УДК 512.543

Д. И. Молдаванский, А. В. Якушев

О КОНЕЧНЫХ ГОМОМОРФНЫХ ОБРАЗАХ НЕКОТОРЫХ ГРУПП С ОДНИМ ОПРЕДЕЛЯЮЩИМ СООТНОШЕНИЕМ

1. Пусть $\mathcal{F}(G)$ обозначает семейство всех конечных групп, являющихся гомоморфными образами группы G, и, если p — простое число, пусть $\mathcal{F}_p(G)$ обозначает семейство всех конечных p-групп, являющихся гомоморфными образами группы G. Пусть, далее, для произвольного целого числа $k \neq 0$ G_k — группа, определяемая в образующих a, b единственным соотношением $a^{-1}ba = b^k$. В работе [2] показано, что для любых целых чисел k и l равенство $\mathcal{F}(G_k) = \mathcal{F}(G_l)$ выполнено в точности тогда, когда $k = l$. Более того, если G — произвольная финитно аппроксимируемая группа, определяемая одним соотношением, то равенство $\mathcal{F}(G_k) = \mathcal{F}(G)$ возможно, лишь если группы G и G_k изоморфны. Иначе говоря, каждая группа G_k в классе финитно аппроксимируемых групп с одним определяющим соотношением однозначно определяется семейством своих конечных гомоморфных образов. Тем не менее, если рассматривать лишь те конечные гомоморфные образы, которые являются p-группами (при фиксированном простом p), это утверждение перестает быть справедливым, даже если ограничиться группами вида G_k. В действительности, ситуация для групп G_k полностью описывается следующим утверждением, доказательству которого и посвящена данная статья:

Теорема. *Пусть p — простое число. Тогда:*

(1) *если $\mathcal{F}_p(G_k) = \mathcal{F}_p(G_l)$ и одно из чисел $k-1$ и $l-1$ делится на p, то и другое делится на p;*

(2) *если числа $k-1$ и $l-1$ не делятся на p, то $\mathcal{F}_p(G_k) = \mathcal{F}_p(G_l)$;*

(3) *если числа $k-1$ и $l-1$ делятся на p, то следующие утверждения равносильны:*

- (3.1) $\mathcal{F}_p(G_k) = \mathcal{F}_p(G_l)$;
- (3.2) *для любого целого числа $s > 0$ элементы $k + p^s\mathbb{Z}$ и $l + p^s\mathbb{Z}$ группы $\mathbb{Z}^*_{p^s}$ (мультипликативной группы кольца $\mathbb{Z}_{p^s} = \mathbb{Z}/p^s\mathbb{Z}$ вычетов целых чисел по модулю p^s) порождают в этой группе одну и ту же циклическую подгруппу;*
- (3.3) *числа $k-1$ и $l-1$ делятся на одни и те же степени числа p, причем если $p = 2$ и числа $k-1$ и $l-1$ не делятся на 4, то числа k^2-1 и l^2-1 делятся на одни и те же степени числа 2.*

Поскольку всякая конечная p-группа нильпотентна, то из этой теоремы следует, что если группы G_k и G_l имеют одни и те же нильпотентные гомоморфные образы, то $|k-1| = |l-1|$. Нетрудно показать, однако, что в этом случае имеет место равенство $k = l$.

В самом деле, легко понять (см., впрочем,[3, с. 288]), что для любого целого числа $n > 1$ n-й член $\gamma_n(G_k)$ нижнего центрального ряда группы G_k совпадает с нормальным замыканием в этой группе элемента $b^{(k-1)^{n-1}}$. Поэтому фактор-группа

$$G_k/\gamma_n(G_k) =< a, b; a^{-1}ba = b^k, b^{(k-1)^{n-1}} = 1 >$$

является бесконечной циклической, если $k = 2$, а в остальных случаях — расширением при помощи бесконечной циклической группы конечной циклической группы порядка $|k-1|^{n-1}$. Следовательно, если множества нильпотентных гомоморфных образов групп G_k и G_l совпадают и $k = 2$, то и $l = 2$. Пусть $k \neq 2$ и пусть φ — гомоморфизм группы G_l на группу $G_k/\gamma_n(G_k)$. Тогда $\gamma_n(G_l) \subseteq \operatorname{Ker}\varphi$ и потому φ проходит через некоторый гомоморфизм ψ группы $G_l/\gamma_n(G_l)$ на группу $G_k/\gamma_n(G_k)$. Так как $|k-1| = |l-1|$, легко видеть, что отображение ψ должно быть изоморфным, и потому из [1] следует, что или $k \equiv l \pmod{|k-1|^{n-1}}$, или $kl \equiv 1 \pmod{|k-1|^{n-1}}$. Поскольку $|k-1| > 1$ и для любого $n > 1$ должно выполняться хотя бы одно из этих сравнений, получаем $k = l$, что и требовалось.

