Вестник Ивановского государственного университета

Серия «Биология, Химия, Физика, Математика»

Вып. 3 / 2007 С. 89 – 94

Д. И. Молдаванский

ОБ АППРОКСИМИРУЕМОСТИ ОТНОСИТЕЛЬНО СОПРЯЖЕННОСТИ КОНЕЧНЫМИ *P*-ГРУППАМИ НЕКОТОРЫХ ГРУПП С ОДНИМ ОПРЕДЕЛЯЮЩИМ СООТНОШЕНИЕМ

Известно, что группа $G_k = \langle a, b;\ a^{-1}ba = b^k \rangle$ $(k \neq 0)$ аппроксимируема конечными p-группами в точности тогда, когда p является делителем числа $k-1$. Здесь доказано, что при $k \neq \pm 1$ для любого простого числа p группа G_k не является аппроксимируемой относительно сопряженности конечными p-группами.

It is known that group $G_k = \langle a, b;\ a^{-1}ba = b^k \rangle$ $(k \neq 0)$ is residually a finite p-group if and only if p divides the integer $k - 1$. We prove here that if $k \neq \pm 1$ then for any prime p group G_k is not conjugacy separable in the class of finite p-groups.

УДК 512.543.

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, несопряженных) 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). Пусть $\mathcal{F}$ обозначает класс всех конечных групп и для простого числа p пусть $\mathcal{F}_p$ обозначает класс всех конечных p-групп. Очевидно, что всякая $\mathcal{F}$- или $\mathcal{F}_p$-аппроксимируемая относительно сопряженности группа является соответственно $\mathcal{F}$- или $\mathcal{F}_p$-аппроксимируемой. Известно, что каждое из этих утверждений необратимо, причем ряд результатов (см. [1, 3]) говорит о том, что свойство $\mathcal{F}_p$-аппроксимируемости относительно сопряженности является гораздо более жестким ограничением, чем свойство $\mathcal{F}$-аппроксимируемости относительно сопряженности. Основной результат данной статьи можно рассматривать как еще одно подтверждение этого.

Для произвольного целого числа $k \neq 0$ символом 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 произвольная группа G_k $\mathcal{F}$-аппроксимируема относительно сопряженности [6], а также что для любого простого числа p группа G_k является $\mathcal{F}_p$-аппроксимируемой в точности тогда, когда p является делителем числа $k - 1$ [5]. Тем не менее здесь будет доказана

Теорема. *Если число k отлично от ± 1, то группа G_k не является $\mathcal{F}_p$-аппроксимируемой относительно сопряженности ни для какого простого числа p.*

Заметим, что при $k = 1$ группа G_k является свободной абелевой и потому $\mathcal{F}_p$-аппроксимируемой (и, следовательно, $\mathcal{F}_p$-аппроксимируемой относительно сопряженности) для любого простого p. Если же $k = -1$, то, как отмечено выше, для нечетных простых p группа G_k не является уже $\mathcal{F}_p$-аппроксимируемой и потому не является $\mathcal{F}_p$-аппроксимируемой относительно сопряженности. С другой стороны, группа G_{-1} сверхразрешима и элементы a^2 и b порождают в ней абелеву нормальную подгруппу без кручения индекса 2. Следовательно, в силу теоремы 1 из работы [1] группа G_{-1} $\mathcal{F}_2$-аппроксимируема относительно сопряженности.

Для доказательства теоремы нам понадобятся условия сопряженности некоторых элементов в группах G_k и в конечных гомоморфных образах этих групп.

Предложение 1. *Элементы b^m и b^n сопряжены в группе G_k 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.*

В самом деле, если, скажем, $m = nk^t$, то $a^{-t}b^n a^t = b^{nk^t} = b^m$. Обратно, пусть $g^{-1}b^m g = b^n$ для некоторого элемента $g \in G_k$. Хорошо известно, что элемент g (как и любой элемент группы G_k) может быть записан в виде $g = a^r b^q a^{-s}$ для подходящих целых чисел $r \geqslant 0$, $s \geqslant 0$ и q. Переписывая равенство $g^{-1}b^m g = b^n$ в виде $b^{-q}a^{-r}b^m a^r b^q = a^{-s}b^n a^s$, получаем $b^{mk^r} = b^{nk^s}$, откуда ввиду отсутствия кручения в группе G_k имеем $mk^r = nk^s$.

