О. А. Иванова, Д. И. Молдаванский

Аппроксимируемость конечными π-группами некоторых групп с одним определяющим соотношением

Для произвольной группы с одним определяющим соотношением, входящей в семейство групп Баумслага – Солитэра и являющейся метабелевой, указаны все одно- и двухэлементные минимальные множества π простых чисел такие, что эта группа аппроксимируема конечными π-группами.

§ 1. Введение. Формулировка результатов

Напомним, что группа G называется аппроксимируемой группами из некоторого класса $\boldsymbol{K}$ (или $\boldsymbol{K}$-аппроксимируемой), если для любого неединичного элемента $g \in G$ существует такой гомоморфизм группы G на некоторую группу из класса $\boldsymbol{K}$, образ элемента g относительно которого отличен от единицы. В случае, когда $\boldsymbol{K}$ совпадает с классом $\boldsymbol{F}$ всех конечных групп, такая группа называется финитно аппроксимируемой. Естественно возникает вопрос нахождения всех минимальных множеств π простых чисел таких, что данная финитно аппроксимируемая группа является $\boldsymbol{F}_\pi$-аппроксимируемой (где $\boldsymbol{F}_\pi$ – класс всех конечных π-групп; если π состоит из единственного простого числа p, будем писать $\boldsymbol{F}_p$ вместо $\boldsymbol{F}_\pi$).

Очевидно, что свойство финитной аппроксимируемости группы совпадает со свойством $\boldsymbol{F}_\pi$-аппроксимируемости, где π состоит из всех простых чисел, и существуют примеры финитно аппроксимируемых групп, не являющихся $\boldsymbol{F}_\pi$-аппроксимируемыми при любом собственном подмножестве π множества всех простых чисел. Простейшим таким примером служит прямое произведение счетного семейства групп $C_1, C_2, \dots$, где C_n – конечная циклическая группа порядка n, а из результатов работы [1] следует и существование конечно порожденной группы с аналогичным свойством. С другой стороны, известны и примеры противоположного характера. Так, произвольная свободная группа $\boldsymbol{F_p}$-аппроксимируема для любого простого числа p, и, следовательно, для свободных групп все минимальные множества π с указанным свойством являются одноэлементными.

В данной работе с этой точки зрения рассматривается семейство групп с одним определяющим соотношением, входящих в известное семейство групп Баумслага – Солитэра, а именно – семейство групп вида

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

где k – произвольное целое число, отличное от нуля. Хорошо известно, что все эти группы финитно аппроксимируемы [2] и что группа G_k является $\boldsymbol{F_p}$-аппроксимируемой тогда и только тогда, когда число $k-1$ делится на p [3]. Первым результатом данной работы является следующий критерий $\boldsymbol{F_\pi}$-аппроксимируемости группы G_k:

Теорема 1. *Пусть π – произвольное множество простых чисел. Группа G_k $\boldsymbol{F_\pi}$-аппроксимируема тогда и только тогда ,когда существует π-число $s>1$, взаимно простое с k, порядок по модулю которого числа k также является π-числом.*

Упомянутый выше критерий $\boldsymbol{F_p}$-аппроксимируемости группы G_k является непосредственным следствием теоремы 1. Из этого критерия следует, очевидно, что если в множество π входит хотя бы один простой делитель числа $k-1$, то группа G_k $\boldsymbol{F_\pi}$-аппроксимируема. Условия $\boldsymbol{F_\pi}$-аппроксимируемости группы G_k конечными π-группами, для двухэлементного множества π, не содержащего делителей числа $k-1$, доставляет доказываемая с помощью теоремы 1

Теорема 2. *Пусть $\pi = \{p, q\}$, где простые числа p и q таковы, что $p<q$ и каждое из них не является делителем числа $k-1$. Группа G_k $\boldsymbol{F_\pi}$-аппроксимируема тогда и только тогда*

,когда $(k,q)=1$, p делит $q-1$ и порядок числа k по модулю q является p-числом.