2. Для любых положительных целых чисел r и s таких, что $k^r \equiv 1 \pmod{s}$, обозначим через $G_k(r, s)$ фактор-группу группы G_k по нормальному замыканию элементов a^r и b^s:

$$G_k(r, s) =< a, b; a^{-1}ba = b^k, a^r = 1, b^s = 1 > .$$

Хорошо известно, что группа $G_k(r, s)$ является метациклической конечной группой порядка rs, произвольный элемент ее однозначно представим в виде $a^\alpha b^\beta$, где $0 \leq \alpha < r$ и $0 \leq \beta < s$, и, в частности, порядки элементов a и b равны r и s соответственно. Легко видеть также, что коммутант группы $G_k(r, s)$ совпадает с циклической подгруппой, порожденной элементом b^{k-1}, так что эта группа является абелевой в точности тогда, когда $s|k-1$.

Очевидная индукция показывает, что для любого целого числа $n > 0$ в группе G_k имеет место равенство $a^{-n}ba^n = b^{k^n}$. Поэтому если φ — гомоморфизм группы G_k на некоторую конечную группу H и если элементы $a\varphi$ и $b\varphi$ имеют порядки r и s соответственно, то должно выполняться соотношение $k^r \equiv 1 \pmod{s}$. Следовательно, гомоморфизм φ раскладывается в произведение естественного отображения группы G_k на группу $G_k(r, s)$ и некоторого гомоморфизма последней на группу H.

Лемма 1. *Группа G_k обладает гомоморфизмом на нециклическую конечную p-группу тогда и только тогда, когда $p|k-1$. Если $\mathcal{F}_p(G_k) \subseteq \mathcal{F}_p(G_l)$, то для любого целого числа $t \geq 0$ из $p^t|k-1$ следует $p^t|l-1$.*

Доказательство. Предположим, что существует гомоморфизм φ группы G_k на некоторую конечную p-группу такой, что $b\varphi \neq 1$. Пусть p^r и p^s — порядки элементов $a\varphi$ и $b\varphi$ соответственно. Тогда $s > 0$ и потому сравнение $k^{p^r} \equiv 1 \pmod{p^s}$ влечет сравнение $k^{p^r} \equiv 1 \pmod{p}$. Так как, к тому же, в этом случае по теореме Ферма имеет место сравнение $k^{p-1} \equiv 1 \pmod{p}$, получаем $k \equiv 1 \pmod{p}$. Следовательно, если число $k-1$ не делится на p, то любой гомоморфизм группы G_k на конечную p-группу P переводит элемент b в единицу, так что группа P является циклической.

С другой стороны, пусть $p|k-1$ и пусть $t > 0$ — наибольшее целое число такое, что $k \equiv 1 \pmod{p^t}$. Так как тогда $k^p \equiv 1 \pmod{p^{t+1}}$, гомоморфным образом группы G_k является неабелева конечная p-группа $G_k(p, p^{t+1})$, и первое утверждение леммы 1 доказано.

Сохраняя обозначения предыдущего абзаца, предположим, далее, что $\mathcal{F}_p(G_k) \subseteq \mathcal{F}_p(G_l)$. Тогда группа $G_k(p^t, p^t)$ — прямое произведение двух циклических групп порядка p^t — является гомоморфным образом группы G_l, и потому существует гомоморфизм на группу $G_k(p^t, p^t)$ некоторой группы вида $G_l(p^m, p^n)$, причем поскольку порядок любого элемента группы $G_k(p^t, p^t)$ является делителем числа p^t, можно считать, что числа m и n не превосходят t. Сравнивая порядки групп $G_k(p^t, p^t)$ и $G_l(p^m, p^n)$, мы видим, что $m = n = t$, и потому эти группы изоморфны. Следовательно, группа $G_l(p^t, p^t)$ должна быть абелевой, так что $p^t|l-1$. Лемма доказана.

