УДК 512.543

Е. А. Иванова, Д. И. Молдаванский

ОБ АППРОКСИМИРУЕМОСТИ ОТНОСИТЕЛЬНО СОПРЯЖЕННОСТИ КОНЕЧНЫМИ ГРУППАМИ РАЗРЕШИМЫХ ГРУПП БАУМСЛАГА — СОЛИТЭРА

Показано, что произвольная группа вида $\langle a, b;\ a^{-1}ba = b^k\rangle$, где k отлично от нуля и ±1, не является аппроксимируемой относительно сопряженности конечными π-группами для любого множества π, состоящего из двух простых чисел.

Ключевые слова: группы Баумслага — Солитэра, аппроксимируемость конечными π-группами, аппроксимируемость относительно сопряженности конечными π-группами.

It is shown that any group $\langle a, b;\ a^{-1}ba = b^k\rangle$ where integer k differs from zero and ±1 is not conjugacy separable by finite π-groups for every set π consisting of two prime numbers.

Key words: Baumslag — Solitar groups, residuality a finite π-groups, conjugacy separability by finite π-groups.

Напомним, что если $\mathcal{K}$ — некоторый класс групп, то группа G называется $\mathcal{K}$-аппроксимируемой ($\mathcal{K}$-аппроксимируемой относительно сопряженности), если для любых различных (соответственно не сопряженных) ее элементов a и b существует такой гомоморфизм группы G на некоторую группу X из класса $\mathcal{K}$, что образы этих элементов различны (соответственно не сопряжены в группе X).

Через $\mathcal{F}$ будет обозначаться класс всех конечных групп, и для некоторого простого числа p и некоторого множества π простых чисел символы $\mathcal{F}_p$ и $\mathcal{F}_\pi$ будут обозначать соответственно класс всех конечных p-групп и класс всех конечных π-групп.

Для произвольного целого числа $k \neq 0$ через G_k будем обозначать группу, задаваемую представлением вида $\langle a, b;\ a^{-1}ba = b^k\rangle$. Группы G_k входят в известный класс групп Баумслага — Солитэра, и многие их свойства хорошо изучены. Известно, в частности, что все они разрешимы (точнее, метабелевы) и что нециклическая группа с одним определяющим соотношением удовлетворяет нетривиальному тождеству тогда и только тогда, когда она изоморфна некоторой группе G_k. $\mathcal{F}$-аппроксимируемость групп этого семейства, отмеченная в [10], вытекает, в действительности, уже из основного результата статьи [11], утверждающего $\mathcal{F}$-аппроксимируемость произвольных конечно порожденных метабелевых групп. Утверждение об $\mathcal{F}$-аппроксимируемости относительно сопряженности групп G_k, доказанное в [8], вытекает и из полученного в [9] более общего результата об $\mathcal{F}$-аппроксимируемости относительно сопряженности любого нисходящего HNN-расширения конечно порожденной абелевой группы.

Известно также [6], что группа G_k является $\mathcal{F}_p$-аппроксимируемой в точности тогда, когда число $k-1$ делится на p. В работе [2] доказано, что группа G_k почти $\mathcal{F}_p$-аппроксимируема (т. е. обладает $\mathcal{F}_p$-аппроксимируемой нормальной подгруппой конечного индекса) тогда и только тогда, когда k не делится на p. Теорема 2 из работы [4] утверждает, что если $\pi = \{p, q\}$, где $p < q$ — простые числа, не делящие число $k-1$, то группа G_k $\mathcal{F}_\pi$-аппроксимируема тогда и только тогда, когда $(k, q) = 1$, p является делителем числа $q-1$ и порядок числа k по модулю q является p-числом. (Здесь, как обычно, (x, y) обозначает наибольший общий делитель чисел x и y. Напомним также (см. [3, с. 60]), что для любого целого числа k, взаимно простого с целым числом $m > 0$, порядком числа k по модулю m называется наименьшее положительное число r такое, что $k^r \equiv 1 \pmod{m}$.)

