УДК 512.543.76

В. В. Беняш-Кривец

О разложимости конечно порожденных групп в свободное произведение с объединенной подгруппой

В работе исследуется проблема, когда конечно порожденная группа Γ разложима в нетривиальное свободное произведение с объединенной подгруппой. Доказано, что если $\dim X^s(\Gamma) \geqslant 2$, где $X^s(\Gamma)$ – многообразие характеров неприводимых представлений Γ в $\mathrm{SL}_2(\mathbb{C})$, то Γ является нетривиальным свободным произведением с объединенной подгруппой. Далее, мы рассматриваем случай, когда $\Gamma = \langle a, b \mid a^n = b^k = R^m(a,b)\rangle$ является обобщенной треугольной группой. Доказано, что если одна из образующих Γ имеет бесконечный порядок, то Γ является нетривиальным свободным произведением с объединенной подгруппой. В общем случае найдены некоторые достаточные условия для того, чтобы Γ являлась нетривиальным свободным произведением с объединенной подгруппой.

Библиография: 26 названий.

Введение

Будем говорить, что группа G является нетривиальным свободным произведением с объединенной подгруппой, если $G = G_1 *_A G_2$, где $G_1 \neq A \neq G_2$ (см. [1]). Уолл [2] поставил следующий вопрос:

Какие группы с одним соотношением являются нетривиальным свободным произведением с объединенной подгруппой?

Пусть $G = \langle g_1, \dots, g_m \mid R_1 = \dots = R_n = 1\rangle$ – группа с m образующими и n соотношениями такая, что $\operatorname{def} G = m - n \geqslant 2$. В [3] доказано, что G является нетривиальным свободным произведением с объединенной подгруппой. В частности, если G – группа с $m \geqslant 3$ образующими и одним соотношением, то G – нетривиальное свободное произведение с объединенной подгруппой. Случай групп с двумя образующими и одним соотношением более сложен. Например, свободная абелева группа $G = \langle a, b \mid [a,b] = 1\rangle$ ранга 2, где $[a,b] = aba^{-1}b^{-1}$, очевидно, не является нетривиальным свободным произведением с объединенной подгруппой. Другой пример дает группа $G_n = \langle a, b \mid aba^{-1} = b^n\rangle$. Для любого n группа G_n разрешима, и, используя результаты из [3], нетрудно показать, что при $n \neq -1$ группа G_n не является нетривиальным свободным произведением с объединенной подгруппой.

Следующая гипотеза высказана в [4].

Гипотеза 1. *Пусть $G = \langle a, b \mid R^m(a,b) = 1\rangle$, $m \geqslant 2$, – группа с двумя образующими и одним соотношением с кручением. Тогда G является нетривиальным свободным произведением с объединенной подгруппой.*

Работа профинансирована Институтом математики НАН Беларуси в рамках государственной программы фундаментальных исследований “Математические структуры”.

Цишанг [5] исследовал проблему разложения в свободное произведение с объединенной подгруппой для вполне разрывных групп преобразований плоскости. Он дал полный ответ на вопрос, когда такая группа является свободным произведением с объединенной подгруппой, во всех случаях, за исключением групп $H_1 = \langle a, b \mid [a,b]^n = 1\rangle$ и $H_2 = \langle a, b \mid a^2 = [a,b]^n = 1\rangle$, $n \geqslant 2$. Розенбергер [6] доказал, что группы H_1 и H_2 являются свободным произведением с объединенной подгруппой в случае, когда n не является степенью 2. В недавних работах [7], [8] доказано, что H_1 является свободным произведением с объединенной подгруппой для произвольного $n \geqslant 2$. В [9], [10] дано независимое доказательство этого факта.

В предлагаемой работе мы исследуем более общий случай, а именно мы рассматриваем так называемые *обобщенные треугольные группы*, т.е. группы G, имеющие копредставление вида

$$G = \langle a, b \mid a^m = b^n = R^l(a,b) = 1\rangle,$$

где $l \geqslant 2$ и $R(a,b)$ – циклически редуцированное слово в свободной группе, порожденной a, b. Не все из этих групп разложимы в нетривиальное свободное произведение с объединенной подгруппой. Например, Цишанг [5] доказал, что *обычная треугольная группа*

$$T(m,n,l) = \langle a, b \mid a^m = b^n = (ab)^l = 1\rangle,$$

где $m, n, l \geqslant 2$, не является свободным произведением с объединенной подгруппой. С другой стороны, в [10] показано, что группа $G = \langle a, b \mid a^{2m} = R^l(a,b) = 1\rangle$, где $m \geqslant 0$, $l \geqslant 2$, является свободным произведением с объединенной подгруппой. Теоремы 2 и 3 предлагаемой работы содержат более общие результаты о разложимости обобщенных треугольных групп в нетривиальное свободное произведение с объединенной подгруппой.

В теореме 1 мы доказываем, что конечно порожденная группа Γ является свободным произведением с объединенной подгруппой, если размерность некоторого алгебраического многообразия (так называемого многообразия характеров неприводимых представлений группы Γ в $\mathrm{SL}_2(\mathbb{C})$) больше 1. Чтобы сформулировать этот результат, напомним некоторые обозначения и факты из геометрической теории представлений (см. также [11]–[14]).

Пусть $\Gamma = \langle g_1, \ldots, g_m\rangle$ – конечно порожденная группа и $G \subset \mathrm{GL}_n(K)$ – связная линейная алгебраическая группа, определенная над алгебраически замкнутым полем K нулевой характеристики. Очевидно, для любого гомоморфизма $\rho\colon \Gamma \to G(K)$ набор элементов

$$(\rho(g_1), \ldots, \rho(g_m)) \in G(K)^m = G(K) \times \cdots \times G(K)$$

удовлетворяет всем определяющим соотношениям группы Γ. Поэтому соответствие $\rho \to (\rho(g_1), \ldots, \rho(g_m))$ является биекцией между множеством $\mathrm{Hom}(\Gamma, G(K))$ и множеством K-точек некоторого аффинного K-многообразия $R(\Gamma, G) \subset G^m$. Многообразие $R(\Gamma, G)$ обычно называют многообразием представлений группы Γ в алгебраическую группу G.

Группа G действует на $R(\Gamma, G)$ естественным образом (одновременным сопряжением компонент), и ее орбиты находятся во взаимно однозначном соответствии с классами эквивалентных представлений Γ. В общем случае орбиты группы G

относительно этого действия не обязательно замкнуты, и, следовательно, многообразие орбит (геометрический фактор) не является алгебраическим многообразием. Однако если G – редуктивная группа, то можно рассмотреть категорный фактор $X(\Gamma, G) = R(\Gamma, G)/G$ (см. [15]). Его точки параметризуют замкнутые G-орбиты. В случае $G = \mathrm{GL}_n(K)$ или $G = \mathrm{SL}_n(K)$ орбита G замкнута тогда и только тогда, когда соответствующее представление вполне приводимо. Поэтому в этом случае точки многообразия $X(\Gamma, G)$ находятся во взаимно однозначном соответствии с классами эквивалентных вполне приводимых представлений группы Γ в G или, другими словами, с характерами представлений Γ в G.

Всюду ниже мы будем рассматривать лишь случай $G = \mathrm{SL}_2(K)$ и для краткости обозначать $R(\Gamma, \mathrm{SL}_2(K)) = R(\Gamma)$, $X(\Gamma, \mathrm{SL}_2(K)) = X(\Gamma)$. Все используемые ниже сведения о многообразиях $R(\Gamma)$, $X(\Gamma)$ можно найти в [12]; [16]–[18]. Положим

$$R^s(\Gamma) = \{\rho \in R(\Gamma) : \rho \ \text{ неприводимо}\}, \qquad X^s(\Gamma) = \pi(R^s(\Gamma)),$$

где $\pi\colon R(\Gamma) \to X(\Gamma)$ – каноническая проекция. В [12] показано, что $R^s(\Gamma)$, $X^s(\Gamma)$ – открытые в топологии Зарисского подмножества $R(\Gamma)$, $X(\Gamma)$ соответственно.

Цель настоящей работы – доказать следующие теоремы.

Теорема 1. *Пусть Γ – конечно порожденная группа такая, что $\dim X^s(\Gamma) \geqslant 2$. Тогда Γ является нетривиальным свободным произведением с объединенной подгруппой.*

Теорема 2. *Пусть $\Gamma_n = \langle a, b \mid a^n = b^k = R^m(a, b) = 1\rangle$, где $n, k, m \in \mathbb{Z}$, $n, k, m \geqslant 2$, и $R(a, b) = a^{u_1} b^{v_1} \cdots a^{u_s} b^{v_s}$ – такое слово, что $0 < u_i < n$, $0 < v_i < k$ и $s \geqslant 1$. Предположим, что существует $i \in \{1, \dots, s\}$ с $|u_i| \geqslant 2$. Кроме того, предположим, что $n = u_i p f$, где $f \in \mathbb{Z}$, p – простое число и $u_i p$ не делит u_j при $j \neq i$. Тогда в следующих случаях группа Γ_n является нетривиальным свободным произведением с объединенной подгруппой.*

1) *$m = 2$, p не принадлежит некоторому конечному множеству простых чисел S. Множество S полностью определяется показателем k и словом R.*
2) *$m = 3$ или $m = 2^l > 3$, $p \neq 2$.*
3) *$m > 3$ и $m \neq 2^l$.*

Отметим, что условие $u_i p \nmid u_j$ при $j \neq i$ в теореме 2 выполняется автоматически, если $u_i = \max_{1 \leqslant j \leqslant s} u_j \geqslant 2$ либо $u_i \nmid u_j$ для любого $j \neq i$.

Теорема 3. *Пусть $\Gamma = \langle a, b \mid a^n = R^m(a, b) = 1\rangle$, где $n = 0$ или $n \geqslant 2$, $m \geqslant 2$, $R(a, b) = a^{u_1} b^{v_1} \cdots a^{u_s} b^{v_s}$, $s \geqslant 1$, $v_i \neq 0$, $0 < u_i < n$. Тогда Γ является нетривиальным свободным произведением с объединенной подгруппой.*

В качестве непосредственного следствия теоремы 3 получаем доказательство гипотезы 1.

Следствие 1. *Пусть $\Gamma = \langle a, b \mid R^m(a, b) = 1\rangle$, $m \geqslant 2$, – группа с двумя образующими и одним соотношением с кручением. Тогда Γ является нетривиальным свободным произведением с объединенной подгруппой.*

В конце § 2 мы покажем, что группа Γ из следствия 1 при $m \geqslant 3$ удовлетворяет условию теоремы 1, т.е. $\dim X^s(\Gamma) \geqslant 2$, так что мы получаем другое доказательство гипотезы 1.

Следствие 2. *Фуксовы группы* $H_1 = \langle a, b \mid [a,b]^n = 1\rangle$ *и* $H_2 = \langle a, b \mid a^2 = [a,b]^n = 1\rangle$, $n \geqslant 2$, *являются нетривиальным свободным произведением с объединенной подгруппой.*

§ 1. Доказательство теоремы 1

Ниже через $\mathbb{Q}_p$ мы будем обозначать поле p-адических чисел, $\mathbb{Z}_p$ – кольцо целых p-адических чисел, $\mathbb{Z}_p^*$ – группу обратимых элементов в $\mathbb{Z}_p$, $|\cdot|_p$ – p-адическое нормирование, $\operatorname{tr} A$ – след матрицы A, E – единичную матрицу второго порядка.

Напомним некоторые сведения о многообразии характеров $X(\Gamma)$ представлений конечно порожденной группы Γ в $\mathrm{SL}_2(\mathbb{C})$ (см. [12]). Для произвольного элемента $g \in \Gamma$ рассмотрим регулярную функцию

$$\tau_g : R(\Gamma) \to \mathbb{C}, \qquad \tau_g(\rho) = \operatorname{tr}\rho(g).$$

Обычно τ_g называют *характером Фрике* элемента g. Известно, что $\mathbb{Z}$-алгебра $T(\Gamma)$, порожденная всеми функциями τ_g, $g \in \Gamma$, является конечно порожденной. Более того, если $\tau_{g_1}, \dots, \tau_{g_s}$ – образующие $T(\Gamma)$, то $\mathbb{C}$-алгебра $\mathrm{SL}_2(\mathbb{C})$-инвариантных регулярных функций $\mathbb{C}[R(\Gamma)]^{\mathrm{SL}_2(\mathbb{C})}$ совпадает с $\mathbb{C}[\tau_{g_1}, \dots, \tau_{g_s}]$. Рассмотрим морфизм

$$\pi : R(\Gamma) \to \mathbb{A}^s, \qquad \pi(\rho) = (\tau_{g_1}(\rho), \dots, \tau_{g_s}(\rho)).$$

В [12] показано, что образ $\pi(R(\Gamma))$ замкнут в $\mathbb{A}^s$. Поскольку $X(\Gamma)$ и $\pi(R(\Gamma))$ бирегулярно изоморфны, то в дальнейшем мы будем отождествлять $X(\Gamma)$ и $\pi(R(\Gamma))$.

Идея доказательства теоремы 1 состоит в том, чтобы построить представление $\rho : \Gamma \to \mathrm{SL}_2(\mathbb{Q}_p)$ для некоторого простого p такое, что группа $\rho(\Gamma)$ плотна в $\mathrm{SL}_2(\mathbb{Q}_p)$ в p-адической топологии. После этого теорема 1 будет следовать из следующих хорошо известных фактов.

