1} + b_0\binom{|N|}{0}, \tag{27}$$

где b_s — целые неотрицательные коэффициенты, зависящие от $N_1, \ldots, N_t$. Более того, если $N \in \{N_i\}_{i=1}^t$, то $b_0 = 0$, а при $N_1 = \cdots = N_t$ все b_s равны нулю.

Доказательство. Разобьем множество V на попарно не пересекающиеся классы $V_0, \ldots, V_t$ по следующему правилу: $(v_1, \ldots, v_t) \in V_s$ тогда и только тогда, когда среди $v_1, \ldots, v_t$ найдется ровно s компонент, значения которых принадлежат N. Ввиду условий:

$$v_1 < \cdots < v_t; \qquad [\min N, \max N] \cap (N_i \backslash N) = \varnothing, \quad i \in \overline{1, t},$$

справедливо утверждение: если $i < j < k$ и $v_i, v_k \in N$, то $v_j \in N$. Значит, для любого набора $(v_1, \ldots, v_t) \in V_s$ существует k от 0 до $t - s$ такое, что $v_{k+1}, \ldots, v_{k+s} \in N$. При этом $v_i < \min N$ для $i \in \overline{1, k}$, и $v_i > \max N$ для $i \in \overline{k + s + 1, t}$. Таким образом, имеет место равенство

$$|V_s| = \sum_{k=0}^{t-s} c_k d_k e_k,$$

где d_k, c_k, e_k равны, соответственно, мощностям множеств

$$\{(v_{k+1}, \ldots, v_{k+s}) \in V | v_{k+1}, \ldots, v_{k+s} \in N\},$$

$$\{(v_1, \ldots, v_k) \in V | v_k < \min N\}, \{(v_{k+s+1}, \ldots, v_t) \in V | \max N < v_{k+s+1}\}.$$

Нетрудно видеть, что d_k равно числу сочетаний из $|N|$ по s для любого k от 1 до $t - s$, поэтому

$$|V_s| = \binom{|N|}{s} \sum_{k=0}^{t-s} c_k e_k = \binom{|N|}{s} b_s.$$

В итоге, имеем

$$|V| = |V_t| + \cdots + |V_0| = b_t \binom{|N|}{t} + b_{t-1} \binom{|N|}{t-1} + \cdots + b_1 \binom{|N|}{1} + b_0 \binom{|N|}{0},$$

где, как легко проверить, $b_t = 1$.

Предположим, что $N = N_k$ для некоторого k. Тогда в любом наборе из V значение компоненты v_k принадлежит пересечению N, а значит, $b_0 = |V_0| = 0$. Рассуждая аналогично, если $N_1 = \cdots = N_t$, то $b_{t-1} = \cdots = b_0 = 0$. $\square$

Лемма 1.3.4. *Пусть $\{M_i\}_{i=1}^r$ — семейство конечных непустых подмножеств некоторого линейно упорядоченного множества. Если*

$$M = M_1 \cap \dots \cap M_r \neq \varnothing; \qquad [\min M, \max M] \cap (M_i \backslash M) = \varnothing, \quad i \in \overline{1, r},$$

то для любого упорядоченного разбиения $(I_1, \dots, I_t)$ множества $\{1, \dots, r\}$ имеет место равенство

$$\left| \left\langle {}^{M_1 \times \dots \times M_r}_{(I_1, \dots, I_t)} \right\rangle \right| = \binom{|M|}{t} + b_{t-1} \binom{|M|}{t-1} + \dots + b_1 \binom{|M|}{1} + b_0 \binom{|M|}{0}, \qquad (28)$$

где b_s — целые неотрицательные коэффициенты, зависящие от $M_1, \dots, M_r$, и $(I_1, \dots, I_t)$. Более того, если $M \in \{M_i\}_{i=1}^r$, то $b_0 = 0$, а при $M_1 = \dots = M_r$ все b_s равны нулю.

Доказательство. Из определения класса $\left\langle {}^{M_1 \times \dots \times M_r}_{(I_1, \dots, I_t)} \right\rangle$ следует, что его мощность равна мощности множества

$$V = \{(v_1, \dots, v_t) \mid v_1 < \dots < v_t ; v_i \in \bigcap_{j \in I_i} M_j, i = 1, \dots, t\},$$

где, как нетрудно заметить,

$$\bigcap_{i=1}^{t} \bigcap_{j \in I_i} M_j = M \neq \varnothing.$$

Из условий леммы и свойств операций пересечения и разности множеств следуют равенства

$$\varnothing = \bigcap_{j \in I_i} [\min M, \max M] \cap (M_j \backslash M) = [\min M, \max M] \cap \left(\left(\bigcap_{j \in I_i} M_j \right) \backslash M \right)$$

для любого i от 1 до t. Таким образом, множество V удовлетворяет условиям предыдущей леммы и мы получаем равенство (28).

Предположим, что $M = M_k$ для некоторого k от 1 до r. Тогда найдется такое i, что $k \in I_i$, а следовательно,

$$\bigcap_{j \in I_i} M_j = M = \bigcap_{i=1}^{t} \bigcap_{j \in I_i} M_j,$$

и мы попадаем в условия предыдущей леммы. Аналогично, если $M_1 = \dots = M_r$, то

$$\bigcap_{j\in I_1} M_j = \dots = \bigcap_{j\in I_t} M_j.$$

$\square$

Теорема 1.3.1. *Пусть $M_1, \dots, M_r$ — непустые конечные подмножества некоторого линейно упорядоченного множества, C — произвольное L-условие ранга не выше r. Если выполнены условия:*

$$M = M_1 \cap \dots \cap M_r \neq \varnothing; \qquad [\min M, \max M] \cap (M_i \backslash M) = \varnothing, \quad i \in \overline{1, r};$$

то количество элементов из $M_1 \times \dots \times M_r$, удовлетворяющих условию C, выражается в виде

$$\sum_{t=1}^{r} a_t \binom{|M|}{t} + \sum_{t=0}^{r-1} b_t \binom{|M|}{t}, \tag{29}$$

где a_s, b_s — целые неотрицательные коэффициенты, b_s зависят от $M_1, \dots, M_r$ и C, a_s зависят только от C. Более того, если $M \in \{M_i\}_{i=1}^r$, то $b_0 = 0$, а при $M_1 = \dots = M_r$ все b_s равны нулю.

Доказательство. Обозначим через $C_{M_1\times\dots\times M_r}$ множество всех элементов из $M_1 \times \dots \times M_r$, удовлетворяющих условию C. Согласно лемме 1.3.1 и лемме 1.3.2 $C_{M_1\times\dots\times M_r}$ является объединением классов $\left\langle\substack{M_1\times\dots\times M_r \\ (I_1,\dots,I_t)}\right\rangle$, удовлетворяющих C. Обозначив за P_t множество всех разбиений $(I_1, \dots, I_t)$, соответствующих таким классам, из леммы 1.3.1 и предыдущей леммы получаем равенства

$$|C_{M_1\times\dots\times M_r}| = \sum_{t=1}^{r} \sum_{(I_1,\dots,I_t)\in P_t} \left| \left\langle\substack{M_1\times\dots\times M_r \\ (I_1,\dots,I_t)}\right\rangle \right| =$$

$$= \sum_{t=1}^{r} \sum_{(I_1,\dots,I_t)\in P_t} \left(\binom{|M|}{t} + \sum_{j=0}^{t-1} B_j \left(\left\langle\substack{M_1\times\dots\times M_r \\ (I_1,\dots,I_t)}\right\rangle \right) \binom{|M|}{j} \right).$$

После упрощения и приведения подобных будем иметь

$$|C_{M_1\times\dots\times M_r}| = \sum_{t=1}^{r} |P_t| \binom{|M|}{t} + \sum_{t=1}^{r}\sum_{j=0}^{t-1} \binom{|M|}{j} \sum_{(I_1,\dots,I_t)\in P_t} B_j\left(\left\langle {M_1\times\dots\times M_r \atop (I_1,\dots,I_t)} \right\rangle\right) =$$
$$= \sum_{t=1}^{r} a_t \binom{|M|}{t} + \sum_{t=0}^{r-1} b_t \binom{|M|}{t}.$$

Согласно предыдущей лемме, если $M \in \{M_i\}_{i=1}^r$, то все $B_0(\left\langle {M_1\times\dots\times M_r \atop (I_1,\dots,I_t)} \right\rangle)$ равны нулю, а следовательно, $b_0 = 0$. Если же $M_1 = \dots = M_r$, то все $B_j(\left\langle {M_1\times\dots\times M_r \atop (I_1,\dots,I_t)} \right\rangle)$, $j \in \overline{0, t-1}$, равны нулю, а значит, $b_t = 0$ для всех t. $\square$

В условиях предыдущей теоремы, если $M \in \{M_i\}_{i=1}^r$, то выражение (29) обладает свойством делимости: если $|M|$ есть степень простого числа p^α и $r < p$, то (29) делится на $|M|$.

Примером семейства множеств $\{M_i\}_{i=1}^r$, удовлетворяющих всем этим условиям, может послужить любое семейство непустых отрезков целых чисел с фиксированным левым или правым концом.

До этого момента в рассуждениях мы использовали классический биномиальный коэффициент, определенный для целых $n \geqslant 0$, k следующим образом:

$$\binom{n}{k} = \begin{cases} \frac{n!}{k!\,(n-k)!}, \text{ если } n \geqslant k \geqslant 0; \\ 0, \text{ если } n < k \text{ или } k < 0. \end{cases}$$

В комбинаторных задачах бывает полезным расширить область определения биномиального коэффициента на все целые n и k, чтобы, например, не заботиться об ограничениях на параметры или индексы в комбинаторных выражениях (см. [36]). Хотя задавать расширение можно по-разному, целесообразнее это делать с сохранением некоторых свойств классического биномиального коэффициента, например, рекуррентного соотношения

$$\binom{n-1}{k-1} + \binom{n-1}{k} = \binom{n}{k}. \tag{30}$$

В условиях этого соотношения расширение по-прежнему определяется неоднозначно, необходимо и достаточно определить $\binom{n}{k}$ для каждого отрицательного

n при любом фиксированном k (k может быть разным для разных n). В работе [36] автор задавал такое расширение, распространяя свойство $\binom{n}{n} = 1$ на все целые n. Далее в настоящей работе мы, распространяя свойство $\binom{n}{k} = 0$, $k < 0$, используем следующее определение расширенного биномиального коэффициента:

$$\binom{n}{k} = \begin{cases} \frac{1}{k!}\prod\limits_{i=0}^{k-1}(n-i), \text{ если } k \geqslant 0; \\ 0, \text{ если } k < 0. \end{cases} \qquad n, k \in \mathbb{Z}. \tag{31}$$

Нетрудно проверить выполнение соотношения (30) для (31).

Также мы введем мультиномиальный коэффициент, определив его для целых $n, k_1, \ldots, k_s$ следующим образом:

$$\binom{n}{k_1, \ldots, k_s} = \binom{n}{k_1}\binom{n-k_1}{k_2}\cdots\binom{n-k_1-\cdots-k_{s-1}}{k_s}.$$

В следующей лемме мы отметим ряд важных для нас свойств биномиального коэффициента, некоторые из которых будут использоваться часто и без дополнительных упоминаний.

Лемма 1.3.5. *Пусть $n, k_1, \ldots, k_s \in \mathbb{Z}$.*

1. *Если среди чисел $k_1, \ldots, k_s$ найдется хотя бы одно отрицательное, то*
$$\binom{n}{k_1, \ldots, k_s} = 0.$$

2. *Если все числа $k_1, \ldots, k_s$ неотрицательны, $n = k_1 + \cdots + k_s$, то имеет место равенство*
$$\binom{n}{k_1, \ldots, k_s} = \frac{n!}{k_1! \ldots k_s!},$$
в правой части которого записано количество неупорядоченных разбиений множества мощности n на s подмножеств мощностей $k_1, \ldots, k_s$.

3. *Для любого $i \in \overline{1, s-1}$ имеет место тождество*
$$\binom{n}{k_1, \ldots, k_i, k_{i+1}, \ldots, k_s} = \binom{n}{k_1, \ldots, k_{i+1}, k_i, \ldots, k_s}. \tag{32}$$

4. Если $n \geqslant 0$, то

$$\binom{n}{k} = \binom{n}{n-k}. \tag{33}$$

5. Имеет место тождество

$$(n-k)\binom{n}{k} = (k+1)\binom{n}{k+1}. \tag{34}$$

Доказательство. Первое утверждение очевидно. Из условий второго имеем

$$\binom{n}{k_1,\ldots,k_s} = \frac{1}{k_1!}\prod_{i=0}^{k_1-1}(n-i)\cdots\frac{1}{k_s!}\prod_{i=0}^{k_s-1}(n-k_1-\cdots-k_{s-1}-i) = \frac{n!}{k_1!\cdots k_s!}.$$

Далее, докажем (32) при $s=2$. Тождество выполнено, если $k_1<0$ или $k_2<0$. Далее полагая $k_1 \geqslant 0$, $k_2 \geqslant 0$, имеем

$$\binom{n}{k_1,k_2} = \binom{n}{k_2,k_1} \Leftrightarrow \binom{n}{k_1}\binom{n-k_1}{k_2} = \binom{n}{k_2}\binom{n-k_2}{k_1} \Leftrightarrow$$
$$\Leftrightarrow \prod_{i=0}^{k_1-1}(n-i)\prod_{i=0}^{k_2-1}(n-k_1-i) = \prod_{i=0}^{k_2-1}(n-i)\prod_{i=0}^{k_1-1}(n-k_2-i) \Leftrightarrow$$
$$\Leftrightarrow \prod_{i=0}^{k_1-1}(n-i)\prod_{i=k_1}^{k_1+k_2-1}(n-i) = \prod_{i=0}^{k_2-1}(n-i)\prod_{i=k_2}^{k_1+k_2-1}(n-i).$$

Индукция по s и тождества

$$\binom{n}{k_1,\ldots,k_{s+1}} = \binom{n}{k_1,\ldots,k_s}\binom{n-k_1-\cdots-k_s}{k_{s+1}} = \binom{n}{k_1}\binom{n-k_1}{k_2,\ldots,k_{s+1}}$$

завершают доказательство третьего утверждения.

Если $n<k$ или $k<0$, то обе части равенства (33) равны нулю. Пусть $n \geqslant k \geqslant 0$, тогда из третьего утверждения получаем

$$\binom{n}{k,n-k} = \binom{n}{n-k,k} \Leftrightarrow \binom{n}{k}\binom{n-k}{n-k} = \binom{n}{n-k}\binom{k}{k} \Leftrightarrow \binom{n}{k} = \binom{n}{n-k}.$$

Докажем последнее утверждение. При $k \geqslant 0$ имеем

$$(n-k)\binom{n}{k} = (n-k)\frac{1}{k!}\prod_{i=0}^{k-1}(n-i) = \frac{k+1}{(k+1)!}\prod_{i=0}^{k}(n-i) = (k+1)\binom{n}{k+1}.$$

Если $k<0$, то обе части (34) равны нулю. $\square$

Следующие два комбинаторных результата, связывающие L-условия и функцию бинарного веса числа $\omega(i)$, будут существенно использоваться в главе 2 для нахождения явного вида показателей степеней коммутаторов в собирательной формуле Ф. Холла.

Лемма 1.3.6. *Пусть C — произвольное L-условие ранга не выше r, $r \in \mathbb{N}$. Тогда для любых целых неотрицательных чисел $m, u_1, \ldots, u_r$ мощность множества*

$$\big\{(\mu_1, \ldots, \mu_r) \in \{0, \ldots, 2^m - 1\}^r \mid C(\mu_1, \ldots, \mu_r) = 1;\, \omega(\mu_i) = u_i,\, i \in \overline{1, r}\big\} \quad (35)$$

выражается в виде

$$\sum_{t=0}^{u_1+\cdots+u_r} a_t \binom{m}{t}, \quad (36)$$

где a_t — целые неотрицательные коэффициенты, зависящие только от C и $u_1, \ldots, u_r$. Более того, $a_0 \neq 0$, только когда набор $(0, \ldots, 0)$ принадлежит множеству (35).

Доказательство. Вначале рассмотрим случай, когда параметры $u_1, \ldots, u_r$ положительны. Введя для удобства записи константу $u_0 = 0$, каждому набору $(\mu_1, \ldots, \mu_r)$ поставим в соответствие набор

$$(\lambda_1, \ldots, \lambda_{u_1}, \lambda_{u_1+1}, \ldots, \lambda_{u_1+u_2}, \ldots, \lambda_{u_1+\cdots+u_r}),$$

где $\lambda_{u_{k-1}+j}$ — номер разряда j-ой единицы в двоичной записи μ_k (единицы считаем слева направо, номера разрядов, как обычно, справа налево, начиная с нулевого). Т.к. любое натуральное число однозначно определяется номерами разрядов единиц в его двоичной записи, следующие множества равномощны:

$$\big\{(\mu_1, \ldots, \mu_r) \in \{0, \ldots, 2^m - 1\}^r \mid \omega(\mu_i) = u_i,\, i \in \overline{1, r}\big\}, \quad (37)$$

$$\big\{(\lambda_1, \ldots, \lambda_{u_1+\cdots+u_r}) \in \{0, \ldots, m-1\}^{u_1+\cdots+u_r} \mid \lambda_{u_{i-1}+1} > \cdots > \lambda_{u_{i-1}+u_i},\, i \in \overline{1, r}\big\}. \quad (38)$$

Далее, введем функцию γ_A, сопоставляющую высказыванию A его истинностное значение. Построим формулу $\tilde{C}$ путем замены в L-условии C всех предикатов типа $[\lambda_i = \lambda_j]$, $[\lambda_i < \lambda_j]$, соответственно, на следующие выражения:

$$\gamma_{u_i=u_j} \wedge E, \qquad \text{где } E = \bigwedge_{k=1}^{\min\{u_i,u_j\}} [\lambda_{u_{i-1}+k} = \lambda_{u_{j-1}+k}];$$

$$\big(\gamma_{u_i<u_j} \wedge E\big) \vee \bigvee_{k=1}^{\min\{u_i,u_j\}} [\lambda_{u_{i-1}+k} < \lambda_{u_{j-1}+k}] \wedge \bigwedge_{h=1}^{k-1} [\lambda_{u_{i-1}+h} = \lambda_{u_{j-1}+h}].$$

Теперь введем обозначение

$$M = \tilde{C} \wedge \bigwedge_{k=1}^{r} \bigwedge_{h=1}^{u_k-1} [\lambda_{u_{k-1}+h+1} < \lambda_{u_{k-1}+h}].$$

Полученная формула является L-условием ранга не выше $u_1 + \cdots + u_r$ при любых фиксированных параметрах $u_1, \ldots, u_r$. Более того, всякий элемент из множества (38) удовлетворяет M тогда и только тогда, когда соответствующий ему элемент из множества (37) удовлетворяет C. Таким образом, по теореме 1.3.1 мощность множества (35) выражается в виде

$$\sum_{t=1}^{u_1+\cdots+u_r} a_t \binom{m}{t},$$

где целые неотрицательные коэффициенты a_t зависят только от M. Как следствие, a_t зависят от C и параметров $u_1, \ldots, u_r$.