С другой стороны, в работе [7] было доказано, что если число k отлично от ± 1, то для любого простого числа p группа G_k не является $\mathcal{F}_p$-аппроксимируемой относительно сопряженности. Основным результатом данной статьи является справедливость аналогичного утверждения для любого множества π, состоящего из двух простых чисел. А именно здесь будет доказана

Теорема. *Для любого целого числа k, отличного от 0 и ± 1, и для любого множества $\pi = \{p, q\}$, состоящего из двух различных простых чисел p и q, группа G_k не является $\mathcal{F}_\pi$-аппроксимируемой относительно сопряженности.*

По поводу ограничения $k \neq \pm 1$ следует заметить, что при $k = 1$ группа G_k является свободной абелевой и потому $\mathcal{F}_\pi$-аппроксимируемой относительно сопряженности для любого множества π простых чисел. Легко видеть также, что если группа G_{-1} является $\mathcal{F}_\pi$-аппроксимируемой, то множество π должно содержать число 2. Наоборот, если $2 \in \pi$, то группа G_{-1} $\mathcal{F}_\pi$-аппроксимируема относительно сопряженности в силу теоремы 1 из работы [1].

Доказательство теоремы начнем с формулировок ряда вспомогательных утверждений.

Прежде всего, введем в рассмотрение одно семейство конечных гомоморфных образов группы G_k, а именно семейство групп вида

$$G_k(r, s) = \langle a, b;\ a^{-1}ba = b^k,\ a^r = 1,\ b^s = 1 \rangle,$$

где положительные целые числа r и s удовлетворяют сравнению $k^r \equiv 1 \pmod{s}$. Хорошо известно (см., напр., [5, с. 31]), что группа $G_k(r, s)$ является конечной порядка rs, порядки ее элементов a и b равны числам

r и s соответственно и произвольный ее элемент однозначно представим в виде $a^i b^j$, где $0 \leqslant i < r$ и $0 \leqslant j < s$. Каждая группа $G_k(r,s)$ является, очевидно, гомоморфным образом группы G_k, и, как легко видеть, любой гомоморфизм φ группы G_k на конечную группу проходит через группу $G_k(r,s)$, где r и s — порядки элементов $a\varphi$ и $b\varphi$ соответственно. В частности, для любого множества π простых чисел произвольный гомоморфизм группы G_k на конечную π-группу проходит через некоторую π-группу $G_k(r,s)$.

Предложение 1. (Предложения 1 и 2 из [7].) *Для любых целых чисел m и n элементы b^m и b^n группы G_k сопряжены в этой группе тогда и только тогда, когда или $m = nk^t$, или $n = mk^t$ для некоторого $t \geqslant 0$. В частности, если m и n — различные целые числа, не делящиеся на k, то элементы b^m и b^n не сопряжены в группе G_k.*

Для любых целых чисел m и n элементы b^m и b^n группы $G_k(r,s)$ сопряжены в этой группе тогда и только тогда, когда для некоторого целого числа $x \geqslant 0$ выполнено сравнение $mk^x \equiv n \pmod{s}$.

Содержащийся в этом предложении критерий сопряженности степеней элемента b в группе $G_k(r,s)$ допускает следующую теоретико-групповую формулировку. Рассмотрим мультипликативную группу $\mathbb{Z}_s^*$ кольца $\mathbb{Z}_s$ вычетов целых чисел по модулю s. Для произвольного целого числа n элемент $n + s\mathbb{Z}$ кольца $\mathbb{Z}_s$ будем обозначать через $\overline{n}$. Элемент $\overline{n}$ входит в группу $\mathbb{Z}_s^*$ в точности тогда, когда $(n,s) = 1$, и в этом случае порядок числа n по модулю s совпадает с порядком элемента $\overline{n}$ группы $\mathbb{Z}_s^*$. Для любых чисел m и n, взаимно простых с числом s, предложение 1 утверждает, что элементы b^m и b^n сопряжены в группе $G_k(r,s)$ тогда и только тогда, когда в группе $\mathbb{Z}_s^*$ элементы $\overline{m}$ и $\overline{n}$ принадлежат одному и тому же смежному классу по подгруппе $\overline{K}$, порождаемой в $\mathbb{Z}_s^*$ элементом $\overline{k}$.