1) Если H – плотная в p-адической топологии подгруппа $\mathrm{SL}_2(\mathbb{Q}_p)$, то H является нетривиальным свободным произведением с объединенной подгруппой (см. [19]).

2) Если $f : G_1 \to G_2$ – эпиморфизм групп и G_2 – нетривиальное свободное произведение с объединенной подгруппой, то и G_1 – также нетривиальное свободное произведение с объединенной подгруппой.

Будем говорить, что подгруппа $H \subset \mathrm{SL}_2(\mathbb{Q}_p)$ неограничена, если H не содержится в группе $\mathrm{SL}_2(\mathbb{Z}_p[p^{-s}])$ для любого $s \geqslant 1$.

Лемма 1. *Пусть H – подгруппа* $\mathrm{SL}_2(\mathbb{Q}_p)$. *Тогда H плотна в* $\mathrm{SL}_2(\mathbb{Q}_p)$ *в p-адической топологии тогда и только тогда, когда H абсолютно неприводима (т.е. неприводима над алгебраическим замыканием* $\mathbb{Q}_p$*), неограничена, недискретна и не содержится в нормализаторе максимального тора.*

Доказательство. Если H плотна в $\mathrm{SL}_2(\mathbb{Q}_p)$ в p-адической топологии, то утверждение леммы очевидно. Докажем обратное утверждение. Пусть $\overline{H}$ – замыкание H в p-адической топологии. Тогда $\overline{H}$ является p-адической группой Ли. Пусть $\mathfrak{h}$ и $\mathfrak{s}$ – алгебры Ли групп $\overline{H}$ и $\mathrm{SL}_2(\mathbb{Q}_p)$ соответственно. Покажем вначале, что $\mathfrak{h} = \mathfrak{s}$. Для этого в силу [7; теорема 4.6] достаточно показать, что алгебра $\mathfrak{h}$ неразрешима. Допустим противное. Тогда $\overline{H}$ содержит открытую разрешимую подгруппу G (см. [20; гл. 4]). Пусть

$$\Gamma_j = \left\{ \begin{pmatrix} 1+p^j a & p^j b \\ p^j c & 1+p^j d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Q}_p) : a,b,c,d \in \mathbb{Z}_p \right\}, \qquad j \geqslant 0,$$

– главная конгруэнц-подгруппа уровня j в $\mathrm{SL}_2(\mathbb{Q}_p)$. Группы Γ_j, $j \geqslant 0$, образуют базу окрестностей единицы в $\mathrm{SL}_2(\mathbb{Q}_p)$. Поэтому без ограничения общности мы можем считать, что $G = \Gamma_j \cap \overline{H}$ для некоторого $j \geqslant 2$. Недискретность $\overline{H}$ влечет, что G недискретна. В частности, для любого $i > j$ группа $G_i = \Gamma_i \cap \overline{H} \subset G$ бесконечна.

Покажем, что G приводима над $\overline{\mathbb{Q}}_p$. В самом деле, в противном случае в силу [21; следствие 2] G содержит нормальную абелеву подгруппу A индекса 2 и для любого $x \in G \setminus A$ мы имеем $\operatorname{tr} x = 0$. С другой стороны, если $x \in \mathrm{SL}_2(\mathbb{Q}_p)$ и $\operatorname{tr} x = 0$, то $x \notin \Gamma_i$ при $i > 1$, следовательно, $x \notin G$ – противоречие.

Чтобы завершить доказательство неразрешимости $\mathfrak{h}$, рассмотрим следующие случаи.

1) G – абелева группа. Тогда так как H асолютно неприводима и не содержится в нормализаторе максимального тора, существует $x \in H$ такой, что $xGx^{-1} \cap G = \{E\}$. Таким образом, мы получаем, что $\{E\}$ – открытая подгруппа в G, т.е. G дискретна – противоречие.

2) G – неабелева группа. Тогда без ограничения общности мы можем считать, что все G_i неабелевы при $i > j$ (в противном случае мы можем положить $G = G_i$ для некоторого i). Тогда коммутант $U = [G, G]$ – нетривиальная абелева унипотентная подгруппа в G. В силу абсолютной неприводимости H существует $x \in H$ такой, что $xUx^{-1} \cap U = \{E\}$. С другой стороны, так как xGx^{-1} – открытая подгруппа, то найдется такое i, что $G_i \subset xGx^{-1}$. Так как G_i неабелева, то $V = [G_i, G_i] \neq \{E\}$ и легко видеть, что $V \subset xUx^{-1} \cap U$ – противоречие.

Итак, мы показали, что $\mathfrak{h} = \mathfrak{s}$. Тогда найдется конгруэнц-подгруппа Γ_i такая, что $\Gamma_i \subset \overline{H}$ (см. [22; гл. 5]). В частности, $\overline{H}$ содержит унипотентные подгруппы вида

$$U_1 = \left\{ \begin{pmatrix} 1 & 0 \\ p^i a & 1 \end{pmatrix} : a \in \mathbb{Z}_p \right\}, \qquad U_2 = \left\{ \begin{pmatrix} 1 & p^i a \\ 0 & 1 \end{pmatrix} : a \in \mathbb{Z}_p \right\}.$$

Далее, неограниченность H означает, что найдется элемент $h \in H$ такой, что $|\operatorname{tr} h|_p > 1$. В самом деле, если мы предположим противное, то следы всех элементов из H принадлежат $\mathbb{Z}_p$, откуда группа H сопряжена подгруппе $\mathrm{SL}_2(\mathbb{Z}_p)$ (см. [23] или [12; лемма I.4.3]), т.е. H ограничена. Это противоречит условию теоремы. Покажем, что собственные значения матрицы h принадлежат $\mathbb{Q}_p$. Пусть $\operatorname{tr} h = p^{-s}\alpha$, где $\alpha \in \mathbb{Z}_p^*$, $s > 0$. Тогда характеристический многочлен h имеет вид $f(y) = y^2 - p^{-s}\alpha y + 1$, а его дискриминант равен $D = p^{-2s}\alpha^2 - 4 = p^{-2s}(\alpha^2 - 4p^{2s})$. Таким образом, D является квадратом в $\mathbb{Q}_p$, следовательно, корни $f(y)$ лежат в $\mathbb{Q}_p$. Итак, h сопряжен в $\mathrm{GL}_2(\mathbb{Q}_p)$ с диагональной матрицей вида

$$\operatorname{diag}(\lambda, \lambda^{-1}), \qquad \lambda = p^{-s}\gamma, \quad s > 0, \quad \gamma \in \mathbb{Z}_p^*.$$

Без ограничения общности мы можем считать, рассматривая при необходимости сопряженную с H группу, что $h = \operatorname{diag}(\lambda, \lambda^{-1}) \in H$. Теперь легко показать, что $\overline{H}$ содержит следующие унипотентные подгруппы в $\mathrm{SL}_2(\mathbb{Q}_p)$:

$$V_1 = \left\{ \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix} : a \in \mathbb{Q}_p \right\}, \qquad V_2 = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} : a \in \mathbb{Q}_p \right\}.$$

В самом деле, пусть $x = \begin{pmatrix} 1 & 0 \\ p^r\beta & 1 \end{pmatrix} \in V_1$, где $r < i$ и $\beta \in \mathbb{Z}_p^*$. Выберем m так, чтобы $2sm + r \geqslant i$. Тогда легко видеть, что $h^m x h^{-m} \in U_1$, следовательно, $x \in \overline{H}$.

Таким образом, $V_1 \subset \overline{H}$. Аналогично, $V_2 \subset \overline{H}$. Хорошо известно, что подгруппы V_1 и V_2 порождают $\mathrm{SL}_2(\mathbb{Q}_p)$. Следовательно, $\overline{H} = \mathrm{SL}_2(\mathbb{Q}_p)$, что и требовалось показать. Лемма 1 доказана.

Лемма 2. *Пусть X, Y – неприводимые $\mathbb{Q}$-определенные аффинные многообразия, $\dim Y \geqslant 1$, и пусть $f\colon X \to Y$ – доминантный $\mathbb{Q}$-определенный регулярный морфизм. Тогда существуют простое $p \neq 2$ и точка $x \in X(\mathbb{Q}_p)$ такие, что не все координаты точки $f(x) \in Y(\mathbb{Q}_p)$ принадлежат кольцу $\mathbb{Z}_p$.*

Доказательство. Пусть K – алгебраическое замыкание поля $\mathbb{Q}$. Пусть D – произвольная неприводимая кривая в $Y(K)$, и пусть $L \subset f^{-1}(D)$ – произвольная неприводимая кривая такая, что $f(L)$ плотно в D. Пусть $\overline{D}$ и $\overline{L}$ – проективные замыкания D и L соответственно, а $\widetilde{L}$ – гладкая проективная модель $\overline{L}$. Регулярный морфизм $f\colon L \to D$ определяет рациональный морфизм $\widetilde{f}: \widetilde{L} \to \overline{D}$. Так как каждый рациональный морфизм из гладкой кривой в проективное многообразие регулярен, а образ проективного многообразия при регулярном отображении замкнут (см. [24]), то $\widetilde{f}$ – регулярный сюръективный морфизм. Пусть $v \in \overline{D} \setminus D$ – бесконечно удаленная точка на $\overline{D}$, и пусть $w \in \widetilde{f}^{-1}(v)$. Координаты точек v и w порождают конечное расширение $K_1/\mathbb{Q}$. По теореме плотности Н.Г. Чеботарева существует бесконечно много простых p таких, что $K_1 \subset \mathbb{Q}_p$. Выберем одно из таких p. Тогда $w \in \widetilde{L}(\mathbb{Q}_p)$, $v \in \overline{D}(\mathbb{Q}_p)$. Так как w – простая точка на $\widetilde{L}$, то w имеет p-адическую окрестность $W \subset \widetilde{L}(\mathbb{Q}_p)$ такую, что W гомеоморфна открытому диску в $\mathbb{Q}_p$ (см. [24; глава II]). Это означает, что существует бесконечная последовательность элементов $w_i \in W$ таких, что $w_i \in L(\mathbb{Q}_p)$ и $\lim_{i\to\infty} w_i = w$ в p-адической топологии. Тогда в силу непрерывности $\widetilde{f}$ мы имеем $\lim_{i\to\infty} \widetilde{f}(w_i) = v$. Поскольку $v \in \overline{D}(\mathbb{Q}_p)$ является бесконечно удаленной точкой, то последовательность элементов $f(w_i) = \widetilde{f}(w_i) \in D(\mathbb{Q}_p)$ не ограничена. Это означает, что найдется такое i, что не все координаты точки $f(w_i)$ принадлежат $\mathbb{Z}_p$. Лемма 2 доказана.

Доказательство теоремы 1. Пусть элементы $g_1, \dots, g_s \in \Gamma$ таковы, что функции $\tau_{g_1}, \dots, \tau_{g_s}$ порождают кольцо $T(\Gamma)$. Тогда проекция $\pi\colon R(\Gamma) \to X(\Gamma)$ определяется формулой $\pi(\rho) = (\tau_{g_1}(\rho), \dots, \tau_{g_s}(\rho))$. Так как по условию теоремы 1 мы имеем $\dim X^s(\Gamma) \geqslant 2$, то найдется неприводимая компонента Z замыкания $\overline{X^s(\Gamma)}$ в топологии Зарисского такая, что $\dim Z \geqslant 2$ и $U = Z \cap X^s(\Gamma) \neq \varnothing$. Пусть Z_1 – содержащая Z неприводимая компонента $X(\Gamma)$. Так как $X^s(\Gamma)$ открыто в $X(\Gamma)$ и $X^s(\Gamma) \cap Z_1 = U$, то множество U, а следовательно и Z, плотно в Z_1 в топологии Зарисского, т.е. $Z = Z_1$. Пусть $p_i\colon Z \to \mathbb{A}^1$ – проекция, определяемая формулой $p_i(z_1, \dots, z_s) = z_i$. Так как $\dim Z \geqslant 2$, то существует такое i, что проекция p_i доминантна, следовательно, $p_i(U)$ плотно в $\mathbb{A}^1$ в топологии Зарисского. Поэтому найдется целое число $n > 2$ такое, что $n \in p_i(U)$. Пусть $Y = p_i^{-1}(n) \subset Z$. Тогда по теореме о размерности слоев морфизма $\dim Y \geqslant \dim Z - 1 \geqslant 1$ и $Y \cap U \neq \varnothing$. Далее, пусть X – такая неприводимая компонента $\pi^{-1}(Y)$, что $\pi(X)$ плотно в Y. Применяя лемму 2 к многообразиям X, Y и морфизму π, мы получаем, что существует такое простое p, что $R(\mathbb{Q}_p)$ содержит представление ρ со следующим свойством: ρ неприводимо и не все координаты точки $\pi(\rho)$ принадлежат $\mathbb{Z}_p$. Последнее означает, что найдется j такое, что $\tau_{g_j}(\rho) = \operatorname{tr}\rho(g_j) \notin \mathbb{Z}_p$. Следовательно, группа $\rho(\Gamma)$ – неограниченная подгруппа $\mathrm{SL}_2(\mathbb{Q}_p)$. Кроме того, из построения представления ρ следует, что $\tau_{g_i}(\rho) = \operatorname{tr}\rho(g_i) = n > 2$. Таким образом, циклическая подгруппа в $\rho(\Gamma)$, порожденная $\rho(g_i)$, бесконечна и ограничена. Следовательно, $\rho(\Gamma)$ – недискретная подгруппа $\mathrm{SL}_2(\mathbb{Q}_p)$.