Для произвольных положительных целых чисел r и s, удовлетворяющих сравнению $k^r \equiv 1 \pmod s$, введем в рассмотрение группу $G_k(r,s) = \langle a, b;\ a^{-1}ba = b^k, a^r = b^s = 1\rangle$. Хорошо известно (см., напр., [4, с. 31]), что группа $G_k(r,s)$ является конечной порядка rs, порядки ее элементов a и b равны r и s соответственно и произвольный ее элемент однозначно представим в виде $a^i b^j$, где $0 \leqslant i < r$ и $0 \leqslant j < s$. Группа $G_k(r,s)$ является фактор-группой группы G_k, и легко видеть, что произвольный гомоморфизм группы G_k в конечную группу проходит через естественный гомоморфизм ε группы G_k на группу $G_k(r,s)$: если φ — гомоморфизм группы G_k в некоторую конечную группу X и числа r и s являются порядками элементов $a\varphi$ и $b\varphi$ соответственно, то существует гомоморфизм ψ группы $G_k(r,s)$ в группу X такой, что $\varphi = \varepsilon\psi$.

Предложение 2. *Элементы b^m и b^n сопряжены в группе $G_k(r,s)$ тогда и только тогда, когда сравнение $mk^x \equiv n \pmod s$ (с неизвестной x) имеет решение.*

Предположим, в самом деле, что $g^{-1}b^m g = b^n$ для некоторого элемента $g \in G_k(r,s)$. Так как элемент g имеет вид $g = a^i b^j$ для подходящих неотрицательных целых чисел i и j, это равенство может быть переписано в виде $b^{-j}a^{-i}b^m a^i b^j = b^n$, откуда получаем $b^{mk^i} = b^n$, и т. к. порядок элемента b группы $G_k(r,s)$ равен s, имеем

$$mk^i \equiv n \pmod s.$$

Обратно, если $mk^t \equiv n \pmod{s}$ для некоторого целого $t \geqslant 0$, то $a^{-t}b^m a^t = b^{mk^t} = b^n$.

Критерию сопряженности степеней элемента b группы $G_k(r,s)$, доставляемому предложением 2, удобно придать теоретико-групповую формулировку. Рассмотрим для этого 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 $\overline{n}$, и, если число n взаимно просто с s (и потому $\overline{n}$ является элементом группы $\mathbb{Z}_s^*$), $\overline{N}$ будет обозначать циклическую подгруппу группы $\mathbb{Z}_s^*$, порождаемую элементом $\overline{n}$. Порядок элемента $\overline{n}$ группы $\mathbb{Z}_s^*$ называют также порядком числа n по модулю s. Очевидно, что из предложения 2 следует

Предложение 3. *Пусть каждое из чисел m и n взаимно просто с числом s. Элементы b^m и b^n сопряжены в группе $G_k(r,s)$ тогда и только тогда, когда элементы $\overline{m}$ и $\overline{n}$ группы $\mathbb{Z}_s^*$ принадлежат одному и тому же смежному классу по подгруппе $\overline{K}$, порождаемой элементом $\overline{k}$.*

Сделанные выше замечания говорят о том, что для доказательства утверждения теоремы достаточно ограничиться рассмотрением лишь тех простых чисел p, которые являются делителями числа $k - 1$. В этом случае число k представимо в виде $k = 1 + pu$, и нам понадобится здесь следующее хорошо известное и легко проверяемое утверждение (где, как обычно, (x, y) обозначает наибольший общий делитель чисел x и y):