Предложение 2. *Пусть простое число p является делителем числа $k-1$ и пусть t — наибольший показатель степени числа p, делящей $k-1$.*

Если $p > 2$ или $t > 1$, то для любого $i \geqslant t$ порядок числа k по модулю p^i равен p^{i-t}.

Если $p = 2$, $t = 1$ и t_1 — наибольший показатель степени числа 2, делящей число $k^2 - 1$, то для любого $i \geqslant t_1$ порядок числа k по модулю 2^i равен 2^{i-t_1+1}.

Для доказательства этого заметим, что по условию число k записывается в виде $k = 1 + p^t u$ для некоторого целого числа u, взаимно простого с p. Если $p > 2$ или $t > 1$, то с помощью очевидной индукции нетрудно показать, что для любого целого $l \geqslant 0$ существует такое целое число u_l, взаимно простое с p, что выполнено равенство

$$k^{p^l} = 1 + p^{t+l} u_l. \tag{1}$$

Отсюда для любого $i \geqslant t$ при $l = i - t$ получаем $k^{p^{i-t}} \equiv 1 \pmod{p^i}$, и если для некоторого $l > 0$ выполнено сравнение $k^{p^l} \equiv 1 \pmod{p^i}$, то из (1) следует, что число $p^{t+l}u_l$ должно делиться на p^i, откуда $l \geqslant i - t$. Следовательно, порядок числа k по модулю p^i равен p^{i-t}.

Пусть теперь $p = 2$ и $k = 1+2u$, где u — нечетное число. Тогда число $k^2 = 1+4u(1+u)$ имеет вид $k^2 = 1+2^{t_1}v$ для некоторых целых $t_1 \geqslant 3$ и v, где v нечетно. Ввиду рассмотренного случая для любого $i \geqslant t_1$ порядок числа k^2 по модулю 2^i равен 2^{i-t_1}. Так как $\mathbb{Z}^*_{2^i}$ является 2-группой и число $k-1$ не делится на 2^i, отсюда следует, что для любого $i \geqslant t_1$ порядок числа k по модулю 2^i равен 2^{i-t_1+1}.

Начиная с этого места, будем считать, что множество π состоит из двух простых чисел p и q, причем $p < q$. Обозначим через $S(k, \pi)$ множество всех положительных π-чисел s таких, что порядок по модулю s числа k является π-числом. Очевидно, что для произвольного π-числа s сравнение $k^r \equiv 1 \pmod{s}$ выполнено для некоторого π-числа r тогда и только тогда, когда $s \in S(k, \pi)$. Очевидно также, что если $s \in S(k, \pi)$, то все натуральные делители числа s также принадлежат множеству $S(k, \pi)$.

Предложение 3. *Если $p \in S(k, \pi)$,то число $k - 1$ делится на p. Если $q \in S(k, \pi)$, то порядок числа k по модулю q является p-числом.*

В самом деле, если $p \in S(k, \pi)$, то для некоторого π-числа r выполнено сравнение $k^r \equiv 1 \pmod{p}$. Так как к тому же по теореме Ферма $k^{p-1} \equiv 1 \pmod{p}$ и числа r и $p-1$ взаимно просты, имеем $k \equiv 1 \pmod{p}$, и первое утверждение предложения доказано.

Аналогично, если $q \in S(k, \pi)$, то порядок числа k по модулю q является π-числом, делящим число $q - 1$, и потому является p-числом (возможно, равным 1). Предложение 3 доказано.

Наоборот, из предложения 2 следует, очевидно, что если p является делителем числа $k - 1$, то $p^i \in S(k, \pi)$ для любого $i \geqslant 1$. Аналогичное обращение второго утверждения предложения 3 также справедливо. Более точно, имеет место

Предложение 4. *Пусть порядок числа k по модулю q равен p^l для некоторого $l \geqslant 0$ и пусть t — наибольший показатель степени числа q, делящей $k^{p^l} - 1$. Тогда для любого $j \geqslant t$ порядок числа k по модулю q^j равен $p^l q^{j-t}$ и потому $q^i \in S(k, \pi)$ для любого $i \geqslant 1$.*

