УДК 512.543

Д. И. Молдаванский

ОБ ОТДЕЛИМОСТИ ЦИКЛИЧЕСКИХ ПОДГРУПП В ПРЯМОМ ПРОИЗВЕДЕНИИ ГРУПП

Получено достаточное условие отделимости в классе конечных π-групп всех π'-изолированных циклических подгрупп прямого произведения двух групп. Построен пример, показывающий, что это условие не является необходимым.

Ключевые слова: аппроксимируемость группы в некотором классе групп, отделимость подгрупп в некотором классе групп, прямое произведение групп.

The sufficient condition for any π'-isolated cyclic subgroup of a direct product of two groups to be separable in the class of all finite π-groups is obtained. An example showing that this condition is not necessary is constructed.

Key words: residuallity of group in some class of groups, separability of subgroups in some class of groups, direct product of groups.

1. Введение. Формулировка результатов

Напомним, что если $\mathcal{K}$ — некоторый класс групп, то группа G называется аппроксимируемой в классе $\mathcal{K}$ (или, короче, $\mathcal{K}$-аппроксимируемой), если для любого неединичного элемента $g \in G$ найдется гомоморфизм группы G на некоторую группу из класса $\mathcal{K}$, при котором образ $g\varphi$ элемента g отличен от единицы (или, что равносильно, элемент g не входит в некоторую нормальную подгруппу N группы G, фактор-группа G/N по которой принадлежит классу $\mathcal{K}$).

Подгруппа H группы G называется отделимой в классе $\mathcal{K}$ (или, короче, $\mathcal{K}$-отделимой), если для любого элемента $g \in G$, не принадлежащего подгруппе H, найдется гомоморфизм группы G на некоторую группу из класса $\mathcal{K}$, при котором образ $g\varphi$ элемента g не принадлежит образу $H\varphi$ подгруппы H (или, что равносильно, элемент g не входит в подгруппу HN для некоторой нормальной подгруппы N группы G такой, что фактор-группа G/N принадлежит классу $\mathcal{K}$).

Очевидно, что произвольная группа является $\mathcal{K}$-аппроксимируемой тогда и только тогда, когда ее единичная подгруппа $\mathcal{K}$-отделима. Для гомоморфно замкнутых классов (т. е. классов, содержащих вместе с каждой группой все ее гомоморфные образы) имеет место более общее утверждение: нормальная подгруппа H некоторой группы G является $\mathcal{K}$-отделимой тогда и только тогда, когда фактор-группа G/H $\mathcal{K}$-аппроксимируема.

Если $\mathcal{F}$ — класс всех конечных групп, то понятия $\mathcal{F}$-аппроксимируемости групп и $\mathcal{F}$-отделимости подгрупп совпадают с хорошо известными и наиболее изученными понятиями финитной аппроксимируемости и финитной отделимости соответственно. Значительное число публикаций посвящено также изучению свойств $\mathcal{F}_\pi$-аппроксимируемости групп и $\mathcal{F}_\pi$-отделимости подгрупп. Здесь π — некоторое множество простых чисел и $\mathcal{F}_\pi$ — класс всех конечных π-групп, т. е. конечных групп, порядок которых является π-числом (целое число называется π-числом, если все простые делители его принадлежат множеству π).

Опубликованные результаты получены в рамках выполнения государственного задания Минобрнауки России № 1.8695.2017/8.9

Очевидно, что если множество π пусто, то класс $\mathcal{F}_\pi$ содержит только единичную группу, а если π совпадает с множеством всех простых чисел, то $\mathcal{F}_\pi$ совпадает с классом $\mathcal{F}$. Если множество π состоит из единственного простого числа p, вместо $\mathcal{F}_\pi$ пишут $\mathcal{F}_p$, а π-числа называют p-числами.

Исследования, связанные с понятием отделимости подгрупп, направлены, в основном, на решения вопросов о том, какие подгруппы данной группы являются $\mathcal{K}$-отделимыми и сохраняются ли свойства $\mathcal{K}$-отделимости подгрупп некоторого типа (всех, всех конечно порожденных, всех циклических и т. п.) при теоретико-групповых конструкциях.

