Группы отражений и группы Кокстера

О. В. Шварцман

Группы отражений, о которых говорилось в статье Э. Б. Винберга [3], допускают два описания. Одно из них — геометрическое, как групп движений, порождённых отражениями. Другое — алгебраическое, как абстрактных групп с образующими и порождающими соотношениями. В этой статье сначала доказывается равносильность этих описаний, а затем рассказывается об алгоритме Ж. Титса, который решает проблему тождества слов для групп отражений.

Часть 1. Группы отражений как группы Кокстера

1. Задание группы образующими и определяющими соотношениями [4, 5]

1.1. Пусть $S = \{s_1, \ldots, s_n\}$ — некоторое (для простоты) конечное множество элементов из группы G. Рассмотрим алфавит над множеством S, состоящий из $2n$ «букв» $\{s_1, \ldots, s_n, s_1^{-1}, \ldots, s_n^{-1}\}$, и всевозможные конечные слова вида $w = \left(s_{i_1}^{\varepsilon(1)}, \ldots, s_{i_l}^{\varepsilon(l)}\right)$, $\varepsilon(i) = \pm 1$, составленные из букв нашего алфавита. Через $W(S)$ обозначим множество всех таких слов, включая и пустое слово, не содержащее букв. Каждое слово $w \in W(S)$ представляет элемент $[w] = s_{i_1}^{\varepsilon(1)} \ldots s_{i_l}^{\varepsilon(l)}$ группы G. Договоримся, что пустое слово представляет единицу группы. Элементы вида $[w]$, $w \in W(S)$ образуют подгруппу в группе G, которая называется подгруппой, порожденной множеством S, и обозначается $\langle S \rangle$.

Задача 1. Докажите, что подмножество $\{[w] : w \in W(S)\}$ является подгруппой в G.

Пример. Если множество S состоит из одного элемента s, то $\langle S \rangle$ — это циклическая подгруппа, порожденная элементом s.

Если $\langle S \rangle = G$, то говорят, что S является *множеством образующих группы* G или что S *порождает* G.

Задача 2. (Группы диэдра D_m и D_∞). Пусть множество S состоит из двух элементов: $S = \langle t, s \rangle$, причем $t^2 = s^2 = 1$, а порядок элемента ts в группе G конечен и равен m. Докажите, что тогда

а) группа $\langle S\rangle$ порождается элементами $x = ts$ и t;
б) $\langle x\rangle$ — циклическая подгруппа в $\langle S\rangle$ порядка m;
в) $\langle x\rangle$ — нормальная подгруппа индекса 2. В частности, порядок $\langle S\rangle$ равен $2m$;
г) $\langle S\rangle = \{1, x, \ldots, x^{m-1}, t, xt, \ldots, x^{m-1}t\}$.

Если же ts — элемент бесконечного порядка, то $\langle x\rangle$ — бесконечная нормальная подгруппа индекса 2 в $\langle S\rangle$.

Группа $\langle S\rangle$ называется группой диэдра D_m, $m = 1, 2, \ldots, \infty$.

1.2. Пусть $G{=}\langle S\rangle$. Назовем два слова w и w' из $W(S)$ *эквивалентными* ($w \sim w'$), если они представляют один и тот же элемент группы G, т. е. $[w]{=}[w']$.

Если r — непустое слово, представляющее единицу группы, то мы говорим, что в группе G между образующими S выполняется соотношение r. Именно наличие соотношений между образующими приводит к тому, что один и тот же элемент группы может быть представлен разными словами из $W(S)$. Фиксируем некоторое множество R соотношений и назовем слова w и w' эквивалентными в силу соотношений R (или R-эквивалентными), если одно из этих слов можно перевести в другое с помощью последовательности элементарных преобразований одного из следующих типов и обратных к ним преобразований:

$$w = (u, v) \;\to\; w' = (u, s, s^{-1}, v), \quad s \in S$$
$$w = (u, v) \;\to\; w' = (u, r, v), \quad r \in R.$$

(Чтобы получить обратное преобразование, нужно в каждой строке обратить направление стрелки.)

Множество R называется *системой определяющих соотношений*, если любые два эквивалентных слова эквивалентны в силу соотношений R. Для группы G с множеством образующих S и соотношений R используются обозначения

$$G = \langle S\,|R\rangle = \langle s_1, \ldots, s_n \,|\, r_1, r_2, \ldots\rangle$$
$$\text{или } G = \langle s_1, \ldots, s_n \,|\, [r_1] = 1, [r_2] = 1, \ldots\rangle\,.$$

Задача 3. Доказать, что соотношение $x^q = 1$ является определяющим для циклической группы $\langle x\rangle$ порядка q.

Задача 4. Доказать, что $D_m = \langle t, s \,|\, t^2 = 1, s^2 = 1, (ts)^m = 1\rangle$ (если $m = \infty$, то $D_\infty = \langle t, s \,|\, t^2 = 1, s^2 = 1\,\rangle$).

Пример. Рассмотрим на евклидовой плоскости два отражения t и s, зеркала которых пересекаются в точке O, образуя угол π/m. Произведение t и s (в любом порядке) представляет из себя поворот вокруг O (по или против часовой стрелки) на угол $2\pi/m$ (при $m = \infty$ нужно считать, что зеркала отражений параллельны, но не совпадают). Следовательно, в группе $G = \langle t, s\rangle$ выполнены соотношения: $t^2 = 1$, $s^2 = 1$, $(ts)^m = 1$.

Последнее соотношение в силу первых двух можно переписать в симметричном виде $\underbrace{tst\ldots}_{m} = \underbrace{sts\ldots}_{m}$ (почему?). Например, при $m = 3$ это соотношение выглядит так: $tst = sts$.

Контрольный вопрос: каким движением плоскости является произведение ts (st) при $m = \infty$?

Дальше начинается «игра в слова» по следующим правилам: за один ход разрешается: а) либо фрагмент $(\underbrace{t, s, t, s\ldots}_{m})$ заменить фрагментом $(\underbrace{s, t, s, t\ldots}_{m})$ (или наоборот); б) либо вычеркнуть в слове любую пару рядом стоящих одинаковых букв или, наоборот, вставить такую пару в слово. В процессе игры мы все время будем получать слова, эквивалентные исходному слову в силу выписанных выше соотношений. Цель игры — получить эквивалентное слово минимальной длины.

Например, если $m = 3$, то для исходного слова (t, s, t, s, t) игра заканчивается после трех ходов: $(t, s, t, s, t) \to (s, t, s, s, t) \to (s, t, t) \to (s)$.