Доказательство. По условию число k^{p^l} имеет вид

$$k^{p^l} = 1 + q^t u,$$

где $t > 0$ и u взаимно просто с q. Поскольку $q > 2$, из предложения 2 следует, что для любого $j \geqslant t$ порядок числа k^{p^l} по модулю q^j равен q^{j-t}. Поэтому для любого $j \geqslant t$ выполнено сравнение

$$k^{p^l q^{j-t}} \equiv 1 \pmod{q^j},$$

из которого следует, что для $j \geqslant t$ порядок числа k по модулю q^j является числом вида $p^x q^y$, где $0 \leqslant x \leqslant l$ и $0 \leqslant y \leqslant j - t$. Так как из сравнения

$$k^{p^x q^y} \equiv 1 \pmod{q^j} \tag{2}$$

следует сравнение $k^{p^x q^y} \equiv 1 \pmod{q}$ и порядок числа k по модулю q равен p^l, число $p^x q^y$ должно делиться на p^l и потому $l \leqslant x$. Таким образом, $x = l$. Теперь сравнение (2) может быть переписано в виде

$$\left(k^{p^l}\right)^{q^y} \equiv 1 \pmod{q^j},$$

и, так как порядок числа k^{p^l} по модулю q^j равен q^{j-t}, число q^y должно делиться на q^{j-t}. Следовательно, $y = j - t$, и предложение 4 доказано.

Предложение 5. *Пусть простое число p является делителем числа $k-1$ и пусть t_1 — наибольший показатель степени числа p, делящей $k-1$. Предположим также, что порядок числа k по модулю q равен p^l для некоторого $l \geqslant 0$, и пусть t_2 — наибольший показатель степени числа q, делящей $k^{p^l} - 1$. Если $p > 2$ или $t_1 > 1$, то для любых $i \geqslant t_1 + l$ и $j \geqslant t_2$ порядок числа k по модулю $p^i q^j$ равен $p^{i-t_1} q^{j-t_2}$.*

Доказательство. В силу предложения 2 для любого $i \geqslant t_1 + l$ порядок числа k по модулю p^i равен p^{i-t_1}, а из предложения 4 имеем, что для любого $j \geqslant t_2$ порядок числа k по модулю q^j равен $p^l q^{j-t_2}$. Из сравнений

$$k^{p^{i-t_1}} \equiv 1 \pmod{p^i} \quad \text{и} \quad k^{p^l q^{j-t_2}} \equiv 1 \pmod{q^j}$$

вытекает, очевидно, сравнение

$$k^{p^{i-t_1+l} q^{j-t_2}} \equiv 1 \pmod{p^i q^j}.$$

Поэтому для $i \geqslant t_1 + l$ и $j \geqslant t_2$ порядок числа k по модулю $p^i q^j$ является числом вида $p^x q^y$, где $0 \leqslant x \leqslant i - t_1 + l$ и $0 \leqslant y \leqslant j - t_2$. Так как из сравнения

$$k^{p^x q^y} \equiv 1 \pmod{p^i q^j} \tag{3}$$

следует сравнение $k^{p^x q^y} \equiv 1 \pmod{p^i}$, число $p^x q^y$ должно делиться на p^{i-t_1}, откуда имеем $x \geqslant i - t_1$.

Аналогично, поскольку из (3) следует сравнение

$$k^{p^x q^y} \equiv 1 \pmod{q^j},$$

получаем $x \geqslant l$ и $y \geqslant j - t_2$ Таким образом, $y = j - t_2$, а x удовлетворяет системе неравенств

$$\begin{cases} x \leqslant i - t_1 + l, \\ x \geqslant i - t_1, \\ x \geqslant l. \end{cases}$$

Очевидно, что наименьшим решением этой системы является

$$x = \max\{i - t_1, l\},$$

и, так как $i \geqslant t_1 + l$, порядок числа k по модулю $p^i q^j$ действительно равен $p^{i-t_1} q^{j-t_2}$.