Так, из замечания, сделанного выше, следует, что ядро гомоморфизма произвольной нециклической свободной группы F на 2-порожденную группу, не являющуюся финитно аппроксимируемой (относительно существования таких групп см., напр., [7]), не является финитно отделимой подгруппой группы F. В силу теоремы 2.10 из монографии [3] такая неотделимая подгруппа группы F не является конечно порожденной. С другой стороны, из теоремы М. Холла [6] следует, что произвольная конечно порожденная подгруппа любой свободной группы финитно отделима. Обобщением этого утверждения выступает результат Н. С. Романовского [4], состоящий в том, что (обычное) свободное произведение произвольного семейства групп, все конечно порожденные подгруппы каждой из которых финитно отделимы, также является группой, все конечно порожденные подгруппы которой финитно отделимы. Отметим, что, поскольку группа, раскладывающаяся в свободное произведение хотя бы двух неединичных групп и не имеющая нециклических свободных подгрупп, есть свободное произведение двух групп порядка 2, наследование свободным произведением групп от свободных сомножителей финитной отделимости всех подгрупп имеет место только в этом исключительном случае. Отметим также, что для обобщенного свободного произведения групп справедливость аналога теоремы Романовского, вообще говоря, не имеет места.

Для прямого произведения групп аналогичное утверждение тоже может не выполняться: в работе [5] было доказано, что прямое произведение двух свободных групп ранга 2 обладает конечно порожденной подгруппой, которая не является финитно отделимой. Тем не менее известно [9, теорема 4], что прямое произведение двух групп, все циклические подгруппы которых финитно отделимы, является группой, в которой все циклические подгруппы также финитно отделимы.

Цель данной статьи состоит в нахождении условий, при которых прямое произведение групп наследует от сомножителей свойства $\mathcal{F}_\pi$-отделимости циклических подгрупп, где π — непустое собственное подмножество множества всех простых чисел. Для более точной постановки этой проблемы следует учитывать, что существует условие, которому должна удовлетворять любая $\mathcal{F}_\pi$-отделимая подгруппа. Его формулировка основана на следующем понятии.

Напомним, что если p — некоторое простое число, то подгруппа H группы G называется p-изолированной, если для любого элемента $g \in G$ из включения $g^p \in H$ следует включение $g \in H$. Если π — некоторое множество простых чисел, то подгруппа H группы G называется π-изолированной, если она p-изолирована для любого $p \in \pi$. Наконец, через π' обозначается дополнение множества π в множестве всех простых чисел (так

что, в частности, p' обозначает множество всех простых чисел, отличных от p).

Так вот, хорошо известно (см., напр.: [8, предложение 1.3]), что любая $\mathcal{F}_\pi$-отделимая подгруппа группы является π'-изолированной в этой группе. Отметим, что обратное утверждение, вообще говоря, неверно: В. Г. Бардаков [1], отвечая автору данной статьи [2, вопрос 15.60], доказал, что во всякой свободной неабелевой группе для любого простого числа p существует конечно порожденная p'-изолированная подгруппа, которая не является $\mathcal{F}_p$-отделимой. Легко видеть, тем не менее, что для любого множества простых чисел π в любой свободной группе каждая π'-изолированная циклическая подгруппа $\mathcal{F}_\pi$-отделима.

Следовательно, проблема, отмеченная выше, может быть уточнена следующим образом: при каких условиях прямое произведение двух групп, все π'-изолированные циклические подгруппы которых $\mathcal{F}_\pi$-отделимы, является группой, в которой все π'-изолированные циклические подгруппы также $\mathcal{F}_\pi$-отделимы? Некоторым ответом на этот вопрос служит следующая

Теорема. *Пусть π — некоторое множество простых чисел, группы A и B $\mathcal{F}_\pi$-аппроксимируемы и в каждой из этих групп любая π'-изолированная циклическая подгруппа $\mathcal{F}_\pi$-отделима. Пусть также в группах A и B π'-изолятор любой циклической подгруппы является циклической подгруппой. Тогда в прямом произведении групп A и B все π'-изолированные циклические подгруппы являются $\mathcal{F}_\pi$-отделимыми.*

Напомним, что π'-изолятором подгруппы H группы G называется наименьшая π'-изолированная подгруппа группы G, содержащая подгруппу H. Е. В. Соколов [8, лемма 1.6] доказал, что в $\mathcal{F}_\pi$-аппроксимируемой группе π'-изолятор любой локально циклической подгруппы является локально циклической подгруппой. Поэтому имеет место

Следствие 1. *Пусть группы A и B $\mathcal{F}_\pi$-аппроксимируемы и в каждой из этих групп любая π'-изолированная циклическая подгруппа $\mathcal{F}_\pi$-отделима. Пусть также группы A и B удовлетворяют условию максимальности для циклических подгрупп (т. е. каждая возрастающая последовательность циклических подгрупп стабилизируется). Тогда в прямом произведении групп A и B все π'-изолированные циклические подгруппы являются $\mathcal{F}_\pi$-отделимыми.*

В частности, отметим

Следствие 2. *В прямом произведении двух свободных групп все π'-изолированные циклические подгруппы являются $\mathcal{F}_\pi$-отделимыми.*