Формулировка теоремы 2 оставляет открытым вопрос, для каких целых чисел k действительно существуют простые числа p и q, удовлетворяющие ее условиям. Очевидно, что таких чисел нет при $k=1$. Более того, группа G_1 является свободной абелевой и потому $\boldsymbol{F_p}$-аппроксимируема при любом простом p. Легко понять также, что для любого множества π группа G_{-1} является $\boldsymbol{F}_\pi$-аппроксимируемой в точности тогда, когда множество π содержит число 2. Действительно, если G_{-1} $\boldsymbol{F}_\pi$-аппроксимируема, то в силу теоремы 1 для подходящих π-чисел r и $s>1$ должно выполняться сравнение $(-1)^r \equiv 1(\bmod s)$, невозможное, если оба числа r и s нечетны. Таким образом, при $k=\pm 1$ двухэлементного множества π, удовлетворяющего условиям теоремы 2, не существует. В остальных случаях имеет место

Теорема 3. *Если $|k|>1$, то для любого простого числа p, не делящего число $k-1$, существует простое число q, не делящее $k-1$ и такое, что группа G_k $\boldsymbol{F}_\pi$-аппроксимируема при $\pi=\{p,q\}$.*

Из этих результатов получается следующее описание состоящих из не более двух элементов минимальных множеств π простых чисел, для которых группа G_k является $\boldsymbol{F}_\pi$-аппроксимируемой:

если $k=1$, то все одноэлементные множества обладают требуемым свойством, и других минимальных множеств нет;

если $k=-1$, то единственным минимальным является множество $\pi=\{2\}$;

если $|k|>1$, то все одноэлементные минимальные множества имеют вид $\pi=\{p\}$, где p – произвольный простой делитель числа $k-1$, и для любого простого числа, не делящего $k-1$, *существует двухэлементное минимальное множество, содержащее это число.*

В частности, при $k=2$ одноэлементных минимальных множеств не существует, и произвольное простое число входит в некоторое двухэлементное минимальное множество. Заметим также, что поскольку число 2 является примитивным корнем по модулю 29, т. е. порядок числа 2 по модулю 29 равен 28, в силу теоремы 1 группа G_2 является $\boldsymbol{F}_\pi$-аппроксимируемой, где $\pi=\{2, 7, 29\}$. Более того, поскольку порядок числа по модулю 7 равен 3, из теоремы 2 следует, что это множество для группы G_2 является минимальным. В общем случае вопрос об описании минимальных множеств с числом элементов, большим 2, остается открытым.

§ 2. Доказательство теоремы 1

Необходимость условия в теореме 1 почти очевидна. В самом деле, если для некоторого множества π простых чисел группа $G_k=\langle a,b;\, a^{-1}ba=b^k\rangle$ является $\boldsymbol{F}_\pi$-аппроксимируемой, то поскольку ее элемент b отличен от единицы, найдется гомоморфизм φ группы G_k на конечную π-группу такой, что $b\varphi\neq 1$. Обозначим порядки элементов $a\varphi$ и $b\varphi$ через r и s соответственно. Тогда r и s являются π-числами, причем $s>1$. Непосредственной индукцией проверяется, что для любого целого числа $t\geq 0$ в группе G_k выполнено равенство $a^{-t}ba^t=b^{k^t}$. Переходя к φ-образам и полагая $t=r$, имеем $b\varphi=(b\varphi)^{k^r}$, откуда $k^r\equiv 1(\operatorname{mod} s)$. Следовательно, порядок числа k по модулю s делит r и потому является π-числом. Поскольку, к тому же, числа r и s являются, очевидно, взаимно простыми, число s искомое.