Теперь, если $\rho(\Gamma)$ не содержится в нормализаторе максимального тора, то в силу леммы 1 $\rho(\Gamma)$ плотна в $\mathrm{SL}_2(\mathbb{Q}_p)$ в p-адической топологии, откуда $\rho(\Gamma)$ (а следовательно Γ) является нетривиальным свободным произведением с объединенной подгруппой.

Предположим, что $\rho(\Gamma)$ содержится в нормализаторе максимального тора. Покажем, что существует эпиморфизм $f\colon \rho(\Gamma) \to D_\infty$, где $D_\infty = \langle c, d \mid dcd^{-1} = c^{-1}, d^2 = 1\rangle = \mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/2\mathbb{Z}$ – бесконечная группа диэдра. В самом деле, поскольку по построению $\rho(\Gamma)$ абсолютно неприводима и бесконечна, то в силу [21; следствие 2] $\rho(\Gamma)$ содержит нормальную абелеву подгруппу A индекса 2 и для любых $x \in G \setminus A$, $a \in A$ мы имеем $\operatorname{tr} x = 0$, т.е. $x^2 = -E$, и $xax^{-1} = a^{-1}$. Пусть $\rho(\Gamma) = A \cup xA$ – разложение $\rho(\Gamma)$ на два смежных класса. Так как A бесконечна, то существует эпиморфизм $f\colon A \to C$, где $C = \langle c\rangle$ – бесконечная циклическая подгруппа в D_∞, порожденная c. Положим $f(xa) = df(a)$ для произвольного $a \in A$. Легко проверить, что мы имеем корректно определенное отображение $f\colon \rho(\Gamma) \to D_\infty$ и что f является эпиморфизмом. Так как D_∞ – нетривиальное свободное произведение, то $\rho(\Gamma)$ (а следовательно Γ) является нетривиальным свободным произведением с объединенной подгруппой. Теорема 1 доказана.

§ 2. Некоторые вспомогательные результаты

В этом параграфе мы докажем ряд вспомогательных результатов, используемых при доказательстве теорем 2 и 3. Ниже будем обозначать кольцо целых алгебраических чисел в $\mathbb{C}$ через $\mathscr{O}$, группу обратимых элементов в $\mathscr{O}$ через $\mathscr{O}^*$, свободную группу ранга 2 с образующими g и h через $F_2 = \langle g, h\rangle$, наибольший общий делитель целых чисел a и b через (a, b). Если $K \supset L$ – конечное расширение полей и $x \in K$, то через $N_{K/L}(x)$ мы будем обозначать норму элемента x.

Следующая лемма характеризует элементы конечного порядка в $\mathrm{SL}_2(\mathbb{C})$.

Лемма 3. *Пусть $2 < m \in \mathbb{Z}$ и $\pm E \neq X \in \mathrm{SL}_2(\mathbb{C})$. Тогда $X^m = E$ тогда и только тогда, когда $\operatorname{tr} X = \varepsilon + \varepsilon^{-1}$, где $\varepsilon^m = 1$, $\varepsilon \neq \pm 1$ (другими словами, $\operatorname{tr} X = 2\cos(2r\pi/m)$ для некоторого $r \in \{1, \dots, m-1\}$). В частности, если $\operatorname{tr} X = 0$, то $X^2 = -E$.*

Доказательство. Если $X^m = E$, то утверждение очевидно. Если $\operatorname{tr} X = \varepsilon + \varepsilon^{-1}$, то $\varepsilon, \varepsilon^{-1}$ – собственные значения матрицы X. Следовательно, X сопряжена матрице $\operatorname{diag}(\varepsilon, \varepsilon^{-1})$, т.е. $X^m = E$, что и требовалось показать.

Для свободной группы $F_2 = \langle g, h\rangle$ многообразие представлений $R(F_2)$ равно, очевидно, $\mathrm{SL}_2(\mathbb{C}) \times \mathrm{SL}_2(\mathbb{C})$. Известно, что кольцо $T(F_2)$ порождается функциями $\tau_g, \tau_h, \tau_{gh}$ (см. [12], [16], [17]). Для элемента $u \in F_2$ функцию τ_u часто называют характером Фрике элемента u.

Лемма 4. *Для произвольных $\alpha, \beta, \gamma \in \mathbb{C}$ существуют матрицы $A, B \in \mathrm{SL}_2(\mathbb{C})$ такие, что $\tau_g(A, B) = \operatorname{tr} A = \alpha$, $\tau_h(A, B) = \operatorname{tr} B = \beta$, $\tau_{gh}(A, B) = \operatorname{tr} AB = \gamma$.*

Эту лемму нетрудно доказать непосредственным вычислением.

Из леммы 4 следует, в частности, что $X(F_2) = \pi(R(F_2)) = \mathbb{A}^3$. Кроме того, функции $\tau_g, \tau_h, \tau_{gh}$ алгебраически независимы над $\mathbb{C}$ и для любого $u \in F_2$ мы

имеем
$$\tau_u = Q_u(\tau_g, \tau_h, \tau_{gh}),$$
где $Q_u \in \mathbb{Z}[x, y, z]$ – однозначно определенный многочлен с целыми коэффициентами. Многочлен Q_u обычно называют многочленом Фрике элемента u. Следующие соотношения между характерами Фрике следуют из соотношений между следами произвольных матриц в $\mathrm{SL}_2(\mathbb{C})$:
$$1)\ \ \tau_{u^{-1}} = \tau_u;\quad 2)\ \ \tau_{uv} = \tau_{vu};\quad 3)\ \ \tau_{vuv^{-1}} = \tau_u;\quad 4)\ \ \tau_{uv} = \tau_u\tau_v - \tau_{uv^{-1}}. \quad (1)$$

Далее, нам нужна более детальная информация о многочленах Фрике (см. [25]). Рассмотрим многочлены $P_n(\lambda)$, которые удовлетворяют начальным условиям
$$P_{-1}(\lambda) = 0, \qquad P_0(\lambda) = 1$$
и рекуррентному соотношению
$$P_n(\lambda) = \lambda P_{n-1}(\lambda) - P_{n-2}(\lambda).$$
Если $n < 0$, положим $P_n(\lambda) = -P_{|n|-2}(\lambda)$. Степень многочлена $P_n(\lambda)$ равна n, если $n > 0$, и равна $|n| - 2$, если $n < 0$. Индукцией по n легко проверить, что
$$P_n(2\cos(\varphi)) = \frac{\sin((n+1)\varphi)}{\sin(\varphi)}\,. \tag{2}$$
Из (2) следует, что многочлен $P_n(\lambda)$, $n \geqslant 1$, имеет n нулей, определенных формулой
$$\lambda_{n,k} = 2\cos\left(\frac{k\pi}{n+1}\right), \qquad k = 1, 2, \ldots, n. \tag{3}$$
Кроме того, по индукции легко проверить, что при $n > 0$ мы имеем
$$\begin{aligned} P_{2n}(\lambda) &= \lambda^{2n} + \cdots + (-1)^n, \\ P_{2n-1}(\lambda) &= \lambda(\lambda^{2n-2} + \cdots + (-1)^{n-1}n). \end{aligned} \tag{4}$$
Далее, пусть $w = g^{\alpha_1}h^{\beta_1}\ldots g^{\alpha_s}h^{\beta_s}$ – циклически редуцированное слово в F_2, и пусть $x = \tau_g$, $y = \tau_h$, $z = \tau_{gh}$. Рассмотрим многочлен Фрике $Q_w(x, y, z)$ как многочлен от z. Пусть
$$Q_w(x, y, z) = M_n(x, y)z^n + M_{n-1}(x, y)z^{n-1} + \cdots + M_0(x, y).$$

Лемма 5 [25]. *Степень многочлена Фрике $Q_w(x, y, z)$ относительно z равна s, т.е. равна числу блоков вида $g^{\alpha_i}h^{\beta_i}$ в w. Старший коэффициент $M_s(x, y)$ многочлена $Q_w(x, y, z)$ имеет вид*
$$M_s(x, y) = \prod_{i=1}^{s} P_{\alpha_i - 1}(x)P_{\beta_i - 1}(y). \tag{5}$$

Следующая лемма играет важную роль в доказательстве теорем 2 и 3.

Лемма 6. *Пусть* $\Gamma = \langle a, b \mid a^n = R^m(a,b) = 1\rangle$, *где* $n = 0$ *или* $n \geqslant 2$, $m \geqslant 2$ *и* $R(a,b)$ – *циклически редуцированное содержащее* b *слово в свободной группе, порожденной* a *и* b. *Предположим, что существуют такие матрицы* $A, B \in \mathrm{SL}_2(\mathbb{C})$, *что* $\operatorname{tr} A = \alpha = 2\cos(t\pi/n)$ *для некоторого* $t \in \{1, \dots, n-1\}$ *и* $\operatorname{tr} R(A,B) = Q_R(\alpha, y, z) = c$, *где* Q_R – *многочлен Фрике элемента* $R(g,h) \in F_2$, $c = 2\cos(r\pi/m)$ *для некоторого* $r \in \{1, \dots, m-1\}$, $y = \operatorname{tr} B$, $z = \operatorname{tr} AB$. *Пусть* $H = \langle A, B\rangle$ – *группа, порожденная матрицами* A *и* B. *Предположим, что выполнены следующие два условия*:

1) *существует унипотентный (либо конечного порядка) элемент* $W \in H$ *вида* $W = A^{\alpha_1}B^{\beta_1}\cdots A^{\alpha_s}B^{\beta_s}$, $\alpha_i, \beta_i \neq 0$ *для* $i = 1, \dots, s$, *такой, что* $l = \sum_{i=1}^{s}\beta_i \neq 0$;
2) *существует элемент* $h \in H$ *такой, что* $\operatorname{tr} h \notin \mathscr{O}$.

Тогда группа Γ *является нетривиальным свободным произведением с объединенной подгруппой.*

Предположим, что вместо условия 1) *выполнено следующее условие.*

1′) B *имеет конечный порядок, т.е.* $\operatorname{tr} B = 2\cos(k_1\pi/k)$ *для некоторых* $k \geqslant 2$ *и* $k_1 \in \{1, \dots, k-1\}$.

Тогда группа $\Gamma_1 = \langle a, b \mid a^n = b^{kv} = R^m(a,b) = 1\rangle$ *является нетривиальным свободным произведением с объединенной подгруппой для любого целого* v.

Доказательство этой леммы опирается на классификацию Басса конечно порожденных подгрупп в $\mathrm{SL}_2(\mathbb{C})$ [26].

Предложение 1 [26]. *Пусть* $H \subset \mathrm{GL}_2(\mathbb{C})$ – *конечно порожденная подгруппа. Тогда имеет место один из следующих случаев*:

1) *существует эпиморфизм* $f\colon H \to \mathbb{Z}$ *такой, что* $f(u) = 0$ *для всех унипотентных элементов* $u \in H$;
2) $\operatorname{tr} h \in \mathscr{O}$ *для любого элемента* $h \in H$;
3) H *является нетривиальным свободным произведением с объединенной подгруппой.*

Доказательство леммы 6. Легко видеть, что группа H из леммы не удовлетворяет случаям 1), 2) предложения 1. В самом деле, предположим, что $f\colon H \to \mathbb{Z}$ – такой эпиморфизм, что $f(z) = 0$ для любого унипотентного элемента $z \in H$. Тогда $f(A) = 0$, поскольку $A^{2n} = E$ в силу леммы 3. Далее, $f(u) = lf(B) = 0$, откуда $f(B) = 0$, поскольку по условию u либо унипотентен, либо имеет конечный порядок, а $l \neq 0$. Таким образом, $f(H) = \{0\}$ – противоречие. По условию леммы H не удовлетворяет также случаю 2) предложения 1. Следовательно, H является нетривиальным свободным произведением с объединенной подгруппой, т.е. $H = H_1 *_F H_2$, где $H_1 \neq F \neq H_2$. Пусть $\overline{A}, \overline{B}, \overline{H}, \overline{H}_1, \overline{H}_2, \overline{F}$ являются образами A, B, H, H_1, H_2, F в $\mathrm{PSL}_2(\mathbb{C})$ соответственно. Если $-E \notin H$, то группы H и $\overline{H}$ изоморфны. Если же $-E \in H$, то $-E$ лежит в центре H, следовательно, $-E \in F$. В любом из этих случаев $\overline{H}_1 \neq \overline{F} \neq \overline{H}_2$ и, следовательно, $\overline{H} = \overline{H}_1 *_{\overline{F}} \overline{H}_2$ является нетривиальным свободным произведением с объединенной подгруппой. Условия $\operatorname{tr} A = \alpha$ и $Q_R(\alpha, y, z) = c$ влекут в силу леммы 3, что $A^{2n} = R^{2m}(A,B) = E$. Следовательно, $\overline{A}^n = R^m(\overline{A}, \overline{B}) = 1$ в $\mathrm{PSL}_2(\mathbb{C})$. Таким образом, $\overline{H}$ является эпиморфным образом Γ, поэтому Γ также является нетривиальным свободным произведением с объединенной подгруппой.

Далее, если мы заменим условие 1) на 1′), то группа $\overline{H}$ снова является нетривиальным свободным произведением с объединенной подгруппой. Кроме того, мы имеем $\overline{A}^n = \overline{B}^k = R^m(\overline{A}, \overline{B}) = 1$ в $\mathrm{PSL}_2(\mathbb{C})$. Следовательно, $\overline{H}$ является эпиморфным образом Γ_1. Таким образом, Γ_1 является нетривиальным свободным произведением с объединенной подгруппой. Лемма 6 доказана.