Задача 5. Покажите, что:
а) играя по правилам, любое слово можно привести к виду $(\underbrace{t, s, t, \ldots}_{p})$, $0 \leqslant p < m$ или $(\underbrace{s, t, s, \ldots}_{q})$, $0 < q \leqslant m$.
б) исходя из геометрических соображений, докажите, что $2m$ слов такого вида представляют разные элементы группы $\langle t, s\rangle$.

Ясно, что если исходное слово было соотношением, то в конце мы получим пустое слово, а это значит, что соотношения $t^2 = 1$, $s^2 = 1$ и $(ts)^m = 1$ являются определяющими. Подведем итог: группа диэдра допускает геометрическую реализацию в виде группы отражений на евклидовой плоскости (рекомендуем ещё раз вернуться к рассказу «Два зеркала» в [3]).

1.3. *Длина элемента группы.*

Пусть в группе G выбрана система образующих S. *Длиной слова* $w \in W(S)$ называется число входящих в его запись букв. Для длины слова выберем обозначение $l(w)$. *Длину* $l(g)$ *элемента* $g \in G$ определим как минимум длин всевозможных слов, его представляющих, т. е.

$$l(g) = \min_{w:[w]=g} l(w).$$

Любое слово w, на котором этот минимум достигается, называется *кратчайшим словом*, представляющим элемент g, или просто кратчайшим словом (их может быть несколько).

Пример. а) В циклической группе третьего порядка $\mathrm{Z}_3 = \langle x \rangle$ слово (x, x) не является кратчайшим, так как $\left[x^2\right] = \left[x^{-1}\right]$. Таким образом, $l\left(x^2\right) = 1$.
б) В группе $D_3 = \langle t, s \rangle$ элемент $g = tst$ представлен двумя кратчайшими словами (t, s, t) и (s, t, s). Здесь $l\left(g\right) = 3$.

Задача 6. Проверьте следующие свойства функции длины $l\left(g\right)$ на группе:
1) $l\left(1\right) = 0$;
2) $l\left(g\right) = l\left(g^{-1}\right)$;
3) $l\left(g_1 g_2\right) \leqslant l\left(g_1\right) + l\left(g_2\right)$;
4) $l\left(g_1 g_2^{-1}\right) \geqslant \left|l\left(g_1\right) - l\left(g_2\right)\right|$.

Наша ближайшая цель — указать естественную систему образующих и определяющих соотношений для дискретной группы отражений.

2. Кокстеровское представление дискретной группы отражений

Суть дела рассказана в [3]. А вот как это выглядит на словах.

2.1. Пусть G — дискретная группа отражений, действующая в любом из трех пространств X: сферическом, евклидовом или гиперболическом. Через $\pi\left(r\right)$ договоримся обозначать зеркало отражения r из группы G. Семейство зеркал всех отражений, входящих в группу G, разбивает пространство X на выпуклые многогранники Кокстера, которые мы будем называть *камерами*, а их $(n-1)$-мерные грани (фасеты) — *стенками*.

Две камеры называются *смежными*, если у них есть общая стенка. И так как гиперплоскость, содержащая общую стенку, является зеркалом отражения из группы G, то смежные камеры можно переставить с помощью этого отражения. Отсюда, в частности, следует, что любые две камеры одинаковы в том смысле, что одну из них можно перевести в другую движением из группы G. Для этого соединим их цепочкой смежных камер и будем двигаться вдоль цепочки, переходя из камеры в соседнюю камеру с помощью отражений из группы G.

Фиксируем какую-нибудь камеру P_0 нашего разбиения.

Задача 7. Докажите, что а) если $s \in G$ — отражение в зеркале π, то gsg^{-1} — отражение в зеркале $g\pi$. б) Любое отражение из группы G сопряжено одному из отражений в стенках камеры P_0.

Пусть у камеры P_0 имеется n стенок. Присвоим им произвольным образом номера $1, \ldots, n$, и пусть s_i — отражение в стенке с номером i

(математический жаргон!), а $S = \{s_1, \dots, s_n\}$. Если стенки с номерами i и j образуют двугранный угол π/m_{ij}, то подгруппа $\langle s_i, s_j \rangle$ является группой диэдра $D_{m_{ij}}$. В частности, выполняется соотношение $(s_i s_j)^{m_{ij}} = 1$ или в симметричном виде $\underbrace{s_i s_j \dots}_{m_{ij}} = \underbrace{s_j s_i \dots}_{m_{ij}}$. (см. раздел «Общая теория» в [3]).

Теорема 1. *Группа отражений G порождается множеством S с определяющими соотношениями $s_i^2 = 1$, $i = 1, \dots, l$, $(s_i s_j)^{m_{ij}} = 1$.*

Такая система образующих и определяющих соотношений, целиком определяемая комбинаторным типом многогранника P_0, называется *кокстеровским представлением* группы G.

Доказательство этой теоремы требует немалых приготовлений. Впрочем, все хлопоты связаны с простой и красивой геометрией.

2.2. *Слова и цепи камер.*

Последовательность камер $(P_0, P_1, \dots, P_l)$ называется *цепью*, если камеры P_{k-1} и P_k смежны. Пусть $w = (s_{i_1}, \dots, s_{i_l})$ произвольное слово из $W(S)$. Поставим ему в соответствие цепь камер

$$(P_0,\ P_1 = s_{i_1} P_0,\ P_2 = s_{i_1} s_{i_2} P_0,\ \dots,\ P_l = s_{i_1} \dots s_{i_l} P_0) \tag{1}$$

Вот менее формальное описание цепи (1): в камере P_0 находим стенку с номером i_1 и с помощью отражения s_{i_1} переходим в камеру P_1, смежную с P_0 по этой стенке. Далее в камере P_1 находим стенку с номером i_2. Эта стенка лежит на зеркале отражения $r_{i_2} = s_{i_1} s_{i_2} s_{i_1}^{-1} = s_{i_1} s_{i_2} s_{i_1}$. С помощью этого отражения переходим в смежную камеру P_2 и т. д. Ясно, что камера P_2 получается из P_0 с помощью элемента $g = r_{i_2} r_{i_1}$ из группы G. Но $g = r_{i_2} r_{i_1} = s_{i_1} s_{i_2} s_{i_1} s_{i_1} = s_{i_1} s_{i_2}$, т. е. $P_2 = s_{i_1} s_{i_2} P_0$.

Аналогично выглядит процесс последовательного построения цепи и на любом шаге k: камера P_k получается из камеры P_{k-1} с помощью отражения

$$r_{i_k} = s_{i_1} \dots s_{i_{k-1}} s_{i_k} s_{i_{k-1}} \dots s_{i_1},$$

т. е.

$$P_k = \left(s_{i_1} \dots s_{i_{k-1}} s_{i_k} s_{i_{k-1}} \dots s_{i_1}\right)\left(s_{i_1} s_{i_2} \dots s_{i_{k-1}} P_0\right) = \left(s_{i_1} \dots s_{i_{k-1}} s_{i_k} P_0\right).$$

(см. рис. 1).