Замечание. Второе утверждение леммы 1 фактически совпадает с утверждением леммы 1 из работы [2]. Тем не менее ее доказательство, содержащееся в [2], оказалось неверным, так что доказательство, приведенное здесь, устраняет этот пробел в работе [2].

Утверждения (1) и (2) нашей теоремы являются очевидными следствиями первого утверждения леммы 1.

3. Предполагая теперь, что оба числа $k-1$ и $l-1$ делятся на p, докажем равносильность утверждений (3.1) и (3.2) теоремы.

Пусть сначала имеет место (3.2). Ввиду замечаний, приведенных в начале п. 2, для доказательства включения $\mathcal{F}_p(G_k) \subseteq \mathcal{F}_p(G_l)$ достаточно показать, что группа G_l гомоморфно отображается на произвольную группу вида $G_k(p^r, p^s)$.

Это очевидно, если $s = 0$, и мы без потери общности можем предполагать, что $s > 0$. Тогда элементы $k + p^s\mathbb{Z}$ и $l + p^s\mathbb{Z}$ порождают в группе $\mathbb{Z}^*_{p^s}$ одну и ту же циклическую подгруппу. Так как из $k \equiv 1 \pmod{p}$ следует, что для любого числа $s \geq 1$ $k^{p^{s-1}} \equiv 1 \pmod{p^s}$, эта подгруппа является p-группой, и потому найдется натуральное число n, взаимно простое с p, такое, что $k^n \equiv l \pmod{p^s}$. Так как тогда в группе $G_k(p^r, p^s)$

выполнено равенство $a^{-n}ba^n = b^{k^n} = b^l$, отображение, посылающее элемент a в a^n, а элемент b — в b, определяет гомоморфизм группы G_l на группу $G_k(p^r, p^s)$. А так как $(n, p) = 1$, элементы a^n и b порождают группу $G_k(p^r, p^s)$, т.е. этот гомоморфизм сюръективен. Тем самым доказано включение $\mathcal{F}_p(G_k) \subseteq \mathcal{F}_p(G_l)$ и, ввиду очевидной симметрии, — утверждение (3.1).

Будем теперь считать выполненным условие (3.1). В силу второго утверждения леммы 1 числа k и l можно записать в виде

$$k = 1 + p^n k_1, \qquad l = 1 + p^n l_1,$$

где $n > 0$, а числа k_1 и l_1 на p не делятся.

Фиксируем произвольное целое число $s > n$. Так как из $k \equiv 1 \pmod{p^n}$ следует, что $k^{p^{s-n}} \equiv 1 \pmod{p^s}$, группа $G_k(p^s, p^s)$ принадлежит семейству $\mathcal{F}_p(G_k)$ и потому должна быть гомоморфным образом группы G_l. Если при таком гомоморфизме образами элементов a и b являются элементы $f = a^\alpha b^\beta$ и $g = a^\gamma b^\delta$ соответственно, то в группе $G_k(p^s, p^s)$ имеет место равенство $f^{-1}gf = g^l$. Непосредственные вычисления показывают, что

$$f^{-1}gf = a^\gamma b^{\delta k^\alpha - \beta(k^\gamma - 1)}$$

и

$$g^l = a^{\gamma l} b^{\delta(1 + k^\gamma + k^{2\gamma} + \cdots + k^{(l-1)\gamma})}.$$

Поэтому предыдущее равенство равносильно следующим двум сравнениям:

$$\gamma l \equiv \gamma \pmod{p^s},$$
$$\delta k^\alpha - \beta(k^\gamma - 1) \equiv \delta(1 + k^\gamma + k^{2\gamma} + \cdots + k^{(l-1)\gamma}) \pmod{p^s}.$$

Первое из них означает, что число $\gamma p^n l_1$ делится на p^s, т.е. что число γ делится на p^{s-n}. Так как $k^{p^{s-n}} \equiv 1 \pmod{p^s}$, отсюда следует, что $k^\gamma \equiv 1 \pmod{p^s}$, и потому второе сравнение принимает вид

$$\delta k^\alpha \equiv \delta l \pmod{p^s}.$$

Напомним, далее, что элементы f и g должны порождать группу $G_k(p^s, p^s)$, а потому их образы a^α и a^γ при очевидном гомоморфизме этой группы на циклическую группу с образующим a порядка p^s порождают последнюю. Так как число γ делится на p, отсюда следует, что числа α и p взаимно просты.

