УДК 512.543.7+512.546.1

ЧИСЛО НЕРЕШЕНИЙ УРАВНЕНИЯ В ГРУППЕ И НЕТОПОЛОГИЗИРУЕМЫЕ ГРУППЫ БЕЗ КРУЧЕНИЯ

Антон А. Клячко Антон В. Трофимов
Механико-математический факультет
Московского государственного университета
Москва 119992, Ленинские горы, МГУ
klyachko@daniil.math.msu.su anton_tr@rambler.ru

Показано, что для любой пары кардиналов с бесконечной суммой найдётся такая группа и такое уравнение над этой группой, что первый кардинал является числом решений этого уравнения, а второй кардинал является числом нерешений этого уравнения. Построена бесконечная счётная нетопологизируемая группа без кручения.

Ключевые слова: уравнения над группами, топологизация групп, градуированные копредставления

1. Введение

Основная теорема. *Существует такая конечно порождённая группа без кручения H и такое уравнение $w(x) = 1$ (где $w(x) \in H * \langle x\rangle_\infty$) над ней, что решениями этого уравнения являются все элементы группы H, кроме одного:*

$$\{h \in H \mid w(h) \neq 1\} = \{1\}. \tag{1}$$

Замечание. Из теоремы Лёвенгейма–Сколема следует, что слова «конечно порождённая» в основной теореме могут быть заменены на слова «произвольной бесконечной мощности» (вместе с группой H требуемым свойством обладают, например, любые её ультрастепени, и их подгруппы, содержащие диагональ).

Поскольку множество решений любого уравнения замкнуто в любой отделимой групповой топологии, мы получаем ответ на вопрос П. И. Кирку [НЗТА85, вопрос 1.4]:

Следствие. *Существует нетривиальная счётная нетопологизируемая группа без кручения.*

Отметим, что, согласно теореме Маркова [M46], дополнение до единицы во всякой счётной нетопологизируемой группе должно разлагаться в объединение множеств решений конечного числа систем уравнений. В известных примерах бесконечных счётных нетопологизируемых групп эти разложения выглядят так:

$$G \setminus \{g_1, \ldots, g_n\} = \bigcup_{i=1}^{n-1} \{g \in G \mid g^n = g_i\} \quad \text{(пример Ольшанского** [O80], [O89] и его модификации [MO98]);}$$

$$G \setminus \{g_1, \ldots, g_{2n}\} = \{g \in G \mid [g, a]^n = 1\} \quad \text{(примеры из [T04]).}$$

Здесь g_i и a — некоторые фиксированные элементы соответствующей группы G, а число n в обоих случаях является большим (по меньшей мере 665) и нечётным. Разложение (1) представляется максимально простым. Отметим однако, что уравнение $w(x) = 1$, построенное при доказательстве основной теоремы, является гораздо более замысловатым (см. формулы (**) и (*)), чем уравнения $x^n = a$ и $[x, a]^n = 1$, фигурирующие в ранее известных примерах счётных нетопологизируемых групп. Отметим ещё, что пример Ольшанского и его модификации является периодическим (при этом примеры Морриса и Образцова [MO98] являются квазициклическими); примеры из [T04] имеют кручение, но периодическими не являются, более того, в [T04] показано, что любая счётная группа может быть вложена в один из таких примеров.

Естественно задать вопрос, какие значения могут принимать мощность множества решений уравнения в группе и мощность дополнения до этого множества? Из основной теоремы нетрудно вывести такой факт:

Теорема 1. *Для любых двух кардиналов $\mathbf{s}$ и $\mathbf{n}$, по крайней мере один из которых бесконечен, найдётся такая группа G (мощности $\mathbf{s} + \mathbf{n}$) и такое уравнение $u(x) = 1$ над ней, что ровно $\mathbf{s}$ элементов группы G являются решениями этого уравнения и ровно $\mathbf{n}$ элементов группы G не являются решениями этого уравнения.*

Замечание. Условие бесконечности одного из кардиналов здесь существенно. Например, нетрудно сообразить, что в группе порядка три число решений никакого уравнения не может быть равно двум.