Обратите внимание на ассоциированную с цепью камер (1) последовательность отражений $r_{i_1}, r_{i_2}, \dots, r_{i_l}$. Формально эти отражения однозначно определяются алгебраическими условиями: $s_{i_1} s_{i_2} \dots s_{i_k} = r_{i_k} r_{i_{k-1}} \dots r_{i_1}$. Но полезнее запомнить их геометрический смысл: камера P_k смежна с камерой P_{k-1} по стенке, содержащейся в зеркале отражения r_{i_k} (см. рис. 1).

Итак, каждому слову соответствует цепь камер. Пусть, наоборот, задана цепь камер $(P_0, \dots, P_l)$. Можно ли по цепи камер восстановить

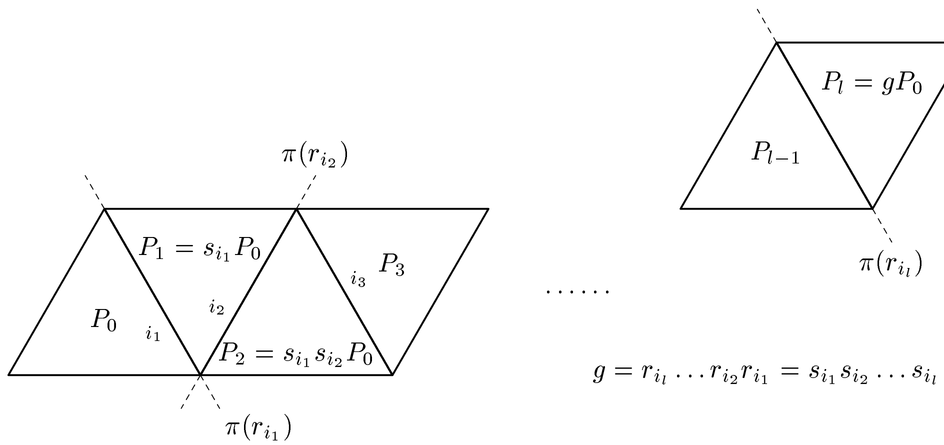

Рис. 1.

соответствующее ей слово? Оказывается, что можно и притом однозначно. Делается это так: пусть камера P_1 получается из P_0 с помощью отражения $r_{i_1} = s_{i_1}$, камера P_2 — из камеры P_1 с помощью отражения $r_{i_2} = s_{i_1}s_{i_2}s_{i_1}$, а в общем случае — камера P_{i_k} получается из камеры $P_{i_{k-1}}$ с помощью отражения $r_{i_k} = s_{i_1}\dots s_{i_{k-1}}s_{i_k}s_{i_{k-1}}\dots s_{i_1}$. Тогда $w = (s_{i_1},\dots,s_{i_l})$ — искомое слово.

Контрольный вопрос: какая цепь соответствует пустому слову?

Ясно, что число камер в цепи на единицу больше длины слова, соответствующего этой цепи. Хитрее вопрос о том, как «увидеть» длину элемента $g = [w]$.

2.3. *Принцип четности.*

Ясно, что цепь камер, ассоциированная с любым словом $w = (s_{i_1},\dots, s_{i_l})$, представляющим элемент $g \in G$, соединяет камеру P_0 с камерой gP_0 (см. рис. 1).

Рассмотрим последовательность отражений $r_{i_1}, r_{i_2},\dots, r_{i_l}$, и, выбрав любое отражение r из группы G, зададим вопрос: сколько раз входит r в последовательность $r_{i_1},\dots, r_{i_l}$? Ответ геометрически очевиден: столько раз, сколько рассматриваемая цепь камер пересекает зеркало $\pi(r)$. Это наглядное соображение приводит к важному выводу: четность числа вхождений r в последовательность $r_{i_1},\dots, r_{i_l}$ определяется только зеркалом r и самим элементом g и не зависит от представления g через образующие. А именно, выполняется

Принцип четности. *Если зеркало $\pi(r)$ разделяет камеры P и gP, то число вхождений r в последовательность $(r_{i_1}, r_{i_2},\dots, r_{i_l})$ нечетно, а если не разделяет — то четно.*

2.4. *Лемма о кратчайшем слове.*

Слово $w = (s_{i_1}, \dots, s_{i_l})$ тогда и только тогда является кратчайшим, когда в последовательности отражений $r_{i_1}, \dots, r_{i_l}$ все элементы различны.

В [3] кратчайшие слова называются приведенными и интерпретируются как «реальные траектории световых лучей».

Доказательство. Пусть в указанной последовательности отражений встречаются одинаковые. Будем считать для простоты, что $r_{i_1} = r_{i_q}$, то есть $s_{i_1} = s_{i_1} \dots s_{i_{q-1}} s_{i_q} s_{i_{q-1}} \dots s_{i_1}$. Но тогда

$$g = s_{i_1} \dots s_{i_l} = \big(s_{i_1} \dots s_{i_{q-1}} s_{i_q}\big)\, s_{i_{q+1}} \dots s_{i_l} = \\ = s_{i_2} s_{i_3} \dots s_{i_{q-1}} s_{i_{q+1}} \dots s_{i_l} = \hat{s}_{i_1} s_{i_2} \dots \hat{s}_{i_q} \dots s_{i_l}$$

(крышечка над буквой означает ее отсутствие в записи), и нам удалось уменьшить длину слова, представляющего элемент g. Следовательно, у кратчайшего слова повторений в последовательности отражений $r_{i_1}, \dots,$ r_{i_l} не бывает. Мы доказали необходимость условия леммы.

Задача 8. Проверьте, что $g = s_{i_1} \dots \hat{s}_{i_p} \dots \hat{s}_{i_q} \dots s_{i_l}$, если $r_{i_p} = r_{i_q}$.

Продолжим доказательство. Пусть все отражения в последовательности $r_{i_1}, \dots, r_{i_l}$ различны. По принципу четности все зеркала $\pi\,(r_{i_t})$, $t = 1, \dots, l$, разделяют камеры P_0 и gP_0. Поэтому, если через $R\,(g)$ обозначить множество тех отражений r из G, зеркала которых разделяют камеры P_0 и gP_0, то $l\,(g) \leqslant l \leqslant |R\,(g)|$ (почему?). С другой стороны, $l\,(g) \geqslant |R\,(g)|$, так как любая цепь камер, соединяющая P_0 и gP_0, обязана хотя бы раз пересечь каждое зеркало из $R\,(g)$. Следовательно, слово w является кратчайшим, а длина элемента $g = [w]$ равна $|R\,(g)\,|$.