Ниже мы покажем также, что и число δ взаимно просто с p. Тогда из последнего сравнения будет следовать, что $k^\alpha \equiv l \pmod{p^s}$, и тем самым будет доказано, что для любого числа $s > n$ элементы $k + p^s\mathbb{Z}$ и $l+p^s\mathbb{Z}$ порождают в группе $\mathbb{Z}^*_{p^s}$ одну и ту же циклическую подгруппу. Так как при $t < s$ группа $\mathbb{Z}^*_{p^t}$ является естественным гомоморфным образом группы $\mathbb{Z}^*_{p^s}$, справедливость утверждения (3.2) будет доказана.

Итак, остается показать, что предположение $p|\delta$ ведет к противоречию. Пусть порядки элементов f и g равны числам p^u и p^v соответственно. Учитывая, что γ делится на p и $k^\gamma \equiv 1 \pmod{p^s}$, имеем

$$g^{p^{s-1}} = a^{\gamma p^{s-1}} b^{\delta p^{s-1}} = 1,$$

так что $v \leq s-1$. Докажем, далее, что $u \leq s$.

Так как $(\alpha, p) = 1$, то $k^\alpha = 1+p^n k_2$, где k_2 не делится на p. Поскольку число

$$\left(1 + k^\alpha + k^{2\alpha} + \cdots + k^{(p^s-1)\alpha}\right)(k^\alpha - 1) = k^{p^s\alpha} - 1$$

делится на p^{s+n}, то число $\left(1 + k^\alpha + k^{2\alpha} + \cdots + k^{(p^s-1)\alpha}\right)$ должно делиться на p^s. Поэтому

$$f^{p^s} = a^{\alpha p^s} b^{\beta\left(1+k^\alpha+k^{2\alpha}+\cdots+k^{(p^s-1)\alpha}\right)} = 1,$$

и, следовательно, $u \leq s$.

Таким образом, группа $G_k(p^s, p^s)$ порядка p^{2s} является гомоморфным образом группы $G_k(p^u, p^v)$ порядка $p^{u+v} \leq p^{2s-1}$. Полученное противоречие завершает доказательство равносильности утверждений (3.1) и (3.2).

4. Для доказательства равносильности утверждений (3.2) и (3.3) нам понадобится следующая элементарная

Лемма 2. *Пусть p — простое число и пусть целое число k имеет вид $k = 1 + p^m u$, где $m \geq 1$ и $(u, p) = 1$. Тогда*

- a) *если $p > 2$ или $m > 1$, то для любого целого числа $t \geq 0$ $k^{p^t} = 1 + p^{m+t}v$ для некоторого числа v, взаимно простого с p;*
- b) *если $p = 2$ и $m = 1$, то $k^2 = 1 + 2^n u_1$, где $n \geq 3$ и число u_1 нечетно, и для любого целого числа $t \geq 0$ $k^{2^{t+1}} = 1 + 2^{n+t}v$ для некоторого нечетного числа v.*

В частности, для любого целого числа $s > 0$ порядок элемента $k + p^s\mathbb{Z}$ группы $\mathbb{Z}^*_{p^s}$ равен в случае a) p^{s-m}, если $s \geq m$, и 1, если $s < m$, а в случае b) — 2^{s-n+1}, если $s \geq n$, 2, если $1 < s < n$, и 1, если $s = 1$.

Таким образом, условие (3.3) означает, что для любого целого числа $s > 0$ элементы $k + p^s\mathbb{Z}$ и $l + p^s\mathbb{Z}$ группы $\mathbb{Z}^*_{p^s}$ имеют одинаковые порядки. Это замечание делает утверждение о равносильности условий (3.2) и (3.3) очевидным, если p — нечетное простое число, т.к. в этом случае группа $\mathbb{Z}^*_{p^s}$ циклична. Кроме того, и в оставшемся случае $p = 2$ очевидна импликация (3.2) $\Rightarrow$ (3.3). Остается показать, что в этом случае из (3.3) следует (3.2).