Лемма 7. 1) *Пусть $r, s \in \mathbb{Z}$, где $s \geqslant 3$ и $(r, s) = 1$. Тогда $\cos(r\pi/s) \notin \mathcal{O}$.*

2) *Пусть $s \in \mathbb{Z}$, $s \geqslant 1$, и $r \not\equiv 0 \pmod{2s+1}$. Тогда $2\cos(r\pi/(2s+1)) \in \mathcal{O}^*$.*

3) *Пусть $0 \neq u \in \mathbb{Z}$, p – некоторое простое число и ε – примитивный корень из 1 степени $4pu$. Положим*

$$x_r = 2\cos\left(\frac{r\pi}{2pu}\right), \qquad y_r = 2\sin\left(\frac{r\pi}{2pu}\right), \qquad K = \mathbb{Q}(\varepsilon).$$

Тогда существуют $r, r_1 \not\equiv 0 \pmod p$ такие, что p делит оба числа $N_{K/\mathbb{Q}}(x_r)$ и $N_{K/\mathbb{Q}}(y_{r_1})$. В частности, $x_r, y_{r_1} \notin \mathcal{O}^*$.

4) *Пусть $u, c \in \mathbb{Z}$, $|u| \geqslant 2$, $c \neq 0$, и пусть p – простое число, не делящее c. Положим $x_0 = -2\cos(\pi/u)$, $x_r = 2\cos(r\pi/(pu))$. Тогда существует $r \not\equiv 0 \pmod p$ такое, что $c/(x_r - x_0) \notin \mathcal{O}$.*

5) *Пусть $p > 2$ – простое число. Тогда для любого $r \not\equiv 0 \pmod p$ и $s \geqslant 1$ имеем $\sin(r\pi/p^s) \notin \mathcal{O}^*$.*

6) *Пусть $t \geqslant 1$. Тогда для любого нечетного r имеем $2\sin(r\pi/2^t) \notin \mathcal{O}^*$.*

Доказательство. 1) Предположим, что $\cos(r\pi/s) \in \mathcal{O}$. Тогда для любого $d \in \mathbb{Z}$ имеем $\cos(dr\pi/s) \in \mathcal{O}$. Поскольку по условию $(r, s) = 1$, то для любого целого l найдется такое d, что $dr \equiv l \pmod s$. Следовательно, для любого целого l мы имеем $\cos(l\pi/s) \in \mathcal{O}$. В силу (3) многочлен $P_{s-1}(\lambda)$ имеет корни $2\cos(l\pi/s)$, $l = 1, \dots, s-1$. Тогда многочлен $P_{s-1}(2\lambda)$ имеет корни $\cos(l\pi/s)$, $l = 1, \dots, s-1$. Если $s = 2s_1 + 1$ нечетно, то в силу (4) мы имеем $P_{2s_1}(2\lambda) = 2^{2s_1}\lambda^{2s_1} + \dots + (-1)^{s_1}$. Поскольку $1/2^{2s_1} \notin \mathbb{Z}$, то $P_{2s_1}(2\lambda)$ имеет корень, не принадлежащий $\mathcal{O}$, т.е. найдется такое l, что $\cos(l\pi/s) \notin \mathcal{O}$ – противоречие. Если $s = 2s_1$ четно, то (4) влечет, что $P_{2s_1-1}(2\lambda) = 2\lambda(2^{2s_1-2}\lambda^{2s_1-2} + \dots + (-1)^{s_1-1}s_1)$. По условию $s \geqslant 3$, следовательно, $s_1 \geqslant 2$. Тогда $s_1/2^{2s_1-2} \notin \mathbb{Z}$ и $P_{2s_1-1}(2\lambda)$ имеет корень, не принадлежащий $\mathcal{O}$. Снова мы получили противоречие, доказывающее п. 1).

2) В силу (3), (4) число $2\cos(r\pi/(2s+1))$ является корнем многочлена $P_{2s}(\lambda) = \lambda^{2s} + \dots + (-1)^s$ и, следовательно, принадлежит $\mathcal{O}^*$.

3) Поскольку $y_r = 2\cos((pu - r)\pi/(2pu)) = x_{pu-r}$, то достаточно доказать утверждение для x_r. Пусть $u = p^f u'$, где $f \geqslant 0$, $p \nmid u'$, и пусть $r = r_1 u'$, где $p \nmid r_1$. Тогда $x_r = 2\cos(r_1\pi/(2p^{f+1}))$. В силу (3), (4) многочлен

$$P_{2p^{f+1}-1}(\lambda) = \lambda(\lambda^{2p^{f+1}-2} + \dots + (-1)^{p^{f+1}-1}p^{f+1})$$

имеет корни $2\cos(r'\pi/(2p^{f+1}))$, $r' = 1, \dots, 2p^{f+1} - 1$, а многочлен

$$P_{2p^f-1}(\lambda) = \lambda(\lambda^{2p^f-2} + \dots + (-1)^{p^f-1}p^f)$$

имеет корни $2\cos(r'\pi/(2p^f))$, $r' = 1, \dots, 2p^f - 1$. Следовательно, многочлен $P_{2p^f-1}(\lambda)$ делит многочлен $P_{2p^{f+1}-1}(\lambda)$, т.е.

$$P_{2p^{f+1}-1}(\lambda) = P_{2p^f-1}(\lambda)F(\lambda), \tag{6}$$

где, как легко видеть, $F(\lambda)$ – многочлен степени $2(p^{f+1}-p^f)$ со старшим коэффициентом 1 и свободным коэффициентом p. Корнями $F(\lambda)$ являются числа $2\cos(r'\pi/(2p^{f+1}))$, $r'\not\equiv 0 \pmod p$. Легко видеть, что найдется $r_1\not\equiv 0 \pmod p$ такое, что $N_{K/\mathbb{Q}}(2\cos(r_1\pi/(2p^{f+1})))=\pm p^s$ для некоторого $s\geqslant 1$, что и требовалось показать.

4) Заметим, что

$$x_r-x_0=2\cos\left(\frac{r\pi}{pu}\right)+2\cos\left(\frac{\pi}{u}\right)=\left(2\cos\left(\frac{(r+p)\pi}{2pu}\right)\right)\left(2\cos\left(\frac{(r-p)\pi}{2pu}\right)\right).$$

Поэтому нам достаточно показать, что для некоторого $r\not\equiv 0 \pmod p$ мы имеем $c/\alpha_r\notin \mathscr{O}$, где $\alpha_r=2\cos((r+p)\pi/(2pu))$. Пусть $K_r=\mathbb{Q}(\alpha_r)$ и $d_r=[K_r:\mathbb{Q}]$. В силу доказанного выше п. 3) существует $r\not\equiv 0 \pmod p$ такое, что p делит $N_{K_r/\mathbb{Q}}(\alpha_r)$. Тогда

$$N_{K_r/\mathbb{Q}}\left(\frac{c}{\alpha_r}\right)=\frac{c^{d_r}}{N_{K_r/\mathbb{Q}}(\alpha_r)}\notin\mathbb{Z},$$

поскольку по условию $p\nmid c$. Следовательно, $c/\alpha_r\notin\mathscr{O}$, что и требовалось показать.

5) Заметим, что $1/\sin(r\pi/p^s)=2/(2\cos((p^s-2r)\pi/(2p^s)))$. Из доказательства п. 4) следует, что существует такое $r_0\not\equiv 0 \pmod p$, что

$$\frac{1}{\sin(r_0\pi/p^s)}=\frac{2}{2\cos((p^s-2r_0)\pi/(2p^s))}\notin\mathscr{O}.$$

Покажем теперь, что для любого $r\not\equiv 0 \pmod p$ имеем $\sin(r\pi/p^s)\notin\mathscr{O}$. Предположим противное. Пусть для некоторого r, $(r,p)=1$, имеем $1/\sin(r\pi/p^s)\in\mathscr{O}$. Так как $(p,r_0)=1$, то найдется такое d, что $r\equiv dr_0 \pmod{p^s}$. Тогда в силу (2) имеем

$$P_d\left(2\cos\left(\frac{r_0\pi}{p^s}\right)\right)=\frac{\sin(dr_0\pi/p^s)}{\sin(r_0\pi/p^s)}=\pm\frac{\sin(r\pi/p^s)}{\sin(r_0\pi/p^s)}\,,$$

откуда мы немедленно получаем, что

$$\frac{1}{\sin(r_0\pi/p^s)}=\pm\frac{1}{\sin(r\pi/p^s)}P_d\left(2\cos\left(\frac{r_0\pi}{p^s}\right)\right)\in\mathscr{O}$$

– противоречие.

6) При $t=1$ утверждение очевидно. Предположим, что $t>1$. В силу п. 3) найдется нечетное r_0 такое, что $2\sin(r_0\pi/2^t)\notin\mathscr{O}^*$. Покажем, что для любого нечетного r имеем $2\sin(r\pi/2^t)\notin\mathscr{O}^*$. Допустим противное. Пусть для некоторого нечетного r имеем $2\sin(r\pi/2^t)\in\mathscr{O}^*$. Легко видеть, что найдется такое целое d, что $r\equiv dr_0 \pmod{2^t}$. Тогда в силу (2) мы имеем

$$P_d\left(2\cos\left(\frac{r_0\pi}{2^t}\right)\right)=\pm\frac{2\sin(r\pi/2^t)}{2\sin(r_0\pi/2^t)}\,.$$

Последнее равенство влечет, что $2\sin(r_0\pi/2^t)\in\mathscr{O}^*$ – противоречие. Лемма 7 доказана.

Лемма 8. 1) *Пусть* $s, t \geqslant 0$. *Тогда*

$$P_s(\lambda)P_t(\lambda) = \sum_{i=0}^{t} P_{s-t+2i}(\lambda). \qquad (7)$$

2) *Многочлен* $P_s(\lambda) - P_{s-1}(\lambda)$ *имеет корни* $\lambda_r = 2\cos((2r+1)\pi/(2s+1))$, $r \in \{0, 1, \ldots, s-1\}$.

3) *Если* $\gamma = 2\cos(2r\pi/(2s+1))$, *где* $s \geqslant 1$, $r \in \{1, \ldots, s\}$, $(r, 2s+1) = 1$, *то* $P_s(\gamma) - P_{s-1}(\gamma) \notin \mathcal{O}^*$.

4) *Если* $\gamma = 2\cos((2r+1)\pi/(2s)) \neq 0$, *где* $s \geqslant 2$, $(s, 2r+1) = 1$, *то* $0 \neq P_{s-1}(\gamma) \notin \mathcal{O}^*$.

5) *Пусть* $\gamma \in \mathcal{O}$. *Предположим, что* γ *не равно* $2\cos(r\pi/s)$, *где* $r, s \in \mathbb{Z}$. *Тогда существует такое целое* $l > 0$, *что* $P_l(\gamma) \notin \mathcal{O}^*$.

Доказательство. 1) Зафиксируем s и проведем индукцию по t. Если $t = 0$, то $P_s(\lambda)P_0(\lambda) = P_s(\lambda)$. Если $t = 1$, то $P_s(\lambda)P_1(\lambda) = P_s(\lambda)\lambda = P_{s+1}(\lambda) + P_{s-1}(\lambda)$ по определению. Далее, по индукции имеем

$$\begin{aligned} P_s(\lambda)P_t(\lambda) &= P_s(\lambda)(\lambda P_{t-1}(\lambda) - P_{t-2}(\lambda)) \\ &= \lambda \sum_{i=0}^{t-1} P_{s-t+1+2i}(\lambda) - \sum_{i=0}^{t-2} P_{s-t+2+2i}(\lambda) \\ &= \sum_{i=0}^{t-1} (P_{s-t+2+2i}(\lambda) + P_{s-t+2i}(\lambda)) - \sum_{i=0}^{t-2} P_{s-t+2+2i}(\lambda) \\ &= P_{s+t}(\lambda) + \sum_{i=0}^{t-1} P_{s-t+2i}(\lambda) = \sum_{i=0}^{t} P_{s-t+2i}(\lambda), \end{aligned}$$

что и требовалось показать.

2) Принимая во внимание (2), получаем

$$P_s(\lambda_r) - P_{s-1}(\lambda_r) = \frac{\sin((2r+1)(s+1)\pi/(2s+1)) - \sin((2r+1)s\pi/(2s+1))}{\sin((2r+1)\pi/(2s+1))} = 0.$$

3) Используя (2), получаем

$$\frac{1}{P_s(\gamma) - P_{s-1}(\gamma)} = \frac{\sin(2r\pi/(2s+1))}{2\sin(r\pi/(2s+1))\cos(r\pi)} = \pm\cos\left(\frac{r\pi}{2s+1}\right) \notin \mathcal{O}$$

в силу п. 1) леммы 7.

4) Используя (2), имеем

$$\frac{1}{P_{s-1}(\gamma)} = \frac{\sin((2r+1)\pi/(2s))}{\sin((2r+1)\pi/2)} = (-1)^r \cos\left(\frac{(s-2r-1)\pi}{2s}\right) \notin \mathcal{O}$$

в силу п. 1) леммы 7.

5) Поскольку в силу (3) многочлен $P_l(\lambda)$ имеет корни $2\cos(r\pi/(l+1))$, $r = 1, \ldots, l$, то можно записать $P_l(\gamma) = \prod_{r=1}^{l}(\gamma - 2\cos(r\pi/(l+1)))$. Следовательно, нам достаточно показать, что $\gamma - (\varepsilon + \varepsilon^{-1}) \notin \mathcal{O}^*$, где $\varepsilon \neq \pm 1$ – некоторый корень из 1.