Лемма полностью доказана.

А заодно получена полезная геометрическая информация, которая и позволяет «увидеть» длину $l\,(g)$ элемента $g \in G$:

Длина $l(g)$ элемента g равна числу зеркал отражений из группы G, разделяющих камеры P_0 и gP_0.

2.5. *Правило вычеркивания.*

Пусть $l\,(gs) = l\,(g) - 1$ для некоторого элемента $g \in G$ и некоторого $s \in S$. Тогда кратчайшее слово элемента gs получается из кратчайшего слова элемента g вычеркиванием какой-то одной буквы.

Доказано [9], что это свойство выделяет группы Кокстера среди групп, порожденных инволюциями.

Контрольный вопрос: а бывает ли так, что а) $|l\,(gs) - l\,(g)| > 1$, б) $l\,(gs) = l\,(g)$?

Доказательство. Пусть $g = s_{i_1} \dots s_{i_l}$ — кратчайшая запись элемента g через образующие. Тогда в последовательности $r_{i_1}, \dots, r_{i_l}$ нет повторяющихся отражений. Нам дано, что слово $(s_{i_1}, \ldots, s_{i_l}, s)$ уже не является кратчайшим, то есть в последовательности $r_{i_1}, \ldots, r_{i_l}, r_{i_{l+1}}$ есть повторения. Ясно, что повториться может только отражение $r_{i_{l+1}}$. А тогда, как мы уже видели в п. 2.4. (задача 8), $gs = s_{i_1} \ldots \hat{s}_{i_m} \ldots s_{i_l} \hat{s}$.

Задача 9. Докажите, что правило вычеркивания работает и в том случае, когда $l\,(sg) = l\,(g) - 1$.

2.6. *Пример симметрической группы S_n.*

Эта группа действует в E^n перестановками координат вектора $x = (x_1, \ldots, x_n)$. Группа S_n порождается смежными транспозициями $s_1 = (1,2)$, $s_2 = (2,3)$, ..., $s_{n-1} = (n-1, n)$, переставляющими соответственно первую и вторую координаты, вторую и третью, и т. д. При этом отражения в S_n — это в точности транспозиции. Можно проверить выполнение соотношений Кокстера: $s_i^2 = 1$, $s_i s_{i+1} s_i = s_{i+1} s_i s_{i+1}$ или $(s_i s_{i+1})^3 = 1$, и $s_i s_j = s_j s_i$, если $|i - j| > 1$.

Хорошо известно, что длина $l\,(g)$ перестановки $g \in S_n$ равна числу инверсий (беспорядков) среди координат вектора $g\,(1, 2, \ldots, n)$. Правило вычеркивания интерпретируется для этой группы так: пусть g принадлежит S_n, а s — такая смежная транспозиция, что $l(sg) < l(g)$. Такое бывает, только если транспозиция s переставляет в векторе $g(1, \ldots, n)$ пару смежных символов i и j, образующих инверсию. Но такая пара может появиться только за счет того, что одна из смежных транспозиций, входящих в кратчайшую запись g, поменяла местами символы i и j. Исключив эту транспозицию, мы получим кратчайшую запись элемента sg.

2.7. *Доказательство теоремы* 1.

Доказательство опирается на одно интересное геометрическое наблюдение.

Лемма. *Пусть $l\,(gs_i) < l\,(g)$ и $l\,(gs_j) < l\,(g)$. Тогда $l(g \underbrace{s_i s_j \ldots}_{k}) = |k - m_{ij}| + l\,(g) - m_{ij}$ (на рис. 2 представлен график длины элемента $(g \underbrace{s_i s_j \ldots}_{k})$ как функции от k, $0 \leqslant k \leqslant 2m_{ij}$.)*

Доказательство. Длина $l(g)$ элемента $g \in G$ равна числу $|R(g)|$ зеркал, отделяющих камеру P_0 от камеры gP_0. Пусть $s \in S$. Камеры $(gs)P_0$ и gP_0 смежны по стенке, принадлежащей зеркалу $\pi(r)$ отражения $r = gsg^{-1}$, и $\pi(r)$ — единственное из зеркал, разделяющее эти смежные камеры. Поэтому верно следующее утверждение:

Утверждение. *Длина элемента gs на единицу меньше (больше) длины g тогда и только тогда, когда зеркало $\pi(r)$ отражения gsg^{-1} разделяет (не разделяет) камеры P_0 и gP_0.*

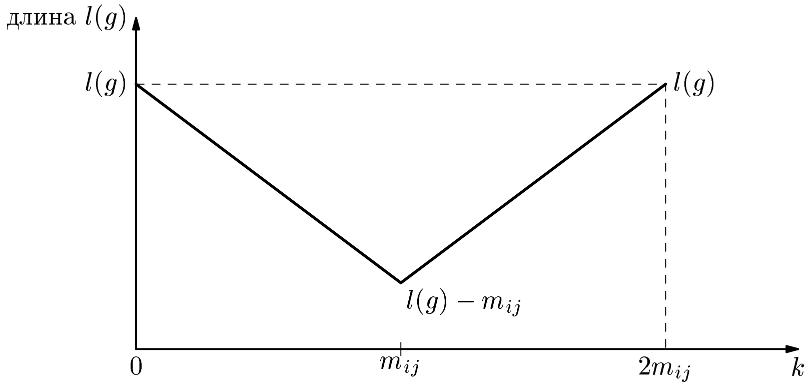

Рис. 2.

◀ В самом деле, в этом случае камеры P_0 и $(gs)P_0$ оно уже не разделяет (разделяет), и, тем самым, число зеркал в множестве $R(gs)$ уменьшается (увеличивается) на единицу по сравнению с их числом в $R(g)$. ▶

В нашей ситуации сказанное означает, что как зеркало $\pi(r_i)$ отражения $r_i = gs_ig^{-1}$, так и зеркало $\pi(r_j)$ отражения $r_j = gs_jg^{-1}$ отделяют камеру P_0 от камеры gP_0 (см. рис. 3, где дело происходит на плоскости). Но в таком случае зеркала этих отражений должны пересекаться, что, равносильно смежности соответствующих стенок многогранника gP_0 [1]. Двугранный угол между ними равен π/m_{ij}. Теперь ясно, что вместе с зеркалами $\pi(r_i)$ и $\pi(r_j)$ камеры P_0 и gP_0 разделяют все зеркала, проходящие через грань $O = \pi(r_i) \cap \pi(r_j) \cap P_0$. Число таких зеркал равно m_{ij} (почему?).