В действительности, утверждение следствия 1 представляет собой частный случай более общего результата, полученного в статье [8]. В этой статье рассматриваются условия $\mathcal{F}_\pi$-отделимости циклических подгрупп свободного произведения двух групп A и B с коммутирующими подгруппами $H \leqslant A$ и $K \leqslant B$, т. е. фактор-группы (обычного) свободного произведения $A * B$ групп A и B по нормальному замыканию взаимного коммутанта $[H, K]$ подгрупп A и B. Поскольку при $H = A$ и $K = B$ эта фактор-группа оказывается прямым произведением групп A и B, в данном частном случае утверждение следствия 1 совпадает с утверждением следствия 3.4 из [8].

В связи с этим естественно возникает вопрос о том, является ли утверждение теоремы более общим, чем утверждение следствия 1. Другими словами, существует ли не удовлетворяющая условию максимальности для циклических подгрупп $\mathcal{F}_\pi$-аппроксимируемая группа, в которой все π'-изолированные циклические подгруппы $\mathcal{F}_\pi$-отделимы и π'-изолятор каждой циклической подгруппы является циклической группой?

Насколько известно автору, ответа на этот вопрос пока нет. С другой стороны, здесь будет построен пример, говорящий о том, что цикличность π'-изоляторов циклических подгрупп в сомножителях не является необходимым условием $\mathcal{F}_\pi$-отделимости всех π'-изолированных подгрупп прямого произведения.

2. Доказательство теоремы

Для доказательства теоремы нам понадобится следующее простое замечание:

Лемма. *Пусть a — элемент бесконечного порядка группы G и A — циклическая подгруппа этой группы, порожденная элементом a. Пусть также π — некоторое множество простых чисел. Предположим, что подгруппа A π'-изолирована и что любая подгруппа группы G, лежащая в A и π'-изолированная в группе G, является $\mathcal{F}_\pi$-отделимой в этой группе. Тогда для произвольного целого π-числа $m > 0$ существует нормальная подгруппа N конечного π-индекса группы G такая, что порядок по модулю N элемента a делится на m.*

В самом деле, поскольку порядок элемента a бесконечен, ни один из элементов a, a^2, …, a^{m-1} не принадлежит подгруппе A^m, порожденной элементом a^m. Так как для любого целого числа n включение $a^n \in A^m$ равносильно делимости числа n на число m, подгруппа A^m является p-изолированной в группе A для любого простого числа p, не входящего в π, т. е. является π'-изолированной в группе A. Поскольку π'-изолированная подгруппа π'-изолированной подгруппы π'-изолирована, подгруппа A^m π'-изолирована в группе G и потому $\mathcal{F}_\pi$-отделима. Следовательно, существует нормальная подгруппа N конечного π-индекса группы G такая, что ни один из элементов a, a^2, …, a^{m-1} не принадлежит подгруппе $A^m N$. Обозначим через r порядок по модулю N элемента a; другими словами, r есть наименьшее положительное число такое, что $a^r \in N$. Пусть также d — наибольший общий делитель чисел m и r и пусть целые числа x и y таковы, что $mx + ry = d$. Тогда, поскольку $1 \leqslant d \leqslant m$ и

$$a^d = a^{mx+ry} = (a^m)^x \cdot (a^r)^y \in A^m N,$$

неравенство $d < m$ невозможно. Следовательно, $d = m$, т. е. число r делится на m, что и требовалось.

Предположим теперь, что $G = A \times B$ — прямое произведение групп A и B, т. е. A и B — подгруппы группы G, $G = AB$, $A \cap B = 1$ и $[A, B] = 1$. Предположим также, что группы A и B $\mathcal{F}_\pi$-аппроксимируемы и в каждой из этих групп любая π'-изолированная циклическая подгруппа $\mathcal{F}_\pi$-отделима и π'-изолятор любой циклической подгруппы является циклической подгруппой.

Пусть H — циклическая подгруппа группы G и ее порождающий элемент h имеет вид $h = cd$, где $c \in A$ и $d \in B$. Предположим, что подгруппа H π'-изолирована и элемент $g = ab$ (где $a \in A$ и $b \in B$) группы G не принадлежит подгруппе H. Требуется показать, что существует нормальная подгруппа N конечного π-индекса группы G такая, что $g \notin HN$.

Поскольку группа G является $\mathcal{F}_\pi$-аппроксимируемой и, как нетрудно видеть, в $\mathcal{F}_\pi$-аппроксимируемой группе любая конечная подгруппа $\mathcal{F}_\pi$-отделима, подгруппу H можно считать бесконечной.