Авторы благодарят А. Ю. Ольшанского за ряд полезных замечаний.

Работа выполнена при поддержке Российского фонда фундаментальных исследований, грант №02-01-00170.

** Пример Ольшанского является факторгруппой по центральной подгруппе группы, построенной Адяном [A71].

2. Подход Ольшанского к построению групп с заданными свойствами

Градуированным копредставлением мы называем групповое копредставление $G(\infty) = \langle \mathcal{A} \mid \mathcal{R} \rangle$, на множестве определяющих соотношений которого задана фильтрация

$$\mathcal{R} = \bigcup_{i=0}^{\infty} \mathcal{R}_i, \quad \varnothing = \mathcal{R}_0 \subseteq \mathcal{R}_1 \subseteq \ldots .$$

Соотношения из $\mathcal{R}_i \setminus \mathcal{R}_{i-1}$ мы называем *соотношениями ранга* i, а копредставление $\langle \mathcal{A} \mid \mathcal{R}_i \rangle$ мы обозначаем $G(i)$ и рассматриваем как градуированное копредставление (полагая $\mathcal{R}_j = \mathcal{R}_i$ при $j > i$).

В соответствии с [O89], мы говорим, что градуированное копредставление $G(\infty)$ без периодических соотношений удовлетворяет *условию* R (с параметрами α, h, d и n), если, для каждого i, найдётся такое множество $\mathcal{X}_i \subseteq F$ слов (называемых *периодами ранга* i), что

1) длина каждого слова из $\mathcal{X}_i$ равна i и никакое слово из $\mathcal{X}_i$ не сопряжено в $G(i-1)$ степени слова меньшей длины;
2) различные слова из $\mathcal{X}_i$ не сопряжены между собой и не сопряжены к обратным друг другу в $G(i-1)$;
3) каждое соотношение $R \in \mathcal{R}_i \setminus \mathcal{R}_{i-1}$ имеет вид

$$R \equiv \prod_{k=1}^{h} (T_k A^{n_k}), \text{ где } A \in \mathcal{X}_i,$$

причём выполнены условия:

R1. $n_k \geqslant n$.

R2. $|n_i|/|n_j| \leqslant 1 + \frac{1}{2}h^{-1}$.

R3. никакое из слов T_k не равно в $G(i-1)$ слову меньшей длины и $|T_k| < di$.

R4. $T_k \notin \langle A \rangle$ в группе $G(i-1)$.

R5. Слово R не является истинной степенью в свободной группе и, если $V \equiv A^{n_{s-1}} \prod_{k=s}^{s+l} (T_k A^{n_k})$ — циклическое подслово в R, $l \geqslant \alpha^{-1} - 4$ и VV_1, VV_2 — циклические сдвиги слова R, то $V_1 \equiv V_2$;

R6. Пусть $V \equiv A^{m_1} T_k A^{n_k} \ldots T_{k+l} A^{m_2}$ — подслово циклического сдвига соотношения R, где $l \geqslant \alpha^{-1} - 2$, а $V' \equiv A^{m_1'} T_{k'}' A^{n_k'} \ldots T_{k'+l}' A^{m_2'}$ — подслово циклического сдвига соотношения $(R')^{\pm 1}$ с тем же периодом A, причём знаки показателей m_1 и m_1', n_k и n_k', …, m_2 и m_2' совпадают. Пусть V и V' графически разлагаются в произведения $V_0 \ldots V_l$ и $V_0' \ldots V_l'$, где $V_0 \equiv A^{m_1} T_k A^{c_1}$, $V_1 \equiv A^{b_1} T_{k+1} A^{c_2}$, …, $V_l \equiv A^{b_l} T_{k+l} A^{m_2}$, $V_0' \equiv A^{m_1'} T_{k'}' A^{c_1'}$, $V_1' \equiv A^{b_1'} T_{k'+1}' A^{c_2'}$, …, $V_l \equiv A^{b_l'} T_{k'+l}' A^{m_2'}$; причём в группе $G(i-1)$ имеют место равенства $V_j = V_j'$ при $j = 0, \ldots, l$. Тогда $R' \equiv R$, $V' \equiv V$ и V не является подсловом циклического слова R^{-1}.