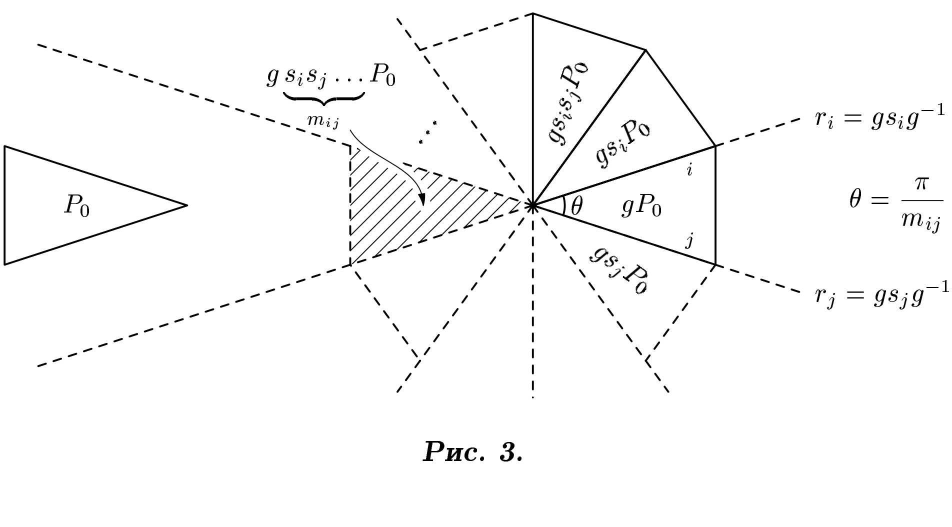

Рис. 3.

Далее, цепь камер $gP_0, (gs_i)P_0, (gs_is_j)P_0, \ldots, (g\underbrace{s_is_j\ldots}_{2m_{ij}-1})P_0$ образует обход вокруг грани O в пространстве X. В силу нашего утверждения при движении по этой цепи функция $l\,(k) = l(g\underbrace{s_is_j\ldots}_{k})$ будет с ростом k монотонно уменьшаться до тех пор, пока мы не достигнем камеры, противоположной исходной камере $g(P_0)$ (на рис. 3 эта камера заштрихована). С этого момента длина начнет снова расти, достигнув начального значения при $k = 2m_{ij}$. Утверждение леммы доказано.

Теперь все готово для того, чтобы доказать, что любое соотношение в группе отражений есть следствие кокстеровских соотношений.

Рассмотрим любое соотношение $r = (q_1, \ldots, q_n)$, $q_i \in S$. Если в слове r встречается пара рядом стоящих одинаковых букв, то их можно сократить в силу соотношения вида (s, s). Повторяя эту операцию нужное число раз, получим эквивалентное слово (соотношение), уже не содержащее рядом стоящих одинаковых букв. Поэтому можно с самого начала считать r таким. Слову $r = (q_1, \ldots q_n)$ отвечает замкнутая цепь камер $P_0, q_1P_0, q_1q_2P_0, \ldots, q_1q_2\ldots q_{n-1}P_0$. Пусть $g_s = q_1\ldots q_s$. Рассмотрим функцию длины $l\,(s) = l\,(g_s)$. Если слово r не пусто, то эта функция достигает максимума, равного U, для некоторого значения $s = t$ (возможно, таких значений несколько). По определению максимума $l\,(g_tq_t) < l\,(g_t) = U$ и $l\,(g_tq_{t+1}) < l\,(g_t) = U$. Применим к слову r разрешенное элементарное преобразование «вставки»:

$$(q_1, \ldots, q_t, q_{t+1}, \ldots q_n) \to (q_1, \ldots, q_t, \underbrace{q_t, q_{t+1}, q_t, \ldots q_{t+1}}_{2m}, q_{t+1}, \ldots q_n).$$

Вычеркивая в полученном слове рядом стоящие одинаковые буквы, получим новое слово $(q_1, \ldots, q_{t-1}, q_{t+1}, \ldots, q_t, q_{t+2}, \ldots, q_n)$, которое по доказанной лемме обладает таким свойством: у него число тех значений s, где функция длины достигает значения U, на единицу меньше, чем у исходного. Если же с самого начала существовала единственная точка максимума, то в полученном слове само значение максимума длины будет меньше по крайней мере на единицу. Продолжая действовать в том же духе, т.е. последовательно «срезать» максимумы, мы в итоге непременно получим пустое слово.

У нашей операции «уничтожения» максимума есть простой геометрический смысл. А именно, в изображенном на рис. 4 случае часть цепи $(\ldots, g_iq_iP_0, g_iP_0, g_iq_{i+1}P_0, \ldots)$ мы заменяем «объездом» вокруг грани O по цепи камер, отмеченной пунктиром, а затем избавляемся от тех «пунктирных» камер, которые уже входили в нашу начальную цепь. В

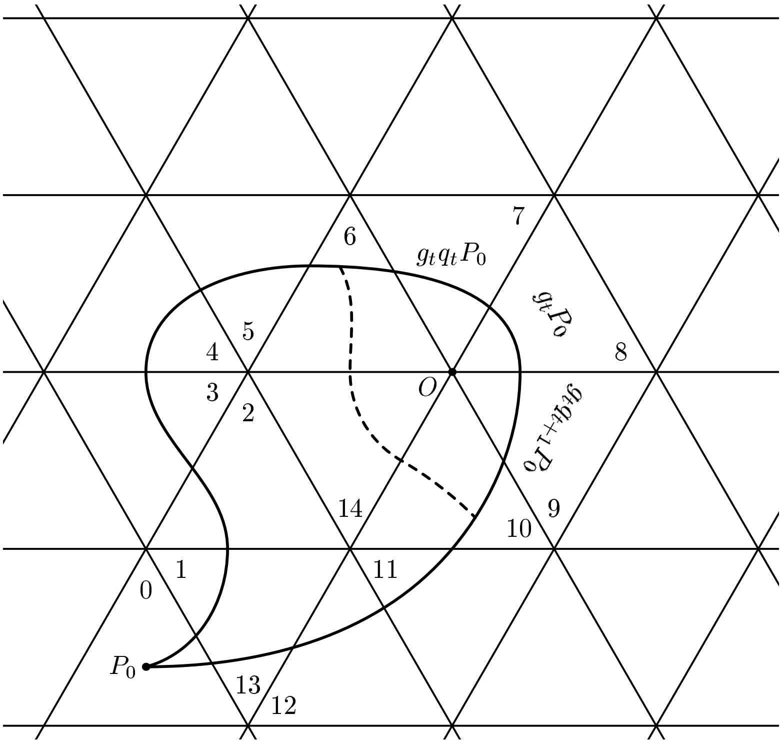

Рис. 4. *Показано «снятие с гвоздя» O «замкнутой цепи» камер* $(0, 1, 2, \ldots, 13)$. *Результат — цепь* $(0, 1, 2, 3, 4, 6, 14, 10, 11, 12, 13)$

результате, мы снимаем цепь с очередного «гвоздя» O, стремясь «стянуть» ее в единственную камеру P_0.