Перейдем к оставшимся случаям. Если все параметры $u_1, \ldots, u_r$ равны нулю, то множество (35) содержит не более одного элемента, а именно элемент $(0, \ldots, 0)$. Поэтому, если $C(0, \ldots, 0) = 1$, то в сумме (36) имеем $a_0 = 1$, если же $C(0, \ldots, 0) = 0$, то $a_0 = 0$.

Далее, предположим, что среди чисел $u_1, \ldots, u_r$ найдутся как положительные, так и нулевые. Считая для определенности $u_k = 0$, имеем $\mu_k = 0$. Как следствие, мощность множества (35) равна количеству наборов

$$(\mu_1, \ldots, \mu_{k-1}, \mu_{k+1}, \ldots, \mu_r) \in \{0, \ldots, 2^m - 1\}^{r-1},$$

удовлетворяющих условиям:

$$\tilde{C}(\mu_1, \dots, \mu_{k-1}, \mu_{k+1}, \dots, \mu_r) = 1; \quad \omega(\mu_i) = u_i, i \in \{1, \dots, k-1, k+1, \dots r\},$$

где L-условие $\tilde{C}$ получено из C заменой каждого предиката, содержащего в своей записи λ_k, на соответствующие логические константы, а именно

$$[\lambda_j < \lambda_k] = 0; \quad [\lambda_k < \lambda_j] = \gamma_{u_j > 0}; \quad [\lambda_k = \lambda_j] = [\lambda_j = \lambda_k] = \gamma_{u_j = 0}, \qquad j \in \overline{1, r}.$$

Таким образом, данный случай можно последовательно свести к ситуации, рассмотренной ранее, когда все параметры $u_1, \dots, u_r$ положительны. □

Далее мы рассматриваем два частных случая предыдущей леммы, для которых находим коэффициенты a_t из (36) в явном виде.

Лемма 1.3.7. *Для любых натуральных m, u, v мощности множеств*

$$\{(\mu_1, \mu_2) \in \{0, \dots, 2^m - 1\}^2 \mid \omega(\mu_1) = u; \, \omega(\mu_2) = v\}, \tag{39}$$

$$\{(\mu_1, \mu_2) \in \{0, \dots, 2^m - 1\}^2 \mid \omega(\mu_1) = u; \, \omega(\mu_2) = v; \, \mu_1 < \mu_2\} \tag{40}$$

равны, соответственно,

$$\sum_{i=1}^{u+v} \binom{m}{i} \binom{i}{i-u, i-v, u+v-i},$$

$$\sum_{i=1}^{u+v} \binom{m}{i} \sum_{k=1}^{v} \binom{i-k}{i-u-1, i-v, u+v-i-k+1}.$$

Доказательство. Поскольку мощность множества (39), очевидно, равна $\binom{m}{u}\binom{m}{v}$, утверждение леммы для (39) следует из известной формулы произведения биномиальных коэффициентов. Тем не менее, мы проведем доказательство для (39), т.к. оно послужит основой для рассуждений о множестве (40).

Обозначим множества (39) и (40) через A и B, соответственно. Непосредственно из леммы 1.3.6 следует, что

$$|A| = \sum_{i=1}^{u+v} a_i \binom{m}{i}, \qquad |B| = \sum_{i=1}^{u+v} b_i \binom{m}{i},$$

где коэффициенты a_s, b_s равны количеству классов $\left\langle {\{0,\dots,m-1\}^{u+v} \atop (I_1,\dots,I_s)} \right\rangle$ множества

$$\left\{(\lambda_1,\dots,\lambda_u,\lambda_{u+1},\dots,\lambda_{u+v}) \in \{0,\dots,m-1\}^{u+v}\right\},$$

удовлетворяющих, соответственно, L-условиям

$$C_1 = \bigwedge_{h=1}^{u-1}[\lambda_{h+1} < \lambda_h] \wedge \bigwedge_{h=1}^{v-1}[\lambda_{u+h+1} < \lambda_{u+h}],$$
$$C_2 = C_1 \wedge \left(\gamma_{u<v} \wedge \bigwedge_{k=1}^{\min\{u,v\}}[\lambda_k = \lambda_{u+k}] \vee \bigvee_{k=1}^{\min\{u,v\}}[\lambda_k < \lambda_{u+k}] \wedge \bigwedge_{h=1}^{k-1}[\lambda_h = \lambda_{u+h}]\right).$$

Начнем с вычисления a_s, $s \in \overline{1,u+v}$. Нужно пересчитать все разбиения $(I_1,\dots,I_s)$ множества индексов $\{1,\dots,u+v\}$, удовлетворяющие условиям:

$$\lambda_1 > \dots > \lambda_u,\ \lambda_{u+1} > \dots > \lambda_{u+v}.$$

Отождествим множества $I_1,\dots,I_s$ с урнами, а индексы $1,\dots,u$ и $u+1,\dots,u+v$, соответственно, с красными и синими шарами. В каждой урне может находиться либо один красный шар, либо один синий, либо один красный и один синий. Пусть в этих случаях урны окрашиваются, соответственно, в красный, синий и фиолетовый цвета. Получаем, что каждому разбиению $(I_1,\dots,I_s)$ соответствует своя цветовая гамма урн $I_1,\dots,I_s$, и наоборот. Предположим, что красные шары уже некоторым образом расположены в урнах, тогда остается ровно $s-u$ пустых урн, в которые будут помещены только синие шары. Таким образом, мы всегда имеем $s-u$ синих урн, $s-v$ красных, и $u+v-s$ фиолетовых. Значит, коэффициент a_s равен количеству разбиений множества из s элементов на три подмножества с мощностями $s-u$, $s-v$, и $u+v-s$, т.е.

$$a_s = \binom{s}{s-u, s-v, u+v-s}.$$

Переходим к вычислению b_s, $s \in \overline{1,u+v}$, продолжая использовать комбинаторную интерпретацию. После раскрытия скобок L-условие C_2 будет записано в ДНФ так, что никакие два дизъюнкта не могут принимать одновременно истинные значения. Значит, остается для каждого дизъюнкта в отдельности пересчитать количество соответствующих разбиений $(I_1, \dots, I_s)$. При любом k от 1 до $\min\{u, v\}$ для дизъюнкта

$$C_1 \wedge [\lambda_k < \lambda_{u+k}] \wedge \bigwedge_{h=1}^{k-1} [\lambda_h = \lambda_{u+h}]$$

имеем: урны $I_1, \dots, I_{k-1}$ окрашены в фиолетовый цвет, урна I_k — в синий, остальные урны допускают любую окраску. Значит, в этом случае количество разбиений $(I_1, \dots, I_s)$ равно $\binom{s-k}{s-u, s-v-1, u+v-s-k+1}$. Далее, для дизъюнкта

$$C_1 \wedge \gamma_{u<v} \wedge \bigwedge_{k=1}^{\min\{u,v\}} [\lambda_k = \lambda_{u+k}]$$

существует не более одной цветовой гаммы урн $I_1, \dots, I_s$, а именно $I_1, \dots, I_u$ окрашены в фиолетовый цвет, $I_{u+1}, \dots, I_s$ окрашены в синий. Это возможно только при $s = v$. Значит, количество разбиений $(I_1, \dots, I_s)$ выражается в виде $\delta_{[u<v]\wedge[s=v]}$, где δ_A — функция, переводящая высказывание A в целое число 1, если оно истинно, в 0, если ложно. Таким образом, имеем

$$b_s = \delta_{[u<v]\wedge[s=v]} + \sum_{k=1}^{\min\{u,v\}} \binom{s-k}{s-u-1, s-v, u+v-s-k+1}.$$

Поскольку

$$\delta_{[u<v]\wedge[s=v]} = \sum_{k=\min\{u,v\}+1}^{v} \binom{s-k}{s-u-1, s-v, u+v-s-k+1},$$

b_s принимает искомый вид. $\square$

1.4 Делимость показателей степеней коммутаторов в собирательных формулах

Ввиду следствия 1.2.3 и определения 1.3.2 мы немедленно получаем следующее утверждение.

Лемма 1.4.1. *Пусть коммутатор $R \in \Gamma(a_1, \ldots, a_n)$ возник в ходе некоторого варианта собирательного процесса $\{W_j\}_{j \geqslant 0}$. Если условия существования и предшествования E_{a_i}, P_{a_i,a_j} в формуле из следствия 1.2.3 выражаются некоторыми L-условиями на множествах $D(a_i)$, $D(a_i) \times D(a_j)$ соответственно, тогда E_R выражается некоторым L-условием на $D(R)$.*

Далее сформулируем результат из теоремы 1.3.1 для множества целых чисел.

Лемма 1.4.2. *Пусть конечные множества $M_1, \ldots, M_r \subset \mathbb{Z}$ удовлетворяют следующим условиям:*

$$M = M_1 \cap \cdots \cap M_r \in \{M_j\}_{j=1}^{r}; \qquad [\min M, \max M] \cap (M_i \backslash M) = \varnothing, \quad i \in \overline{1, r}.$$

Тогда количество элементов из $M_1 \times \cdots \times M_r$, удовлетворяющих произвольному L-условию C ранга не выше r, выражается в виде

$$\sum_{t=1}^{r} c_t \binom{|M|}{t}, \quad c_t \in \mathbb{N}_0, \tag{41}$$

где c_t не зависят от $M_1, \ldots, M_r$, если $M_1 = \cdots = M_r$.

Здесь мы допускаем, что некоторые множества $M_1, \ldots, M_r$ могут быть пустыми. Действительно, если некоторое $M_j = \varnothing$, тогда $M_1 \times \cdots \times M_r = \varnothing$, $M = \varnothing$ и все слагаемые в сумме (41) равны нулю.

Пример 1.4.1. Любое семейство отрезков целых чисел с фиксированным левым или правым концом удовлетворяет условиям леммы 1.4.2. Например,

$$M_1 = \{1, 2, 3\}, \quad M_2 = \{1, 2, 3, 4, 5\}, \quad M_3 = \{1, 2, 3, 4, 5, 6, 7\}.$$

Пусть W — положительное слово свободной группы $F(a_1,\dots,a_n)$, $n\in\mathbb{N}$. Согласно нашему подходу, если мы хотим применить собирательный процесс к W и исследовать делимость показателя степени некоторого коммутатора R с бесскобочной записью $(a_{i_1},\dots,a_{i_{w(R)}})$, тогда наша главная цель — найти подходящую разметку для слова W. «Подходящая разметка» означает, что 1) условия существования и предшествования $E_{a_{i_j}}$, $P_{a_{i_j},a_{i_k}}$ для всех $j,k\in\overline{1,w(R)}$ выражаются L-условиями на множествах $D(a_{i_j})$, $D(a_{i_j})\times D(a_{i_k})$ соответственно и 2) множества $D(a_{i_j})$, $j\in\overline{1,w(R)}$, удовлетворяют условиям леммы 1.4.2. Мы будем следовать этим «обычным» путем в доказательстве теоремы 1.4.1.

Однако в теореме 1.4.2 мы будем рассматривать сужение предиката E_R, фиксируя специальные переменные, для получения свойства делимости более сильного, чем мы могли бы получить, следуя «обычным» путем. Наконец, в теореме 1.4.3 мы используем разметку, для которой множества $D(a_{i_j})$ даже не удовлетворяют условиям леммы 1.4.2, пока мы не используем похожий прием из предыдущего случая.

Теорема 1.4.1. *Пусть $\{W_j\equiv q_1^{e_1}\dots q_j^{e_j}T_j\}_{j\geqslant 0}$ — произвольный вариант собирательного процесса в свободной группе $F(a_1,\dots,a_n)$, $n\in\mathbb{N}$, с начальным словом*

$$W_0\equiv\prod_{i=1}^{N}\left(a_1^{\rho(i,1)}\dots a_n^{\rho(i,n)}\right),\quad N\in\mathbb{N},\ \rho(i,k):\{1,\dots,N\}\times\{1,\dots,n\}\to\{0,1\}.$$

Пусть $M_k=\{i\mid\rho(i,k)=1\}$, $k\in\overline{1,n}$, и $(a_{k_1},\dots,a_{k_{w(q_j)}})$ есть бесскобочная запись q_j. Если множество $M=M_{k_1}\cap\dots\cap M_{k_{w(q_j)}}$ удовлетворяет следующим условиям:

$$M\in\{M_{k_s}\}_{s=1}^{w(q_j)};\qquad [\min M,\max M]\cap(M_{k_s}\backslash M)=\varnothing,\quad s\in\overline{1,w(q_j)};$$

тогда

$$e_j=\sum_{t=1}^{w(q_j)}c_t\binom{|M|}{t},\quad c_t\in\mathbb{N}_0.$$

Доказательство. Рассмотрим положительное слово $W \equiv (a_1 \dots a_n)^N$ со следующей разметкой:

$$W \equiv \prod_{i=1}^{N} (a_1(i) \dots a_n(i)); \qquad D(a_k) = \{1, \dots, N\}, \quad k \in \overline{1, n}.$$

Видно, что для любых $\lambda_1 \in D(a_{k_1})$, $\lambda_2 \in D(a_{k_2})$, $k_1, k_2 \in \overline{1, n}$, справедливы равенства:

$$E^{(\lambda_1)}_{a_{k_1}} = 1, \quad P^{(\lambda_1, \lambda_2)}_{a_{k_1}, a_{k_2}} = \begin{cases} [\lambda_1 < \lambda_2], & \text{если } k_1 = k_2; \\ [\lambda_1 < \lambda_2] \vee [\lambda_1 = \lambda_2], & \text{если } k_1 < k_2; \\ [\lambda_1 < \lambda_2], & \text{если } k_1 > k_2. \end{cases}$$

Теперь для каждого $k \in \overline{1, n}$ удалим все вхождения буквы a_k в слове W, метки которых принадлежат множеству $D(a_k) \backslash M_k$. Таким образом, мы получим помеченное слово W_0, для которого $D(a_k) = M_k$, $k \in \overline{1, n}$. Более того, равенства для условий существования и предшествования, приведенные выше, будут справедливы и для W_0. Действительно, поскольку $D(a_k)$ содержит только метки вхождений a_k из W_0, имеем $E^{(\lambda_1)}_{a_k} = 1$ для любого $\lambda_1 \in D(a_k)$. Далее, удаление вхождений букв в слове W не меняет относительное расположение оставшихся букв. Иными словами, вхождение $a_{k_1}(\lambda_1)$ предшествует вхождению $a_{k_2}(\lambda_2)$ в W_0 тогда и только тогда, когда $a_{k_1}(\lambda_1)$ предшествует $a_{k_2}(\lambda_2)$ в W. Таким образом, равенство для $P^{(\lambda_1, \lambda_2)}_{a_{k_1}, a_{k_2}}$ не меняется при переходе от W к W_0.

Пусть $(a_{i_1}, \dots, a_{i_{w(q_j)}})$ — бесскобочная запись коммутатора q_j. Из леммы 1.4.1 следует, что условие существования $E^{\Lambda}_{q_j}$ выражается L-условием на множестве $D(q_j) = D(a_{k_1}) \times \dots \times D(a_{k_{w(q_j)}}) = M_{k_1} \times \dots \times M_{k_{w(q_j)}}$. Если множество $M = M_{k_1} \cap \dots \cap M_{k_{w(q_j)}}$ удовлетворяет следующим условиям:

$$M \in \{M_{k_s}\}_{s=1}^{w(q_j)}; \qquad [\min M, \max M] \cap (M_{k_s} \backslash M) = \varnothing, \quad s \in \overline{1, w(q_j)},$$

тогда согласно предложению 1.2.1 и лемме 1.4.2 мы получаем

$$e_j = |\{\Lambda \in D(q_j) \mid E^{\Lambda}_{q_j} = 1\}| = \sum_{t=1}^{w(q_j)} c_t \binom{|M|}{t}, \quad c_t \in \mathbb{N}_0.$$

□

Доказанная теорема показывает, что для любого семейства множеств, удовлетворяющих условиям леммы 1.4.2, можно построить соответствующее начальное слово W_0. Отсюда мы получаем многочисленные примеры собирательных формул с нетривиальными свойствами делимости показателей степеней коммутаторов. Далее мы рассмотрим лишь несколько таких примеров.

Пример 1.4.2. Пусть $M_k = \{1, \ldots, m\}$, $k \in \overline{1, n}$, где $m \in \mathbb{N}$. Тогда мы имеем начальное слово $W_0 \equiv (a_1 \ldots a_n)^m$ в варианте собирательного процесса $\{W_j \equiv q_1^{e_1} \ldots q_j^{e_j} T_j\}_{j \geqslant 0}$. Если коммутаторы собирались в порядке возрастания весов, то справедлива следующая собирательная формула в свободной группе $F = F(a_1, \ldots, a_n)$:

$$(a_1 \ldots a_n)^m = q_1^{e_1} \ldots q_{j(s)}^{e_{j(s)}} \pmod{\Gamma_s(F)}, \quad s \in \mathbb{N}.$$

Для любого коммутатора q_j имеем $M = \{1, \ldots, m\}$, $|M| = m$. Следовательно, e_j делится на m, если m есть степень простого числа p^α и $w(q_j) < p$.