В книге [O89] можно найти много полезных свойств копредставлений с условием R. Упомянем некоторые из этих свойств.

Лемма 1. *Пусть градуированное копредставление $G(\infty)$ удовлетворяют условию* R *для достаточно маленького числа α и достаточно больших чисел h, d и n ($1 \ll \alpha^{-1} \ll h \ll d \ll n$). Тогда*

1) *абелевы подгруппы группы $G(\infty)$ являются циклическими;*
2) *группа $G(\infty)$ не имеет кручения;*
3) *если элементы X и Y сопряжены в $G(\infty)$, то найдётся такой элемент $Z \in G(\infty)$, что $X = ZYZ^{-1}$ и $|Z| \leqslant (\frac{1}{2} + \alpha)(|X| + |Y|)$;*
4) *если A, B и C — неединичные элементы группы $G(\infty)$ и X — такой элемент, что $X^{-1}AXB$ и C сопряжены в $G(\infty)$, то в двойном смежном классе $\langle A \rangle X \langle B \rangle$ найдётся элемент X' длины меньшей, чем $(\frac{1}{2} + \alpha)(|A| + |B| + |C|) + \left[\frac{1}{2}|A|\right] + \left[\frac{1}{2}|B|\right]$* (здесь квадратные скобки обозначают целую часть числа);
5) если слово X равно единице в $G(\infty)$, то $X = 1$ в группе $\left\langle \mathcal{A} \;\middle|\; \{R \in \mathcal{R} \mid |R| < (1-\alpha)^{-1}|X|\} \right\rangle$.
6) если элементы X и ZXZ^{-1} коммутируют в $G(\infty)$, то X и Z коммутируют в $G(\infty)$.

Доказательство. Все эти свойства доказаны в [O89]: первое утверждение является одним из утверждений теоремы 26.5; второе утверждение является частным случаем леммы 25.2; третье утверждение представляет собой лемму 25.4; четвёртое утверждение есть перевод на алгебраический язык несколько ослабленной формулировки леммы 22.2 о разрезах диаграмм на сфере с тремя дырами; пятое утверждение есть перевод на алгебраический язык леммы 23.16; а шестое утверждение совпадает леммой 25.14.

3. Конструкция группы H

Зафиксируем достаточно большое чётное число h и целое число $n \gg h$. В качестве алфавита $\mathcal{A}$ возьмём множество букв $\{a, b, c_1, c_2, \dots, c_h\}$. Свободную группу с базисом $\mathcal{A}$ обозначим буквой F.

Положим $\mathcal{R}_0 = \mathcal{R}_1 = \mathcal{R}_2 = \varnothing$. Далее, при $i > 2$, предполагая, что копредставление $G(i-1) = \langle \mathcal{A} \mid \mathcal{R}_{i-1} \rangle$ уже определено, определим копредставление $G(i) = \langle \mathcal{A} \mid \mathcal{R}_i \rangle$. В качестве периодов ранга i возьмём некоторое множество слов $\mathcal{X}_i \subset F$ длины i, удовлетворяющее условиям

1) никакое слово из $\mathcal{X}_i$ не сопряжено в $G(i-1)$ слову меньшей длины;
2) различные слова из $\mathcal{X}_i$ не сопряжены между собой и не сопряжены к обратным друг другу в группе $G(i-1)$;
3) каждое слово из $\mathcal{X}_i$ равно ab в $G(i-1)/([G(i-1), G(i-1)] \langle c_1 c_2 \dots c_h \rangle)$;
4) множество $\mathcal{X}_i$ максимально среди всех множеств, удовлетворяющих условиям 1), 2) и 3).