Часть 2. Теорема Титса о разрешимости проблемы слов

1. Абстрактная группа Кокстера и проблема слов

1.1. Обозначим через I конечное множество индексов, и пусть M — матрица с элементами m_{ij}, $i, j \in I$, которые принимают значения в множестве $\{1, 2, \ldots, \infty\}$, причем $m_{ii} = 1$, и $m_{ij} = m_{ji} > 2$ для всех $i \neq j$.

Группа G с множеством образующих $S = \{s_i : i \in I\}$ и множеством определяющих соотношений $R = \{(s_i s_j)^{m_{ij}} = 1 : i, j \in I,\ m_{ij} < \infty\}$ называется абстрактной группой Кокстера типа (S, M). Это означает, что любой элемент g группы G записывается через образующие S: $g = s_{i_1} \ldots s_{i_l}$, и, если $s_{j_1} \ldots s_{j_m} = 1$ — любое соотношение между образующими, то слово $(s_{j_1}, \ldots, s_{j_m})$ эквивалентно в силу соотношений R пустому слову (см. п. 1.2 части I).

1.2. Говорят, что в группе $G = \langle s_1, \ldots, s_n \mid r_1, \ldots, r_m \rangle$ разрешима проблема слов, если можно указать алгоритм, который работает с произвольным словом $w \in W(T)$ и после конечного числа шагов говорит «Да», если $[w] = 1$, т. е. слово w представляет единицу в группе G, или «Нет», если $[w] \neq 1$.

Нетрудно сообразить, как с помощью такого алгоритма решается вопрос о том, представляют ли два слова u и v один и тот же элемент группы G.

Группы Кокстера, как будет вскоре доказано, попадают в компанию групп с разрешимой проблемой слов. Среди «счастливчиков» встречаются уже знакомые читателям этого журнала фундаментальные группы дополнений к узлам в трехмерной сфере, фундаментальные группы замкнутых поверхностей и группы кос. Многолетние наблюдения показывают, что и в других геометрически интересных группах, действующих на интересных геометрических объектах, проблема слов разрешима.

Существование групп с отрицательным решением проблемы слов составляет содержание знаменитой теоремы П. С. Новикова [6].

2. Представление Титса

2.1. *Группа Кокстера как группа отражений*

Пусть G — группа Кокстера типа (S, M). Рассмотрим конечномерное вещественное векторное пространство V с базисом $\{e_i : i \in I\}$. Зададим в V скалярное произведение $(\cdot,\cdot)\colon V \times V \to \mathbb{R}$ по формуле

$$\Big(\sum_{i\in I} x_i e_i, \sum_{j\in I} y_j e_j\Big) = -\sum x_i y_j \cos(\pi/m_{ij}) \qquad (*)$$

(если $m_{ij} = \infty$, то $\cos(\pi/m_{ij}) = 1$).

Для простоты будем считать, что скалярное произведение $(*)$ невырожденно. Для любого базисного вектора e_i скалярный квадрат (e_i, e_i) равен 1 и $(e_i, e_j) = -\cos\pi/m_{ij}$. Через l_i обозначим отражение в гиперплоскости $\pi(l_i) = \{v \in V \mid (v, e_i) = 0\}$, т. е. такое линейное преобразование, которое сохраняет скалярное произведение, действует тождественно на зеркале $\pi(l_i)$ и умножает вектор e_i на -1. Легко проверить, что

$$l_i(v) = v - 2(v, e_i)\, e_i. \qquad (2)$$

В силу невырожденности скалярного произведения замкнутые полупространства $\pi_i^+ = \{v \in V \mid (v, e_i) \geqslant 0\}$ дают в пересечении замкнутый выпуклый n-гранный конус C. Через $\mathring{C}$ обозначим (непустое) множество его внутренних точек. Далее, обозначим через L группу линейных преобразований пространства V, порожденную отражениями l_i, $i \in I$, и рассмотрим естественное отображение $\varphi\colon S \to L$ множества S в группу

L: $\varphi(s_i) = l_i$. Прямое вычисление с использованием формулы (2) показывает, что линейные преобразования l_i удовлетворяют тем же кокстеровским соотношениям: $l_i^2 = 1$, $(l_i l_j)^{m_{ij}} = 1$. Следовательно, отображение $\varphi\colon S \to L$ можно продолжить до гомоморфизма группы Кокстера G в линейную группу отражений L, и, пользуясь этим, установить такой важный факт.

Лемма. *Порядок элемента $s_i s_j$ в группе Кокстера G равен m_{ij}.*

Доказательство. Порядок элемента $l_i l_j$ в группе L равен m_{ij} (почему?). Но $\varphi(s_i s_j) = l_i l_j$, а, с другой стороны, при гомоморфизме порядок образа делит порядок прообраза.

Ж. Титс [2,11] открыл гораздо более глубокие свойства отображения φ и группы L.

Теорема (группа Кокстера — группа отражений).
а) *отображение φ (однозначно) продолжается до гомоморфизма $\varphi\colon G \to L$ с тривиальным ядром.*
б) *группа L действует в выпуклом конусе $D = \bigcup\limits_{l \in L} l(\mathring{C})$ (конус Титса) как дискретная группа отражений.*

Замечание. Для произвольного скалярного произведения $(*)$ конус Титса «переезжает» в двойственное пространство V^*, а теорема по-прежнему утверждает, что у абстрактной группы Кокстера G имеется точное линейное представление $\varphi\colon G \to GL(V^*)$ (представление Титса) и что $\varphi(G)$ — дискретная группа отражений в некотором выпуклом конусе $D \subset V^*$ с, вообще говоря, весьма замысловатой геометрией границы.

Задача 10. Доказать теорему Титса для группы G типа (S, M) с невырожденной матрицей M второго порядка.

2.2. *Геометрическое решение проблемы слов в группе Кокстера*

Рассмотрим элемент $g \in G$ и его запись через образующие $g = s_{i_1} \dots s_{i_t}$. Зафиксируем вектор v_0 из внутренности фундаментальной камеры C.

Применим к вектору v_0 линейное преобразование $\varphi(g) = l_{i_1} \dots l_{i_t}$. Если в результате окажется, что $\varphi(g)v_0 = v_0$, то $g = 1$. В противном случае $g \neq 1$ (почему?).