Пример 1.4.3. Пусть $M_k = \{1, \ldots, m\}$ для $k \neq s$, и $M_s = \{1, \ldots, m + r\}$, где $s \in \overline{1, n}$, $m, r \in \mathbb{N}$. Тогда мы имеем начальное слово $W_0 \equiv (a_1 \ldots a_n)^m a_s^r$ в варианте собирательного процесса $\{W_j \equiv q_1^{e_1} \ldots q_j^{e_j} T_j\}_{j \geqslant 0}$. Таким образом, справедлива следующая собирательная формула в свободной группе $F(a_1, \ldots, a_n)$:

$$(a_1 \ldots a_n)^m a_s^r = q_1^{e_1} \ldots q_j^{e_j} T_j.$$

Предположим, что $w(q_j) \geqslant 2$. Тогда бесскобочная запись q_j содержит букву отличную от a_s. Следовательно, $M = \{1, \ldots, m\}$, $|M| = m$, и e_j делится на m, если m есть степень простого числа p^α и $1 < w(q_j) < p$.

Определение 1.4.1. Для элементов множества $\Gamma(a_1, \ldots, a_n)$ определим индуктивно веса w_{a_i}, $i \in \overline{1, n}$:

1) $w_{a_i}(a_k) = 0$ для $k \neq i$, $w(a_i) = 1$;

2) если $[c_1, c_2] \in \Gamma(a_1, \ldots, a_n)$, то $w_{a_i}([c_1, c_2]) = w_{a_i}(c_1) + w_{a_i}(c_2)$.

Если $(a_{i_1}, \ldots, a_{i_{w(R)}})$ — бесскобочная запись $R \in \Gamma(a_1, \ldots, a_n)$, то вес $w_{a_i}(R)$ равен количеству вхождений a_i в последовательности $(a_{i_1}, \ldots, a_{i_{w(R)}})$.

Пример 1.4.4. Пусть M_1, M_2, M_3 взяты из примера 1.4.1. Тогда мы имеем слово $W_0 \equiv (a_1 a_2 a_3)^3 (a_2 a_3)^2 a_3^2$. Если $w_{a_1}(q_j) \geqslant 1$ и $3 > w(q_j) \geqslant 1$, то e_j делится на 3. Если $w_{a_1}(q_j) = 0$, $w_{a_2}(q_j) \geqslant 1$ и $5 > w(q_j) \geqslant 1$, то e_j делится на 5.

Теорема 1.4.2. *Пусть* $\left\{W_j \equiv q_1^{e_1} \ldots q_j^{e_j} T_j\right\}_{j \geqslant 0}$ *— произвольный вариант собирательного процесса в свободной группе* $F(a_1, \ldots, a_n)$, $n \in \mathbb{N}$, *с начальным словом*

$$W_0 \equiv a_1^{m_1} \ldots a_n^{m_n}, \quad m_1, \ldots, m_n \in \mathbb{N}.$$

Если $w_{a_{s_1}}(q_j) \geqslant 1, \ldots, w_{a_{s_r}}(q_j) \geqslant 1$, *тогда показатель степени* e_j *выражается в виде*

$$e_j = \sum_{t_1=1}^{w_{a_{s_1}}(q_j)} \cdots \sum_{t_r=1}^{w_{a_{s_r}}(q_j)} c(t_1, \ldots, t_r) \binom{m_{s_1}}{t_1} \cdots \binom{m_{s_r}}{t_r},$$

где целые числа $c(t_1, \ldots, t_r)$ *не зависят от* $m_{s_1}, \ldots, m_{s_r}$.

Доказательство. Рассмотрим положительное слово W_0 со следующей разметкой:

$$W_0 \equiv \prod_{i=1}^{n} a_i(1) \ldots a_i(m_i); \qquad D(a_i) = \{1, \ldots, m_i\}, \quad i \in \overline{1, n}.$$

Видно, что для любых $\lambda_1 \in D(a_{i_1})$, $\lambda_2 \in D(a_{i_2})$, $i_1, i_2 \in \overline{1, n}$, справедливы равенства:

$$E_{a_{i_1}}^{(\lambda_1)} = 1, \quad P_{a_{i_1}, a_{i_2}}^{(\lambda_1, \lambda_2)} = \begin{cases} [\lambda_1 < \lambda_2], & i_1 = i_2; \\ 1, & i_1 < i_2; \\ 0, & i_2 < i_1. \end{cases}$$

Пусть $(a_{i_1}, \ldots, a_{i_{w(q_j)}})$ — бесскобочная запись коммутатора q_j. Из леммы 1.4.1 следует, что условие существования $E_{q_j}^{\Lambda}$, $\Lambda = (\lambda_1, \ldots, \lambda_{w(q_j)})$, выражается L-условием на множестве $D(q_j) = D(a_{i_1}) \times \cdots \times D(a_{i_{w(q_j)}})$.

Пусть $w_{a_{s_1}}(q_j) \geqslant 1$. Произвольным образом зафиксируем те переменные из $\lambda_1, \ldots, \lambda_{w(q_j)}$ в $E^{\Lambda}_{q_j}$, которые соответствуют меткам букв a_k, $k \neq s_1$. Полученный предикат обозначим через $\widetilde{E}^M_{q_j}$, где M — упорядоченный набор оставшихся $w_{a_{s_1}}(q_j)$ переменных.

Заметим, что предикат $\widetilde{E}^M_{q_j}$ на декартовой степени $D(a_{s_1})^{w_{a_{s_1}}(q_j)}$ все еще выражается L-условием. Действительно, из равенств выше для E_{a_i} и P_{a_i,a_j} следует, что для любого предиката $[\lambda_u < \lambda_v]$ в L-условии $E^{\Lambda}_{q_j}$ переменные λ_u и λ_v соответствуют меткам одной и той же буквы. Это же справделиво для предикатов $[\lambda_u = \lambda_v]$, что следует из рекуррентных соотношений в теореме 1.2.2. Значит, $\widetilde{E}^M_{q_j}$ содержит не более чем константы 0, 1 и предикаты вида $[\lambda_u < \lambda_v]$, $[\lambda_u = \lambda_v]$, где λ_u, λ_v являются переменными.

Таким образом, ил леммы 1.4.2 следует, что

$$|\{M \in D(a_s)^{w_{a_{s_1}}(q_j)} \mid \widetilde{E}^M_{q_j} = 1\}| = \sum_{t=1}^{w_{a_{s_1}}(q_j)} b_t \binom{m_{s_1}}{t},$$

где целые неотрицательные числа b_t не зависят от m_{s_1}.

Рассматривая всевозможные значения переменных в $E^{\Lambda}_{q_j}$, которые соответствуют меткам букв a_k, $k \neq s_1$, и суммируя соответствующие выражения, мы, наконец, получаем

$$e_j = |\{\Lambda \in D(q_j) \mid E^{\Lambda}_{q_j} = 1\}| = \sum_{t=1}^{w_{a_{s_1}}(q_j)} c_t \binom{m_{s_1}}{t}, \quad c_t \in \mathbb{N}_0,$$

где коэффициенты c_t не зависят от m_{s_1}, но могут зависеть от $m_{s_2}, \ldots, m_{s_r}$.

Дальнейшее доказательство проводится индукцией по r. Пусть $w_{a_{s_1}}(q_j) \geqslant 1, \ldots, w_{a_{s_{r-1}}}(q_j) \geqslant 1$ для $r \geqslant 2$. Предположим, что

$$e_j = \sum_{t_1=1}^{w_{a_{s_1}}(q_j)} \cdots \sum_{t_{r-1}=1}^{w_{a_{s_{r-1}}}(q_j)} c(t_1, \ldots, t_{r-1}) \binom{m_{s_1}}{t_1} \cdots \binom{m_{s_{r-1}}}{t_{r-1}},$$

где целые числа $c(t_1, \ldots, t_{r-1})$ не зависят от $m_{s_1}, \cdots m_{s_{r-1}}$. Если $w_{a_{s_r}}(q_j) \geqslant 1$, то

$$e_j = \sum_{t=1}^{w_{a_{s_r}}(q_j)} a_t \binom{m_{s_r}}{t} = \sum_{t_1=1}^{w_{a_{s_1}}(q_j)} \cdots \sum_{t_{r-1}=1}^{w_{a_{s_{r-1}}}(q_j)} c(t_1, \ldots, t_{r-1}) \binom{m_{s_1}}{t_1} \cdots \binom{m_{s_{r-1}}}{t_{r-1}},$$

где a_t не зависят от m_{s_r}. Следовательно, a_t зависят от $m_{s_1}, \ldots, m_{s_{r-1}}$, а числа $c(t_1, \ldots, t_{r-1})$ зависят от m_{s_r}. Если $m_{s_r} = 1$, имеем

$$a_1 = \sum_{t_1=1}^{w_{a_{s_1}}(q_j)} \cdots \sum_{t_{r-1}=1}^{w_{a_{s_{r-1}}}(q_j)} c(t_1, \ldots, t_{r-1}; 1) \binom{m_{s_1}}{t_1} \cdots \binom{m_{s_{r-1}}}{t_{r-1}},$$

Далее, если $m_{s_r} = 2$, то

$$2a_1 + a_2 = \sum_{t_1=1}^{w_{a_{s_1}}(q_j)} \cdots \sum_{t_{r-1}=1}^{w_{a_{s_{r-1}}}(q_j)} c(t_1, \ldots, t_{r-1}; 2) \binom{m_{s_1}}{t_1} \cdots \binom{m_{s_{r-1}}}{t_{r-1}},$$

$$a_2 = \sum_{t_1=1}^{w_{a_{s_1}}(q_j)} \cdots \sum_{t_{r-1}=1}^{w_{a_{s_{r-1}}}(q_j)} (c(t_1, \ldots, t_{r-1}; 2) - 2c(t_1, \ldots, t_{r-1}; 1)) \binom{m_{s_1}}{t_1} \cdots \binom{m_{s_{r-1}}}{t_{r-1}}.$$

Продолжая рассуждения аналогичным образом, видим, что для любого $t \in \overline{1, w_{a_{s_r}}(q_j)}$ существуют целые числа $h_t(t_1, \ldots, t_{r-1})$ такие, что

$$a_t = \sum_{t_1=1}^{w_{a_{s_1}}(q_j)} \cdots \sum_{t_{r-1}=1}^{w_{a_{s_{r-1}}}(q_j)} h_t(t_1, \ldots, t_{r-1}) \binom{m_{s_1}}{t_1} \cdots \binom{m_{s_{r-1}}}{t_{r-1}}.$$

Значит,

$$e_j = \sum_{t=1}^{w_{a_{s_r}}(q_j)} \left(\sum_{t_1=1}^{w_{a_{s_1}}(q_j)} \cdots \sum_{t_{r-1}=1}^{w_{a_{s_{r-1}}}(q_j)} h_t(t_1, \ldots, t_{r-1}) \binom{m_{s_1}}{t_1} \cdots \binom{m_{s_{r-1}}}{t_{r-1}} \right) \binom{m_{s_r}}{t}$$
$$= \sum_{t_1=1}^{w_{a_{s_1}}(q_j)} \cdots \sum_{t_r=1}^{w_{a_{s_r}}(q_j)} c(t_1, \ldots, t_r) \binom{m_{s_1}}{t_1} \cdots \binom{m_{s_r}}{t_r},$$

где $c(t_1, \ldots, t_r)$ не зависят от $m_{s_1}, \ldots, m_{s_r}$ □

Пример 1.4.5. Пусть коммутаторы собираются в порядке возрастания весов, и коммутаторы веса 1 собираются в следующем порядке: a_{s+1}, a_{s+2}, …, a_n, a_1, a_2, …, a_s для некоторого $s \in \overline{1, n-1}$. Тогда рассматриваемый вариант собирательного процесса $\left\{W_j \equiv q_1^{e_1} \ldots q_j^{e_j} T_j\right\}_{j \geqslant 0}$ приводит к следующей собирательной формуле в свободной группе $F = F(a_1, \ldots, a_n)$:

$$[a_1^{m_1} \ldots a_s^{m_s}, a_{s+1}^{m_{s+1}} \ldots a_n^{m_n}] = q_{n+1}^{e_{n+1}} \ldots q_{j(k)}^{e_{j(k)}} \pmod{\Gamma_k(F)}, \quad k \geqslant 2,$$

где $q_{n+1},\dots,q_{j(k)}$ — коммутаторы весов не меньше, чем k, и e_j делится на m_i, если m_i есть степень простого числа p^α и $1 \leqslant w_{a_i}(q_j) < p$.

Теорема 1.4.3. *Пусть* $\{W_j \equiv q_1^{e_1}\dots q_j^{e_j}T_j\}_{j\geqslant 0}$ *— произвольный вариант собирательного процесса в свободной группе* $F(a_1,\dots,a_n)$*,* $n\in\mathbb{N}$*, с начальным словом*

$$W_0 \equiv \prod_{i=1}^{N}\left(a_{k_1}^{\rho(i,1)}\dots a_{k_s}^{\rho(i,s)}\right),\quad N,s\in\mathbb{N},\ \rho(i,j):\{1,\dots,N\}\times\{1,\dots,s\}\to\{0,1\},$$

где $k_1,\dots,k_s\in\overline{1,n}$*. Пусть*

$$M_k=\{(i,j)\mid k_j=k,\ \rho(i,j)=1\},\qquad M_k(\mu)=\{i\mid (i,\mu)\in M_k\},\quad k\in\overline{1,n},$$

и $(a_{i_1},\dots,a_{i_{w(q_j)}})$ *— бесскобочная запись коммутатора* q_j*. Если для любых* $\mu_1,\dots,\mu_{w(q_j)}$ *множество* $M=M(\mu_1,\dots,\mu_{w(q_j)})=M_{i_1}(\mu_1)\cap\dots\cap M_{i_{w(q_j)}}(\mu_{w(q_j)})$ *удовлетворяет условиям:*

$$M\in\{M_{i_k}(\mu_k)\}_{k=1}^{w(q_j)};\qquad [\min M,\max M]\cap(M_{i_k}(\mu_k)\backslash M)=\varnothing,\quad k\in\overline{1,w(q_j)};$$

тогда

$$e_j=\sum_{t=1}^{w(q_j)}\sum_{\mu_1,\dots,\mu_{w(q_j)}}c_t(\mu_1,\dots,\mu_{w(q_j)})\binom{|M(\mu_1,\dots,\mu_{w(q_j)})|}{t},$$

где $c_t(\mu_1,\dots,\mu_{w(q_j)})\in\mathbb{N}_0$*.*

Доказательство. Рассмотрим положительное слово $W\equiv(a_{k_1}\dots a_{k_s})^N$ со следующей разметкой:

$$W\equiv\prod_{i=1}^{N}(a_{k_1}(i,1)\dots a_{k_s}(i,s));$$

$$D(a_k)=\{(i,j)\mid 1\leqslant i\leqslant N,k_j=k\}=\{1,\dots,N\}\times\{j\mid k_j=k\},\quad k\in\overline{1,n}.$$

Видно, что для любых $(\lambda_1,\lambda_2)\in D(a_i)$, $(\lambda_3,\lambda_4)\in D(a_j)$, $i,j\in\overline{1,n}$, справедливы равенства:

$$E_{a_i}^{(\lambda_1,\lambda_2)}=1,\quad P_{a_i,a_j}^{(\lambda_1,\lambda_2,\lambda_3,\lambda_4)}=[\lambda_1<\lambda_3]\vee[\lambda_1=\lambda_3][\lambda_2<\lambda_4].$$

Теперь для каждого $k = \overline{1,n}$ удалим все вхождения буквы a_k в слове W, метки которых принадлежат множеству $D(a_k)\backslash M_k$. Таким образом, мы получаем помеченное слово W_0, для которого $D(a_k) = M_k$, $k \in \overline{1,n}$. Используя те же рассуждения, что и в доказательстве теоремы 1.4.1, заключаем, что равенства выше для $E_{a_i}^{(\lambda_1,\lambda_2)}$ и $P_{a_i,a_j}^{(\lambda_1,\lambda_2,\lambda_3,\lambda_4)}$ не меняются при переходе от W к W_0.

Пусть $(a_{i_1},\ldots,a_{i_{w(q_j)}})$ — бесскобочная запись коммутатора q_j. Из леммы 1.4.1 следует, что условие существования $E_{q_j}^{\Lambda}$ выражается L-условием на множестве $D(q_j) = D(a_{i_1})\times\cdots\times D(a_{i_{w(q_j)}}) = M_{i_1}\times\cdots\times M_{i_{w(q_j)}}$, где последовательность $\Lambda = (\lambda_1,\ldots,\lambda_{2w(q_j)})$ такая, что

$$(\lambda_1,\lambda_2)\in M_{i_1},\ (\lambda_2,\lambda_3)\in M_{i_2},\ \ldots,\ (\lambda_{2w(q_j)-1},\lambda_{2w(q_j)})\in M_{i_{w(q_j)}}.$$

Введем следующие обозначения:

$$\Lambda_1 = (\lambda_1,\lambda_3\ldots,\lambda_{2w(q_j)-1}), \qquad \Lambda_2 = (\lambda_2,\lambda_4\ldots,\lambda_{2w(q_j)}).$$

Зафиксируем произвольным образом $\lambda_2,\lambda_4,\ldots,\lambda_{2w(q_j)}$ в $E_{q_j}^{\Lambda}$. Полученный предикат обозначим через

$$P_{\Lambda_2}^{\Lambda_1}, \quad \text{где } \Lambda_1 \in M_{i_1}(\lambda_2)\times\cdots\times M_{i_{2w(q_j)-1}}(\lambda_{2w(q_j)}).$$

Из равенств выше для E_{a_i} и P_{a_i,a_j} следует, что $P_{\Lambda_2}^{\Lambda_1}$ содержит не более чем константы 0, 1 и предикаты вида $[\lambda_u<\lambda_v]$, $[\lambda_u=\lambda_v]$, где λ_u,λ_v являются переменными. Иными словами, для любой фиксированной последовательности Λ_2 предикат $P_{\Lambda_2}^{\Lambda_1}$ выражается L-условием на множестве $M_{i_1}(\lambda_2)\times\cdots\times M_{i_{2w(q_j)-1}}(\lambda_{2w(q_j)})$.