Пусть $f(\lambda)$ – неприводимый над $\mathbb{Q}$ многочлен для γ, K_0 – поле разложения $f(\lambda)$, и пусть $K_1 = K_0(x_0)$, где x_0 – корень уравнения $x + x^{-1} = \gamma$. Пусть Z_1 – целое замыкание $\mathbb{Z}$ в K_1 и $p \neq 2$ – некоторое простое число. Пусть $\mathfrak{p}_1$ – некоторый простой идеал в Z_1, лежащий над (p). Тогда $k_1 = Z_1/\mathfrak{p}_1 \supset \mathbb{Z}/p\mathbb{Z} = k$ – конечное расширение полей. Мы имеем $x_0, y_0 \in Z_1$. Пусть $\bar{x}_0$, $\overline{\gamma}$ – образы x_0, γ в поле k_1 соответственно. Тогда справедливо равенство

$$\bar{x}_0 + \bar{x}_0^{-1} = \overline{\gamma}.$$

Пусть $l = |k_1^*|$ – порядок мультипликативной группы поля k_1. Тогда $\bar{x}_0^l = 1$ в k_1. Пусть $K_2 = K_1(\xi)$, где ξ – примитивный корень из 1 степени l в $\mathbb{C}$. Пусть Z_2 – целое замыкание Z_1 в K_2, $\mathfrak{p}_2$ – некоторый простой идеал Z_2, лежащий над $\mathfrak{p}_1$, и $k_2 = Z_2/\mathfrak{p}_2 \supset k_1$. Обозначим через Δ группу корней из 1 степени l в K_2, а через $\overline{\Delta}$ – ее образ в k_2. Покажем, что $\overline{\Delta} = k_1^*$. Предположим противное, т.е. $\overline{\Delta} \neq k_1^*$. Тогда для некоторого целого r, $0 < r < l$, мы имеем $\overline{\xi}^r = 1$, где $\overline{\xi}$ – образ ξ в k_2. Это означает, что $\xi^r = 1 + y$, где $y \in \mathfrak{p}_2$. Тогда $(1+y)^l = 1$, т.е. $1 + C_l^1 y + \dots + C_l^l y^l = 1$, где C_l^i – соответствующий биномиальный коэффициент. Следовательно, $y(l + yy_1) = 0$, где $y_1 = C_l^2 y + \dots + C_l^l y^{l-1}$. Так как $y \neq 0$, то мы получаем, что $l \in \mathfrak{p}_2 \cap \mathbb{Z} = (p)$. Но $l = |k_1^*| = p^t - 1$ для некоторого t – противоречие. Итак, найдется корень ε из 1 степени l такой, что $\overline{\varepsilon} = \bar{x}_0$. Это означает, что $\gamma - (\varepsilon + \varepsilon^{-1}) \in \mathfrak{p}_2$ и, следовательно, $\gamma - (\varepsilon + \varepsilon^{-1})$ не является единицей в кольце $\mathscr{O}$. Лемма 8 доказана.

Лемма 9. *Пусть $F_2 = \langle g, h\rangle$ – свободная группа с образующими g и h. Положим $x = \tau_g$, $y = \tau_h$, $z = \tau_{gh}$, $t = \tau_{ghg^{-1}h^{-1}}$. Справедливы следующие утверждения.*

1) $t = x^2 + y^2 + z^2 - xyz - 2$.

2) *Пусть $R = gh(ghg^{-1}h^{-1})^s$. Тогда*

$$\tau_R = (P_s(t) - P_{s-1}(t))z.$$

3) *Пусть $T = (gh)^{-1}(ghg^{-1}h^{-1})^s(gh)^2(ghg^{-1}h^{-1})^s$. Тогда*

$$\tau_T = (t-2)P_{s-1}(t)^2 z^3 + (2 - P_{2s-1}(t) + P_{2s-2}(t))z.$$

Доказательство. 1) Равенство доказывается непосредственным вычислением с помощью соотношений (1) (см. [16]).

2) Пусть u, v – произвольные элементы F_2. Тогда, используя индукцию и соотношения (1), легко показать, что для любых целых p и q справедливо равенство

$$\tau_{u^p v^q} = P_{p-1}(\tau_u)P_{q-1}(\tau_v)\tau_{uv} - P_{p-2}(\tau_u)P_q(\tau_v) - P_p(\tau_u)P_{q-2}(\tau_v). \tag{8}$$

Положим теперь $u = gh, v = ghg^{-1}h^{-1}$. Тогда

$$\tau_u = z, \quad \tau_v = t, \quad \tau_{uv} = \tau_{gh(ghg^{-1}h^{-1})} = zt - \tau_{g^{-1}h^{-1}} = z(t-1).$$

Следовательно,

$$\begin{aligned}\tau_{uv^s} &= P_{s-1}(\tau_v)\tau_{uv} - P_{s-2}(\tau_v)\tau_u = P_{s-1}(t)(t-1)z - P_{s-2}(t)z \\ &= z(tP_{s-1}(t) - P_{s-1}(t) - P_{s-2}(t)) = z(P_s(t) + P_{s-2}(t) - P_{s-1}(t) - P_{s-2}(t)) \\ &= z(P_s(t) - P_{s-1}(t)).\end{aligned}$$

3) Пусть u, v такие же, как и выше. Тогда, используя соотношения (1), (8), мы имеем

$$\begin{aligned}\tau_{u^{-1}v^s} &= \tau_{u^{-1}}\tau_{v^s} - \tau_{uv^s} = z(P_s(t) - P_{s-2}(t)) - z(P_s(t) - P_{s-1}(t))\\ &= z(P_{s-1}(t) - P_{s-2}(t));\\ \tau_{u^2v^s} &= \tau_u\tau_{uv^s} - \tau_{v^s} = z^2(P_s(t) - P_{s-1}(t)) - P_s(t) + P_{s-2}(t);\\ \tau_{u^3} &= z^3 - 3z.\end{aligned}$$

Следовательно,

$$\begin{aligned}\tau_{u^{-1}v^su^2v^s} = \tau_{u^{-1}v^s}\tau_{u^2v^s} - \tau_{u^3} &= z^3\big((P_s(t) - P_{s-1}(t))(P_{s-1}(t) - P_{s-2}(t)) - 1\big)\\ &+ z\big(3 - (P_{s-1}(t) - P_{s-2}(t))(P_s(t) - P_{s-2}(t))\big).\end{aligned}$$

Упростим полученное выражение, используя (7). Вначале рассмотрим коэффициент при z^3:

$$\begin{aligned}&(P_s(t) - P_{s-1}(t))(P_{s-1}(t) - P_{s-2}(t)) - 1\\ &\quad= P_s(t)P_{s-1}(t) + P_{s-1}(t)P_{s-2}(t) - P_s(t)P_{s-2}(t) - P_{s-1}(t)^2 - 1\\ &\quad= P_{s-1}(t)(P_s(t) + P_{s-2}(t)) - \sum_{i=1}^{s-1} P_{2i}(t) - P_0(t) - P_{s-1}(t)^2\\ &\quad= tP_{s-1}(t)^2 - 2P_{s-1}(t)^2 = (t-2)P_{s-1}(t)^2.\end{aligned}$$

Теперь рассмотрим коэффициент при z:

$$\begin{aligned}&3 - (P_{s-1}(t) - P_{s-2}(t))(P_s(t) - P_{s-2}(t))\\ &\quad= 3 - P_s(t)P_{s-1}(t) + P_{s-1}(t)P_{s-2}(t) + P_s(t)P_{s-2}(t) - P_{s-2}(t)^2\\ &\quad= 3 - \sum_{i=1}^{s} P_{2i-1}(t) + \sum_{i=1}^{s-1} P_{2i-1}(t) + \sum_{i=1}^{s-1} P_{2i}(t) - \sum_{i=0}^{s-2} P_{2i}(t)\\ &\quad= 2 - P_{2s-1}(t) + P_{2s-2}(t).\end{aligned}$$

Лемма 9 доказана.

В заключение §2 покажем, как можно вывести следствие 1 из теоремы 1. Это даст нам другое доказательство гипотезы 1. Пусть $\Gamma = \langle a, b \mid R^m(a,b) = 1\rangle$, где $m \geqslant 2$, $R(a,b) = a^{u_1}b^{v_1}\cdots a^{u_s}b^{v_s}$, $u_i, v_i \neq 0$, $s \geqslant 1$, и $R(a,b)$ не является собственной степенью.

Рассмотрим сначала случай $m \geqslant 3$. Покажем, что $\dim X^s(\Gamma) \geqslant 2$. Теорема 1 тогда немедленно влечет, что Γ является нетривиальным свободным произведением с объединенной подгруппой. В многообразии характеров $X(F_2) = \mathbb{A}^3$ свободной группы $F_2 = \langle g, h\rangle$ рассмотрим гиперповерхность V, определенную уравнением

$$\tau_{R(g,h)}(x,y,z) = 2\cos\left(\frac{2\pi}{m}\right), \tag{9}$$

где $x = \tau_g$, $y = \tau_h$, $z = \tau_{gh}$. В силу леммы 5 уравнение (9) можно записать в виде

$$f(x,y,z) = M_s(x,y)z^s + \cdots + M_0(x,y) - 2\cos\left(\frac{2\pi}{m}\right) = 0. \tag{10}$$

Мы утверждаем, что $V \subset X(\Gamma)$. В самом деле, пусть $v = (x_0, y_0, z_0) \in V$, и пусть $A, B \in \mathrm{SL}_2(\mathbb{C})$ – такие матрицы, что $\operatorname{tr} A = x_0$, $\operatorname{tr} B = y_0$, $\operatorname{tr} AB = z_0$. Тогда в силу леммы 3 $R^m(A, B) = E$. Следовательно, пара матриц (A, B) определяет представление ρ группы Γ в $\mathrm{SL}_2(\mathbb{C})$. Кроме того, образ представления ρ в $X(\Gamma)$ совпадает с v. Следовательно, $v \in X(\Gamma)$. Далее, пусть $V_1, \dots, V_r$ – неприводимые компоненты V. Легко видеть (см. [24]), что $\dim V_i = 2$ для любого i. Нам остается показать, что $V \cap X^s(\Gamma) \neq \varnothing$. Допустим противное. Тогда все представления, соответствующие точкам из V, приводимы. Это означает, что регулярная функция $\tau_{ghg^{-1}h^{-1}} - 2$ тождественно равна 0 на V. Следовательно, в силу п. 1) леммы 9 имеем

$$g(x, y, z) = x^2 + y^2 + z^2 - xyz - 4 \equiv 0$$

на V. Таким образом,

$$f(x, y, z) = Cg(x, y, z)^d, \tag{11}$$

где C – отличная от 0 константа и $d \geqslant 1$.

Если для некоторого i мы имеем $|u_i| \geqslant 2$ либо $|v_i| \geqslant 2$, то тогда в силу леммы 5 старший коэффициент $M_s(x, y)$ в (10) не константа и равенство (11) невозможно.

Пусть теперь $|u_i| = |v_i| = 1$ для $i = 1, \dots, s$. Прежде всего, если для некоторого i мы имеем $u_i = u_{i+1}$ либо $v_i = v_{i+1}$ ($u_1 = u_s$ либо $v_1 = v_s$ при $i = s$), то можно рассмотреть новые образующие группы Γ. Предположим для определенности, что $u_1 = u_2$. Положим $a_1 = a^{u_1} b^{v_1}$, $b_1 = b$. Тогда $\Gamma = \langle a_1, b_1 \mid R_1^m(a_1, b_1) = 1 \rangle$, где $R_1^m(a_1, b_1) = a_1^{u'_1} b_1^{v'_1} \cdots a_1^{u'_r} b_1^{v'_r}$, $u'_i, v'_i \neq 0$, $r \geqslant 1$ и $u'_1 \geqslant 2$. Этот случай был рассмотрен выше.

Таким образом, мы можем предположить, что $u_{i+1} = -u_i$, $v_{i+1} = -v_i$. Поскольку по условию $R(a, b)$ не является собственной степенью, то для $R(a, b)$ имеются с точностью до циклической перестановки лишь две возможности: $R(a, b) = aba^{-1}b^{-1}$ либо $R(a, b) = ab^{-1}a^{-1}b$. В обоих случаях мы имеем

$$f(x, y, z) = x^2 + y^2 + z^2 - xyz - 2 - 2\cos\left(\frac{2\pi}{m}\right) = g(x, y, z) + 2 - 2\cos\left(\frac{2\pi}{m}\right).$$

Так как $2 - 2\cos\left(\frac{2\pi}{m}\right) \neq 0$, то очевидно, что $g(x, y, z)$ не имеет в этом случае нулей на V.

Итак, при $m \geqslant 3$ мы доказали, что группа Γ является нетривиальным свободным произведением с объединенной подгруппой.

Пусть теперь $m = 2$. В этом случае рассмотрим группу $\Gamma_1 = \langle a, b \mid R^4(a, b) = 1 \rangle$. Выше мы показали, что $\dim X^s(\Gamma_1) \geqslant 2$. Из доказательства теоремы 1 тогда следует, что найдется представление $\rho\colon \Gamma_1 \to \mathrm{SL}_2(\mathbb{Q}_p)$ для некоторого простого p такое, что $\rho(\Gamma_1)$ плотно в $\mathrm{SL}_2(\mathbb{Q}_p)$ в p-адической топологии. Следовательно, $\rho(\Gamma_1)$ является нетривиальным свободным произведением с объединенной подгруппой. Пусть $G = \overline{\rho(\Gamma_1)}$ – образ $\rho(\Gamma_1)$ в $\mathrm{PSL}_2(\mathbb{Q}_p)$. Тогда легко видеть, что G также является нетривиальным свободным произведением с объединенной подгруппой. Но G является эпиморфным образом Γ, откуда Γ является нетривиальным свободным произведением с объединенной подгруппой, что и требовалось показать.