Докажем достаточность условия. Для произвольной пары положительных целых чисел r и s, удовлетворяющих сравнению $k^r\equiv 1(\operatorname{mod} s)$, обозначим через $G_k(r, s)$ фактор-группу группы

G_k по нормальному замыканию элементов a^r и b^s, а через φ_{rs} – естественный гомоморфизм группы G_k на группу $G_k(r,s)$. Хорошо известно (см., напр., [5, с. 31]), что произвольный элемент группы $G_k(r,s)$ однозначно представим в виде $a^i b^j$, где $0 \le i < r$, $0 \le j < s$. В частности, порядок группы $G_k(r,s)$ равен rs, а порядки ее элементов a и b равны r и s соответственно. Таким образом, если r и s – π-числа, то группа $G_k(r,s)$ является конечной π-группой.

Пусть Ω – некоторое множество пар (r,s) положительных целых чисел таких, что $k^r \equiv 1 (\operatorname{mod} s)$. Утверждается, что если обе проекции множества Ω бесконечны, то группа G_k аппроксимируема семейством групп $G_k(r,s)$, где $(r,s) \in \Omega$.

В самом деле, пусть g – произвольный неединичный элемент группы G_k. Легко видеть, что элемент g может быть представлен в виде $g = a^m b^t a^{-n}$, для подходящих целых чисел $m \ge 0$, $n \ge 0$ и t. Следовательно, заменяя его сопряженным, мы можем без потери общности считать, что наш элемент имеет вид $g = a^u b^v$ для подходящих целых u и v. Поскольку хотя бы одно из этих чисел отлично от нуля, из предположения относительно множества Ω следует существование пары $(r,s) \in \Omega$ такой, что или u не делится на r, или v не делится на s. Очевидно, что тогда $g\varphi_{rs} \ne 1$, и наше утверждение доказано.

Для произвольного множества π простых чисел обозначим через $\Omega(\pi)$ множество всех пар (r,s) положительных целых π-чисел, удовлетворяющих сравнению $k^r \equiv 1 (\operatorname{mod} s)$. Ввиду предыдущего замечания, для завершения доказательства теоремы 1 достаточно показать, что если множество $\Omega(\pi)$ содержит хотя бы одну пару (r, s) с $s > 1$, то обе проекции этого множества бесконечны.

Поскольку из сравнения $k^r \equiv 1(\operatorname{mod} s)$ при любом целом $n > 0$ следует сравнение $k^{rn} \equiv 1(\operatorname{mod} s)$, бесконечность первой проекции множества $\Omega(\pi)$ очевидна.

Пусть $(r, s) \in \Omega(\pi)$, где $s > 1$, и пусть p – простой делитель числа s. Так как тогда $p \in \pi$ и из сравнения $k^r \equiv 1(\operatorname{mod} p)$ следует сравнение $k^{rp^n} \equiv 1(\operatorname{mod} p^{n+1})$, то для любого целого положительного π-числа n имеем $(rp^n, p^{n+1}) \in \Omega(\pi)$, что и доказывает бесконечность второй проекции множества $\Omega(\pi)$.

Теорема 1 доказана. Частным случаем этой теоремы является упомянутый выше результат из работы [3]:

Следствие. *Для любого простого числа p группа* G_k *является* $\boldsymbol{F_p}$*-аппроксимируемой тогда и только тогда, когда p делит число* $k-1$.

Действительно, если группа G_k $\boldsymbol{F_p}$-аппроксимируема, то в силу теоремы 1 для некоторых целых чисел m и $n > 0$ имеет место сравнение $k^{p^m} \equiv 1(\operatorname{mod} p^n)$ и потому $k^{p^m} \equiv 1(\operatorname{mod} p)$. Поскольку тогда $(k, p)=1$, по теореме Ферма имеем также $k^{p-1} \equiv 1(\operatorname{mod} p)$. Так как числа p^m и $p-1$ взаимно просты, из последних двух сравнений следует, что $k \equiv 1(\operatorname{mod} p)$. Обратно, если $k \equiv 1(\operatorname{mod} p)$, то множество $\pi = \{p\}$ и число $s = p$ удовлетворяют условиям теоремы 1.