Аналогично доказывается

Предложение 6. *Пусть $p = 2$ и число $k - 1$ делится на 2 и не делится на 4. Пусть t_1 — наибольший показатель степени числа 2, делящей $k^2 - 1$. Предположим также, что порядок числа k по модулю q равен 2^l для некоторого $l \geqslant 0$ и пусть t_2 — наибольший показатель степени числа q, делящей $k^{2^l} - 1$. Тогда для любых $i \geqslant t_1 + l - 1$ и $j \geqslant t_2$ порядок числа k по модулю $2^i q^j$ равен $2^{i-t_1+1} q^{j-t_2}$.*

Переходя непосредственно к доказательству утверждения теоремы, покажем, что для произвольного числа k, отличного от нуля и ± 1, и любого множества π, состоящего из двух простых чисел p и q, $p < q$, группа G_k не является $\mathcal{F}_\pi$-аппроксимируемой относительно сопряженности. Это очевидно, если при каждом гомоморфизме группы G_k на конечную π-группу элемент b переходит в единицу: в этом случае группа G_k не является уже $\mathcal{F}_\pi$-аппроксимируемой. Таким образом, мы можем считать, что существует гомоморфизм группы G_k на конечную π-группу, при котором образ элемента b отличен от единицы, т. е. множество $S(k, \pi)$ содержит числа, отличные от 1.

Для доказательства теоремы нам достаточно указать целое число m такое, что элементы b и b^m не сопряжены в группе G_k, но их образы при естественном гомоморфизме группы G_k на произвольную π-группу вида $G_k(r, s)$ сопряжены в этой группе. Выбор числа m будет зависеть от делимости на p числа $k - 1$ и от порядка числа k по модулю q, и мы рассмотрим отдельно три случая.

Случай 1. Число $k - 1$ не делится на p.

Из предложения 3 следует, что в этом случае все элементы множества $S(k, \pi)$ являются q-числами, и, так как множество $S(k, \pi)$ содержит числа, отличные от 1, в него входит число q. Поэтому из предложения 3 вытекает, что порядок числа k по модулю q является p-числом. Обозначая, как в формулировке предложения 4, порядок числа k по модулю q через p^l и наибольший показатель степени числа q, делящей $k^{p^l} - 1$, через t, имеем в силу этого предложения, что для любого $j \geqslant t$ порядок числа k по модулю q^j равен $p^l q^{j-t}$. Отметим, что, поскольку p^l является делителем числа $q - 1$, $q - 1 = p^l x$ для некоторого целого x.

Таким образом, для любого $j \geqslant t$ порядок подгруппы $\overline{K}$, порождаемой в группе $\mathbb{Z}^*_{q^j}$ элементом $\overline{k}$, равен $p^l q^{j-t}$. Поэтому индекс подгруппы $\overline{K}$ в группе $\mathbb{Z}^*_{q^j}$ равен

$$\frac{q^{j-1}(q-1)}{p^l q^{j-t}} = q^{t-1} x.$$

Пусть $n > 1$ — целое число, взаимно простое с числами k и q, и пусть $m = n^{q^{t-1}x}$. Тогда $\overline{n} = n + q^j\mathbb{Z}$ является элементом группы $\mathbb{Z}^*_{q^j}$ и потому при любом $j \geqslant t$ элемент $\overline{m} = \overline{n}^{\,q^{t-1}x}$ входит в ее подгруппу $\overline{K}$. Таким образом, в группе $\mathbb{Z}^*_{q^j}$ элементы $\overline{1}$ и $\overline{m}$ лежат в одном классе по подгруппе $\overline{K}$. Поэтому из предложения 1 следует, что элементы b и b^m группы G_k не сопряжены в этой группе, но их образы сопряжены в любой группе вида $G_k(r, q^j)$, где $j \geqslant t$. Так как число j может быть выбрано сколь угодно большим и так как при $i \leqslant j$ группа $G_k(r, q^i)$ является гомоморфным образом группы $G_k(r, q^j)$, образы элементов b и b^m при любом гомоморфизме группы G_k на конечную π-группу сопряжены.

Случай 2. Число $k-1$ делится на p, а порядок числа k по модулю q не является p-числом.