Предположим сначала, что $k = 1 + 2^m k_1$ и $l = 1 + 2^m l_1$, где $m > 1$ и числа k_1 и l_1 нечетны. Необходимо показать, что для любого целого числа $s > 0$ элементы $k + 2^s\mathbb{Z}$ и $l + 2^s\mathbb{Z}$ порождают в группе $\mathbb{Z}^*_{2^s}$ одну и ту же подгруппу. Если $s \leq m$, это очевидно. Пусть $s > m$. Тогда порядок подгруппы, порождаемой элементом $k + 2^s\mathbb{Z}$, равен 2^{s-m}, произвольный элемент, порождающий ту же подгруппу, имеет вид $k^\alpha + 2^s\mathbb{Z}$, где α нечетно и $0 < \alpha < 2^{s-m}$, и число таких элементов равно 2^{s-m-1}. Кроме того, любой представитель смежного класса $k^\alpha + 2^s\mathbb{Z}$ имеет вид $1 + 2^m u$, где u нечетно. Так как, далее, сравнение $1+2^m u \equiv 1+2^m v \pmod{2^s}$ равносильно сравнению $u \equiv v \pmod{2^{s-m}}$, то и число всех классов, состоящих из чисел указанного вида, равно 2^{s-m-1}. Следовательно, каждый такой класс (в том числе и $l + 2^s\mathbb{Z}$) порождает ту же подгруппу, что и $k + 2^s\mathbb{Z}$.

Наконец, пусть $k = 1 + 2k_1$, $l = 1 + 2l_1$, $k^2 = 1 + 2^n k_2$, $l^2 = 1 + 2^n l_2$, где числа k_1, k_2, l_1, l_2 нечетны. Здесь снова, как и в п. 3, достаточно рассмотреть случай $s > n$. Тогда порядок элементов $k + 2^s\mathbb{Z}$ и $l + 2^s\mathbb{Z}$ группы $\mathbb{Z}^*_{2^s}$ больше 2. Кроме того, смежные классы $k + 2^s\mathbb{Z}$ и $l + 2^s\mathbb{Z}$ состоят из чисел вида $1 + 2u$, $(u, 2) = 1$, а общее число классов, состоящих из таких чисел, равно 2^{s-2}.

Для каждого $i = 0, 1, \ \ldots, s-2$ полагаем

$$x_i = 1 + 2\left(2^{s-i-1} - 1\right).$$

Пусть также X_i — циклическая подгруппа группы $\mathbb{Z}^*_{2^s}$, порожденная элементом $x_i + 2^s\mathbb{Z}$, а Y_i — множество элементов этой группы, каждый из которых порождает подгруппу X_i. Очевидно, что каждый смежный класс, входящий в любое из множеств Y_i, состоит из чисел вида $1 + 2u$, где u нечетно. Так как

$$x_i^2 = 1 + 2^{s-i+1}\left(2^{s-i-1} - 1\right),$$

порядок элемента $x_i + 2^s\mathbb{Z}$ равен 2^i, если $1 \leq i \leq s-2$, и 2, если $i = 0$. Поэтому Y_0 содержит лишь один элемент, а для $i = 1, 2, \ \ldots, s-2$ множество Y_i состоит из 2^{i-1} элементов. Поскольку, к тому же, эти множества попарно не пересекаются, то их объединение содержит

$$1 + \sum_{i=1}^{s-2} 2^{i-1} = 1 + \left(2^{s-2} - 1\right) = 2^{s-2}$$

элементов и потому совпадает с множеством всех классов, состоящих из чисел вида $1 + 2u$, $(u, 2) = 1$.

Таким образом, каждый из элементов $k + 2^s\mathbb{Z}$ и $l + 2^s\mathbb{Z}$ группы $\mathbb{Z}^*_{2^s}$ должен входить в одно из подмножеств Y_i. Элементы одинакового порядка могут входить в разные подмножества Y_i и Y_j лишь в том случае, когда их порядок равен 2. Следовательно, элементы $k + 2^s\mathbb{Z}$ и $l + 2^s\mathbb{Z}$ входят в некоторое множество Y_i и потому порождают одну и ту же циклическую подгруппу X_i.

Список использованной литературы

1. *Baumslag G.* Residually finite groups with the same finite images // Compositio Math. 1974. Vol 29 P. 249 – 252.
2. *Moldavanski D., Sibyakova N.* On the finite images of some one-relator groups // Proc. Amer. Math. Soc. 1995. Vol. 123. P. 2017 – 2020.
3. *Raptis E., Varsos D.* Residual properties of HNN-extensions with base group an abelian group // J. Pure Appl. Algebra. 1989. Vol. 59. P. 285 – 290.