Обозначим через C циклическую подгруппу группы A, порожденную элементом c, и через D — циклическую подгруппу группы B, порожденную элементом d.

Поскольку подгруппа H бесконечна и потому бесконечен порядок элемента h, для элементов c и d имеются две возможности: либо оба эти элемента имеют бесконечный порядок, либо бесконечен порядок в точности одного из них.

Рассмотрим сначала первую возможность, т. е. будем считать, что c и d — элементы бесконечного порядка.

Пусть $U = (u)$ — π'-изолятор в группе A подгруппы C, $V = (v)$ — π'-изолятор в группе B подгруппы D. Тогда $c = u^k$ и $d = v^l$ для некоторых целых k и l (которые можно без потери общности считать положительными). При этом k и l являются π'-числами.

Действительно, пусть, скажем, $k = k_1 p$ для некоторого простого $p \in \pi$. Так как индекс подгруппы U^p в группе U равен p, подгруппа U^p является π'-изолированной подгруппой группы U и потому π'-изолирована в группе A. Поскольку $c = (u^p)^{k_1}$ и, значит, $C \subseteq U^p$, это противоречит тому, что U является наименьшей π'-изолированной подгруппой, содержащей C.

Заметим также, что числа k и l взаимно просты. Действительно, если t — общий делитель этих чисел и $k = k_1 t$, $l = l_1 t$ для подходящих целых k_1 и l_1, то $(u^{k_1} v^{l_1})^t = cd \in H$, и так как подгруппа H π'-изолирована и t является π'-числом, имеем $u^{k_1} v^{l_1} \in H$. Поскольку тогда $u^{k_1} v^{l_1} = (u^k v^l)^x$ для некоторого целого x, очевидно, что $|t| = 1$.

Если элемент a не принадлежит подгруппе U, то в силу условия теоремы существует нормальная подгруппа R конечного π-индекса группы A такая, что $a \notin UR$. Тогда $N = RB$ — нормальная подгруппа конечного π-индекса группы G и утверждается, что элемент g не принадлежит подгруппе HN.

В самом деле, в противном случае для некоторого целого числа t и некоторых элементов $x \in R$ и $y \in B$ должно выполняться равенство $g = u^t xy$. Переписав его в виде $ab = c^t x \cdot d^t y$, имеем $a = c^t x \in UR$, что противоречит выбору подгруппы R.

Так как случай, когда элемент b не принадлежит подгруппе V, рассматривается аналогично, остается предположить, что элементы a и b лежат в подгруппах U и V соответственно, т. е. $a = u^m$ и $b = v^n$ для некоторых целых m и n.

Предположим сначала, что m делится на k, т. е. $m = kx$ для некоторого целого числа x. Тогда $n \neq lx$, поскольку иначе

$$ab = u^m v^n = u^{kx} v^{lx} = (u^k v^l)^x = (cd)^x \in H.$$

Таким образом, $v^{n-lx} \neq 1$, и потому элемент v^{n-lx} не входит в некоторую нормальную подгруппу S конечного π-индекса группы B.

Пусть s — порядок элемента v по модулю подгруппы S. Так как числа l и s взаимно просты, существует целое число y такое, что $ly \equiv n \pmod{s}$. Отметим, что числа x и y не сравнимы по модулю s. Действительно, из $x \equiv y \pmod{s}$ следовало бы сравнение $n - lx \equiv n - ly \pmod{s}$, откуда, в свою очередь, мы имели бы

$$v^{n-lx} \equiv v^{n-ly} \equiv 1 \pmod{S},$$

что противоречит выбору S.

В соответствии с леммой в группе A можно выбрать такую нормальную подгруппу R конечного π-индекса, что порядок r по модулю R элемента u делится на s. Тогда $N = RS$ — нормальная подгруппа конечного π-индекса группы G и утверждается, что элемент g не принадлежит подгруппе HN.

Действительно, если, напротив, $g \in h^t N$ для некоторого целого числа t, то $a \equiv c^t \pmod{R}$ и $b \equiv d^t \pmod{S}$, т. е. $u^m \equiv u^{kt} \pmod{R}$ и $v^n \equiv v^{lt} \pmod{S}$. Следовательно, $kx \equiv kt \pmod{r}$ и $ly \equiv lt \pmod{s}$. Так как числа k и r взаимно просты и s делит r, из первого сравнения получаем $x \equiv t \pmod{s}$, и поскольку из второго сравнения следует $y \equiv t \pmod{s}$, имеем $x \equiv y \pmod{s}$, что невозможно, как отмечено выше.