Таким образом, используя предложение 1.2.1 и лемму 1.4.2, получаем

$$\begin{aligned}
e_j &= |\{\Lambda\in D(q_j)\mid E_{q_j}^{\Lambda}=1\}| \\
&= \sum_{\Lambda_2}\left|\{\Lambda_1\in M_{i_1}(\lambda_2)\times\cdots\times M_{i_{2w(q_j)-1}}(\lambda_{2w(q_j)})\mid P_{\Lambda_2}^{\Lambda_1}=1\}\right| \\
&= \sum_{\Lambda_2}\sum_{t=1}^{w(q_j)} c_t(\Lambda_2)\binom{|M(\Lambda_2)|}{t} = \sum_{t=1}^{w(q_j)}\sum_{\Lambda_2} c_t(\Lambda_2)\binom{|M(\Lambda_2)|}{t}.
\end{aligned}$$

□

Пример 1.4.6. Пусть $W_0 \equiv (a_{k_1} \dots a_{k_s})^m$, где $m \in \mathbb{N}$. Тогда мы положим

$$M_k = \{1, \dots, m\} \times \{j \mid k_j = k\}, \quad k \in \overline{1, n}.$$

Следовательно, для любого μ множество $M_k(\mu)$ равно $\{1, \dots, m\}$ или $\varnothing$. Тогда для любых $\mu_1, \dots, \mu_{w(q_j)}$ пересечение $M = M(\mu_1, \dots, \mu_{w(q_j)})$ совпадает с $\{1, \dots, m\}$ или $\varnothing$, поэтому мощность $|M|$ равна m или 0. Таким образом, если коммутаторы собираются в порядке возрастания весов, тогда мы получаем следующую собирательную формулу в свободной группе $F = F(a_1, \dots, a_n)$:

$$(a_{k_1} \dots a_{k_s})^m = q_1^{e_1} \dots q_{j(c)}^{e_{j(c)}} \pmod{\Gamma_c(F)}, \quad c \in \mathbb{N},$$

где e_j делится m, если m есть степень простого числа p^α и $w(q_j) < p$.

Пример 1.4.7. Пусть $W_0 \equiv a_l^r \, (a_{k_1} \dots a_{k_s})^m$, где $l \in \overline{1, n}$, $m, r \in \mathbb{N}$. Тогда мы положим

$$M_k = \{r+1, \dots, m+r\} \times \{j \mid k_j = k\}, \quad k \neq l;$$
$$M_l = \Big(\{1, \dots, m+r\} \times \{j'\}\Big) \cup \Big(\{r+1, \dots, m+r\} \times \{j \mid k_j = l\}\Big);$$

где j' такое, что $k_{j'} = l$. Следовательно, для любого μ множество $M_k(\mu)$, $k \neq l$, равно $\{r+1, \dots, m+r\}$ или $\varnothing$. Предположим, что $w(q_j) \geqslant 2$, тогда $w_{a_k}(q_j) \geqslant 1$ для некоторого $k \neq l$. Значит, для любых $\mu_1, \dots, \mu_{w(q_j)}$ пересечение $M = M(\mu_1, \dots, \mu_{w(q_j)})$ совпадет с $\{r+1, \dots, m+r\}$ или $\varnothing$, поэтому мощность $|M|$ равна m или 0. Таким образом, получаем следующую собирательную формулу в свободной группе $F(a_1, \dots, a_n)$:

$$a_l^r \, (a_{k_1} \dots a_{k_s})^m = q_1^{e_1} \dots q_j^{e_j} T_j,$$

где e_j делится на m, если m есть степень простого числа p^α и $1 < w(q_j) < p$.

Глава 2. Собирательная формула Ф. Холла

В главе 2 диссертации вычисляются в явном виде показатели степеней коммутаторов в собирательной формуле Ф. Холла для выражения $(xy)^n$, $n \in \mathbb{N}$.

В § 2.1 представлена параметризация несобранной части формулы Ф. Холла с помощью функции бинарного веса числа. С использованием этой параметризации и ряда установленных комбинаторных утверждений получены в явном холловском виде показатели степеней для двух серий коммутаторов в § 2.2. Как следствие, для данных показателей степеней найдены выражения по модулю простого n, в частности, когда вес коммутатора равен n.

2.1 Параметризация несобранной части

Теорема 2.1.1. *Пусть G — группа, $x, y \in G$. Тогда для любого $n \in \mathbb{N}$ справедливо следующее тождество:*

$$(xy)^n = x^n y^n \prod_{k=1}^{n-1} \prod_{i_1=1}^{2^{n-k}-1} \prod_{i_2=0}^{2^{n-k}-1} [y,_{\omega(i_1)} x,_{\omega(i_2)} y].$$

Доказательство. В свободной группе $F(x, y)$ рассмотрим слово

$$W_0 \equiv (xy)^n \equiv \prod_{k=1}^{n} xy.$$

Применим к W_0 два этапа собирательного процесса (соберем x, затем y). Согласно следствию 1.2.2 получаем слова

$$W_1 \equiv x^n \cdot \prod_{k=1}^{n} \prod_{i_1=0}^{2^{H_n^1}-1} [y,_{\omega(i_1)} x], \qquad W_2 \equiv x^n y^n \cdot \prod_{k=1}^{n} \prod_{\substack{i_1=0 \\ [y,_{\omega(i_1)} x] \neq y}}^{2^{H_n^1}-1} \prod_{i_2=0}^{2^{H_n^2}-1} [y,_{\omega(i_1)} x,_{\omega(i_2)} y],$$

здесь $H_n^1 = n - k$ — количество вхождений x после вхождения y на позиции k, $H_n^2 = n - k$ — количество вхождений y после вхождения $[y,_{\omega(i_1)} x]$ на позиции (k, i_1). Чтобы в полученном произведении учесть условие $[y,_{\omega(i_1)} x] \neq y$ и получить искомое тождество, изменим нижний предел по i на 1, как следствие, верхний предел по k изменится на $n - 1$. $\square$

Определение 2.1.1. Для фиксированной последовательности формальных коммутаторов $c_0, \ldots, c_r$ будем говорить, что коммутаторы $[c_0,_{i_1} c_1, , \ldots ,_{i_r} c_r]$ и $[c_0,_{j_1} c_1, , \ldots ,_{j_r} c_r]$ *одного вида* тогда и только тогда, когда $i_1 = j_1, \ldots, i_r = j_r$.

Определение 2.1.2. Для любых $q, x \in \mathbb{Z}$ положим

$$W(q, x) = \{i \mid \omega(i) = x,\ 0 \leqslant i \leqslant q\}.$$

Следствие 2.1.1. *Пусть G — группа, $x, y \in G$. Применим собирательный процесс к слову $(xy)^n$, $n \geqslant 1$: на первом и втором этапах соберем $c_1 = x$,*

$c_2 = y$, далее собираем коммутаторы в произвольном порядке $c_3, \ldots, c_r$, $r \geqslant 3$. Тогда c_r имеет вид $[c_2, {}_{l_1}c_1, \ldots, {}_{l_{r-1}}c_{r-1}]$ для некоторых $l_1, \ldots, l_{r-1} \geqslant 0$, и справедлива формула

$$(xy)^n = c_1^{e_n^1} c_2^{e_n^2} \ldots c_r^{e_n^r} \prod_{k=1}^{n} \prod_{i_1=0}^{2^{H_n^1}-1} \prod_{i_2=0}^{2^{H_n^2}-1} \cdots \prod_{i_r=0}^{2^{H_n^r}-1} [c_2, {}_{\omega(i_1)}c_1, {}_{\omega(i_2)}c_2, \ldots, {}_{\omega(i_r)}c_r]^{\rho(i_1,\ldots,i_r)}, \tag{42}$$

$$e_n^r = \sum_{k=1}^{n} \sum_{i_1 \in W(2^{H_n(k;c_1)}-1, l_1)} \sum_{i_2 \in W(2^{H_n(k,i_1;c_2)}-1, l_2)} \cdots \sum_{i_{r-1} \in W(2^{H_n(k,i_1,\ldots,i_{r-2};c_{r-1})}-1, l_{r-1})} 1.$$

Здесь $\rho(i_1, \ldots, i_r) \in \{0, 1\}$, и числа $H_n^r = H_n(k, i_1, \ldots, i_{r-1}; c_r)$ равны

$$e_n^r - \sum_{m=1}^{k-1} \sum_{j_1 \in W(2^{H_n(m;c_1)}-1, l_1)} \cdots \sum_{j_{r-1} \in W(2^{H_n(m,j_1,\ldots,j_{r-2};c_{r-1})}-1, l_{r-1})} 1$$

$$- \sum_{q=1}^{r} \Delta_q \sum_{j_q \in W(i_q-1, l_q)} \sum_{j_{q+1} \in W(2^{H_n(k,i_1,\ldots,i_{q-1},j_q;c_{q+1})}-1, l_{q+1})} \cdots \sum_{j_{r-1} \in W(2^{H_n(k,i_1,\ldots,i_{q-1},j_q,\ldots,j_{r-2};c_{r-1})}-1, l_{r-1})} 1,$$

где $\Delta_q = \delta_{\omega(i_1), l_1} \ldots \delta_{\omega(i_{q-1}), l_{q-1}}$ и $\delta_{i,j}$ — дельта Кронекера.

Доказательство. Из доказательства предыдущей теоремы следует, что после двух этапов собирательного процесса мы получим слово

$$x^n y^n \prod_{k=1}^{n} \prod_{i_1=0}^{2^{H_n^1}-1} \prod_{i_2=0}^{2^{H_n^2}-1} [y, {}_{\omega(i_1)}x, {}_{\omega(i_2)}y]^{\rho(i_1,i_2)},$$

где $H_n^1 = H_n(k; x) = n - k$ и $H_n^2 = H_n(k, i_1; y) = n - k$, равенство $\rho(i_1, i_2) = 0$ имеет место тогда и только тогда, когда коммутатор $[y, {}_{\omega(i_1)}x]$ имеет вид собранного коммутатора y, иными словами, $\rho(i_1, i_2) = 0$ при $i_1 = 0$, в остальных случаях $\rho(i_1, i_2) = 1$.

Рассуждая аналогично, на этапе r, $r \geqslant 3$, после сбора коммутаторов вида $c_r = [c_2, {}_{l_1}c_1, \ldots, {}_{l_{r-1}}c_{r-1}]$ получим формулу (42), где $H_n^r = H_n(k, i_1, \ldots, i_{r-1}; c_r)$ — количество вхождений c_r правее вхождения $[c_2, {}_{\omega(i_1)}c_1, \ldots {}_{\omega(i_{r-1})}c_{r-1}]$ на позиции $(k, i_1, \ldots, i_{r-1})$ в произведении

$$\prod_{m=1}^{n} \prod_{j_1=0}^{2^{H_n^1}-1} \prod_{j_2=0}^{2^{H_n^2}-1} \cdots \prod_{j_{r-1}=0}^{2^{H_n^{r-1}}-1} [c_2, {}_{\omega(j_1)}c_1, {}_{\omega(j_2)}c_2, \ldots {}_{\omega(j_{r-1})}c_{r-1}]^{\rho(j_1,\ldots,j_{r-1})}. \tag{43}$$

Далее, $\rho(i_1,\dots,i_r)=0$ тогда и только тогда, когда $\rho(i_1,\dots,i_{r-1})=0$ или коммутатор $[c_2,{}_{\omega(i_1)}c_1,\dots{}_{\omega(i_{r-1})}c_{r-1}]$ на позиции $(k,i_1,\dots,i_{r-1})$, $1\leqslant k\leqslant n$, в (43) имеет вид собранного коммутатора $c_r=[c_2,{}_{l_1}c_1,\dots{}_{l_{r-1}}c_{r-1}]$, т.е. $\omega(i_1)=l_1,\dots,\omega(i_{r-1})=l_{r-1}$.

Непосредственно из формулы (42) видно, что показатель степени e_n^r равен

$$\sum_{k=1}^{n}\sum_{i_1\in W(2^{H_n(k;c_1)}-1,l_1)}\sum_{i_2\in W(2^{H_n(k,i_1;c_2)}-1,l_2)}\cdots\sum_{i_{r-1}\in W(2^{H_n(k,i_1,\dots,i_{r-2};c_{r-1})}-1,l_{r-1})}\rho(i_1,\dots,i_{r-1}).$$

Если $\rho(i_1,\dots,i_r)=0$, то для любых $i'_1,\dots,i'_r$, таких что $\omega(i_1)=\omega(i'_1),\dots,\omega(i_r)=\omega(i'_r)$ справедливо равенство $\rho(i'_1,\dots,i'_r)=0$. Иными словами, если в несобранной части (42) коммутатор фиксированного вида имеет степень 1, то и все коммутаторы такого вида будут иметь степень 1. Значит, в полученной сумме $\rho(i_1,\dots,i_{r-1})=1$ для всех допустимых $i_1,\dots,i_{r-1}$.

Далее, $H_n(k,i_1,\dots,i_{r-1};c_r)$ можно выразить как разность общего количества вхождений c_r в (43), т.е. e_n^r, и количества вхождений c_r, расположенных не правее вхождения $[c_2,{}_{\omega(i_1)}c_1,\dots,{}_{\omega(i_{r-1})}c_{r-1}]$ на позиции $(k,i_1,\dots,i_{r-1})$. Выделим в (43) вхождение $[c_2,{}_{\omega(i_1)}c_1,\dots{}_{\omega(i_{r-1})}c_{r-1}]$ на позиции $(k,i_1,\dots,i_{r-1})$ и пересчитаем каждое вхождение $c_r=[c_2,{}_{l_1}c_1,\dots{}_{l_{r-1}}c_{r-1}]$, расположенное не правее него:

$$\begin{aligned}
&\prod_{m=1}^{k-1}\prod_{j_1=0}^{2^{H_n(m;c_1)}-1}\prod_{j_2=0}^{2^{H_n(m,j_1;c_2)}-1}\cdots\prod_{j_{r-1}=0}^{2^{H_n(m,j_1,\dots,j_{r-2};c_{r-1})}-1}[c_2,{}_{\omega(j_1)}c_1,\dots,{}_{\omega(j_{r-1})}c_{r-1}]^{\rho(j_1,\dots,j_{r-1})}\\
&\quad\times\prod_{j_1=0}^{i_1-1}\prod_{j_2=0}^{2^{H_n(k,j_1;c_2)}-1}\cdots\prod_{j_{r-1}=0}^{2^{H_n(k,j_1,\dots,j_{r-2};c_{r-1})}-1}[c_2,{}_{\omega(j_1)}c_1,\dots,{}_{\omega(j_{r-1})}c_{r-1}]^{\rho(j_1,\dots,j_{r-1})}\\
&\qquad\times\prod_{j_2=0}^{i_2-1}\cdots\prod_{j_{r-1}=0}^{2^{H_n(k,i_1,\dots,j_{r-2};c_{r-1})}-1}[c_2,{}_{\omega(i_1)}c_1,\dots,{}_{\omega(j_{r-1})}c_{r-1}]^{\rho(i_1,\dots,j_{r-1})}\\
&\qquad\quad\times\cdots\\
&\qquad\qquad\times\prod_{j_{r-1}=0}^{i_{r-1}-1}[c_2,{}_{\omega(i_1)}c_1,\dots,{}_{\omega(j_{r-1})}c_{r-1}]^{\rho(i_1,\dots,j_{r-1})}\\
&\qquad\qquad\quad\times[c_2,{}_{\omega(i_1)}c_1,\dots,{}_{\omega(i_{r-1})}c_{r-1}]^{\rho(i_1,\dots,i_{r-1})}\\
&\qquad\qquad\qquad\times\cdots.
\end{aligned}$$

Получаем искомое соотношение для чисел $H_n(k, i_1, \dots, i_{r-1}; c_r)$, учитывая, что равенства: $\omega(i_1) = l_1, \dots, \omega(i_{q-1}) = l_{q-1}$ являются необходимым условием присутствия коммутаторов вида $c_r = [c_{2,\,l_1}c_1, \dots {}_{l_{r-1}}c_{r-1}]$ в произведении

$$\prod_{j_q=0}^{i_q-1} \cdots \prod_{j_{r-1}=0}^{2^{H_n(k,j_1,\dots,j_{r-2};c_{r-1})}-1} [c_{2,\,\omega(i_1)}c_1, \dots, {}_{\omega(i_{q-1})}c_{q-1}, {}_{\omega(j_q)}c_q, {}_{\omega(j_{r-1})}c_{r-1}]^{\rho(i_1,\dots,i_{q-1},j_q,\dots,j_{r-1})}.$$

□

Установленная параметризация несобранной части формулы Ф. Холла в совокупности со следующей леммой будут существенно использоваться при вычислении показателей степеней коммутаторов в следующем параграфе.

Лемма 2.1.1. *Для любых целых неотрицательных m, u, v имеют место формулы:*

$$|W(2^m - 1, u)||W(2^m - 1, v)| = \sum_{i=0}^{u+v} \binom{m}{i} \binom{i}{u} \binom{u}{i-v}. \tag{44}$$

$$\sum_{j \in W(2^m-1,v)} |W(j-1, u)| = \sum_{i=0}^{u+v} \binom{m}{i} \sum_{k=1}^{v} \binom{i-k}{i-v} \binom{v-k}{i-u-1}. \tag{45}$$

Доказательство. Заметим, что левая часть (44) для натуральных m, u, v равна мощности множества

$$\{(\mu_1, \mu_2) \in \{0, \dots, 2^m - 1\}^2 \mid \omega(\mu_1) = u;\ \omega(\mu_2) = v\}.$$

Поэтому согласно лемме 1.3.7 имеем

$$|W(2^m - 1, u)||W(2^m - 1, v)| = \sum_{i=1}^{u+v} \binom{m}{i} \binom{i}{i-u,\, i-v,\, u+v-i}.$$

Поскольку триномиальный коэффициент равен 0 при $i = 0$ и $u, v \geqslant 1$, можем распространить суммирование по i до 0. После этого раскроем по определению триномиальный коэффициент и воспользуемся свойствами биномиального коэффициента:

$$\sum_{i=0}^{u+v} \binom{m}{i} \binom{i}{i-u} \binom{u}{i-v} \binom{u+v-i}{u+v-i} = \sum_{i=0}^{u+v} \binom{m}{i} \binom{i}{u} \binom{u}{i-v}.$$

Остается проверить равенство (44), когда хотя бы одно и чисел m, u, v равно 0. Если $m = 0$, обе части равенства равны либо 1 при $u = v = 0$, либо 0 при $u > 0$ или $v > 0$. Если $u = 0$, обе части (44) равны $\binom{m}{v}$. Если $v = 0$, левая и правая части равны $\binom{m}{u}$.