Для алгебраиста предложенный алгоритм выглядит непрактично, не говоря уже о том, что он основан на непростой теореме, которую мы не собираемся доказывать.

Надеемся, что следующий алгоритм, уже удовлетворит алгебраически настроенного читателя, привыкшего играть в слова.

2.3. *Правило вычеркивания и его важные комбинаторные следствия*

Правило вычеркивания — решающее свойство групп Кокстера. Доказывая его для групп отражений (см. ч. I), мы опирались лишь на геометрическое понятие «разделять» и на соображение о том, что отражение с «разделяющим» зеркалом входит в последовательность отражений $\{r_{i_1}, \dots, r_{i_l}\}$, ассоциированную со словом $(s_{i_1}, \dots, s_{i_l})$, нечетное число раз. Если воспользоваться представлением Титса, то геометрическое доказательство правила вычеркивания можно провести и в конусе Титса. Но есть и другой путь: следуя идее Н. Бурбаки, полностью изгнать геометрию из доказательства (смотри цикл задач в конце статьи).

Итак, вооружившись правилом вычеркивания, займемся получением нужных нам комбинаторных свойств группы G.

Для любых $i, j \in I$, таких, что $m_{ij} < \infty$, обозначим через $r(i, j)$ слово $(\underbrace{s_i, s_j, \dots}_{m_{ij}})$. Ясно, что в силу кокстеровских соотношений, слова $r(i, j)$ и $r(j, i)$ представляют один и тот же элемент группы.

Назовем два слова w_1 и w_2 *гомотопными*, и будем писать $w_1 \sim w_2$, если одно из них может быть получено из другого с помощью последовательности преобразований такого вида: в слове $ur(i, j)v$ фрагмент $r(i, j)$ заменяется на $r(j, i)$ (или наоборот). В результате получается слово $ur(j, i)v$.

Задача 11. Проверьте, что в группе Кокстера

$$G = S_4 = \langle s_1, s_2, s_3 \mid s_1^2 = s_2^2 = s_3^2 = 1, (s_1 s_2)^3 = 1, (s_2 s_3)^3 = 1, (s_1 s_3)^2 = 1 \rangle$$

следующие четыре слова попарно гомотопны

$$(s_1, s_2, s_1, s_3, s_2, s_1),\ (s_1, s_2, s_3, s_1, s_2, s_1),$$
$$(s_1, s_2, s_3, s_2, s_1, s_2),\ (s_2, s_3, s_1, s_2, s_3, s_1).$$

Отметим очевидные свойства гомотопии:

а) гомотопные слова представляют один и тот же элемент группы G;
б) гомотопные слова имеют одинаковую длину;
в) гомотопные слова состоят из одних и тех же букв, но при этом могут отличаться кратностью их вхождения.

Теорема (Ж. Титс [11]). *Пусть $g \in G$, а w_1 и w_2 — два кратчайших слова, представляющих элемент g. Тогда слова w_1 и w_2 гомотопны.*

Доказательство. Применим индукцию по длине кратчайшего слова. Рассмотрим два кратчайших слова $w_1 = (p_1, \dots, p_n)$ и $w_2 = (q_1, \dots, q_n)$ длины n, представляющих элемент g. Иными словами, есть две кратчайшие записи $p_1 \dots p_n = g = q_1 \dots q_n$ элемента g через образующие. При этом можно считать, что $p_1 \neq q_1$ (почему?). Ясно, что $l(p_1 g) < l(g)$, т. е. слово $(p_1, q_1, \ldots, q_n)$ уже не является кратчайшим. Тогда по правилу вычеркивания

$$p_1 q_1 \ldots q_l \ldots q_n = q_1 \ldots \hat{q}_l \ldots q_n. \tag{$**$}$$

Рассмотрим два случая $l < n$ и $l = n$.

Если $l < n$, то после умножения равенства $(**)$ на p_1 получаем

$$q_1 \ldots q_l q_{l+1} \ldots q_n = p_1 q_1 \ldots q_{l-1} q_{l+1} \ldots q_n,$$

т. е. $q_1 \ldots q_l = p_1 q_1 \ldots q_{l-1}$. Обе записи являются кратчайшими, и, по индуктивному предположению,

$$(p_1, q_1, \ldots, q_{l-1}) \sim (q_1, \ldots, q_l).$$

Но тогда и

$$(p_1, q_1, \ldots, \hat{q}_l \ldots, q_n) \sim (q_1, \ldots, q_n).$$

С другой стороны, $p_1 q_1 \ldots \hat{q}_l \ldots q_n = g = p_1 \ldots p_n$.

Умножая обе части на p_1 и применяя предположение индукции, имеем

$$(q_1, \ldots, \hat{q}_l \ldots, q_n) \sim (p_2, \ldots, p_n).$$

Но в таком случае и

$$(p_1, \ldots, p_n) \sim (p_1, q_1, \ldots, \hat{q}_l \ldots, q_n) \sim (q_1, \ldots, q_n).$$

Итак, мы доказали, что при $l < n$, $(p_1, \ldots, p_n) \sim (q_1, \ldots, q_n)$.

Во втором случае, когда $l = n$, правило вычеркивания дает $p_1 q_1 \ldots q_n = q_1 \ldots q_{n-1}$. Поменяв ролями p и q в предыдущем рассуждении, можно считать, что и здесь мы столкнулись с трудным случаем, когда $l = n$, т. е. когда $q_1 p_1 \ldots p_n = p_1 \ldots p_{n-1}$. Чтобы продолжить доказательство, заметим, что слова $(q_1, \ldots, q_n)$ и $(q_1, p_1, \ldots, p_{n-1})$ гомотопны. В самом деле, $q_1 p_1 \ldots p_n = p_1 \ldots p_{n-1}$ по правилу вычеркивания. С другой стороны,

$$p_1 \ldots p_{n-1} = q_1 p_1 \ldots p_n = q_1 q_1 \ldots q_n = q_2 \ldots q_n,$$

и в силу предположения индукции

$$(q_2, \ldots, q_n) \sim (p_1, \ldots, p_{n-1}).$$

Следовательно, $(q_1, q_2, \ldots, q_n) \sim (q_1, p_1, \ldots, p_{n-1})$. Точно так же доказывается, что $(p_1, \ldots, p_n) \sim (p_1, q_1, \ldots, q_{n-1})$. Заменим исходные кратчайшие записи элемента g на новые, им гомотопные, а именно

$$q_1 p_1 \ldots p_{n-1} = g = p_1 q_1 \ldots q_{n-1}.$$

К этим новым кратчайшим записям применим все рассуждения первого шага. Тогда в лучшем случае мы получим утверждение теоремы по предположению индукции, показав, что слово $(q_1, p_1, \ldots, p_{n-1})$ гомотопно слову $(p_1, q_1, \ldots, q_{n-1})$, а в худшем — снова получим две кратчайшие записи вида

$$\underbrace{q_1p_1q_1}_{3}\dots q_{n-2} = g = \underbrace{p_1q_1p_1}_{3}\dots p_{n-2},$$

гомотопность которых все еще неясна. Продолжение этого процесса неминуемо приведет нас на каком-то шаге к равенству

$$\underbrace{q_1p_1q_1\dots}_{m}(\dots) = g = \underbrace{p_1q_1p_1\dots}_{m}(\dots),\ \text{(где } m \text{ — порядок элемента } p_1q_1).$$

В силу индуктивного предположения, части слов, стоящие в скобках, справа и слева, гомотопны. А тогда по определению гомотопны и сами слова.