Так как случай, когда n делится на l, рассматривается аналогично, будем считать далее, что m не делится на k и n не делится на l.

Тогда из взаимной простоты чисел k и l следует, что $ml \neq nk$. Поэтому элемент u^{ml-nk} отличен от единицы и потому не входит в некоторую нормальную подгруппу R конечного π-индекса группы A. Следовательно, числа ml и nk не сравнимы по модулю r, где r — порядок элемента u по модулю подгруппы R. Фиксируем также целое число x, удовлетворяющее сравнению $m \equiv kx \pmod{r}$ (и существующее в силу взаимной простоты чисел r и k).

Далее выберем нормальную подгруппу S конечного π-индекса группы B так, чтобы порядок s элемента v по модулю подгруппы S делился на r, и фиксируем целое число y такое, что $n \equiv ly \pmod{s}$ (и потому $n \equiv ly \pmod{r}$).

Тогда $N = RS$ — нормальная подгруппа конечного π-индекса группы G и утверждается, что элемент g не принадлежит подгруппе HN.

Действительно, если, напротив, $g \in h^t N$ для некоторого целого числа t, то $a \equiv c^t \pmod{R}$ и $b \equiv d^t \pmod{S}$, т. е. $u^m \equiv u^{kt} \pmod{R}$ и $v^n \equiv v^{lt} \pmod{S}$. Следовательно, $kx \equiv kt \pmod{r}$ и $ly \equiv lt \pmod{s}$. Так как числа k и r взаимно просты, l и s взаимно просты и s делится на r, из первого сравнения получаем $x \equiv t \pmod{r}$, а из второго имеем $y \equiv t \pmod{r}$. Таким образом, $x \equiv y \pmod{r}$. Отсюда имеем

$$ml \equiv (kx)l = (lx)k \equiv (ly)k \equiv nk \pmod{r},$$

что невозможно в силу выбора R.

Перейдем к рассмотрению второй возможности. Для определенности предположим, что порядок элемента c бесконечен, а порядок элемента d конечен и равен s. Так как группа B $\mathcal{F}_\pi$-аппроксимируема и ее подгруппа D конечна, то D является $\mathcal{F}_\pi$-отделимой и, следовательно, π'-изолиро-

ванной подгруппой группы B. Покажем, что в этом случае и подгруппа C π'-изолирована в группе A.

Пусть, напротив, существуют простое число p, не входящее в множество π, и элемент $f \in A \setminus C$ такие, что $f^p \in C$, т. е. $f^p = c^t$ для некоторого целого t. Так как числа p и s взаимно просты, существует целое x такое, что $t \equiv px \pmod{s}$. Тогда $d^t = d^{px}$ и потому $(fd^x)^p = f^p d^{xp} = c^t d^t = h^t$. Поскольку элемент fd^x не входит в H, это противоречит π'-изолированности H.

Если элемент a не принадлежит подгруппе C или элемент b не принадлежит подгруппе D, то в силу $\mathcal{F}_\pi$-отделимости этих подгрупп найдутся такие нормальные подгруппы R или S конечных π-индексов групп A или B соответственно, что $a \notin CR$ или $b \notin DS$. Как и выше, нетрудно видеть, что тогда $g \notin H(RB)$ или $g \notin H(AS)$.

Остается рассмотреть случай, когда элементы a и b лежат в подгруппах C и D соответственно, т. е. $a = c^m$ и $b = d^n$ для некоторых целых чисел m и n.

Так как группа B $\mathcal{F}_\pi$-аппроксимируема, в ней существует нормальная подгруппа S конечного π-индекса, не содержащая ни одного из (неединичных) элементов d, d^2, …, d^{s-1}; тогда, очевидно, порядок по модулю S элемента d равен s. Выберем также нормальную подгруппу R конечного π-индекса группы A так, чтобы порядок r по модулю R элемента u делился на s. Тогда $N = RS$ — нормальная подгруппа конечного π-индекса группы G и снова утверждается, что элемент g не принадлежит подгруппе HN.

Действительно, включение $g \in HN$, как и выше, означает, что для некоторого целого числа t имеют место сравнения $m \equiv t \pmod{r}$ и $n \equiv t \pmod{s}$. Так как r делится на s, из первого сравнения получаем $m \equiv t \pmod{s}$, так что $m \equiv n \pmod{s}$. Следовательно, в группе B выполняется равенство $d^n = d^m$, и потому в группе G

$$g = ab = c^m d^n = (c^d)^m = h^m,$$

что противоречит предположению $g \notin H$.

Теорема доказана.