Перейдем к доказательству формулы (45). Заметим, что ее левая часть равна мощности множества

$$\{(\mu_1, \mu_2) \in \{0, \ldots, 2^m - 1\}^2 \mid \omega(\mu_1) = u;\ \omega(\mu_2) = v;\ \mu_1 < \mu_2\}.$$

Тогда согласно лемме 1.3.7 получаем равенство для натуральных m, u, v:

$$\sum_{j \in W(2^m - 1, v)} |W(j-1, u)| = \sum_{i=1}^{u+v} \binom{m}{i} \sum_{k=1}^{v} \binom{i-k}{i-u-1,\ i-v,\ u+v-i-k+1}.$$

Поменяв местами параметры $i-u-1$ и $i-v$ в мультиномиальном коэффициенте, выразим его через произведение биномиальных коэффициентов:

$$\binom{i-k}{i-v} \binom{v-k}{i-u-1} \binom{u+v-i-k+1}{u+v-i-k+1}.$$

Имеем равенство

$$\binom{v-k}{i-u-1} \binom{(v-k)-(i-u-1)}{(v-k)-(i-u-1)} = \binom{v-k}{i-u-1},$$

поскольку $v - k \geqslant 0$ и при $(v-k)-(i-u-1) \geqslant 0$ биномиальный коэффициент $\binom{(v-k)-(i-u-1)}{(v-k)-(i-u-1)}$ равен 1, а при $(v-k)-(i-u-1) < 0$ биномиальный коэффициент $\binom{v-k}{i-u-1}$ равен 0.

Распространяем суммирование по i до 0, добавив нулевые слагаемые, и получаем в итоге формулу (45) для любых натуральных m, u, v. Остается заметить, что если $m = 0$ или $v = 0$, то обе части (45) равны 0, а если $u = 0$ и $v \geqslant 1$, $m \geqslant 1$, то обе части (45) равны $\binom{m}{v}$. $\square$

2.2 Явный вид показателей степеней коммутаторов

Теорема 2.2.1. *Пусть G — группа, $x, y \in G$. Тогда в собирательной формуле Ф. Холла для выражения $(xy)^n$, $n \in \mathbb{N}$, показатель степени коммутатора $[y, {}_u x, {}_v y]$, где $u \geqslant 0$, $v \geqslant 0$, и $v = 0$ при $u = 0$, равен*

$$g_n(u,v) = \sum_{i=1}^{u+v+1} \binom{n}{i} \binom{i-1}{u} \binom{u}{i-v-1}. \tag{46}$$

В частности, если $[\Gamma_2(G), \Gamma_2(G)] = 1$, то

$$(xy)^n = x^n y^n \prod_{u=1}^{n-1} \prod_{v=0}^{n-1} [y, {}_u x, {}_v y]^{g_n(u,v)}. \tag{47}$$

Доказательство. Воспользуемся следствием 2.1.1, в котором в качестве собранных коммутаторов рассмотрим любой набор $c_1 = x, c_2 = y, c_3, \ldots, c_{r-1}$, $c_r = [y, {}_u x, {}_v y]$. Коммутатор c_r выражается через $c_1, \ldots, c_{r-1}$ единственным образом: $c_r = [y, {}_u c_1, {}_v c_2, {}_0 c_3 \ldots, {}_0 c_{r-1}]$. Тогда

$$e_n^r = \sum_{k=1}^{n} \sum_{i_1 \in W(2^{H_n^1}-1,u)} \sum_{i_2 \in W(2^{H_n^2}-1,v)} \sum_{i_3 \in W(2^{H_n^3}-1,0)} \cdots \sum_{i_{r-1} \in W(2^{H_n^{r-1}}-1,0)} 1.$$

Поскольку $W(q, 0) = \{0\}$ для любого целого $q \geqslant 0$, мы получаем

$$e_n^r = \sum_{k=1}^{n} \sum_{i_1 \in W(2^{n-k}-1,u)} \sum_{i_2 \in W(2^{n-k}-1,v)} 1 = \sum_{k=1}^{n} |W(2^{n-k}-1, u)||W(2^{n-k}-1, v)|.$$

Из формулы (44) следует, что

$$e_n^r = \sum_{k=1}^{n} \sum_{i=0}^{u+v} \binom{n-k}{i} \binom{i}{u} \binom{u}{i-v} = \sum_{i=0}^{u+v} \sum_{k=0}^{n-1} \binom{k}{i} \binom{i}{u} \binom{u}{i-v}.$$

Применение известной формулы суммирования к сумме по k и последующий сдвиг на единицу суммирования по i завершает доказательство (46).

Если $[\Gamma_2(G), \Gamma_2(G)] = 1$, то все коммутаторы от x и y веса $\geqslant 2$ перестановочны друг с другом. Значит, тождество из теоремы 2.1.1, являющееся результатом двух этапов собирательного процесса, примет вид (47), где для удобства записи коммутаторы сгруппированы по виду, а не по весу. □

Теорема 2.2.2. *Пусть G — группа, $x, y \in G$. Тогда в собирательной формуле Ф. Холла для выражения $(xy)^n$, $n \in \mathbb{N}$, показатель степени коммутатора $[[y, {}_u x], [y, {}_v x]]$, $u > v \geqslant 1$, равен*

$$f_n(u,v) = \sum_{i=1}^{u+v+2} \binom{n}{i} \left(\binom{i-1}{v+1} \binom{v+1}{i-u-1} + \sum_{k=1}^{v} \binom{i-k-1}{i-v-1} \binom{v-k}{i-u-2} \right). \tag{48}$$

В частности, если $[\Gamma_2(G), \Gamma_2(G), \Gamma_2(G)] = 1$ и $y \in C_G(\Gamma_2(G))$, то

$$(xy)^n = x^n y^n \prod_{i=1}^{n-1} [y, {}_i x]^{\binom{n}{i+1}} \prod_{n-1 \geqslant u > v \geqslant 1} [[y, {}_u x], [y, {}_v x]]^{f_n(u,v)}. \tag{49}$$

Доказательство. Воспользуемся следствием 2.1.1, в котором в качестве собранных коммутаторов рассмотрим любой набор $c_1 = x, c_2 = y, \ldots, c_l = [y, {}_v x], \ldots, c_r = [[y, {}_u x], [y, {}_v x]]$. Здесь $u > v$, поскольку коммутаторы собираются по возрастанию веса. Коммутатор c_r выражается через $c_1, \ldots, c_{r-1}$ единственным образом: $c_r = [y, {}_u c_1, {}_0 c_2, \ldots, {}_1 c_l \ldots, {}_0 c_{r-1}]$. Тогда

$$e_n^r = \sum_{k=1}^{n} \sum_{i_1 \in W(2^{H_n^1}-1,u)} \sum_{i_2 \in W(2^{H_n^2}-1,0)} \sum_{i_3 \in W(2^{H_n^3}-1,0)} \cdots \sum_{i_l \in W(2^{H_n^l}-1,1)} \cdots \sum_{i_{r-1} \in W(2^{H_n^{r-1}}-1,0)} 1.$$

Далее,

$$\begin{aligned} e_n^r &= \sum_{k=1}^{n} \sum_{i_1 \in W(2^{H_n^1}-1,u)} \sum_{i_l \in W(2^{H_n^l}-1,1)} 1 = \sum_{k=1}^{n} \sum_{i_1 \in W(2^{H_n^1}-1,u)} |W(2^{H_n^l}-1,1)| \\ &= \sum_{k=1}^{n} \sum_{i_1 \in W(2^{n-k}-1,u)} H_n^l(k, i_1, 0, \ldots, 0; c_l). \end{aligned}$$

Для вычисления $H_n^l = H_n(k, i_1, \ldots, i_{l-1}; c_l)$ применим следствие 2.1.1 к коммутатору $c_l = [y, {}_v c_1, {}_0 c_2, \ldots, {}_0 c_{l-1}]$, получаем

$$H_n(k, i_1, \ldots, i_{l-1}; c_l) = e_n^l - \sum_{m=1}^{k-1} \sum_{j_1 \in W(2^{H_n(m;x)}-1,v)} 1 - \sum_{j_1 \in W(i_1-1,v)} 1$$

$$- \sum_{q=2}^{l} \delta_{\omega(i_1),v} \prod_{c=2}^{q-1} \delta_{\omega(i_c),0} \sum_{j_q \in W(i_q-1,0)} \cdots \sum_{j_{l-1} \in W(2^{H_n(k,i_1,\ldots,i_{q-1},j_q,\ldots,j_{l-2};c_{l-1})}-1,0)} 1.$$

Поскольку $u > v$, при $i_1 \in W(2^{n-k}-1, u)$ имеем $\delta_{\omega(i_1),v} = \delta_{u,v} = 0$. Следовательно, сумма по q равна 0 и

$$H_n(k, i_1, \ldots, i_{l-1}; c_l) = e_n^l - \sum_{m=1}^{k-1} |W(2^{n-m}-1, v)| - |W(i_1 - 1, v)|.$$

Для вычисления e_n^l используем (46) и получаем

$$\begin{aligned} H_n(k, i_1, \ldots, i_{l-1}; c_l) &= \binom{n}{v+1} - \sum_{m=1}^{k-1} \binom{n-m}{v} - |W(i_1 - 1, v)| \\ &= \sum_{m=0}^{n-1} \binom{m}{v} - \sum_{m=n-k+1}^{n-1} \binom{m}{v} - |W(i_1 - 1, v)| \\ &= \sum_{m=0}^{n-k} \binom{m}{v} - |W(i_1 - 1, v)|. \end{aligned}$$

Таким образом,

$$\begin{aligned} e_n^r &= \sum_{k=1}^{n} \sum_{i_1 \in W(2^{n-k}-1, u)} \left(\sum_{m=0}^{n-k} \binom{m}{v} - |W(i_1 - 1, v)| \right) \\ &= \sum_{k=1}^{n} \sum_{i_1 \in W(2^{n-k}-1, u)} \sum_{m=0}^{n-k} \binom{m}{v} - \sum_{k=1}^{n} \sum_{i_1 \in W(2^{n-k}-1, u)} |W(i_1 - 1, v)|. \end{aligned}$$

Преобразуем первую сумму:

$$\begin{aligned} \sum_{k=1}^{n} \sum_{i_1 \in W(2^{n-k}-1, u)} \sum_{m=0}^{n-k} \binom{m}{v} &= \sum_{k=1}^{n} \sum_{m=0}^{n-k} \binom{m}{v} \binom{n-k}{u} \\ &= \sum_{k=1}^{n} \binom{n-k+1}{v+1} \binom{n-k}{u} \\ &= \sum_{k=1}^{n} \binom{n-k}{v+1} \binom{n-k}{u} + \sum_{k=1}^{n} \binom{n-k}{v} \binom{n-k}{u} \end{aligned}$$

Заметим, что

$$\binom{n-k}{v} \binom{n-k}{u} - \sum_{k=1}^{n} \sum_{i_1 \in W(2^{n-k}-1, u)} |W(i_1 - 1, v)| = \sum_{i_1 \in W(2^{n-k}-1, v)} |W(i_1 - 1, u)|,$$

поскольку $u \neq v$ и левая часть равенства равна разности мощностей множеств

$$\{(\mu_1, \mu_2) \in \{0, \ldots, 2^{n-k}-1\}^2 \mid \omega(\mu_1) = u;\, \omega(\mu_2) = v\},$$

$$\{(\mu_1, \mu_2) \in \{0, \ldots, 2^{n-k}-1\}^2 \mid \omega(\mu_1) = u;\, \omega(\mu_2) = v;\, \mu_1 > \mu_2\},$$

а правая часть равна мощности множества

$$\{(\mu_1, \mu_2) \in \{0, \ldots, 2^{n-k} - 1\}^2 \mid \omega(\mu_1) = u;\ \omega(\mu_2) = v;\ \mu_1 < \mu_2\},$$

Значит,

$$e_n^r = \sum_{k=1}^{n} \binom{n-k}{v+1}\binom{n-k}{u} + \sum_{k=1}^{n} \sum_{i_1 \in W(2^{n-k}-1, v)} |W(i_1 - 1, u)|.$$

В первой сумме заменим $n-k$ на k, затем применим (44), во второй сумме заменим $n-k$ на k и применим (45):

$$e_n^r = \sum_{k=0}^{n-1} \sum_{i=0}^{u+v+1} \binom{k}{i}\binom{i}{v+1}\binom{v+1}{i-u} + \sum_{k=0}^{n-1} \sum_{i=0}^{u+v} \binom{k}{i} \sum_{k_0=1}^{v} \binom{i-k_0}{i-v}\binom{v-k_0}{i-u-1}.$$

Далее применяем известную формулу суммирования к суммам по k:

$$e_n^r = \sum_{i=0}^{u+v+1} \binom{n}{i+1}\binom{i}{v+1}\binom{v+1}{i-u} + \sum_{i=0}^{u+v} \binom{n}{i+1} \sum_{k_0=1}^{v} \binom{i-k_0}{i-v}\binom{v-k_0}{i-u-1}.$$

Во второй сумме распространяем суммирование по i до $u+v+1$, добавляя нулевые слагаемые, затем в обеих суммах заменяем $i+1$ на i. Получаем искомое равенство (48).

Перейдем к доказательству собирательной формулы. Ввиду условия $y \in C_G(\Gamma_2(G))$, тождество (2.1.1) принимает вид

$$(xy)^n = x^n y^n \prod_{k=1}^{n-1} \prod_{i=1}^{2^{n-k}-1} [y,_{\omega(i)} x].$$

Условие $[\Gamma_2(G), \Gamma_2(G), \Gamma_2(G)] = 1$ означает, что при собирании коммутаторов $[y,_v x]$ по возрастанию веса возникнут только коммутаторы вида $[[y,_u x], [y,_v x]]$, где $n-1 \geqslant u > v \geqslant 1$. Согласно теореме 2.2.1 показатель степени коммутатора $[y,_{\omega(i)} x]$ в собирательной формуле Ф. Холла равен $g_n(i, 0) = \binom{n}{i+1}$. Таким образом, получаем (49). $\square$

Теперь, используя найденный в теоремах 2.2.1 и 2.2.2 холловский вид для показателей степеней $g_n(u, v)$ и $f_n(u, v)$, мы легко вычислим $g_p(u, v)$ и $f_p(u, v)$ по модулю простого числа p. Нам понадобятся известные свойства биномиальных коэффициентов, приведенные ниже.

Предложение 2.2.1. *Для любого простого p справедливы сравнения:*

$$\binom{p}{u} \equiv 0 \pmod p, \; u \in \overline{1, p-1}; \qquad \binom{p-1}{u} \equiv (-1)^u \pmod p, \; u \in \overline{0, p-1}.$$

Доказательство. По определению имеем

$$\binom{p}{u} = \frac{1}{u!}\prod_{i=0}^{u-1}(p-i) = \frac{p(p-1)\dots(p-u+1)}{u!}.$$

Числитель полученной дроби делится на p, а знаменатель не делится. Далее, если $u \geqslant 1$, то

$$\binom{p-1}{u} = \frac{1}{u!}\prod_{i=0}^{u-1}(p-1-i) = \frac{(p-1)(p-2)\dots(p-u)}{u!} \equiv \frac{(-1)^u u!}{u!} \pmod p.$$

При $u = 0$ полученное сравнение очевидно. Тем самым предложение доказано.

□

Следствие 2.2.1. *Пусть p — простое число, u, v — целые, и $w_1 = u + v + 1 - p$, $w_2 = u + v + 2 - p$. Тогда имеют место сравнения по модулю p:*

$$g_p(u,v) \equiv (-1)^u \binom{u}{w_1} \equiv (-1)^v \binom{v}{w_1}, \quad u, v \in \overline{0, p-1}, \text{ где } v = 0 \text{ при } u = 0;$$

$$f_p(u,v) \equiv (-1)^v \left(-\binom{v+1}{w_2} + \binom{v}{w_2} \sum_{k=1}^{v} (-1)^k \binom{w_2}{k} \right), \quad p-1 \geqslant u > v \geqslant 1.$$

В частности, если вес коммутатора $[y, {}_u x, {}_v y]$ равен p, то показатель его степени в собирательной формуле Ф. Холла для $(xy)^p$ сравним с $(-1)^u$ по модулю p. Аналогично, если вес коммутатора $[[y, {}_u x], [y, {}_v x]]$ равен p, то показатель его степени сравним с $(-1)^{v+1}$ по модулю p.

Доказательство. Ввиду равенств (46) и (48) имеем

$$g_p(u,v) = \sum_{i=1}^{u+v+1} \binom{p}{i}\binom{i-1}{u}\binom{u}{i-v-1},$$

$$f_p(u,v) = \sum_{i=1}^{u+v+2} \binom{p}{i} \left(\binom{i-1}{v+1}\binom{v+1}{i-u-1} + \sum_{k=1}^{v} \binom{i-k-1}{i-v-1}\binom{v-k}{i-u-2} \right).$$

Рассмотрим $g_p(u,v)$. Если $u+v+1 \geqslant p$, то все слагаемые в сумме, кроме одного (при $i=p$), делятся на p, следовательно,

$$g_p(u,v) \equiv \binom{p-1}{u}\binom{u}{p-v-1} \equiv (-1)^u \binom{u}{u-(p-v-1)}$$
$$\equiv (-1)^u \binom{u}{w_1} \pmod{p}.$$

Полученное сравнение по модулю p остается справедливым при $u+v+1<p$, поскольку тогда $g_p(u,v)$ делится на p и $\binom{u}{w_1}=0$, т.к. $w_1<0$. Свойство $g_p(u,v)=g_p(v,u)$ завершает доказательство теоремы для $g_p(u,v)$.