Теорема Ж. Титса доказана.

Контрольный вопрос: Почему наш процесс не может закончиться записью вида $\underbrace{q_1p_1\dots}_{k} = g = \underbrace{p_1q_1\dots}_{k}$, при $k < m$?

2.3. *Алгоритм*

Теорема. *Слово w тогда и только тогда представляет единицу в группе Кокстера G, когда его можно привести к пустому слову с помощью последовательности гомотопий и вычеркиваний двух рядом стоящих одинаковых букв.*

Доказательство. В одну сторону все ясно. Для доказательства необходимости рассмотрим произвольное слово f и будем его «упрощать» с помощью двух типов преобразований, указанных в формулировке теоремы. Через $Z(f)$ обозначим множество всех слов, которые можно получить из исходного цепочкой таких упрощений. Так как на каждом шаге длина слова не увеличивается (не изменяется при гомотопиях и уменьшается при вычеркиваниях), то в $Z(f)$ найдется слово $f' = (t_1, \dots, t_l)$ минимальной длины. Мы утверждаем, что слово $(t_1, \dots, t_l)$ является кратчайшим словом, представляющим элемент $g = [f]$ в группе G.

В самом деле, пусть $(t_1, \dots, t_l)$ не является кратчайшим словом, представляющим элемент g. Так как (t_1) — кратчайшее слово, представляющее элемент t_1, то найдется такое $m \in \{1, \dots l-1\}$, что $(t_1, \dots, t_m)$ — кратчайшее слово, представляющее элемент группы $g' = t_1 \dots t_m$, а слово $(t_1, \dots, t_m, t_{m+1})$ уже таким свойством не обладает. Но тогда по правилу вычеркивания $g' = t_1 \dots \hat{t}_p \dots t_{m+1}$, и это кратчайшая запись элемента g'. По теореме Титса два кратчайших слова, представляющих g', гомотопны. В нашем случае $(t_1, \dots, t_m) \sim (t_1 \dots \hat{t}_p \dots t_{m+1})$. Но тогда слово $(t_1, \dots, t_l)$ гомотопно слову $(t_1, \dots \hat{t}_p, \dots, t_{m+1}, t_{m+1}, \dots t_l)$, и (после сокращения двух рядом стоящих букв t_{m+1}) перед нами слово из $Z(f)$, которое короче слова f'. Противоречие.

Рассмотрим алгоритм, который на каждом шаге либо заменяет слово w ему гомотопным, либо вычеркивает в нем две рядом стоящие одинаковые буквы. Через конечное число шагов наш алгоритм приводит к кратчайшей записи элемента группы $g = [w]$. Если полученное слово не пусто, то $g \neq 1$!

3. Изгнание геометрии (цикл задач) [2, 7]

Сначала зафиксируем обозначения всех нужных нам объектов:

G — группа Кокстера типа (S, M).

T — множество всех элементов группы G, сопряженных какому-нибудь элементу из S.

Через $(r_{i_1}, \ldots, r_{i_l})$ будет обозначаться последовательность элементов из T, ассоциированная со словом $w = (s_{i_1}, \ldots, s_{i_l})$. Напомним, что $r_{i_k} = s_{i_1} \ldots s_{i_{k-1}} s_{i_k} s_{i_{k-1}} \ldots s_{i_1}$.

Для любого элемента $t \in T$ через $N(w, t)$ обозначим число вхождений t в последовательность $(r_{i_1}, \ldots, r_{i_l})$.

Задача 12. Докажите, что если слова w и w' представляют один и тот же элемент группы, т. е. $[w]=[w']$, то

$$N(w', t) \equiv N(w, t) \pmod 2 \text{ для любого } t \in T$$

(проверьте, что четность не меняется при элементарном преобразовании слова).

Задача 13. Пусть $[w] = g$. Докажите, что

$$l(g) = |\{t \in T \mid N(w, t) \equiv 1 \pmod 2\}|\,.$$

Задача 14. Докажите правило вычеркивания для группы Кокстера G: если $s \in S$, $s_{i_1} \ldots s_{i_l}$ — кратчайшая запись элемента g через образующие, и $l(sg) < l(g)$, то у элемента sg существует кратчайшая запись вида $s_{i_1} \ldots \hat{s}_{i_k} \ldots s_{i_l}$.

Список литературы

[1] Андреев Е. М. *О пересечении плоскостей граней многогранников с острыми углами* // Мат.заметки, 1970. Т. 8, №4. С. 521–527.

[2] Бурбаки Н. *Группы и алгебры Ли. Гл. IV, V, VI.* М.: Мир, 1972 (глава IV).

[3] Винберг Э. Б. *Калейдоскопы и группы отражений* // Математическое просвещение, 2003. Сер. 3. Вып. 7. С. 45–63.

[4] Винберг Э. Б. *Линейные представления групп.* Приложение 2. М.: Наука, 1985.

[5] Коксетер Г. С., Мозер У. О. *Порождающие элементы и определяющие соотношения дискретных групп.* М.: Наука, 1980.

[6] Новиков П. С. *Об алгоритмической неразрешимости проблемы тождества слов в теории групп* // Труды МИАН СССР, 1955. Т. 44. С. 3–143.

[7] Aschbacher A. *Finite group theory.* Cambridge Univ. Press, 1986.

[8] Brown K. *Buildings.* Springer, 1989.

[9] Deodhar V. V. *Some characterizations of Coxeter groups* // L'Enseignement Mathematique, 1986. Vol. 32. P. 111–120.

[10] Gutkin E. *Geometry and combinatorics of groups generated by reflections* // L'Enseignement Mathematique, 1986. Vol. 32. P. 95–110.

[11] Tits J. *Le probleme des mots dans les groupes de Coxeter* // Sympozia Math (INDAM). Vol. 1. Academic Press, London, 1969. P. 175–185.