§ 3. Доказательство теорем 2 и 3

Достаточность условий в теореме 2 вытекает, очевидно, непосредственно из теоремы 1. Для доказательства необходимости предположим, что группа G_k $\boldsymbol{F_\pi}$ аппроксимируема, где множество π состоит из простых чисел p и q, $p < q$, не делящих числа $k-1$. По теореме 1 существуют π-числа r и $s>1$, удовлетворяющие сравнению $k^r \equiv 1(\mathrm{mod}\ s)$.

Покажем, прежде всего, что число s не делится на p и потому является q-числом. Действительно, если $p\,|\,s$, то выполнено сравнение $k^r \equiv 1(\mathrm{mod}\ p)$. Так как числа r и $p-1$ взаимно просты, отсюда и из сравнения $k^{p-1} \equiv 1(\mathrm{mod}\ p)$ следует, что $k \equiv 1(\mathrm{mod}\, p)$, что противоречит условию теоремы.

Теперь легко понять, что числа p и q удовлетворяют требованиям теоремы. Взаимная простота чисел k и q очевидна. Кроме того, поскольку имеет место сравнение $k^r \equiv 1(\mathrm{mod}\ q)$, порядок числа k по модулю q делит r и потому является π-числом. Но так как $k^{q-1} \equiv 1(\mathrm{mod}\ q)$, порядок числа k по модулю q делит число $q-1$ и потому взаимно прост с q. Таким образом, порядок числа k по модулю q является p-числом, и теорема 2 доказана.

Для доказательства теоремы 3 фиксируем простое число p, не являющееся делителем числа $k-1$. Пусть $S_n(x)$ обозначает многочлен $x^{n-1} + x^{n-2} + \ldots + x + 1$.

Покажем, что если простое число q не делит число $k-1$ и является делителем числа $S_{p^m}(k)$ для некоторого $m \geq 1$, то числа p и q удовлетворяют требованиям теоремы 2.

Действительно, взаимная простота чисел k и q очевидна. Поскольку число $k^{p^m} - 1 = (k-1)\,S_{p^m}(k)$ делится на q, порядок числа k по модулю q является p-числом. Из сравнения $k^{q-1} \equiv 1(\mathrm{mod} q)$, следует, что порядок числа k по модулю q должен делить и число $q-1$, и так как $k-1$ не делится на q, число $q-1$ делится на p.

Покажем теперь, что при наших предположениях каждый простой делитель числа $S_{p^m}(k)$ не является делителем $k-1$.

Действительно, если для простого числа q выполнены сравнения $S_{p^m}(k) \equiv 0 (\mathrm{mod}\, q)$ и $k \equiv 1 (\mathrm{mod}\, q)$, то поскольку тогда из второго сравнения следует, что $S_{p^m}(k) \equiv p^m (\mathrm{mod}\, q)$, число p^m должно делиться на q. Отсюда $p = q$, что невозможно в силу выбора числа p.

Итак, нам остается заметить, что при $k \neq \pm 1$ абсолютная величина числа $S_{p^m}(k)$ отлична от единицы для некоторого $m \geq 1$. В самом деле, элементарные рассуждения показывают, что если $k \neq -2$ или $p \neq 2$, то уже $S_p(k) \neq \pm 1$. Поскольку $S_{2^2}(-2) = -5$, доказательство теоремы 3 закончено.

Библиографический список

1. *Wilson John S.* Embedding theorems for residually finite groups // Math. J. 1980. 174. №2. p. 149–157.
2. *Baumslag G.*, Solitar D. Some two-generator one-relator non-Hopfian groups. Bull. Amer. Math. Soc. 1962. Vol. 68. P. 199–201.
3. *Молдаванский Д. И.* Аппроксимируемость конечными *p*-группами HNN-расширений. Вестн. Иван. гос. ун-та. 2000. Вып. 3. С. 129–140.
4. *Магнус В., Каррас А., Солитэр Д.* Комбинаторная теория групп. М.: Наука, 1974. 455 с.