Рассмотрим $f_p(u,v)$. Если $u+v+2 \geqslant p$, то все слагаемые в сумме, кроме одного (при $i=p$), делятся на p, следовательно,

$$f_p(u,v) \equiv \binom{p-1}{v+1}\binom{v+1}{p-u-1} + \sum_{k=1}^{v} \binom{p-k-1}{p-v-1}\binom{v-k}{p-u-2} \pmod{p}.$$

Ввиду условия $1 \leqslant v+1 \leqslant p-1$ для первого слагаемого имеем

$$\binom{p-1}{v+1}\binom{v+1}{p-u-1} \equiv (-1)^{v+1}\binom{v+1}{v+1-(p-u-1)}$$
$$\equiv (-1)^{v+1}\binom{v+1}{w_2} \pmod{p}.$$

Преобразуем слагаемые в сумме по k:

$$\binom{p-k-1}{p-v-1} \equiv \binom{p-k-1}{v-k} \equiv \frac{(p-(k+1))(p-(k+2))\dots(p-v)}{(v-k)!}$$
$$\equiv (-1)^{v-k}\frac{(k+1)(k+2)\dots v}{(v-k)!} \equiv (-1)^{v-k}\binom{v}{k} \pmod{p},$$

далее,

$$\binom{v-k}{p-u-2} \equiv \binom{v-k}{v-k-(p-u-2)} \equiv \binom{v-k}{w_2-k} \pmod{p}.$$

Таким образом,

$$\begin{aligned}\binom{p-k-1}{p-v-1}\binom{v-k}{p-u-2} &\equiv (-1)^{v-k}\binom{v}{k}\binom{v-k}{w_2-k}\\ &\equiv (-1)^{v-k}\frac{v!}{k!(v-k)!}\frac{(v-k)!}{(w_2-k)!(v-w_2)!}\\ &\equiv (-1)^{v-k}\frac{v!}{w_2!(v-w_2)!}\frac{w_2!}{k!(w_2-k)!}\\ &\equiv (-1)^{v-k}\binom{v}{w_2}\binom{w_2}{k} \pmod{p}.\end{aligned}$$

В итоге имеем

$$\sum_{k=1}^{v}\binom{p-k-1}{p-v-1}\binom{v-k}{p-u-2} \equiv (-1)^{v}\binom{v}{w_2}\sum_{k=1}^{v}(-1)^k\binom{w_2}{k} \pmod{p}.$$

Комбинируя результаты, получаем искомое выражение для $f_p(u,v)$ по модулю p. Для завершения доказательства остается заметить, что полученное соотношение останется справедливым при $u+v+2<p$, поскольку тогда $f_p(u,v)$ делится на p и $\binom{v+1}{w_2}=\binom{v}{w_2}=0$, т.к. $w_2<0$. $\square$

Глава 3. Проблема Б. Верфрица

В главе 3 диссертации доказывается нерегулярность силовской p-подгруппы общей линейной группы $GL_n(\mathbb{Z}_{p^m})$ в случае, когда p — такое нечетное простое число, что число $(p+2)/3$ — целое, $n \geqslant (p+2)/3$ и $m \geqslant 3$.

В § 3.1 с использованием результатов главы 2 получено необходимое условие регулярности конечной p-группы, к которому в § 3.2 найден контрпример в случае рассматриваемой силовской p-подгруппы при $n = (p+2)/3$ и $m = 3$. Тем самым доказана нерегулярность при $n \geqslant (p+2)/3$ и $m \geqslant 3$, поскольку свойство регулярности наследуется подгруппами и факторгруппами.

3.1 Необходимое условие регулярности p-группы

Лемма 3.1.1. *Если конечная p-группа G регулярна, то для любых $a, b \in G$ существует элемент $d \in \langle a, b\rangle'$ такой, что*

$$d^p = \prod R_i^{f_i(p)},$$

где произведение берется по всем коммутаторам R_i веса $w(R_i) \geqslant p$ из собирательной формулы Ф. Холла. В частности, для любого целого неотрицательного числа j

$$d^p = \prod_{p \leqslant w(R_i) \leqslant p+j} R_i^{f_i(p)} \pmod{\Gamma_{p+j+1}(G)}.$$

Доказательство. Пусть $a, b \in G$. По теореме 12.4.2 из [12], существует элемент $c \in \langle a, b\rangle'$ такой, что $(ab)^p = a^p b^p c^p$. С другой стороны, согласно [16, теорема 3.1], существует последовательность коммутаторов R_i от a и b, упорядоченных по весу, и последовательность целых чисел $f_i(p)$ такие, что

$$(ab)^p = a^p b^p \prod_{2 \leqslant w(R_i) < p} R_i^{f_i(p)} \prod_{w(R_i) \geqslant p} R_i^{f_i(p)}.$$

Так как группа G регулярна, а показатели $f_i(p)$ кратны p, когда $2 \leqslant w(R_i) < p$, то по следствию 12.4.1 из [12] существует элемент $u \in \langle a, b\rangle'$ такой, что

$$u^p = \prod_{2 \leqslant w(R_i) < p} R_i^{f_i(p)}.$$

Отсюда

$$a^p b^p c^p = a^p b^p u^p \prod_{w(R_i) \geqslant p} R_i^{f_i(p)}$$

или

$$\prod_{w(R_i) \geqslant p} R_i^{f_i(p)} = (u^{-1})^p c^p = d^p$$

для некоторого $d \in \langle a, b\rangle'$. $\square$

Следствие 3.1.1. *Пусть G регулярная p-группа, $p > 2$, и $a, b \in G$. Предположим, что всякий коммутатор от a и b : 1) имеющий более двух вхождений b, равен 1, 2) веса больше, чем $p-1$, имеет порядок 1 или p. Тогда существует элемент $d \in \langle a, b\rangle'$ такой, что*

$$d^p = [b, {}_{p-1}a]\,[b, {}_{p-2}a, b]^{-1} \prod_{v=1}^{(p-3)/2} [[b, {}_{p-2-v}a], [b, {}_v a]]^{(-1)^{v+1}} \pmod{\Gamma_{p+1}(G)}.$$

Доказательство. Рассмотрим собирательную формулу Ф. Холла для выражения $(ab)^p$. Согласно теореме 2.1.1 после двух этапов собирательного процесса в несобранной части формулы все коммутаторы имеют вид $[b, {}_u a, {}_v b]$, где $p-1 \geqslant u \geqslant 1$ и $p-1 \geqslant v \geqslant 0$. Далее коммутаторы собираются по возрастанию веса до веса p включительно (порядок среди коммутаторов одного веса может быть произвольным).

Ввиду условия 1 из несобранной части пропадают все коммутаторы, имеющие более двух вхождений b. Значит, остаются лишь коммутаторы $[b, {}_u a]$, $[b, {}_u a, b]$, где $p-1 \geqslant u \geqslant 1$, а также коммутаторы, возникшие при сборе $[b, {}_u a]$, а именно, $[[b, {}_u a], [b, {}_v a]]$, где $p-1 \geqslant u > v \geqslant 1$. Получаем формулу

$$(ab)^p = a^p b^p \prod_{u=1}^{p-1} [b, {}_u a]^{g_p(u,0)} \prod_{u=1}^{p-1} [b, {}_u a, b]^{g_p(u,1)} \prod_{p-1 \geqslant u > v \geqslant 1} [[b, {}_u a], [b, {}_v a]]^{f_p(u,v)},$$

где $g_p(u, v)$, $f_p(u, v)$ определяются теоремами 2.2.1 и 2.2.2 соответственно. В формуле для удобства записи коммутаторы сгруппированы по виду, а не по весу, что является корректным ввиду перестановочности коммутаторов $[b, {}_u a, b]$ и $[[b, {}_u a], [b, {}_v a]]$ со всеми коммутаторами веса $\geqslant 2$.

Согласно предыдущей лемме существует элемент $d \in \langle a, b\rangle'$ такой, что по модулю $\Gamma_{p+1}(G)$ имеет место равенство

$$d^p = [b, {}_{p-1}a]^{g_p(p-1,0)}\,[b, {}_{p-2}a, b]^{g_p(p-2,1)} \prod_{v=1}^{(p-3)/2} [[b, {}_{p-2-v}a], [b, {}_v a]]^{f_p(p-2-v,v)}.$$

Применение к показателям степеней коммутаторов условия 2 и следствия 2.2.1 завершает доказательство. □

Следующие две леммы потребуются для доказательства теоремы 3.2.1.

Лемма 3.1.2. *Пусть G — группа, $y_1, \ldots, y_s \in G$, $s \geqslant 2$. Предположим, что ступень нильпотентности подгруппы $H = \langle y_1, \ldots, y_s \rangle$ равна 2. Тогда для любого натурального числа n имеет место равенство*

$$(y_1 \ldots y_s)^n = y_1^n \ldots y_s^n \prod_{1 \leqslant i < j \leqslant s} [y_j, y_i]^{\binom{n}{2}}.$$

Доказательство. При $n = 1$ утверждение леммы очевидно. Пусть $n \geqslant 2$. Применим собирательный процесс к слову $(y_1 \ldots y_s)^n$: собираем коммутаторы веса 1 в порядке $y_1, \ldots, y_s$, далее собираем коммутаторы веса 2, среди которых будут только коммутаторы вида $[y_j, y_i]$, где $1 \leqslant i < j \leqslant s$, в произвольном порядке. В итоге получаем коммутаторное слово

$$y_1^n \ldots y_s^n \prod_{1 \leqslant i < j \leqslant s} [y_j, y_i]^{e_{ij}} \cdot T_k,$$

где произведение по i, j ведется в некотором фиксированном порядке, слово T_k содержит коммутаторы веса не меньше 3. Для завершения доказательства остается вычислить e_{ij}. Разметку для слова $(y_1 \ldots y_s)^n$ возьмем из доказательства теоремы 1.4.1. Тогда согласно (16) имеем $E_{[y_j, y_i]}^{(\lambda_1, \lambda_2)} = P_{y_j, y_i}^{(\lambda_1, \lambda_2)} = [\lambda_1 < \lambda_2]$ для всех $(\lambda_1, \lambda_2) \in D([y_j, y_i]) = D(y_j) \times D(y_i) = \{1, \ldots, n\}^2$. Таким образом, согласно предложению 1.2.1 показатель степени e_{ij} равен

$$|\{(\lambda_1, \lambda_2) \in D([y_j, y_i]) \mid E_{[y_j, y_i]}^{(\lambda_1, \lambda_2)} = 1\}| = |\{(\lambda_1, \lambda_2) \mid 1 \leqslant \lambda_1 < \lambda_2 \leqslant n\}| = \binom{n}{2}.$$

□

Следствие 3.1.2. *Предположим, что подгруппа H из леммы 3.1.2 является p-группой, $p > 2$, с элементарным абелевым коммутантом, а число n кратно p. Тогда для любых целых чисел $\alpha_1, \ldots, \alpha_s$ и любой перестановки π на множестве $\{1, \ldots, s\}$ имеем*

$$(y_1^{\alpha_1} \ldots y_s^{\alpha_s})^n = \left(y_{\pi(1)}^{\alpha_{\pi(1)}} \ldots y_{\pi(s)}^{\alpha_{\pi(s)}}\right)^n = y_1^{n\alpha_1} \ldots y_s^{n\alpha_s}.$$

Если для некоторого i дополнительно $y_i^n = 1$ или $y_i^p \in H'$ и α_i кратно p, то

$$(y_1^{\alpha_1} \dots y_i^{\alpha_i} \dots y_s^{\alpha_s})^n = (y_1^{\alpha_1} \dots \hat{y}_i^{\alpha_i} \dots y_s^{\alpha_s})^n.$$

Здесь значок $\hat{}$ над элементом означает отсутствие этого элемента в произведении.

3.2 Нерегулярность силовской p-подгруппы $GL_{(p+2)/3}(\mathbb{Z}_{p^3})$

Следуя [6], определим последовательность функций f_n, $n = 1, 2, \dots$, от натуральных аргументов i, j, k, полагая

$$f_n(i,j,k) = -\left[\frac{i-j-k}{n}\right],$$

здесь $[x]$ — целая часть числа x (ближайшее к x слева целое число). Через J обозначим идеал кольца $\mathbb{Z}_{p^m}$, порожденный элементом p, а через E — единичную матрицу порядка n. Выделим в $GL_n(\mathbb{Z}_{p^m})$ подгруппы

$$G^{(k)} = \langle E + A \mid A = (a_{ij}),\ a_{ij} \in J^{f_n(i,j,k)},\ 1 \leqslant i,j \leqslant n\rangle, \quad k = 1, 2, \dots .$$

Здесь и далее по определению $J^0 = \mathbb{Z}_{p^m}$. Согласно [6], $G^{(1)}$ изоморфна группе

$$P_n(\mathbb{Z}_{p^m}) = \{E + (a_{ij}) \mid a_{ij} \in \mathbb{Z}_{p^m} \text{ при } \ i > j;\ a_{ij} \in J, \text{ при } \ i \leqslant j\},$$

а ряд

$$G^{(1)} \supset G^{(2)} \supset \dots \supset G^{(mn-1)} \supset \langle E\rangle$$

является ее нижним центральным рядом, если $p > 2$. Кроме того, при любом простом p и для любых натуральных k, l имеет место соотношение

$$\left[G^{(k)}, G^{(l)}\right] \subseteq G^{(k+l)}. \tag{50}$$

В [4, лемма 2] было показано, что если $A = (a_{ij})$, $B = (b_{ij})$ — такие матрицы, что $a_{ij} \in J^{f_n(i,j,k)}$ и $b_{ij} \in J^{f_n(i,j,l)}$, то элементы c_{ij} матрицы $C = AB$ содержатся в идеалах $J^{f_n(i,j,k+l)}$. Отсюда и из свойств делимости биномиальных коэффициентов легко следует

Лемма 3.2.1. *Если $p > n$, то для любого натурального k имеет место включение $\left[G^{(k)}\right]^p \subseteq G^{(k+n)}$.*

Обозначим через $K_n(J^k)$ конгруэнц-подгруппу группы $GL_n(\mathbb{Z}_{p^m})$, которая определяется как ядро гомоморфизма $GL_n(\mathbb{Z}_{p^m}) \to GL_n(\mathbb{Z}_{p^{m-k}})$, индуцированного кольцевым гомоморфизмом $\mathbb{Z}_{p^m} \to \mathbb{Z}_{p^{m-k}}$. Соотношение 1) следующей леммы можно найти в [6], соотношение 2) легко устанавливается методами доказательства леммы 3.2.1.

Лемма 3.2.2. *Имеют место следующие включения:*

1) $[K_n(J^k), K_n(J^l)] \subseteq K_n(J^{k+l})$;

2) $\left[K_n(J^k)\right]^p \subseteq K_n(J^{k+1})$.

Поскольку свойство регулярности наследуется подгруппами и фактор-группами, то для доказательства теоремы 3.2.1 достаточно установить нерегулярность группы $P_{(p+2)/3}(\mathbb{Z}_{p^3})$. Нам потребуется ряд вспомогательных утверждений.

Лемма 3.2.3. *Для любых $E + X, E + Y \in P_n(\mathbb{Z}_{p^m})$ имеет место тождество*

$$[E + X, E + Y] = E + \sum_{k=2}^{\infty} \sum_{t=0}^{k-2} (-1)^k X^t Y^{k-t-2} (X, Y), \tag{51}$$

где $(X, Y) = XY - YX$.

Доказательство. Ввиду нильпотентности матриц X и Y имеем

$$[E + X, E + Y] = \left(\sum_{i=0}^{\infty} (-X)^i \right) \left(\sum_{j=0}^{\infty} (-Y)^j \right) (E + X)(E + Y).$$

Раскрыв скобки, получим сумму однородных степени k многочленов $f_k(X,Y)$, причем очевидно, что $f_0(X,Y) = E$ и $f_1(X,Y) = O$, где O — нулевая матрица. Зафиксируем $k \geqslant 2$. Тогда

$$\begin{aligned} f_k(X,Y) &= (-X)^k + (-X)^{k-1}(-Y) + (-X)^{k-1}X + (-X)^{k-1}Y \\ &+ \sum_{t=0}^{k-2}(-X)^t\left((-Y)^{k-t} + (-Y)^{k-t-1}X + (-Y)^{k-t-1}Y + (-Y)^{k-t-2}XY\right). \end{aligned}$$

Таким образом,

$$f_k(X,Y) = \sum_{t=0}^{k-2}(-1)^k X^t Y^{k-t-2}(X,Y).$$

□

Заменив X на pX в (51), мы можем представить коммутатор $[E+pX, E+Y]$ в виде ряда по степеням p с коэффициентами, зависящими от X и Y. Далее нас будет интересовать коэффициент при p в разложении сложных коммутаторов.

Лемма 3.2.4. *Пусть $E + pB, E + A \in P_n(\mathbb{Z}_{p^m})$. Коэффициент при p в разложении коммутатора $[E + pB, {}_sE + A]$, $s \in \mathbb{N}$, по степеням p равен*

$$F(s) = \sum_{j=0}^{s-1}\sum_{k=j}^{\infty}(-1)^k \binom{s-1}{j}\binom{s+k-j-1}{s-1} A^k(B,A)A^{s-j-1}. \qquad (52)$$

Доказательство. Индукция по s. По лемме 3.2.3

$$\begin{aligned} [E+pB, E+A] &= E + \sum_{k=2}^{\infty}\sum_{t=0}^{k-2}(-1)^k(pB)^t A^{k-t-2}(pB,A) \\ &= E + p\sum_{k=2}^{\infty}(-1)^k A^{k-2}(B,A) + \dots \\ &= E + p\sum_{k=0}^{\infty}(-1)^k A^k(B,A) + \cdots. \end{aligned}$$

Полученный коэффициент при p, очевидно, равен выражению (52), если в последнем положить $s = 1$.