3. Построение примера

Фиксируем простое число p и обозначим через A группу, заданную представлением

$$\langle a_1, a_2, \ldots;\ a_i = a_{i+1}^p\ (i \in \mathbb{N})\rangle.$$

Пусть также B — бесконечная циклическая группа с порождающим b и $G = A \times B$ — прямое произведение групп A и B. Будет показано, что если π — множество, состоящее из всех простых чисел, отличных от p (так что $\pi' = \{p\}$), то группа A $\mathcal{F}_\pi$-аппроксимируема и любая π'-изолированная подгруппа этой группы является $\mathcal{F}_\pi$-отделимой. Вместе с тем очевидно, что, например, π'-изолятор циклической подгруппы группы A, порождаемой элементом a_i, совпадает со всей группой A и, следовательно, циклической группой не является.

Начнем с перечисления ряда необходимых нам свойств группы A. Очевидной индукцией проверяется, что для любых положительных целых чисел i и k выполнено равенство $a_i = a_{i+k}^{p^k}$. Хорошо известно, что эта груп-

па изоморфна состоящей из p-ичных дробей подгруппе аддитивной группы рациональных чисел. Отсюда следует, что группа A не имеет кручения и произвольный неединичный элемент $g \in A$ однозначно представим в виде $g = a_i^m$ для некоторых целых $i > 0$ и m, причем при $i > 1$ число m на p не делится. Такую запись элемента g будем называть канонической. Вводимые всюду ниже записи элементов группы по умолчанию предполагаются каноническими.

Следующее утверждение, по-видимому, также хорошо известно.

Предложение 1. *Для любого простого числа q, отличного от p, группа A является $\mathcal{F}_q$-аппроксимируемой.*

Действительно, если $C(q^n)$ — циклическая группа порядка q^n с порождающим c и t — решение сравнения $px \equiv 1 \pmod{q^n}$, то отображение $a_i \mapsto c^{t^{i-1}}$ $(i = 1, 2, \dots)$ определяет гомоморфизм φ_n группы A на группу $C(q^n)$. При этом, поскольку числа t и q взаимно просты, для любого i порядок элемента $a_i\varphi_n$ равен q^n. Следовательно, если $g = a_i^m$ — неединичный элемент группы A, то для любого n такого, что число m не делится на q^n, имеем $g\varphi_n \neq 1$.

Перейдем теперь к рассмотрению свойств циклических подгрупп группы G.

Предложение 2. *Пусть H — циклическая подгруппа группы G, порожденная элементом $h = a_i^k b^l$, и пусть $g = a_j^r b^s$ — неединичный элемент группы G. Тогда*

1) *если одно из чисел l и s равно нулю, а другое отлично от нуля, то элемент g не принадлежит подгруппе H;*

2) *если $l = s = 0$, то элемент g принадлежит подгруппе H тогда и только тогда, когда $j \leqslant i$ и r делится на k;*

3) *если числа l и s отличны от нуля, то элемент g принадлежит подгруппе H тогда и только тогда, когда $j \leqslant i$ и существует целое число m такое, что $s = lm$, $m = m_1 p^{i-j}$ для некоторого целого m_1 и $r = km_1$.*

Доказательство. Если $l = 0$ и $s \neq 0$, то $H \leqslant A$, а элемент g не входит в A и потому не входит в H. Если $l \neq 0$ и $s = 0$, то $H \cap A = 1$, а элемент g лежит в подгруппе A и отличен от 1, так что и в этом случае $g \notin H$.

Если $l = s = 0$, то $g \in H$ тогда и только тогда, когда для некоторого целого числа n выполнено равенство $a_j^r = a_i^{kn}$. Если $j > i$, то $a_i = a_j^{p^{j-i}}$ и это равенство принимает вид $a_j^r = a_j^{knp^{j-i}}$, что равносильно равенству $r = knp^{j-i}$. Но это противоречит каноничности записи элемента g.

Таким образом, $j \leqslant i$, и так как тогда $a_j = a_i^{p^{i-j}}$, равенство $a_j^r = a_i^{kn}$ равносильно равенству $rp^{i-j} = kn$. Отсюда ввиду каноничности записи элемента h имеем $n = n_1 p^{i-j}$ для некоторого целого числа n_1, и потому $r = kn_1$.

Будем считать теперь, что числа l и s отличны от нуля и предположим сначала, что элемент g принадлежит подгруппе H, т. е. для некоторого целого числа m выполнено равенство $g = h^m$. Это равенство равносильно, очевидно, системе равенств $a_j^r = a_i^{km}$ и $b^s = b^{lm}$, и в силу второго из них $s = lm$. Докажем теперь, что $j \leqslant i$.

Если, напротив, $j > i$, то $j > 1$, и потому число r не делится на p.