Определим множество $\mathcal{Y}_{i,j,Z} \subseteq F$, где $j = 1, \dots, h$, $Z \in G(i-1)$, как множество всех минимальных (то есть не равных словам меньшей длины) в $G(i-1)$ слов длины меньшей чем di, представляющих в $G(i-1)$ элемент Zc_jZ^{-1}. Положим

$$\mathcal{R}_i = \mathcal{R}_{i-1} \cup \mathcal{T}_i,$$

где $\mathcal{T}_i$ есть максимальное множество попарно несопряжённых в $G(i-1)$ слов вида

$$R = R_{A,Z} = \prod_{j=1}^{h} \left(T_j A^{(-1)^j n} \right), \quad \text{где } A \in \mathcal{X}_i,\ T_j \in \mathcal{Y}_{i,j,Z},\ Z \in G(i-1).$$

Лемма 2. *Градуированное копредставление*

$$H = G(\infty) = \langle \mathcal{A} \mid \mathcal{R} \rangle, \quad \text{где } \mathcal{R} = \bigcup_{i=0}^{\infty} \mathcal{R}_i,$$

удовлетворяет условию R.

Доказательство. Заметим, что по модулю коммутанта каждое из соотношений нашего копредставления имеет вид $c_1 c_2 \dots c_h$, $T_j = c_j$, а каждый период имеет вид $ab(c_1 \dots c_h)^k$; поэтому периоды не являются истинными степенями и условия 1), 2), R1, R2 и R3 выполнены по построению. Условие R4 очевидным образом выполнено даже по модулю коммутанта.

Поскольку, как известно, длинные общие подслова двух слов вида A^n обязаны быть согласованными, из невыполнения условия R5 следовало бы, что либо одно из слов T_j лежит в $\langle A \rangle$, либо два слова T_j с разными номерами j лежат в одном и том же двойном смежном классе по $\langle A \rangle$; ни то, ни другое очевидным образом невозможно даже по модулю коммутанта.

Предположим, что условие R6 не выполнено. Мы имеем равенство вида $T_j^{\pm 1} A^p = A^s T'_{j'}$ в $G(i-1)$. Рассматривая это равенство по модулю коммутанта, мы приходим к выводу, что $j = j'$, $p = s$ и $\pm 1 = 1$. Вспоминая, что $T_j = Zc_jZ^{-1}$ и $T'_j = Z'c_j(Z')^{-1}$ в группе $G(i-1)$, мы видим, что c_j коммутирует с $Z^{-1}A^pZ'$ в группе $G(i-1)$. Поскольку по индукции мы можем считать, что копредставление $G(i-1)$ удовлетворяет условию R, то есть, в частности, коммутировать в $G(i-1)$ могут только степени одного и того же элемента (по лемме 1), а c_j не являются истинными степенями (даже по модулю коммутанта), мы получаем равенство вида $Z^{-1}A^pZ' = c_j^k$. Но то, что условие R6 не выполнено для $G(i)$, означает, что подобные равенства выполняются в $G(i-1)$ для многих номеров j. А рассматривая два таких равенства

$$Z^{-1}A^pZ' = c_j^k \quad \text{и} \quad Z^{-1}A^{p_1}Z' = c_{j_1}^{k_1}$$

при $j \neq j_1$ по модулю коммутанта, мы приходим к выводу, что $k = 0$, то есть $Z' \in \langle A \rangle Z$ и слова R и R' представляют сопряжённые элементы группы $G(i-1)$, что по построению означает $R \equiv R'$.

4. Доказательство основной теоремы

Лемма 3. *Для каждого элемента g коммутанта группы H и слова A, сопряжённого в H элементу $g^{-1}agb$, найдётся такое слово Z длины не большей $\frac{1}{3}d|A|$, что $Z^{-1}AZ = g^{-1}agb$ в H.*

Доказательство. Согласно утверждению 4) леммы 1, $|a^pgb^r| < |A| + 2$ для некоторых целых p и r (здесь и далее речь идёт о длинах элементов в $H = G(\infty)$). Но рассмотрев элемент a^pgb^r по модулю коммутанта, мы видим, что $|a^pgb^r| \geqslant |p| + |r|$ и, следовательно,

$$|g| \leqslant |p| + |r| + |a^pgb^r| \leqslant 2|a^pgb^r| < 2|A| + 4 \quad \text{и} \quad |g^{-1}agb| < 4|A| + 10.$$

Из последнего неравенства по утверждению 3) леммы 1 вытекает, что найдётся такой элемент Z, что $Z^{-1}AZ = g^{-1}agb$ и

$$|Z| \leqslant |A| + |g^{-1}agb| < 5|A| + 10 < \frac{1}{3}d|A|$$

(последнее неравенство обеспечивается тем, что $d \gg 1$).