Пусть $s \geqslant 1$. Чтобы вычислить коэффициент при p в разложении коммутатора $[E + pB,_{s+1} E + A]$ по степеням p, воспользуемся предположением индукции и подставим вместо B в сумме

$$\sum_{k=0}^{\infty}(-1)^k A^k(B, A)$$

выражение (52). Полученную кратную сумму

$$\sum_{t=0}^{\infty}\sum_{j=0}^{s-1}\sum_{k=j}^{\infty}(-1)^k \binom{s-1}{j}\binom{s+k-j-1}{s-1} A^t(A^k(B,A)A^{s-j-1}, A)$$

преобразуем, раскрыв внешний лиев коммутатор:

$$\sum_{t=0}^{\infty}\sum_{j=0}^{s-1}\sum_{k=j}^{\infty}(-1)^{t+k} \binom{s-1}{j}\binom{s+k-j-1}{s-1} A^{t+k}(B,A)A^{s-j}$$
$$+\sum_{t=0}^{\infty}\sum_{j=0}^{s-1}\sum_{k=j}^{\infty}(-1)^{t+k+1} \binom{s-1}{j}\binom{s+k-j-1}{s-1} A^{t+k+1}(B,A)A^{s-j-1}.$$

Зафиксируем число j', $0 \leqslant j' \leqslant s$, и число k', $k' \geqslant j'$. Коэффициент при $A^{k'}(B,A)A^{s-j'}$ равен:

$$\sum_{t=0}^{k'}(-1)^{k'}\binom{s-1}{0}\binom{s+k'-t-1}{s-1} = (-1)^{k'}\binom{s}{0}\sum_{t=0}^{k'}\binom{s-1+k'-t}{s-1}$$
$$= (-1)^{k'}\binom{s}{0}\binom{s+k'}{s-1}$$
$$= (-1)^{k'}\binom{s}{j'}\binom{s+k'-j'}{s},$$

если $j' = 0$;

$$\sum_{t=0}^{k'-s}(-1)^{k'}\binom{s-1}{s-1}\binom{s+k'-s-t-1}{s-1} = \binom{s}{s}\sum_{t=0}^{k'-s}(-1)^{k'}\binom{k'-t-1}{s-1}$$
$$= (-1)^{k'}\binom{s}{s}\binom{k'}{s}$$
$$= (-1)^{k'}\binom{s}{j'}\binom{s+k'-j'}{s},$$

если $j' = s$;

$$\sum_{t=0}^{k'-j'} (-1)^{k'} \binom{s-1}{j'} \binom{s+k'-j'-t-1}{s-1} \left(\binom{s-1}{j'} + \binom{s-1}{j'-1} \right)$$
$$= (-1)^{k'} \binom{s}{j'} \sum_{t=0}^{k'-j'} \binom{s-1+k'-j'-t}{s-1} = (-1)^{k'} \binom{s}{j'} \binom{s+k'-j'}{s},$$

когда $0 < j' < s$. Таким образом, коэффициент при $A^{k'}(B,A)A^{s-j'}$ во всех случаях равен

$$(-1)^{k'} \binom{s}{j'} \binom{s+k'-j'}{s}.$$

□

Далее считаем, что $n \geqslant 3$. Матрицу порядка n с единицами на месте (i,j), где $1 \leqslant i,j \leqslant n$, и нулями на остальных местах будем обозначать через e_{ij} и называть элементарной матрицей. Напомним, что справедлива следующая формула умножения элементарных матриц

$$e_{ij}e_{ts} = \delta_{jt}e_{is},$$

где δ_{ij} — символ Кронекера. Также зафиксируем следующее соглашение: $e_{ij} = O$, если $i \notin \{1,\dots,n\}$ или $j \notin \{1,\dots,n\}$. Сумму, у которой нижний предел больше верхнего, считаем равной нулю (нулевой матрицей O).

Зафиксируем до конца параграфа следующие матрицы

$$A = e_{21} + e_{32} + \dots + e_{n,n-1}, \qquad B = e_{1n}.$$

В леммах ниже вычисляется произведение из следствия 3.1.1 и исследуется коммутант группы, порожденной элементами $E + pB$ и $E + A$.

Лемма 3.2.5. *Для любого натурального s имеет место равенство*

$$F(s) = \sum_{j=0}^{s} \sum_{k=j}^{n-1} (-1)^k \binom{s}{j} \binom{s+k-j-1}{s-1} e_{k+1,n-s+j}.$$

Доказательство. С учетом перечисленных выше соглашений, для любого целого неотрицательного k имеем

$$A^k = \sum_{t=k+1}^{n} e_{t,t-k}.$$

Отсюда выражение $A^k(B,A)A^{s-j-1}$ равно

$$\left(\sum_{t=k+1}^{n} e_{t,t-k}\right)(e_{1,n-1} - e_{2n})\left(\sum_{t=s-j}^{n} e_{t,t-s+j+1}\right) = e_{k+1,n-s+j} - e_{k+2,n-s+j+1}.$$

Подставим в (52) и разобьем на две суммы

$$\begin{aligned} F(s) &= \sum_{j=0}^{s-1}\sum_{k=j}^{n-1}(-1)^k\binom{s-1}{j}\binom{s-1+k-j}{s-1}e_{k+1,n-s+j} \\ &- \sum_{j=0}^{s-1}\sum_{k=j}^{n-1}(-1)^k\binom{s-1}{j}\binom{s-1+k-j}{s-1}e_{k+2,n-s+j+1}. \end{aligned}$$

Во второй двойной сумме заменим k на $k-1$ и j на $j-1$:

$$\begin{aligned} F(s) &= \sum_{j=0}^{s-1}\sum_{k=j}^{n-1}(-1)^k\binom{s-1}{j}\binom{s-1+k-j}{s-1}e_{k+1,n-s+j} \\ &+ \sum_{j=1}^{s}\sum_{k=j}^{n-1}(-1)^k\binom{s-1}{j-1}\binom{s-1+k-j}{s-1}e_{k+1,n-s+j}. \end{aligned}$$

Поскольку $\binom{s-1}{s} = \binom{s-1}{-1} = 0$, распространим суммирование по j в первой сумме до s, а во второй — от 0, и сложим их:

$$\begin{aligned} F(s) &= \sum_{j=0}^{s}\sum_{k=j}^{n-1}(-1)^k\left[\binom{s-1}{j} + \binom{s-1}{j-1}\right]\binom{s-1+k-j}{s-1}e_{k+1,n-s+j} \\ &= \sum_{j=0}^{s}\sum_{k=j}^{n-1}(-1)^k\binom{s}{j}\binom{s+k-j-1}{s-1}e_{k+1,n-s+j}. \end{aligned}$$

$\square$

Заметим, что произвольный элемент $E+C$ из группы $P_n(\mathbb{Z}_{p^m})$ можно представить (конечно, не единственным образом) в виде

$$E + C = E + p^0C_0 + pC_1 + \ldots + p^{m-1}C_{m-1}.$$

Следующая простая лемма часто облегчает вычисления в $P_n(\mathbb{Z}_{p^3})$.

Лемма 3.2.6. *Пусть* $E + pX + p^2Y, E + pU + p^2V \in P_n(\mathbb{Z}_{p^3})$. *Тогда*

1) $(E + pX + p^2Y)^{-1} = E - pX - p^2Y + p^2X^2$;

2) $(E + pX + p^2Y)^p = E + p^2X$;

3) $[E + pX + p^2Y, E + pU + p^2V] = E + p^2(X, U)$.

Лемма 3.2.7. *Пусть простое число* p *такое, что* $n = (p+2)/3$ *— целое число. В группе* $P_n(\mathbb{Z}_{p^3})$ *имеет место равенство*

$$[E + pB,{}_{p-1}E + A]\,[E + pB,{}_{p-2}E + A, E + pB]^{-1}$$
$$\times \prod_{s=1}^{(p-3)/2} [[E + pB,{}_{p-2-s}E + A], [E + pB,{}_sE + A]]^{(-1)^{s+1}}$$
$$= \alpha e_{n,1} - p^2 e_{n,2} - p^2 e_{n-1,1},$$

где $\alpha \in \mathbb{Z}_{p^3}$.

Доказательство. Сначала покажем, что $[E+pB,{}_sE+A] = E$, если $s \geqslant 2n$. В частности, $[E + pB,{}_{p-1}E + A] = E$, поскольку $p \geqslant 7$, а значит, $n \geqslant 3$, и, следовательно,

$$p - 1 = 3n - 3 = 2n + (n - 3) \geqslant 2n.$$

Введем следующие обозначения:

$$\phi(x, {}^r y) = [x, y], \quad \phi(x, {}^l y) = [y, x],$$

по индукции при $q \geqslant 2$ полагаем

$$\phi(x, {}^{\alpha_1}y_1, \ldots, {}^{\alpha_q}y_q) = \phi(\phi(x, {}^{\alpha_1}y_1, \ldots, {}^{\alpha_{q-1}}y_{q-1}), {}^{\alpha_q}y_q),$$

где $\alpha_i = r$ или $\alpha_i = l$.

Разложим матрицы $E + A$ и $E + pB$ в произведение трансвекций:

$$E + A = t_{21}(1)t_{32}(1)\ldots t_{n,n-1}(1), \quad E + pB = t_{1n}(p).$$

Из коммутаторных тождеств

$$[x, yz] = [x, y][x, y, z][x, z], \quad [yz, x] = [z, x][z, [x, y]][y, x]$$

следует, что $[E + pB, {}_sE + A]$ раскладывается в произведение коммутаторов вида

$$\phi(t_{1n}(p), {}^{\alpha_1}t_{i_1,i_1-1}(1), \ldots, {}^{\alpha_q}t_{i_q,i_q-1}(1)), \qquad q \geqslant s. \tag{53}$$

Изучим подробнее выражение (53). Из соотношения

$$\begin{aligned}&[t_{ij}(\alpha), t_{km}(\beta)] = \\ &\quad = (1 - \delta_{jk})(1 - \delta_{im})E + \delta_{jk}(1 - \delta_{im})t_{im}(\alpha\beta) + \delta_{im}(1 - \delta_{jk})t_{kj}(-\alpha\beta),\end{aligned} \tag{54}$$

справедливого, когда $j \neq k$ или $i \neq m$, следует, что, коммутируя трансвекции с разностями между первым и вторым индексами, равными s_1 и s_2, мы получим единичную матрицу либо трансвекцию с разностью индексов $s_1 + s_2$. Значит, выражение (53) при $q = n - 2$ есть единичная матрица, либо трансвекция с разностью индексов, равной, -1, т.е.

$$\phi(t_{1n}(p), {}^{\alpha_1}t_{i_1,i_1-1}(1), \ldots, {}^{\alpha_{n-2}}t_{i_{n-2},i_{n-2}-1}(1)) = t_{i,i+1}(\epsilon_i p),$$

где $\epsilon_i = 0$ или $\epsilon_i = \pm 1$ для некоторого i. Далее, используя соотношение

$$[t_{ij}(\alpha), t_{ji}(\beta)] = t_{ij}(c^{-1}\alpha^2\beta)d_{ij}(c)t_{ji}(-c^{-1}\alpha\beta^2), \tag{55}$$

где $d_{ij}(c) = E + (c-1)e_{ii} + (c^{-1} - 1)e_{jj}$, справедливое, если элемент $c = 1 - \alpha\beta$ обратим (в нашем случае это так, поскольку $c \equiv 1 \pmod p$), находим

$$\begin{aligned}&[t_{i,i-1}(\epsilon_i p), t_{i_{n-1},i_{n-1}-1}(1)] = \\ &\quad = (1 - \delta_{i,i_{n-1}})E + \delta_{i,i_{n-1}}t_{i,i+1}(\epsilon_i^2 p^2)d_{i,i+1}(1 - \epsilon_i p)t_{i+1,i}(-\epsilon_i p(1 - \epsilon_i p)^{-1}).\end{aligned} \tag{56}$$

Здесь мы воспользовались тем, что $p^3 = 0$ в $\mathbb{Z}_{p^3}$ и, следовательно, $\epsilon_i^2 p^2(1 - \epsilon_i p)^{-1} = \epsilon_i^2 p^2$. Наконец, соотношения (54), (55) и

$$[t_{km}(\alpha), \mathrm{diag}(\beta_1, \ldots, \beta_n)] = t_{km}(\alpha(\beta_m\beta_k^{-1} - 1)) \tag{57}$$

показывают, что коммутирование (56) с трансвекцией $t_{i_n,i_n-1}(1)$ дает единичную матрицу, если $i_n \neq i-1, i, i+1$, матрицу из унитреугольной группы $UT_n(\mathbb{Z}_{p^3})$, если $i_n = i-1, i+1$, наконец, матрицу $d_{i,i+1}(1-\epsilon_i^2 p^2)\theta$, где $\theta \in UT_n(\mathbb{Z}_{p^3})$, когда $i_n = i$. Отсюда и (57) следует, что выражение (53) при $q = n+1$ содержится в $UT_n(\mathbb{Z}_{p^3})$ и равно E при $q = 2n$, т.к. группа $UT_n(\mathbb{Z}_{p^3})$ нильпотентна ступени $n-1$.

Заметим, что если $p > 7$, то $p-2 \geqslant 2n$ и поэтому

$$[E+pB,{}_{p-2}E+A, E+pB] = E.$$

Когда $p = 7$, то $n = 3$ и непосредственные вычисления показывают, что

$$[E+pB,{}_{p-2}E+A] = t_{31}(-3p^2), \quad [t_{31}(-3p^2), t_{13}(p)] = E.$$

Таким образом, во всех случаях

$$[E+pB,{}_{p-1}E+A]\,[E+pB,{}_{p-2}E+A, E+pB]^{-1} = E.$$

Вычислим оставшееся произведение. Согласно п. 3 леммы 3.2.6 имеем

$$[[E+pB,{}_{p-2-s}E+A],[E+pB,{}_{s}E+A]] = E + p^2 F(p-2-s)F(s). \qquad (58)$$

Пусть $s \geqslant 2n-1$. Тогда выражение

$$A^k(B,A)A^{s-j-1} = A^kBA^{s-j} + A^{k+1}BA^{s-j-1}$$

равно нулевой матрице, если $0 \leqslant j \leqslant s$ и $k \geqslant j$, поскольку $A^n = O$. В самом деле, когда $0 \leqslant j \leqslant n-2$, имеем $s-j-1 \geqslant n$; если $j = n-1$, то $s-j \geqslant n$ и $k+1 \geqslant n$; наконец, если $j \geqslant n$, то $k \geqslant n$. Отсюда и леммы 3.2.4 следует, что $F(s) = O$, когда $s \geqslant 2n-1$, и $F(p-2-s) = O$, когда $p-2-s \geqslant 2n-1$. Значит, коммутатор (58) отличен от E, когда

$$n-2 \leqslant s \leqslant \min\{2n-2, (p-3)/2\} = (3n-5)/2.$$

Положим $s = n-2+\alpha$. Тогда

$$\prod_{s=1}^{(p-3)/2} [[E+pB, {}_{p-2-s}E+A], [E+pB, {}_{s}E+A]]^{(-1)^{s+1}}$$
$$= \prod_{\alpha=0}^{(n-1)/2} [[E+pB, {}_{2n-2-\alpha}E+A], [E+pB, {}_{n-2+\alpha}E+A]]^{(-1)^{\alpha+1}}$$
$$= E + p^2 \sum_{\alpha=0}^{(n-1)/2} (-1)^{\alpha+1}(F(2n-2-\alpha), F(n-2+\alpha)).$$

Ступень нильпотентности группы $P_n(\mathbb{Z}_{p^3})$ равна $3n-1 = p+1$. Поэтому произведение выше, состоящее из коммутаторов веса p, содержится в гиперцентре и равно

$$E + p^2\theta e_{n,1} + p^2\beta e_{n-1,1} + p^2\gamma e_{n,2}$$

для подходящих θ, β, γ.