В этом случае в силу предложения 3 все элементы множества $S(k,\pi)$ являются p-числами. Из предложения 2 следует, что существует целое число $t > 1$, зависящее только от чисел p и k, такое, что для любого $i \geqslant t$ порядок числа k по модулю p^i равен p^{i-t} или p^{i-t+1}. В любом случае при таких значениях i в группе $\mathbb{Z}^*_{p^i}$ индекс подгруппы $\overline{K}$, порождаемой элементом $\overline{k}$, будет делителем числа $p^{t-1}(p-1)$. Поэтому если целое число $n > 1$ взаимно просто с числами k и p и $m = n^{p^{t-1}(p-1)}$, то при $i \geqslant t$ в группе $\mathbb{Z}^*_{p^i}$ элемент $\overline{m}$ входит в подгруппу $\overline{K}$. Отсюда, как и в случае 1, получаем, что элементы b и b^m не сопряжены в группе G_k, но их образы в любом гомоморфном образе этой группы, являющемся конечной π-группой, сопряжены.

Случай 3. Число $k-1$ делится на p, и порядок числа k по модулю q является p-числом.

Если $p > 2$ или $p = 2$ и $k-1$ делится на 4, а числа t_1, l и t_2 выбраны так, как в формулировке предложения 5, то в силу этого предложения для любых $i \geqslant t_1 + l$ и $j \geqslant t_2$ индекс в группе $\mathbb{Z}^*_{p^iq^j}$ подгруппы $\overline{K}$ равен $p^{t_1-1}q^{t_2-1}(p-1)(q-1)$. Поэтому если

$$m = n^{p^{t_1-1}q^{t_2-1}(p-1)(q-1)},$$

где число $n > 1$ взаимно просто с числами k, p и q, элементы b и b^m не сопряжены в группе G_k, но их образы в любом гомоморфном образе этой группы, являющемся конечной π-группой, сопряжены.

Случай, когда $p = 2$ и $k-1$ не делится на 4, рассматривается аналогично, но с использованием предложения 6 вместо предложения 5.

Библиографический список

1. *Азаров Д. Н., Молдаванский Д. И.* О сверхразрешимых группах, аппроксимируемых конечными p-группами относительно сопряженности // Вестн. Иван. гос. ун-та. 2005. Вып. 3. С. 59—67.
2. *Азаров Д. Н., Сергина Е. А.* О почти аппроксимируемости конечными p-группами некоторых групп Баумслага — Солитэра // Науч. тр. Иван. гос. ун-та. Математика. Вып. 6 (2008). С. 23—28.
3. *Айерлэнд К., Роузен М.* Классическое введение в современную теорию чисел. М. : Мир, 1987. 415 с.
4. *Иванова О. А., Молдаванский Д. И.* Аппроксимируемость конечными π-группами некоторых групп с одним определяющим соотношением // Науч. тр. Иван. гос. ун-та. Математика. Вып. 6 (2008). С. 51—58.
5. *Магнус В., Каррас А., Солитэр Д.* Комбинаторная теория групп. М. : Наука, 1974. 455 с.
6. *Молдаванский Д. И.* Аппроксимируемость конечными p-группами HNN-расширений // Вестн. Иван. гос. ун-та. 2000. Вып. 3. С. 129—140.
7. *Молдаванский Д. И.* Об аппроксимируемости относительно сопряженности конечными p-группами некоторых групп с одним определяющим соотношением // Там же. 2007. Вып. 3. С. 89—94.
8. *Молдаванский Д. И., Кравченко Л. В., Фролова Е. Н.* Финитная аппроксимируемость относительно сопряженности некоторых групп с одним определяющим соотношением // Алгоритмические проблемы теории групп и полугрупп / Тул. гос. пед. ин-т. Тула, 1986. С. 81—91.
9. *Соколов Е. В.* Финитная аппроксимируемость относительно сопряженности нисходящих HNN-расширений конечно порожденных абелевых групп // Мат. заметки. 2005. Т. 78, вып. 5. С. 748—762.
10. *Baumslag G., Solitar D.* Some two-generator one-relator non-Hopfian groups // Bull. Amer. Math. Soc. 1962. Vol. 68. P. 199—201.
11. *Hall P.* On the finiteness of certain soluble groups // Proc. London Math. Soc. 1959. Vol. 9, № 36. P. 595—622.