§ 3. Доказательство теоремы 2

1) Пусть $\Gamma_n = \langle a, b \mid a^n = b^k = R^2(a,b) = 1\rangle$, и пусть $F_2 = \langle g, h\rangle$ – свободная группа с образующими g и h. Положим $x = \tau_g$, $\beta = \tau_h = 2\cos(\pi/k)$, $z = \tau_{gh}$. Рассмотрим уравнение

$$Q_{R(g,h)}(x, \beta, z) = 0, \tag{12}$$

где $Q_{R(g,h)}$ – многочлен Фрике элемента $R(g,h) \in F_2$. В силу леммы 5 мы можем записать (12) в виде

$$A_0(x)z^s + \cdots + A_s(x) = 0, \tag{13}$$

где $A_0(x) = \prod_{i=1}^s P_{u_i-1}(x)P_{v_i-1}(\beta)$. Так как по условию найдется такое i, что $|u_i| \geqslant 2$, то $\deg P_{u_i-1}(x) \geqslant 1$. Пусть $x_0 = -2\cos(\pi/u_i)$ – один из корней $P_{u_i-1}(x)$. Тогда $x - x_0$ делит $A_0(x)$. Пусть $A_0(x) = (x - x_0)B_0(x)$, где $B_0(x) \in \mathscr{O}[x]$. Запишем (13) в виде

$$(x - x_0)B_0(x)z^s + \cdots + A_s(x) = 0. \tag{14}$$

Предположим вначале, что все многочлены $A_1(x), \ldots, A_s(x)$ делятся на $x - x_0$. Тогда (14) можно записать в виде

$$(x - x_0)f(x, z) = 0, \tag{15}$$

где $f(x,z)$ – некоторый многочлен от x, z. Пусть z_0 – произвольный элемент $\mathbb{C}$ такой, что $z_0 \notin \mathscr{O}$, и пусть A, B – такие матрицы из $\mathrm{SL}_2(\mathbb{C})$, что $\operatorname{tr} A = x_0$, $\operatorname{tr} B = \beta$, $\operatorname{tr} AB = z_0$. Пара матриц (A, B) определяет по построению представление группы Γ_n в $\mathrm{PSL}_2(\mathbb{C})$. Применяя лемму 6, получаем, что Γ_n является нетривиальным свободным произведением с объединенной подгруппой.

Предположим теперь, что не все многочлены $A_1(x), \ldots, A_s(x)$ делятся на $x - x_0$. Пусть, например, $A_1(x)$ не делится на $x - x_0$, и пусть $0 \neq \delta = A_1(x_0) \in \mathscr{O}$ – остаток от деления $A_1(x)$ на $x - x_0$. Положим $c = N_{\mathbb{Q}(\delta)/\mathbb{Q}}(\delta) \in \mathbb{Z}$. В качестве конечного множества простых чисел S, о котором идет речь в теореме, возьмем $S = \{p \in \mathbb{Z} : p \text{ делит } c\}$. Предположим, что $n = u_i p f$ для некоторого целого f и простого числа $p \notin S$ такого, что $u_i p \nmid u_j$ при $j \neq i$. Пусть $x_r = 2\cos(r\pi/(pu_i))$ для некоторого $r \not\equiv 0 \pmod p$, и пусть $K_r = \mathbb{Q}(\delta, x_r - x_0)$. В силу п. 3) леммы 7 мы можем выбрать r так, что p делит $N_{K_r/\mathbb{Q}}(x_r - x_0)$ и по построению p не делит c. Тогда $N_{K_r/\mathbb{Q}}(\delta/(x_r - x_0)) \notin \mathbb{Z}$, следовательно, $\delta/(x_r - x_0) \notin \mathscr{O}$. Таким образом, имеем

$$\frac{A_1(x_r)}{x_r - x_0} \notin \mathscr{O}.$$

Далее, так как $p \nmid r$ и $pu_i \nmid u_j$ для любого $j \neq i$, то $B_0(x_r) \neq 0$. Положим теперь $x = x_r$ и запишем уравнение (14) в виде

$$z^s + \frac{A_1(x_r)}{(x_r - x_0)B_0(x_r)} z^{s-1} + \cdots + \frac{A_s(x_r)}{(x_r - x_0)B_0(x_r)} = 0. \tag{16}$$

Ясно, что $A_1(x_r)/((x_r - x_0)B_0(x_r)) \notin \mathscr{O}$, поскольку $B_0(x_r) \in \mathscr{O}$. Следовательно, уравнение (16) имеет корень $z_0 \notin \mathscr{O}$. Рассмотрим матрицы $A, B \in \mathrm{SL}_2(\mathbb{C})$ такие, что

$$\operatorname{tr} A = x_r, \qquad \operatorname{tr} B = \beta, \qquad \operatorname{tr} AB = z_0.$$

По построению пара матриц (A, B) определяет представление группы Γ_n в $\mathrm{PSL}_2(\mathbb{C})$. Применив лемму 6, получаем, что группа Γ_n является нетривиальным свободным произведением с объединенной подгруппой.

2) Сохраним обозначения п. 1). Рассмотрим уравнение

$$Q_{R(g,h)}(x, \beta, z) = \gamma_t, \tag{17}$$

где $\gamma_t = 2\cos(t\pi/m)$, $m \nmid t$. Используя лемму 5, можно записать (17) в виде

$$(x - x_0)B_0(x)z^s + \cdots + A_s(x) - \gamma_t = 0. \tag{18}$$

Пусть $x_r = 2\cos(r\pi/(pu_i))$, где $r \not\equiv 0 \pmod p$. Покажем, что найдутся t и r такие, что $(A_s(x_r) - \gamma_t)/(x_r - x_0) \notin \mathscr{O}$. В самом деле, допустим противное.

Вначале рассмотрим случай $m = 3$. Тогда $\gamma_1 = 1$, $\gamma_2 = -1$. Поскольку оба числа

$$(A_s(x_r) - 1)/(x_r - x_0), \qquad (A_s(x_r) + 1)/(x_r - x_0)$$

принадлежат $\mathscr{O}$, то их разность $2/(x_r - x_0) \in \mathscr{O}$ для любого $r \not\equiv 0 \pmod p$. Поскольку по условию $p \neq 2$, то мы получаем противоречие с п. 4) леммы 7.

Пусть теперь $m = 2^l$. Тогда $\gamma_{2^{l-1}} = 0$, $\gamma_{2^{l-2}} = \sqrt{2}$. Поскольку оба числа

$$A_s(x_r)/(x_r - x_0), \qquad (A_s(x_r) - \sqrt{2})/(x_r - x_0)$$

принадлежат $\mathscr{O}$, то их разность $\sqrt{2}/(x_r - x_0) \in \mathscr{O}$, а следовательно, $2/(x_r - x_0) \in \mathscr{O}$. Опять получаем противоречие с п. 4) леммы 7.

Итак, выберем t и r так, чтобы $(A_s(x_r) - \gamma_t)/(x_r - x_0) \notin \mathscr{O}$. Так как $p \nmid r$ и $pu_i \nmid u_j$ для любого $j \neq i$, то $B_0(x_r) \neq 0$. Положим $x = x_r$ и запишем (18) в виде:

$$z^s + \cdots + \frac{A_s(x_r) - \gamma_t}{(x_r - x_0)B_0(x_r)} = 0. \tag{19}$$

По построению $(A_s(x_r) - \gamma_t)/((x_r - x_0)B_0(x_r)) \notin \mathscr{O}$, следовательно, (19) имеет корень $z_0 \notin \mathscr{O}$. Рассмотрим матрицы $A, B \in \mathrm{SL}_2(\mathbb{C})$ такие, что

$$\operatorname{tr} A = x_r, \qquad \operatorname{tr} B = \beta, \qquad \operatorname{tr} AB = z_0.$$

По построению пара матриц (A, B) определяет представление группы Γ_n в $\mathrm{PSL}_2(\mathbb{C})$. Применив лемму 6, получаем, что группа Γ_n является нетривиальным свободным произведением с объединенной подгруппой.

3) Пусть $m > 3$ и $m \neq 2^l$. Сохраним обозначения п. 2). Покажем, что найдутся такие $t \not\equiv 0 \pmod m$ и $r \not\equiv 0 \pmod p$, что $(A_s(x_r) - \gamma_t)/(x_r - x_0) \notin \mathscr{O}$. В самом деле, допустим противное. Пусть для любых $t \not\equiv 0 \pmod m$ и $r \not\equiv 0 \pmod p$ имеем $(A_s(x_r) - \gamma_t)/(x_r - x_0) \in \mathscr{O}$.

Вначале рассмотрим случай, когда m нечетно и m делится на число вида $4g + 1$, $g \geqslant 1$, т.е. $m = (4g + 1)m_1$. Рассмотрим числа $\delta_t = \gamma_{2tm_1} = 2\cos(2t\pi/(4g + 1))$, $t = 1, \dots, 2g$. Тогда $1 + \sum_{i=1}^{2g} \delta_i = 0$ как сумма всех корней из 1 степени $4g + 1$. Отметим, что $-\delta_t = \gamma_{(4g+1-2t)m_1}$. Пусть $C_i = (A_s(x_r) - (-1)^i\delta_i)/(x_r - x_0)$. Тогда мы имеем

$$\sum_{i=1}^{2g} (-1)^i C_i = -\sum_{i=1}^{2g} \frac{\delta_i}{x_r - x_0} = \frac{1}{x_r - x_0} \in \mathscr{O}$$

для любого $r \not\equiv 0 \pmod p$ – противоречие с п. 4) леммы 7.

Предположим теперь, что m нечетно и m не имеет делителей вида $4g+1$, $g \geqslant 1$. Тогда $m = 4g+3$, $g \geqslant 1$. Мы имеем $1 + \sum_{i=1}^{2g+1} \gamma_{2i} = 0$ как сумма всех корней из 1 степени $4g+3$. Положим $C_0 = (A_s(x_r) + \gamma_1)/(x_r - x_0)$, $C_i = (A_s(x_r) - (-1)^i \gamma_{2i})/(x_r - x_0)$ для $i = 1, \dots, 2g+1$. Тогда

$$C_0 + \sum_{i=1}^{2g+1} (-1)^i C_i = \frac{\gamma_1 - 1}{x_r - x_0} \in \mathcal{O}. \tag{20}$$

Покажем, что $\gamma_1 - 1 \in \mathcal{O}^*$. Так как γ_1 является корнем многочлена $P_{4g+2}(\lambda)$, то $\gamma_1 - 1$ – корень многочлена $P_{4g+2}(\lambda+1)$. Свободный коэффициент многочлена $P_{4g+2}(\lambda+1)$ равен

$$P_{4g+2}(1) = P_{4g+2}\left(2\cos\frac{\pi}{3}\right) = \frac{\sin((4g+3)\pi/3)}{\sin(\pi/3)} \in \{-1, 1, 0\}.$$

Заметим, что $P_{4g+2}(1) = 0$ тогда и только тогда, когда 3 делит $4g+3$, т.е. 3 делит g. Пусть $g = 3g_1$. Тогда $4g+3 = 12g_1 + 3 = 3(4g_1+1)$, т.е. $4g_1+1$ делит m. Это противоречит нашему предположению. Следовательно, $P_{4g+2}(1) = \pm 1$ и $\gamma_1 - 1 \in \mathcal{O}^*$. Тогда из (19) следует, что для любого $r \not\equiv 0 \pmod p$ имеем $1/(x_r - x_0) \in \mathcal{O}$. Мы снова получили противоречие с п. 4) леммы 7.

Наконец, рассмотрим случай, когда m четно, т.е. $m = m_1 2^g$, где $g \geqslant 1$, $m_1 > 1$ нечетно. Рассмотрим числа $\gamma_{i2^g} = 2\cos(i\pi/m_1)$. Теперь, рассуждая точно так же, как и в случае нечетного m выше, мы получаем противоречие с п. 4) леммы 7.

Итак, выберем t и r так, что $(A_s(x_r) - \gamma_t)/(x_r - x_0) \notin \mathcal{O}$. Тогда свободный коэффициент в уравнении (19) не принадлежит $\mathcal{O}$ и уравнение (19) имеет корень $z_0 \notin \mathcal{O}$. Пусть $A, B \in \mathrm{SL}_2(\mathbb{C})$ такие матрицы, что

$$\operatorname{tr} A = x_r, \qquad \operatorname{tr} B = \beta, \qquad \operatorname{tr} AB = z_0.$$

Пара матриц (A, B) определяет по построению представление Γ_n в $\mathrm{PSL}_2(\mathbb{C})$. Применив лемму 6, завершаем доказательство теоремы 2.