Вычислим коэффициент β при $e_{n-1,1}$. Для этого, используя лемму 3.2.4, выделим в разложении $F(2n-2-\alpha)$ через элементарные матрицы слагаемые с первым индексом, равным $n-1$, а в $F(n-2-\alpha)$ — слагаемые со вторым индексом, равным 1:

$$\sum_{j=0}^{n-2}(-1)^{n-2}\binom{2n-2-\alpha}{j}\binom{3n-5-\alpha-j}{2n-3-\alpha}e_{n-1,-n+2+\alpha+j}, \tag{59}$$

$$\sum_{k=\alpha-1}^{n-1}(-1)^{k}\binom{n-2+\alpha}{\alpha-1}\binom{n-2+k}{n-3+\alpha}e_{k+1,1}. \tag{60}$$

Заметим, что в (60) при $\alpha = 0$ и $k = -1$ не только e_{01} равна нулевой матрице, но биномиальный коэффициент $\binom{n-2+\alpha}{\alpha-1} = \binom{n-2}{-1}$ тоже равен нулю. Учитывая, что $-n+2+\alpha+j \leqslant \alpha \leqslant k+1$, коэффициент при $e_{n-1,1}$ в произведении выражений (59) и (60) равен

$$(-1)^{n-2+\alpha-1}\binom{2n-2-\alpha}{n-2}\binom{3n-5-\alpha-n+2}{2n-3-\alpha}\binom{n-2+\alpha}{\alpha-1}\binom{n-2+\alpha-1}{n-3+\alpha}$$
$$= (-1)^{\alpha}\binom{2n-2-\alpha}{n-2}\binom{n-2+\alpha}{n-1}. \tag{61}$$

(При $\alpha = 0$ выражение (61), очевидно, равно нулю.) Далее, выделив в разложении $F(n-2+\alpha)$ слагаемые с первым индексом $n-1$, а в $F(2n-2-\alpha)$ — слагаемые со вторым индексом 1, получим

$$\sum_{j=0}^{n-2}(-1)^{n-2}\binom{n-2+\alpha}{j}\binom{2n-5+\alpha+j}{n-3+\alpha}e_{n-1,2-\alpha+j}, \tag{62}$$

$$\sum_{k=n-1-\alpha}^{n-1}(-1)^k\binom{2n-2-\alpha}{n-1-\alpha}\binom{n-2+k}{2n-3-\alpha}e_{k+1,1}. \tag{63}$$

С учетом того, что $2-\alpha+j \leqslant n-\alpha \leqslant k+1$, коэффициент при $e_{n-1,1}$ в произведении (62) и (63) равен

$$(-1)^{n-2+n-1-\alpha}\binom{n-2+\alpha}{n-2}\binom{2n-5+\alpha-n+2}{n-3+\alpha}\binom{2n-2-\alpha}{n-1-\alpha}\binom{2n-3-\alpha}{2n-3-\alpha}$$
$$= (-1)^{\alpha+1}\binom{n-2+\alpha}{n-2}\binom{2n-2-\alpha}{n-1}. \tag{64}$$

Умножив разность между (61) и (64) на $(-1)^{\alpha+1}$, а затем просуммировав по α, видим, что

$$\beta = -\sum_{\alpha=0}^{(n-1/2)}\left[\binom{2n-2-\alpha}{n-2}\binom{n-2+\alpha}{n-1}+\binom{n-2+\alpha}{n-2}\binom{2n-2-\alpha}{n-1}\right]. \tag{65}$$

Вычислим полученную сумму. Имеем

$$\sum_{\alpha=0}^{(n-1)/2}\binom{2n-2-\alpha}{n-2}\binom{n-2+\alpha}{n-1} = \sum_{\alpha=-(n-1)/2}^{0}\binom{2n-2+\alpha}{n-2}\binom{n-2-\alpha}{n-1}$$
$$= \sum_{\alpha=n-(n-1)/2}^{n}\binom{n-2+\alpha}{n-2}\binom{2n-2-\alpha}{n-1}$$
$$= \sum_{\alpha=(n+1)/2}^{n}\binom{n-2+\alpha}{n-2}\binom{2n-2-\alpha}{n-1}.$$

Поэтому

$$-\beta = \sum_{\alpha=0}^{n}\binom{n-2+\alpha}{n-2}\binom{2n-2-\alpha}{n-1} = \sum_{\alpha=n-2}^{2n-2}\binom{\alpha}{n-2}\binom{3n-4-\alpha}{n-1}$$
$$= \binom{3n-3}{2n-2} = \binom{p-1}{2n-2} \equiv (-1)^{2n-2} \equiv 1 \pmod p.$$

Здесь мы воспользовались тем, что $\binom{3n-4-(2n-2)}{n-1} = 0$, и доказанным в [36] тождеством

$$\sum_{i=b}^{n-a} \binom{n-i}{a}\binom{i}{b} = \binom{n+1}{a+b+1}.$$

Вычислим коэффициент γ. Выделим в разложении $F(2n-2-\alpha)$ слагаемые с первым индексом, равным n, а в $F(n-2-\alpha)$ — слагаемые со вторым индексом, равным 2:

$$\sum_{j=0}^{n-1}(-1)^{n-1}\binom{2n-2-\alpha}{j}\binom{3n-4-\alpha-j}{2n-3-\alpha}e_{n,-n+2+\alpha+j}, \tag{66}$$

$$\sum_{k=\alpha}^{n-1}(-1)^{k}\binom{n-2+\alpha}{\alpha}\binom{n-3+k}{n-3+\alpha}e_{k+1,2}. \tag{67}$$

Поскольку $-n+2+\alpha+j \leqslant \alpha+1 \leqslant k+1$, коэффициент при $e_{n,2}$ в произведении (66) и (67) равен

$$(-1)^{n-1+\alpha}\binom{2n-2-\alpha}{n-1}\binom{2n-3-\alpha}{2n-3-\alpha}\binom{n-2+\alpha}{\alpha}\binom{n-3+\alpha}{n-3+\alpha}$$
$$= (-1)^{\alpha}\binom{2n-2-\alpha}{n-1}\binom{n-2+\alpha}{n-2}. \tag{68}$$

Далее, выделив в разложении $F(n-2+\alpha)$ слагаемые с первым индексом n, а в $F(2n-2-\alpha)$ — слагаемые со вторым индексом 2, получим

$$\sum_{j=0}^{n-1}(-1)^{n-1}\binom{n-2+\alpha}{j}\binom{2n-4+\alpha-j}{n-3+\alpha}e_{n,2-\alpha+j}, \tag{69}$$

$$\sum_{k=n-\alpha}^{n-1}(-1)^{k}\binom{2n-2-\alpha}{n-\alpha}\binom{n-3+k}{2n-3-\alpha}e_{k+1,2}. \tag{70}$$

Отметим, что в (69) при $\alpha = 0$ и $j = n-1$ матрица $e_{n,n+1}$ нулевая и биномиальный коэффициент при ней $\binom{n-2}{n-1}$ равен нулю. Сумма (70) при $\alpha = 0$ тоже по определению равна нулю. С учетом того, что $2-\alpha+j \leqslant n-\alpha+1 \leqslant k+1$, коэффициент при $e_{n,2}$ в произведении (69) и (70) равен

$$(-1)^{n-1+n-\alpha}\binom{n-2+\alpha}{n-1}\binom{n-3+\alpha}{n-3+\alpha}\binom{2n-2-\alpha}{n-\alpha}\binom{2n-3-\alpha}{2n-3-\alpha}$$
$$= (-1)^{\alpha+1}\binom{n-2+\alpha}{n-1}\binom{2n-2-\alpha}{n-2}. \quad (71)$$

(При $\alpha = 0$ выражение (71), очевидно, равно нулю.) Просуммировав по α разность между (68) и (71), умноженную на $(-1)^{\alpha+1}$, снова получим выражение (65). Следовательно, $\gamma = -1$. □

Лемма 3.2.8. *Коммутант подгруппы $H = \langle E + A, E + pB\rangle$ группы $P_n(\mathbb{Z}_{p^3})$ порождается коммутаторами*

$$y_i = [E + pB, {}_iE + A],\ i = 1, 2, \ldots,$$

$$y_{jl} = [[E + pB, {}_jE + A], [E + pB, {}_lE + A]],\ j, l = 0, 1, \ldots .$$

Если $d \in H'$ и $d^p \in G^{(p)}$, где $G^{(p)}$ — p-й член нижнего центрального ряда группы $P_n(\mathbb{Z}_{p^3})$, то

$$d^p = E + \lambda p^2 e_{n,1} - \tau p^2\binom{2n-3}{n-2}e_{n-1,1} + \tau p^2\binom{2n-3}{n-2}e_{n,2}.$$

Доказательство. Заметим, что $y_i \in K_n(J)$ и $y_{jl} \in K_n(J^2)$ для любых i, j, l. Так как $K_n(J^3) = \langle E\rangle$, а по лемме 3.2.2 имеют место следующие включения: $[K_n(J), K_n(J^2)] \subseteq K_n(J^3)$ и $\left[K_n(J^2)\right]^p \subseteq K_n(J^3)$, то $[y_i, y_{jl}] = E$ и $y_{jl}^p = E$. Таким образом, ввиду следствия 3.1.2, можем считать, что

$$d = y_1^{\tau_1} \ldots y_{3n-1}^{\tau_{3n-1}}.$$

Далее, если $i \geqslant 2n - 1$, то $y_i \in G^{(2n)} \subseteq K_n(J^2)$ и поэтому $y_i^p = E$. Значит, произведение $y_{2n-1}^{\tau_{2n-1}} \ldots y_{3n-1}^{\tau_{3n-1}}$ в разложении d тоже можно отбросить.

Пусть $1 \leqslant i \leqslant 2n - 4$. Тогда $y_i \in G^{(i+1)}$ и по лемме 3.2.2 имеем $y_i^p \in G^{(i+n+1)}$. Покажем, что $y_i^p \notin G^{(i+n+2)}$. Действительно, если $1 \leqslant i \leqslant n - 1$, то, используя леммы 3.2.2 и 3.2.6, находим

$$y_i^p = (E + pF(i) + p^2Q(i))^p = E + p^2F(i) =$$
$$= E + \dots + (-1)^0 \binom{i}{0} \binom{i-1}{i-1} p^2 e_{1,n-i} + \dots = E + \dots + p^2 e_{1,n-i} + \dots .$$

В то же время

$$f_n(1, n-i, i+n+2) = -\left[\frac{1-(n-i)-(i+n+2)}{n}\right] = 3,$$

что означает, что элемент, стоящий на позиции $(i, n-i)$ произвольной матрицы из $G^{(i+n+2)}$, лежит в идеале J^3. Аналогично, если $n \leqslant i \leqslant 2n-4$, то

$$y_i^p = E + \ldots + (-1)^{i+1-n} \binom{i}{i+1-n} \binom{i-1}{i-1} p^2 e_{i+2-n,1} + \cdots$$

и $\binom{i}{i+1-n} \not\equiv 0 \pmod p$, а с другой стороны,

$$f_n(i+2-n, 1, i+n+2) = -\left[\frac{i+2-n-1-(i+2+n)}{n}\right] = 3.$$

Значит, $y_i^p \notin G^{(i+n+2)}$. Отсюда и включения $d^p \in G^p = G^{(3n-2)}$ следует, что коммутаторы $y_1, \ldots, y_{2n-4}$ должны входить в разложение d в степенях, кратных p, а потому тоже могут быть отброшены. Следовательно, можем считать, что $d = y_{2n-3}^{\tau} y_{2n-2}^{\mu}$. Снова используя следствие 3.1.2 и лемму 3.2.5, находим

$$d^p = y_{2n-3}^{p\tau} y_{2n-2}^{p\mu} = \left(E + p^2F(2n-3)\right)^{\tau} \left(E + p^2F(2n-2)\right)^{\mu}$$
$$= \left(E + p^2(2n-3)\binom{2n-3}{n-2} e_{n,1} - p^2\binom{2n-3}{n-2} e_{n-1,1} + p^2\binom{2n-3}{n-2} e_{n,2}\right)^{\tau}$$
$$\times \left(E + p^2\binom{2n-2}{n-1} e_{n,1}\right)^{\mu}$$
$$= E + \gamma p^2 e_{n,1} - \tau p^2 \binom{2n-3}{n-2} e_{n-1,1} + \tau p^2 \binom{2n-3}{n-2} e_{n,2}.$$

□

Теорема 3.2.1. *Пусть p — такое нечетное простое число, что число $(p+2)/3$ — целое. Тогда группа $P_n(\mathbb{Z}_{p^m})$ не является регулярной, если $n \geqslant (p+2)/3$ и $m \geqslant 3$.*

Доказательство. Из лемм 3.2.7 и 3.2.8 следует, что в случае регулярности подгруппы H должны быть одновременно разрешимы сравнения

$$-\tau\binom{2n-3}{n-2} \equiv -1 \pmod p, \qquad \tau\binom{2n-3}{n-2} \equiv -1 \pmod p$$

относительно τ. Складывая их, получим $0 \equiv -2 \pmod p$, противоречие. Следовательно, группа $P_{\frac{p+2}{3}}(\mathbb{Z}_{p^3})$ не является регулярной. Из того, что свойство регулярности наследуется подгруппами и факторгруппами, вытекает заключение теоремы. $\square$

Список литературы

[1] Иванов Ф. А., Скопин А. И. Максимальная 2-порожденная трансметабелева группа первого типа экспоненты 9 // Алгебра и анализ. — 1990. — Т. 2. — № 6. — С. 150–160.

[2] Колесников С. Г. О регулярности силовских p-подгрупп групп $GL_n(\mathbb{Z}_{p^m})$ // Иссл. по матем. анализу и алгебре. — 2001. — Т. 3. — С. 117–124.

[3] Колесников С. Г. О регулярных силовских p-подгруппах групп Шевалле над кольцом $\mathbb{Z}_{p^m}$ // Сиб. матем. журн. — 2006. — Т. 47. — № 6. — С. 1289–1295.

[4] Колесников С. Г. О необходимых условиях регулярности силовской p-подгруппы группы $GL_n(\mathbb{Z}_{p^m})$ // Известия Иркутского государственного университета. Серия Математика. — 2013. — Т. 6. — № 2. — С. 18–25.

[5] Магнус В., Каррас А., Солитэр Д. Комбинаторная теория групп. М.: Наука, 1974. — 455 с.

[6] Мерзляков Ю. И. Центральные ряды и ряды коммутантов матричных групп // Алгебра и логика. Семинар. — 1964. — Т. 3. — № 4. — С. 49–59.

[7] Скопин А. И. О собирательной формуле // Зап. научн. сем. ЛОМИ. — 1974. — Т. 46. — С. 59–63.

[8] Скопин А. И. Тождество Якоби и собирательная формула Ф. Холла в трансметабелевых группах двух типов // Зап. научн. сем. ЛОМИ. — 1989. — Т. 175. — С. 106–112.

[9] Скопин А. И. Графическое построение собирательной формулы некоторых типов групп // Зап. научн. сем. ЛОМИ. — 1991. — Т. 191. — С. 140–151.

[10] Скопин А. И., Тетерин Ю. Г. Ускорение алгорифма построения собирательной формулы Ф. Холла // Зап. научн. сем. ПОМИ. — 1995. — Т. 191. — С. 106–112.

[11] Скопин А. И. Нижний центральный ряд максимальной 2-порожденной трансметабелевой группы I типа экспоненты 8 // Алгебра и анализ. — 1990. — Т. 2. — № 5. — С. 197–219.

[12] Холл М. Теория групп. М.: ИИЛ, 1962. — 468 с.

[13] Ягжев А. В. О регулярности силовских подгрупп полных линейных групп над кольцами вычетов // Матем. заметки. — 1994. — Т. 56. — № 6. — С. 106–116.

[14] Gaglione A. M. A commutator identity proved by means of the Magnus Algebra // Houston J. Math. — 1979. — Vol. 5. — № 2. — P. 199–207.

[15] Gaglione A. M., Spellman D. Commutator identities obtained by the Magnus Algebra // Houston J. Math. — 1985. — Vol. 11. — № 4. — P. 491–504.

[16] Hall P. A contribution to the theory of groups of prime-power order // Proc. Lond. Math. Soc. — 1934. — Vol. 36 (2). — P. 29–95.

[17] Krause E. F. On the collection process // Proc. Amer. Math. Soc. — 1964. — Vol. 15. — № 3. — P. 497–504.

[18] Krause E. F. Groups of exponent 8 satisfy the 14th Engel congruence // Proc. Amer. Math. Soc. — 1964. — Vol. 15. — № 3. — P. 491–496.

[19] Unsolved Problems in Group Theory: the Kourovka Notebook. eds. Khukhro E. I. and Mazurov V. D., 20th edition, Sobolev Institute of Mathematics, Novosibirsk. 2022.

[20] Struik R. R. On nilpotent products of cyclic groups. II // Can. J. Math. — 1961. — Vol. 13. — P. 557–568.

[21] Waldinger H. V. Two theorems in the commutator calculus // Trans. Am. Math. Soc. — 1972. — Vol. 167. — P. 389–397.

Работы автора по теме диссертации

[22] Леонтьев В. М. Комбинаторные вопросы, связанные с собирательным процессом Ф. Холла // Сибирские электронные математические известия. — 2020. — Т. 17. — С. 873–889.

[23] Леонтьев В. М. О показателях степеней коммутаторов из собирательной формулы Ф. Холла // Тр. Ин-та математики и механики УрО РАН. — 2022. — Т. 28. — № 1. — С. 182–198.

[24] Kolesnikov S. G., Leontiev V. M., Egorychev G. P. Two collection formulas // J. Group Theory. – 2020. – Vol. 23. — № 4. – P. 607–628.

[25] Kolesnikov S. G., Leontiev V. M. One necessary condition for the regularity of a p-group and its application to Wehrfritz's problem // Sib. Electron. Math. Rep. — 2022. — Vol. 19. — № 1. — P. 138–163.

[26] Leontiev V. M. On the collection process for positive words // Sib. Electron. Math. Rep. — 2022. — Vol. 19. — № 2. — P. 439–459.

[27] Леонтьев В. М. Явный вид собирательной формулы Холла при некоторых ограничениях на вхождение переменных в коммутаторы // Проспект Свободный — 2016: материалы науч. конф., посвященной Году образования в Содружестве Независимых Государств (15–25 апреля 2016 г.) — Красноярск: СФУ. — 2016. — С. 34–35.

[28] Леонтьев В. М. Собирательные формулы холловского типа // Проспект Свободный – 2018: материалы Международной студенческой конференции. — Красноярск: СФУ. — 2018. — С. 724–725.

[29] Egorychev G. P., Kolesnikov S. G., Leontiev V. M. Two collection formulas // Международная алгебраическая конференция, посвященная 110-летию со дня рождения профессора А. Г. Куроша. Тезисы докладов. — М.: Издательство МГУ. — 2018. — С. 232–235.

[30] Леонтьев В. М. О вычислении показателей степеней коммутаторов в собирательной формуле Холла // Математика: Материалы 57-й Междунар. науч. студ. конф. — Новосибирск : ИПЦ НГУ. — 2019. — С. 11.

[31] Леонтьев В. М. О вычислении показателей степеней коммутаторов в собирательной формуле Холла // Проспект Свободный – 2019: материалы XV Международной конференции студентов, аспирантов и молодых ученых, посвященной Международному году Периодической таблицы химических элементов Д. И. Менделеева. — Красноярск: СФУ. — 2019. — С. 1070–1071.

[32] Leontiev V. M. Combinatorial problems connected with P. Hall's collection process // Проспект Свободный – 2020: материалы XVI Международной конференции студентов, аспирантов и молодых ученых, посвященной году памяти и славы (75-летию Победы в Великой Отечественной войне 1941–1945 годов). — Красноярск: СФУ. — 2020. — С. 724–725.

[33] Колесников С. Г., Леонтьев В. М. Об одном необходимом условии регулярности p- группы и его следствиях // Мальцевские чтения: тезисы докладов международной конференции. — Новосибирск: Институт математики им. С. Л. Соболева СО РАН. — 2021. — С. 96.

[34] Леонтьев В. М. О собирательном процессе для положительных слов // Мальцевские чтения: тезисы докладов международной конференции. — Новосибирск: Институт математики им. С. Л. Соболева СО РАН. — 2022. — С. 103.

[35] Leontiev V. M. On the collection formulas for positive words // Международная конференция по теории групп, посвященная 80-летию В. Д. Мазурова: тезисы докладов. — Новосибирск: Институт математики им. С. Л. Соболева СО РАН. — 2023. — С. 9.

[36] Leontiev V. M. On divisibility of some sums of binomial coefficients arising from collection formulas // Journal of Siberian Federal University. Mathematics & Physics. – 2018. – Vol. 11. — № 5. — P. 603–614.