Рассмотрим уравнение

$$v(x) = 1, \quad \text{где } v(x) \equiv \prod_{j=1}^{h} \left(c_j(x^{-1}axb)^{(-1)^j n}\right) \in H * \langle x \rangle_\infty\,, \tag{$*$}$$

над группой H.

Лемма 4. *В группе H всякий неединичный элемент коммутанта является решением уравнения $(*)$, а единица не является решением этого уравнения.*

Доказательство. То, что $v(1) \neq 1$, вытекает из утверждения 5) леммы 1, поскольку $v(1) \neq 1$ в свободной группе, а длина каждого определяющего соотношения R группы H не меньше, чем $3(n-d-2)h$, и

$$\frac{|v(1)|}{|R|} \leqslant \frac{2n+1}{3(n-d-2)} < 1 - \alpha \quad \text{при } \alpha < \frac{1}{3} \text{ и } n \gg d.$$

Покажем теперь, что всякий неединичный элемент g коммутанта группы H является решением уравнения $(*)$. Пусть $u \in F$ — слово минимальной длины, представляющее элемент, сопряжённый к $g^{-1}agb$.

Если $|u| \leqslant 2$, то $u = ab$ или $u = ba$ (в чём легко убедиться рассматривая u по модулю коммутанта). При этом, в соответствии с утверждением 4) леммы 1, u сопряжено с элементом вида $\widetilde{g}^{-1}a\widetilde{g}b$, где $\widetilde{g} \in \langle a \rangle\, g\, \langle b \rangle$ и $|\widetilde{g}| < 3$. Рассматривая $\widetilde{g}$ по модулю коммутанта, мы видим, что

$$\widetilde{g} \text{ есть либо } 1, \text{ либо } a^{\pm 1}, \text{ либо } b^{\pm 1}, \text{ либо } a^{\pm 1}b^{\pm 1}, \text{ либо } b^{\pm 1}a^{\pm 1}.$$

Первые 4 случая невозможны, поскольку они означают, что $g \in \langle a \rangle \langle b \rangle \cap [H,H] = \{1\}$. А в том, что равенство $\widetilde{g} = b^{\pm 1}a^{\pm 1}$ невозможно, легко убедиться рассматривая соотношение $\widetilde{g}^{-1}a\widetilde{g}b \sim u \sim ab$ по модулю нормальной подгруппы $\langle\!\langle c_1, \dots, c_h \rangle\!\rangle$, порождённой $\{c_1, \dots, c_h\}$, так как $G(\infty)/\langle\!\langle c_1, \dots, c_h \rangle\!\rangle$ есть свободная группа с базисом $\{a, b\}$.

Мы показали, что $|u| > 2$. Но в таком случае, u сопряжено с некоторым периодом A ранга $|u|$ (по определению множества $\mathcal{X}_{|u|}$). По лемме 3, $Z^{-1}AZ = g^{-1}agb$ для некоторого слова Z длины не большей, чем $\frac{1}{3}d|A|$. Следовательно, для каждого $j = 1, \dots, h$, некоторое минимальное слово T_j, представляющее в $G(|u|-1)$ элемент Zc_jZ^{-1}, имеет длину меньшую, чем $d|A|$, и, стало быть, по построению, слово

$$\prod_{j=1}^{h} \left(T_j A^{(-1)^j n}\right)$$

сопряжено к одному из определяющих соотношений группы $G(|u|)$, что и доказывает лемму.

Лемма 5. *Множество решений уравнения*

$$[c_1 v([a,x]) c_1^{-1}, v([b,x])] = 1 \tag{$**$}$$

над H есть $H \setminus \{1\}$.