Предложение 4. *Пусть p — простое число и пусть целое число k имеет вид $k = 1 + p^r u$, где $r > 0$ и $(u,p) = 1$. Если $p > 2$ или $r > 1$, то для любого целого числа $t \geqslant 0$ $k^{p^t} = 1 + p^{r+t}v$ для подходящего целого v, взаимно простого с p. В частности, при указанных ограничениях на p и r для любого $s \geqslant r$ порядок элемента $\overline{k}$ группы $\mathbb{Z}_{p^s}^*$ равен p^{s-r}.*

Решающую роль в доказательстве теоремы играет

Предложение 5. *Если простое число p является делителем числа $k - 1$, то справедливы следующие утверждения:*

1) *пусть $p > 2$ и $k = 1 + p^r u$, где $r > 0$ и $(u,p) = 1$. Если числа m и n не делятся на p и удовлетворяют сравнению $m \equiv n \pmod{p^r}$, то для любого $s \geqslant 1$ в группе $\mathbb{Z}_{p^s}^*$ элементы $\overline{m}$ и $\overline{n}$ принадлежат одному и тому же смежному классу по подгруппе $\overline{K}$, порожденной элементом $\overline{k}$;*

2) *пусть $p = 2$ и $k \neq -1$, так что $k^2 = 1 + 2^r u$, где $r > 2$ и число u нечетно. Если числа m и n нечетны и удовлетворяют сравнению $m \equiv n \pmod{2^r}$, то для любого $s \geqslant 1$ в группе $\mathbb{Z}_{2^s}^*$ элементы $\overline{m}$ и $\overline{n}$ принадлежат одному и тому же смежному классу по подгруппе $\overline{K}$, порожденной элементом $\overline{k}$.*

В доказательстве этого предложения используется хорошо известное (см., напр., [2, § 4.1]) описание строения группы $\mathbb{Z}_{p^s}^*$. Если $p > 2$, то для любого $s \geqslant 1$ группа $\mathbb{Z}_{p^s}^*$ является циклической, причем существует такое целое число l, что при любом $s \geqslant 1$ группа $\mathbb{Z}_{p^s}^*$ порождается элементом $\overline{l}$. Если $p = 2$, то при $s \geqslant 3$ группа $\mathbb{Z}_{2^s}^*$ является прямым произведением подгруппы A порядка 2, порожденной элементом $\overline{-1}$, и циклической подгруппы B порядка 2^{s-2}, порожденной элементом $\overline{5}$.

Докажем сначала первое утверждение предложения 5. Так как при $s \leqslant r$ оно очевидно, будем считать, что $s > r$. Из предложения 4 тогда следует, что порядок элемента $\overline{k}$ группы $\mathbb{Z}_{p^s}^*$ равен p^{s-r}. Порядок порождающего $\overline{l}$ группы $\mathbb{Z}_{p^s}^*$ совпадает с порядком этой группы, т. е. с числом $p^{s-1}(p-1)$. Поэтому порядок элемента $\overline{l}^{p^{r-1}(p-1)}$ равен p^{s-r}, и т. к. в конечной циклической группе элементы одинакового порядка порождают одну и ту же подгруппу, подгруппа $\overline{K}$, порождаемая элементом $\overline{k}$, порождается и элементом $\overline{l}^{p^{r-1}(p-1)}$.

Поскольку классы $\overline{m}$ и $\overline{n}$ являются элементами группы $\mathbb{Z}_{p^s}^*$, для подходящих неотрицательных чисел α и β должны выполняться сравнения

$$m \equiv l^\alpha \pmod{p^s} \quad \text{и} \quad n \equiv l^\beta \pmod{p^s}.$$

Так как $s > r$, отсюда следует, что

$$m \equiv l^\alpha \pmod{p^r} \quad \text{и} \quad m \equiv l^\beta \pmod{p^r},$$

откуда и из условия предложения имеем $l^\alpha \equiv l^\beta \pmod{p^r}$. В силу выбора числа l его порядок по модулю p^r равен $p^{r-1}(p-1)$. Поэтому

$$\alpha \equiv \beta \pmod{p^{r-1}(p-1)},$$

и потому в группе $\mathbb{Z}_{p^s}^*$ элемент $\overline{m}(\overline{n})^{-1} = \overline{l}^{\alpha-\beta}$ является степенью элемента $\overline{l}^{p^{r-1}(p-1)}$, порождающего подгруппу $\overline{K}$.