Замечание. В ряде случаев можно получить более точную информацию о том, когда обобщенная треугольная группа Γ является нетривиальным свободным произведением с объединенной подгруппой. Например, рассмотрим следующую группу $\Gamma_k = \langle a, b \mid a^2 = b^k = (ab^2)^3 = 1\rangle$. Тогда из теоремы 2 следует, что если $k = 2k_1$, где $1 < k_1 \neq 2^l$, то Γ_k – нетривиальное свободное произведение с объединенной подгруппой. Однако легко видеть, что и для $k_1 = 2^l$, $l \geqslant 1$, группа Γ_k также является нетривиальным свободным произведением с объединенной подгруппой. В самом деле, пусть $F_2 = \langle g, h\rangle$ – свободная группа, $x = \tau_g = 0$, $y = \tau_h$, $z = \tau_{gh}$. Рассмотрим уравнение

$$Q_{gh^2}(0, y, z) = yz = 2\cos\frac{\pi}{3} = 1.$$

Пусть $y = y_r = 2\cos(r\pi/2^{l+1})$. Тогда в силу п. 6) леммы 7 для любого нечетного r имеем $z_r = 1/y_r \notin \mathcal{O}$. Теперь лемма 6 влечет, что Γ_k является нетривиальным свободным произведением с объединенной подгруппой.

§ 4. Доказательство теоремы 3

Вначале предположим, что для слова $R(a,b) = a^{u_1}b^{v_1}\cdots a^{u_s}b^{v_s}$ мы имеем неравенство $v = \max_{1\leqslant i\leqslant s}|v_i| \geqslant 2$. Тогда в силу теоремы 2 найдется такое простое p, что группа $\Gamma_1 = \langle a, b \mid a^n = b^{pv} = R^m(a,b) = 1\rangle$ является нетривиальным свободным произведением с объединенной подгруппой. Поскольку Γ_1 является эпиморфным образом Γ, то Γ также является нетривиальным свободным произведением с объединенной подгруппой.

Таким образом, без ограничения общности можно предположить, что

$$R(a,b) = a^{u_1}b^{v_1}\cdots a^{u_s}b^{v_s},$$

где $v_i \in \{-1,1\}$, $i = 1,\dots,s$. Предположим, что найдется такое i, $1 \leqslant i \leqslant s$, что либо $v_i = v_{i+1}$, либо $v_1 = v_s$. Пусть для определенности $v_1 = v_2$. В этом случае можно рассмотреть новые образующие группы Γ: $a_1 = a$, $b_1 = a^{u_2}b^{v_1}$. Тогда легко проверить, что $\Gamma = \langle a_1, b_1 \mid a_1^n = R_1^m(a_1,b_1) = 1\rangle$, где $R_1(a_1,b_1) = a_1^{u_1'}b_1^{v_1'}\cdots a_1^{u_l'}b_1^{v_l'}$, $l \geqslant 1$, $0 < u_i' < n$, $v_i' \neq 0$ для $i = 1,\dots,l$. При этом мы имеем $v' = \max_{1\leqslant i\leqslant l}|v_i'| \geqslant 2$. Но мы только что доказали, что в этом случае Γ является нетривиальным свободным произведением с объединенной подгруппой.

Таким образом, без ограничения общности мы можем считать, что

$$R(a,b) = a^{u_1}ba^{u_2}b^{-1}\cdots a^{u_{2k-1}}ba^{u_{2k}}b^{-1},$$

где $k \geqslant 1$, $0 < u_i < n$ для $i = 1,\dots,2k$. Положим $c = ba^{-1}b^{-1}$. Тогда

$$R(a,b) = a^{u_1}c^{-u_2}\cdots a^{u_{2k-1}}c^{-u_{2k}} = R_1(a,c).$$

Пусть $F_2 = \langle g,h\rangle$ – свободная группа ранга 2, $f = hg^{-1}h^{-1}$. Положим $x = \tau_g$, $y = \tau_h$, $z = \tau_{gh}$, $t = \tau_{gf}$. Тогда $\tau_f = \tau_g = x$, $t = \tau_{gf} = \tau_{ghg^{-1}h^{-1}} = x^2+y^2+z^2-xyz-2$ в силу п. 1) леммы 9. Рассмотрим элемент $R_1(g,f) \in F_2$ как слово от g и f. Пусть $q(x,t)$ – многочлен Фрике элемента $R_1(g,f)$, т.е.

$$q(x,t) = Q_{R_1(g,f)}(\tau_g,\tau_f,\tau_{gf}) = Q_{R_1(g,f)}(x,x,t).$$

Так как $R_1(g,f)$ содержит k блоков вида $g^{u_j}f^{-u_{j+1}}$, то в силу леммы 5 степень многочлена $q(x,t)$ относительно t равна k, а старший коэффициент $q(x,t)$ равен $(-1)^k\prod_{i=1}^{2k}P_{u_i-1}(x)$. Так как по построению $R(g,h) = R_1(g,f)$, то

$$Q_{R(g,h)}(x,y,z) = q(x,t) = q(x, x^2+y^2+z^2-xyz-2). \tag{21}$$

Положим теперь $x = \tau_g = \alpha_r = 2\cos(r\pi/n)$, $\gamma_l = 2\cos(l\pi/m)$, где $r \not\equiv 0 \pmod n$, $l \not\equiv 0 \pmod m$, и рассмотрим уравнение

$$Q_{R(g,h)}(\alpha_r,y,z) = \gamma_l. \tag{22}$$

В силу (21) уравнение (22) можно записать в виде

$$q(\alpha_r,t) = \gamma_l. \tag{23}$$

Лемма 10. *Существуют такие $r, l \in \mathbb{Z}$, где $r \not\equiv 0 \pmod n$, $l \not\equiv 0 \pmod m$, что $P_{u_i-1}(\alpha_r) \neq 0$ для $i = 1,\dots,2k$ и уравнение (23) имеет корень $t = t_0 \neq 2$.*

Доказательство. Пусть вначале $m \geqslant 3$. В этом случае $\gamma_1 \neq \gamma_2$. Положим $r = 1$. Тогда степень многочлена $q(\alpha_1, t)$ равна k и ясно, что хотя бы одно из уравнений $q(\alpha_1, t) = \gamma_1$, $q(\alpha_1, t) = \gamma_2$ имеет корень $t_0 \neq 2$.

Предположим теперь, что $m = 2$ и уравнение $q(\alpha_r, t) = 0$ имеет единственный корень $t = 2$. Это означает, что для любых матриц $A, B \in \mathrm{SL}_2(\mathbb{C})$ таких, что $\operatorname{tr} A = \operatorname{tr} B = \alpha_r$, условие $\operatorname{tr} R_1(A, B) = \operatorname{tr} A^{u_1}B^{-u_2}\cdots A^{u_{2k-1}}B^{-u_{2k}} = 0$ влечет, что $\operatorname{tr} AB = 2$. Покажем, что это не так. Чтобы получить противоречие, нам достаточно найти матрицы $A, B \in \mathrm{SL}_2(\mathbb{C})$, удовлетворяющие условиям:

1) $\operatorname{tr} A = \operatorname{tr} B = \alpha_r$,
2) $\operatorname{tr} AB \neq 2$,
3) $\operatorname{tr} R_1(A, B) = \operatorname{tr} A^{u_1}B^{-u_2}\cdots A^{u_{2k-1}}B^{-u_{2k}} = 0$.

Будем искать A и B в виде

$$A = \begin{pmatrix} \varepsilon_r & w \\ 0 & \varepsilon_r^{-1} \end{pmatrix}, \qquad B = \begin{pmatrix} \varepsilon_r & 0 \\ w & \varepsilon_r^{-1} \end{pmatrix},$$

где $\varepsilon_r + \varepsilon_r^{-1} = \alpha_r = 2\cos(r\pi/n)$ и w – некоторая переменная. Легко видеть, что $\operatorname{tr} AB = w^2 + \varepsilon_r^2 + \varepsilon_r^{-2}$. Следовательно, условие $\operatorname{tr} AB \neq 2$ эквивалентно тому, что $w^2 + \varepsilon_r^2 + \varepsilon_r^{-2} \neq 2$, т.е.

$$w^2 \neq 2 - (\varepsilon_r^2 + \varepsilon_r^{-2}) = 2 - 2\cos\left(\frac{2r\pi}{n}\right) = 4\sin^2\left(\frac{r\pi}{n}\right).$$

Легко проверить по индукции, что

$$A^i = \begin{pmatrix} \varepsilon_r^i & P_{i-1}(\alpha_r)w \\ 0 & \varepsilon_r^{-i} \end{pmatrix}, \qquad B^i = \begin{pmatrix} \varepsilon_r^i & 0 \\ P_{i-1}(\alpha_r)w & \varepsilon_r^{-i} \end{pmatrix}.$$

Далее, нетрудно показать, что

$$R_1(A, B) = \begin{pmatrix} \varepsilon_r^d + C_1(\alpha_r)w^2 + \cdots + C_k(\alpha_r)w^{2k} & wf_1(w) \\ wf_2(w) & \varepsilon_r^{-d} + D_1(\alpha_r)w^2 + \cdots + D_{k-1}(\alpha_r)w^{2k-2} \end{pmatrix},$$

где $d = \sum_{i=1}^{2k} u_i$, $C_k(\alpha_r) = (-1)^k \prod_{i=1}^{2k} P_{u_i-1}(\alpha_r)$, $f_1(w)$, $f_2(w)$ – некоторые многочлены от w. Следовательно,

$$\operatorname{tr} R_1(A, B) = C_k(\alpha_r)w^{2k} + \cdots + (C_1(\alpha_r) + D_1(\alpha_r))w^2 + (\varepsilon_r^d + \varepsilon_r^{-d}) = g(w^2).$$

Покажем, что найдется такое r, $1 \leqslant r < n$, что $C_k(\alpha_r) \neq 0$ и многочлен $g(w^2)$ имеет корень w_0 такой, что $w_0^2 \neq 4\sin^2(r\pi/n)$. Предположим противное. Пусть для каждого r такого, что $C_k(\alpha_r) \neq 0$, имеем

$$g(w^2) = C_k(\alpha_r)\left(w^2 - 4\sin^2\left(\frac{r\pi}{n}\right)\right)^k. \tag{24}$$

Сравнивая свободные члены в левой и правой части (24), а также учитывая выражение для $C_k(\alpha_r)$, получаем

$$\left(\prod_{i=1}^{2k} P_{u_i-1}\left(2\cos\left(\frac{r\pi}{n}\right)\right)\right)4^k\left(\sin\left(\frac{r\pi}{n}\right)\right)^{2k} = 2\cos\left(\frac{dr\pi}{n}\right). \tag{25}$$

В силу (2) мы имеем $P_{u_i-1}(2\cos(r\pi/n)) = \sin(u_i r\pi/n)/\sin(r\pi/n)$. Запишем u_i/n в виде u_i'/n_i, где $(u_i', n_i) = 1$. Тогда (25) имеет вид

$$\prod_{i=1}^{2k}\biggl(2\sin\biggl(\frac{u_i' r\pi}{n_i}\biggr)\biggr) = 2\cos\biggl(\frac{dr\pi}{n}\biggr). \tag{26}$$

Таким образом, чтобы завершить доказательство леммы, нам достаточно доказать, что мы получим противоречие, если предположим, что равенство (26) справедливо для любого r такого, что левая часть в (26) отлична от нуля.

Рассмотрим вначале случай, когда n нечетно. Пусть $n_0 = \min_j n_j$, и пусть для определенности $n_0 = n_1$. Тогда n_1 нечетно, и пусть $p > 2$ – произвольный простой делитель n_1. Положим $r = n_1/p$. Тогда $2\sin(u_1' r\pi/n_1) = 2\sin(u_1'\pi/p)$. Если $j > 1$, то $2\sin(u_j' r\pi/n_j) = 2\sin(u_j' n_1\pi/(pn_j)) \neq 0$, поскольку по построению pn_j не делит $u_j' n_1$. Из (26) следует, что

$$\prod_{i=2}^{2k}\biggl(2\sin\biggl(\frac{u_i' n_1\pi}{pn_i}\biggr)\biggr) = \frac{2\cos(dn_1\pi/(pn))}{2\sin(u_1'\pi/p)} \in \mathcal{O}. \tag{27}$$

Если pn делит dn_1, то $2\cos(dn_1\pi/(pn)) = \pm 1$. Если pn не делит dn_1, то в силу п. 2) леммы 7 имеем $2\cos(dn_1\pi/(pn)) \in \mathcal{O}^*$. В обоих случаях из (27) следует, что $1/(2\sin(u_1'\pi/p)) \in \mathcal{O}$ – противоречие с п. 5) леммы 7.

Пусть теперь $n = 2^l n'$, где $l \geqslant 1$ и n' нечетно. Пусть $n_i = 2^{l_i} n_i'$, где $l_i \geqslant 0$, n_i' нечетно, и пусть $n_0' = \min_j n_j'$.

Если $n_0' > 1$, то положим $r = 2^l r'$, где $r' \not\equiv 0 \pmod{n'}$. Тогда (26) имеет вид

$$\prod_{i=1}^{2k}\biggl(2\sin\biggl(\frac{u_i' 2^{l-l_i} r'\pi}{n_i'}\biggr)\biggr) = 2\cos\biggl(\frac{dr'\pi}{n'}\biggr), \tag{28}$$

где n' – нечетно. Выше мы показали, что в этом случае существует r' такое, что левая часть (28) отлична от 0 и равенство (28) не имеет места.