Доказательство. Поскольку a не является истинной степенью (по модулю коммутанта), согласно лемме 1, $[a,g] \neq 1$ при $g \notin \langle a \rangle$. Следовательно, по лемме 4, все элементы группы H, не лежащие в $\langle a \rangle$, являются решениями уравнения $(**)$. По тем же причинам все элементы группы H, не лежащие в $\langle b \rangle$, являются решениями уравнения $(**)$. Но $\langle a \rangle \cap \langle b \rangle = \{1\}$, в чём легко убедиться, опять рассмотрев факторгруппу по коммутанту.

Осталось доказать, что единица не является решением уравнения $(**)$. Предположив противное, мы бы имели $[c_1 v(1) c_1^{-1}, v(1)] = 1$. По утверждению 6) леммы 1, это означает, что $[c_1, v(1)] = 1$. Последнее равенство в свою очередь означает, что $v(1) \in \langle c_1 \rangle$ (по лемме 1 и поскольку c_1 не является истинной степенью (по модулю коммутанта)). Рассматривая равенство $v(1) = c_1^k$ по модулю коммутанта, мы приходим к выводу, что $k = 0$ и $v(1) = 1$, что противоречит лемме 4.

Лемма 5 доказана, а вместе с ней доказана и основная теорема, поскольку, согласно лемме 1, группа H не имеет кручения.

5. Доказательство теоремы 1

Если $\mathbf{n} = 0$, $\mathbf{s} = 0$ или $\mathbf{s} = 1$, то «уравнения» $1 = 1$, $g = 1$ (где g — нетривиальный элемент группы) и $x = 1$ над группой подходящей мощности очевидным образом обладают нужными свойствами.

Если $1 < \mathbf{s} \leqslant \mathbf{n}$, то в качестве группы G можно взять свободное произведение произвольной абелевой группы A мощности $\mathbf{s}$ и произвольной группы B мощности $\mathbf{n}$. Нетрудно сообразить, что решениями уравнения $xa = ax$, где $a \in A \setminus \{1\}$, будут все элементы группы A и только они. Таким образом, число решений будет равно $\mathbf{s}$, а число нерешений будет равно $\mathbf{n}$ (поскольку кардинал $\mathbf{n}$ бесконечен и не меньше, чем $\mathbf{s}$).

Если $\mathbf{s} > \mathbf{n} > 0$, то в качестве группы G можно взять прямое произведение группы H мощности $\mathbf{s}$, существование которой утверждается в основной теореме и в замечании после неё, и произвольной группы K мощности $\mathbf{n}$. В качестве уравнения следует взять уравнение $w(x) = 1$ из основной теоремы. Поскольку построенное при доказательстве основной теоремы уравнение $(**)$ имеет нулевую сумму показателей при x, множеством его решений в группе $G = H \times K$ будет $(H \setminus \{1\}) \times K$, а множеством его нерешений будет $\{1\} \times K$, что и влечёт утверждение теоремы.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

[A71] Адян С. И. О некоторых группах без кручения// Изв. АН СССР, сер. матем. – 1971.– Т.35, №3.– С. 459–468.

[M46] Марков А. А. О безусловно замкнутых множествах // Мат. сб.– 1946.– Т.18, №1.– С. 3–28.

[MO98] Morris S. A., Obraztsov V. N. Nondiscrete topological groups with many discrete subgroups // Topology Appl. – 1998.– V. 84.– pp. 105–120.

[НЗТА85] Нерешённые задачи топологической алгебры. (ред. В.И.Арнаутов, А.В.Архангельский, П.И.Кирку, А.В.Михалёв, Ю.Н. Мухин, И.В.Протасов, М.М.Чобан), Кишинёв: Штиинца, 1985.

[O80] Ольшанский А. Ю. Замечание о счётной нетопологизируемой группе // Вестн. МГУ: мат., мех.– 1980.– №3.– С. 103.

[O89] Ольшанский А. Ю. Геометрия определяющих соотношений в группах. М.: Наука, 1989.

[T04] Трофимов А. В. Теорема вложения в нетопологизируемую группу // Вестн. МГУ: мат., мех. (в печати).