Кроме того, $a_i = a_j^{p^{j-i}}$, и равенство $a_j^r = a_i^{km}$ принимает вид $a_j^r = a_j^{kmp^{j-i}}$. Поскольку A является группой без кручения, отсюда получаем $r = kmp^{j-i}$, что невозможно, так как $j - i > 0$ и r на p не делится.

Таким образом, неравенство $j \leqslant i$ действительно справедливо. Поэтому $a_j = a_i^{p^{i-j}}$, и на этот раз равенство $a_j^r = a_i^{km}$ принимает вид $a_i^{rp^{i-j}} = a_i^{km}$, откуда имеем $rp^{i-j} = km$. Поскольку при $i > j$ число k взаимно просто с p, в этом случае $m = m_1 p^{i-j}$ для некоторого целого числа m_1. Полагая $m_1 = m$ при $i = j$, в любом случае имеем $m = m_1 p^{i-j}$ и $r = km_1$.

Наоборот, если все условия из формулировки предложения выполнены, то

$$h^m = a_i^{km} b^{lm} = a_i^{km_1 p^{i-j}} b^s = a_i^{rp^{i-j}} b^s = a_j^r b^s = g,$$

так что $g \in H$ и предложение доказано.

Предложение 3. *Подгруппа H группы G, порожденная элементом $h = a_i^k b^l$, является p-изолированной тогда и только тогда, когда число l взаимно просто с p.*

Доказательство. Предположим сначала, что числа l и p взаимно просты и что для элемента $g = a_j^r b^s$ группы G имеет место включение $g^p \in H$. Поскольку $g^p = a_j^{rp} b^{sp}$ и $l \neq 0$, то в соответствии с предложением 2 выполнено неравенство $j \leqslant i$ и существует целое число m такое, что $sp = lm$ и $m = m_1 p^{i-j}$ для некоторого целого m_1 и $rp = km_1$. Далее рассмотрим отдельно два случая в зависимости от значения разности $i - j$.

Если $i - j > 0$, то $i > 1$, и потому числа k и p взаимно просты. Поэтому из равенства $rp = km_1$ следует, что $m_1 = m_2 p$ для некоторого целого m_2, откуда получаем $r = km_2$. Кроме того, полагая $m' = m_2 p^{i-j}$, имеем $m = m'p$, и потому из равенства $sp = lm$ следует равенство $s = lm'$. Таким образом, для элемента g и числа m' выполнены все условия предложения 2, гарантирующие включение $g \in H$.

Пусть теперь $i = j$, так что $m_1 = m$. Из равенства $sp = lm$ ввиду взаимной простоты чисел l и p следует, что $m = m'p$ для некоторого целого m', и потому $s = lm'$. Кроме того, равенство $rp = km_1$ принимает вид $r = km'$, и включение $g \in H$ выполнено и в этом случае.

Таким образом, доказано, что при взаимно простых l и p подгруппа H является p-изолированной.

Наоборот, если $l = l_1 p$ для некоторого целого числа l_1, то для элемента $f = a_{i+1}^k b^{l_1}$ будем иметь $f^p = a_{i+1}^{kp} b^{l_1 p} = a_i^k b^l = h$, так что $f^p \in H$. Но элемент f в силу предложения 2 не входит в подгруппу H, так как $i + 1 > i$. Следовательно, H не является p-изолированной.

Предложение 4. *Пусть π — множество всех простых чисел, отличных от числа p. Каждая π'-изолированная циклическая подгруппа группы G является $\mathcal{F}_\pi$-аппроксимируемой.*

Доказательство. Пусть, как и выше, H — циклическая подгруппа группы G, порожденная элементом $h = a_i^k b^l$. Предположим, что H является π'-изолированной подгруппой; поскольку множество π' состоит из единственного числа p, в силу предложения 3 это означает, что число l не делится на p (и потому отлично от 0).

Предположим также, что элемент $g = a_j^r b^s$ не принадлежит подгруппе H, и покажем, что тогда в группе G существует нормальная подгруппа N конечного π-индекса такая, что g не принадлежит подгруппе HN. Поскольку $g \notin H$ и $l \neq 0$, то в силу предложения 2 либо $s = 0$, либо $s \neq 0$ и должно нарушаться одно из условий пункта 3 этого предложения. Рассмотрим последовательно все эти случаи.

1. Число s равно 0. Тогда $r \neq 0$ (так как $g \neq 1$), и потому можно выбрать простое число q, отличное от p и взаимно простое с каждым из чисел r и l. Покажем, что подгруппа $N = A^q B^q$ является искомой.