Пусть теперь $n_0' = 1$. Положим

$$I = \{i : n_i' = 1\}, \qquad l_0 = \min_{i\in I} l_i, \qquad I_0 = \{i \in I : l_i = l_0\}.$$

Далее, положим $r = 2^{l_0-1} r'$, где r' – нечетно. Тогда для $i \in I_0$ имеем

$$2\sin\biggl(\frac{u_i' r\pi}{n_i}\biggr) = 2\sin\biggl(\frac{u_i' 2^{l_0-1} r'\pi}{2^{l_0}}\biggr) = 2\sin\biggl(\frac{u_i' r'\pi}{2}\biggr) = \pm 2.$$

Теперь равенство (26) можно записать в виде

$$\prod_{i\notin I_0}\biggl(2\sin\biggl(\frac{u_i' r'\pi}{2^{l_i-l_0+1} n_i'}\biggr)\biggr) = \pm\frac{1}{2^{|I_0|-1}}\cos\biggl(\frac{dr'\pi}{2^{l-l_0+1} n'}\biggr). \tag{29}$$

Выберем r' так, чтобы левая часть (29) была отлична от 0. Тогда правая часть (29) также должна быть отлична от 0. Если мы имеем $|I_0| > 1$ либо

$|I_0| = 1$, а $\cos(dr'\pi/(2^{l-l_0+1}n')) \neq \pm 1$, то левая часть (29) принадлежит $\mathcal{O}$. Но в силу п. 1) леммы 7 правая часть (29) не принадлежит $\mathcal{O}$ – противоречие.

Итак, осталось рассмотреть случай $|I_0| = |\{i_0\}| = 1$ и $\cos(dr'\pi/(2^{l-l_0+1}n')) = \pm 1$. В этом случае (29) имеет вид

$$\prod_{i\neq i_0}\left(2\sin\left(\frac{u_i'r'\pi}{2^{l_i-l_0+1}n_i'}\right)\right) = \pm 1. \tag{30}$$

Если $|I| > 1$ и $i_0 \neq i \in I$, то $l_i > l_0, n_i = 1$. Следовательно, для любого нечетного r' левая часть (30) отлична от 0 и (30) влечет, что $1/(2\sin(u_i'r'\pi/(2^{l_i-l_0+1}))) \in \mathcal{O}$. Мы получили противоречие с п. 5) леммы 7.

Пусть теперь $I = I_0 = \{i_0\}$. Положим

$$n_{j_0} = \min_{j\neq i_0} n_j \geqslant 3, \qquad J = \{j : n_j = n_{j_0}\}, \qquad l_{j_0} = \min_{j\in J} l_j.$$

Если $l_{j_0} - l_0 + 1 > 0$, то положим $r' = n_{j_0}$. Легко проверить, что в этом случае левая часть (30) отлична от 0 и (30) влечет, что $1/(2\sin(u_{j_0}'\pi/2^{l_{j_0}-l_0+1})) \in \mathcal{O}$. Мы получили противоречие с п. 6) леммы 7.

Наконец, если $l_{j_0} - l_0 + 1 \leqslant 0$, то мы возьмем произвольный простой делитель $p \geqslant 3$ числа n_{j_0} и положим $r' = n_{j_0}/p$. Тогда, как и выше, левая часть (30) отлична от 0 и из (30) мы получаем, что

$$2\sin\left(\frac{u_{j_0}'r'\pi}{2^{l_{j_0}-l_0+1}n_{j_0}'}\right) = 2\sin\left(\frac{u_{j_0}'2^{-l_{j_0}+l_0-1}\pi}{p}\right) \in \mathcal{O}^*.$$

Мы имеем противоречие с п. 5) леммы 7. Лемма 10 доказана.

Теперь мы можем завершить доказательство теоремы 3. В силу леммы 10 мы можем выбрать r, l так, что уравнение (23) имеет корень $t_0 \neq 2$. Поскольку по построению $t = x^2 + y^2 + z^2 - xyz - 2$, $x = \alpha_r$, то y, z удовлетворяют уравнению

$$y^2 + z^2 - \alpha_r yz + \alpha_r^2 - 2 - t_0 = 0. \tag{31}$$

Пусть (y_0, z_0) – некоторое решение (31) и $A, B \in \mathrm{SL}_2(\mathbb{C})$ – такие матрицы, что $\operatorname{tr} A = \alpha_r$, $\operatorname{tr} B = y_0$, $\operatorname{tr} AB = z_0$. Тогда по построению $\operatorname{tr} ABA^{-1}B^{-1} = t_0$, $\operatorname{tr} R(A,B) = \gamma_l$ и пара матриц (A,B) определяет представление группы Γ в $\mathrm{PSL}_2(\mathbb{C})$. Отметим, что это представление неприводимо, поскольку $t_0 \neq 2$. Покажем, что существует такое решение (y_0, z_0) уравнения (31), что выполнены следующие два условия.

1) существует элемент конечного порядка $W_1(A,B) = A^{\alpha_1}B^{\beta_1}\cdots A^{\alpha_g}B^{\beta_g}$ такой, что $\alpha_i, \beta_i \neq 0$ для $i = 1, \ldots, g$ и $\sum_{i=1}^{g}\beta_g \neq 0$;
2) $z_0 = \operatorname{tr} AB \notin \mathcal{O}$.

Тогда мы можем применить лемму 6 и завершить доказательство теоремы 3. Дальнейшее доказательство зависит от вида t_0. Мы рассмотрим следующие случаи:

1) $t_0 \notin \mathcal{O}$;
2) $t_0 = 2\cos((2k+1)\pi/(2s+1))$, где $s \geqslant 1$, $(2k+1, 2s+1) = 1$;
3) $t_0 = 2\cos(2k\pi/(2s+1))$, где $s \geqslant 1$, $(k, 2s+1) = 1$;
4) $t_0 = 2\cos((2k+1)\pi/(2s))$, где $s \geqslant 1$, $(2k+1, s) = 1$;
5) $t_0 \in \mathcal{O}, t_0 \neq 2\cos(k\pi/s)$ для любых целых k и s.

1) Положим $y_0 = 0$ и $W_1(A, B) = B$. Тогда $W_1(A, B)$ имеет порядок 4. Так как $t_0 \notin \mathcal{O}$, то (31) имеет решение $(0, z_0)$ такое, что $z_0 \notin \mathcal{O}$.

2) Положим $W_1(A, B) = AB(ABA^{-1}B^{-1})^s$. Тогда леммы 8 и 9 влекут, что

$$\operatorname{tr} W_1(A, B) = (P_{s+1}(t_0) - P_s(t_0))z_0 = 0 \cdot z_0 = 0.$$

Следовательно, $W_1(A, B)$ имеет порядок 4. Выберем теперь произвольное решение (y_0, z_0) уравнения (31) так, чтобы $z_0 \notin \mathcal{O}$.

3) Положим $W_1(A, B) = AB(ABA^{-1}B^{-1})^s$ и предположим, что

$$\operatorname{tr} W_1(A, B) = 2\cos\frac{\pi}{3} = 1.$$

Тогда $W_1(A, B)$ имеет порядок 6 и п. 2) леммы 9 влечет, что

$$\operatorname{tr} W_1(A, B) = (P_{s+1}(t_0) - P_s(t_0))z_0 = 1.$$

Следовательно, в силу п. 3) леммы 8 мы имеем $z_0 = 1/(P_{s+1}(t_0) - P_s(t_0)) \notin \mathcal{O}$. Пусть теперь (y_0, z_0) – некоторое решение (31).

4) Положим $W_1(A, B) = (AB)^{-1}(ABA^{-1}B^{-1})^s(AB)^2(ABA^{-1}B^{-1})^s$ и предположим, что

$$\operatorname{tr} W_1(A, B) = 2\cos\frac{\pi}{3} = 1. \tag{32}$$

Тогда $W_1(A, B)$ имеет порядок 6 и в силу п. 3) леммы 9 мы можем записать (32) в виде

$$(t_0 - 2)P_{s-1}(t_0)^2 z_0^3 + (2 - P_{2s-1}(t_0) + P_{2s-2}(t_0))z_0 - 1 = 0. \tag{33}$$

В силу п. 4) леммы 8 имеем $0 \neq P_{s-1}(t_0) \notin \mathcal{O}^*$, следовательно,

$$\frac{1}{(t_0 - 2)P_{s-1}(t_0)^2} \notin \mathcal{O}.$$

Таким образом, (33) имеет корень $z_0 \notin \mathcal{O}$. Пусть теперь (y_0, z_0) – некоторое решение (31).

5) Так как $t_0 \in \mathcal{O}$, $t_0 \neq 2\cos(k\pi/s)$ для любых целых k и s, то в силу п. 5) леммы 8 найдется такое целое $l > 0$, что $0 \neq P_l(t_0) \notin \mathcal{O}^*$. Положим $W_1(A, B) = (AB)^{-1}(ABA^{-1}B^{-1})^{l+1}(AB)^2(ABA^{-1}B^{-1})^{l+1}$ и предположим, что выполняется условие (32). Тогда $W_1(A, B)$ имеет порядок 6 и в силу п. 3) леммы 9 мы можем записать (32) в виде

$$(t_0 - 2)P_l(t_0)^2 z_0^3 + (2 - P_{2l+1}(t_0) + P_{2l}(t_0))z_0 - 1 = 0. \tag{34}$$

Поскольку по построению $1/((t_0 - 2)P_l(t_0)^2) \notin \mathcal{O}$, то (34) имеет корень $z_0 \notin \mathcal{O}$. Пусть (y_0, z_0) – некоторое решение (31). Применяя лемму 6, завершаем доказательство теоремы 3 в последнем случае.

Список литературы

1. *Линдон Р., Шупп П.* Комбинаторная теория групп. М.: Мир, 1980.
2. *Wall C. T. C. (ed.).* Homological group theory // Proc. of a conference in Durham. London Math. Soc. Lecture Note Ser. 1977. №36.
3. *Baumslag G., Shalen P. B.* Amalgamated products and finitely presented groups // Comment. Math. Helv. 1990. V. 65. P. 243–254.
4. *Fine B., Levin F., Rosenberger G.* Free subgroups and decompositions of one-relator products of cyclics. Part 2. Normal torsion free subgroups and FPA decompositions // J. Indian Math. Soc. 1985. V. 49. P. 237–247.
5. *Zieschang H.* On decompositions of discontinuous groups of the plane // Math. Z. 1976. V. 151. P. 165–188.
6. *Rosenberger G.* Bemerkungen zu einer Arbeit von H. Zieschang // Arch. Math. (Basel). 1977. V. 29. P. 623–627.
7. *Long D. D., Maclachlan C., Reid A. W.* Splitting groups of signature $(1, n)$ // J. Algebra. 1996. V. 185. P. 329–341.
8. *Dunwoody M. J., Sageev M.* Splittings of certain Fuchsian groups // Proc. Amer. Math. Soc. 1997. V. 125. №7. P. 1953–1954.
9. *Беняш-Кривец В. В.* О разложении свободного произведения циклических групп с одним соотношением в амальгамированное свободное произведение // Матем. сб. 1998. Т. 189. №8. С. 13–26.
10. *Беняш-Кривец В. В.* О разложимости некоторых F-групп в амальгамированное свободное произведение // Докл. АНБ. 1997. Т. 41. №6. С. 1–4.
11. *Lubotzky A., Magid A.* Varieties of representations of finitely generated groups // Memoirs Amer. Math. Soc. 1985. V. 58. P. 1–116.
12. *Culler M., Shalen P.* Varieties of group representations and splittings of 3 manifolds // Ann. of Math. 1983. V. 117. P. 109–147.
13. *Rapinchuk A. S., Benyash-Krivetz V. V., Chernousov V. I.* Representation varieties of the fundamental groups of compact orientable surfaces // Israel J. Math. 1996. V. 93. P. 29–71.
14. *Беняш-Кривец В. В., Черноусов В. И.* Многообразия представлений фундаментальных групп компактных неориентируемых поверхностей // Матем. сб. 1997. Т. 188. №7. С. 47–92.
15. *Мамфорд Д.* Алгебраическая геометрия. М.: Мир, 1979.
16. *Horowitz R.* Characters of free groups represented in the two dimensional linear group // Comm. Pure. Appl. Math. 1972. V. 25. P. 635–649.
17. *Helling H.* Diskrete Untergruppen von $\mathrm{SL}_2(\mathbb{R})$ // Invent. Math. 1972. V. 17. P. 217–229.
18. *Magnus W.* The uses of 2 by 2 matrices in combinatorial group theory // Results Math. 1981. V. 4. №2. P. 171–192.
19. *Serre J.-P.* Arbres, amalgames, SL_2 // Astérisque. 1977. V. 46.
20. *Бурбаки Н.* Группы и алгебры Ли. М.: Мир, 1976.
21. *Majeed A., Mason A. W.* Solvable-by-finite subgroups of $\mathrm{GL}(2, F)$ // Glasgow Math. J. 1978. V. 19. P. 45–48.
22. *Серр Ж.-П.* Алгебры Ли и группы Ли. М.: Мир, 1969.
23. *Винберг Э. Б.* Кольца определения плотных подгрупп полупростых линейных групп // Изв. АН СССР. Сер. матем. 1971. Т. 35. №1. С. 45–55.
24. *Шафаревич И. Р.* Основы алгебраической геометрии. М.: Наука, 1972.
25. *Traina C.* Trace polynomial for two generated subgroups of $\mathrm{SL}_2(\mathbb{C})$ // Proc. Amer. Math. Soc. 1980. V. 79. P. 369–372.
26. *Bass H.* Finitely generated subgroups of $\mathrm{GL}_2(\mathbb{C})$ // The Smith Conjecture. New York: Wiley, 1984. P. 127–136.

Институт математики НАН Беларуси,
Минск
E-mail: benyash@im.bas-net.by

Поступила в редакцию
09.11.1999