Перейдем теперь к доказательству второго утверждения, где снова можно дополнительно предполагать, что $s > r$. Тогда $s > 3$, и в силу сказанного выше группа $\mathbb{Z}_{2^s}^*$ обладает подгруппой B индекса 2, являющейся циклической группой порядка 2^{s-2} с порождающим $\overline{5}$. Поскольку квадраты всех элементов группы $\mathbb{Z}_{2^s}^*$ входят в подгруппу B, имеем $\overline{k^2} = \overline{k}^2 \in B$. В силу предложения 4 порядок элемента $\overline{k}^2$ равен 2^{s-r}. Так как порядок порождающего $\overline{5}$ подгруппы B равен 2^{s-2}, рассуждая, как выше, видим, что подгруппа $\overline{K}^2$, порождаемая элементом $\overline{k}^2$, порождается и элементом $\overline{5}^{2^{r-2}}$.

Поскольку классы $\overline{m}$ и $\overline{n}$ являются элементами группы $\mathbb{Z}_{2^s}^*$, для подходящих неотрицательных чисел α, β, γ и δ должны выполняться сравнения

$$m \equiv (-1)^\alpha 5^\beta \pmod{2^s} \quad \text{и} \quad n \equiv (-1)^\gamma 5^\delta \pmod{2^s}.$$

Так как $s > r$, отсюда и из условия предложения следует, что

$$(-1)^\alpha 5^\beta \equiv (-1)^\gamma 5^\delta \pmod{2^r}.$$

С учетом неравенства $r \geqslant 3$ и сравнения $5 \equiv 1 \pmod 4$ имеем, в частности, $(-1)^\alpha \equiv (-1)^\gamma \pmod 4$, так что числа α и γ имеют одинаковую четность. Поэтому $5^\beta \equiv 5^\delta \pmod{2^r}$, и т. к. порядок числа 5 по модулю 2^r равен 2^{r-2}, элементы $\overline{m}$ и $\overline{n}$ сравнимы по модулю подгруппы $\overline{K}^2$, а потому и по модулю подгруппы $\overline{K}$.

Предложение 5 доказано, и мы можем теперь доказать утверждение теоремы. Как уже отмечалось, достаточно показать, что G_k не является $\mathcal{F}_p$-аппроксимируемой относительно сопряженности для простых чисел p, являющихся делителем числа $k-1$. Пусть $m = 1$ и $n = 1+p^r k$, где r является максимальным показателем степени числа p, делящей число $k-1$, если $p > 2$, или число k^2-1, если $p = 2$. Тогда в силу предложения 1 элементы b^m и b^n группы G_k не сопряжены в этой группе. С другой стороны, из предложений 3 и 5 следует, что образы этих элементов в каждой фактор-группе группы G_k вида $G_k(p^t, p^s)$ сопряжены. Поскольку произвольный гомоморфизм группы G_k в конечную p-группу проходит через некоторую такую группу, образы этих элементов сопряжены в каждом гомоморфном образе группы G_k, принадлежащем классу $\mathcal{F}_p$.

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. *Айерлэнд К., Роузен М.* Классическое введение в современную теорию чисел. М.: Мир, 1987. 415 с.
3. *Иванова Е. А., Молдаванский Д. И.* Об аппроксимируемости относительно сопряженности конечно порожденных нильпотентных групп // Вестн. Иван. гос. ун-та. 2004. Вып. 3. С. 125—130.
4. *Магнус В., Каррас А., Солитэр Д.* Комбинаторная теория групп. М.: Наука, 1974. 455 с.
5. *Молдаванский Д. И.* Аппроксимируемость конечными p-группами *HNN*-расширений // Вестн. Иван. гос. ун-та. 2000. Вып. 3. С. 129—140.
6. *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. Тула: Тул. гос. пед. ин-т, 1986. С. 81—91.