Действительно, ее индекс в группе G равен π-числу q^2, а предположение о том, что $g \in HN$, равносильно выполнимости равенств $a_j^r = a_i^{kx} a_u^{yq}$ и $1 = b^{lx+zq}$ для некоторых целых чисел x, y, z и натурального u. Второе из них влечет $q|x$, и потому из первого вытекает включение $a_j^r \in A^q$, что противоречит взаимной простоте чисел r и q.

2. Число s отлично от 0, но не делится на l. Так как тогда $|l| > 1$, число l обладает простым делителем q, который в силу взаимной простоты l и p отличен от p и потому входит в π. Легко видеть, что подгруппа $N = AB^q$ является в этом случае искомой.

В самом деле, если элемент g принадлежит подгруппе HN, то $g = h^n uv$ для некоторого целого числа n и некоторых элементов $u \in A$ и $v \in B^q$. Очевидно, что тогда выполнено равенство $b^s = b^{ln} v$, из которого следует включение $b^s \in B^l$, противоречащее предположению.

3. Число s отлично от 0, для некоторого целого числа m выполнено равенство $s = lm$ и $j > i$. Так как в этом случае r не делится на p (поскольку $j > 1$), число $r - kmp^{j-i}$ отлично от нуля. Выберем простое число q, отличное от p, взаимно простое с l и не делящее числа $r - kmp^{j-i}$. Покажем, что в этом случае искомой является подгруппа $N = A^q B^q$.

В самом деле, если элемент g принадлежит подгруппе HN, то $g = h^n uv$ для некоторого целого числа n и некоторых элементов $u \in A^q$ и $v \in B^q$. Это равенство равносильно системе равенств $a_j^r = a_i^{kn} u$ и $b^s = b^{ln} v$. Поскольку в этом случае $a_i = a_j^{p^{j-i}}$, первое из них принимает вид $a_j^r = a_j^{knp^{j-i}} u$ и потому равносильно сравнению $r \equiv knp^{j-i} \pmod q$. Второе равенство равносильно сравнению $s \equiv ln \pmod q$, которое в силу того, что $s = lm$ и $(l, q) = 1$, равносильно сравнению $n \equiv m \pmod q$. Поэтому сравнение $r \equiv knp^{j-i} \pmod q$ принимает вид $r \equiv kmp^{j-i} \pmod q$, что противоречит выбору q.

4. Предположим теперь, что $s \neq 0$, $j \leqslant i$, $s = lm$ для некоторого целого числа m и число m не делится на p^{i-j}. Так как в этом случае $i - j > 0$ и числа k и p взаимно просты, то число $rp^{i-j} - km$ отлично от нуля. Поэтому можно выбрать простое число q, отличное от p, взаимно простое с l и не делящее числа $rp^{i-j} - km$. Покажем, что и в этом случае подгруппа $N = A^q B^q$ является искомой.

Действительно, из предположения о справедливости включения $g \in HN$ следует, в частности, что для некоторого целого числа n имеют место сравнения $a_j^r \equiv a_i^{kn} \pmod{A^q}$ и $b^s \equiv b^{ln} \pmod{B^q}$. Так как в этом случае $a_j = a_i^{p^{i-j}}$, из первого имеем $a_i^{rp^{i-j}} \equiv a_i^{kn} \pmod{A^q}$, откуда получаем $rp^{i-j} \equiv kn \pmod q$. Сравнение $b^s \equiv b^{ln} \pmod{B^q}$ дает $s \equiv ln \pmod q$,

что вместе с равенством $s = lm$ и условием $(l, q) = 1$ влечет сравнение $n \equiv m \pmod q$. Таким образом, приходим к сравнению $rp^{i-j} \equiv km \pmod q$, противоречащему выбору q.

5. Оставшийся случай, когда $s \neq 0$, $j \leqslant i$, $s = lm$ для некоторого целого числа m и $m = m_1 p^{i-j}$ для некоторого m_1, но $r \neq km_1$, рассматривается аналогично. Если простое число q выбрать отличным от p, взаимно простым с l и не делящим разности $r - km_1$ и снова положить $N = A^q B^q$, то предположение о справедливости включения $g \in HN$ повлечет сравнение $rp^{i-j} \equiv km_1 p^{i-j}$, равносильное сравнению $r \equiv km_1$. Предложение 4 доказано.

Таким образом, в силу предложений 1 и 4 группа G $\mathcal{F}_\pi$-аппроксимируема и любая ее π'-изолированная циклическая подгруппа $\mathcal{F}_\pi$-отделима. Вместе с тем прямой сомножитель A группы G обладает циклическими подгруппами, π'-изоляторы которых циклическими не являются.

Библиографический список

1. *Бардаков В. Г.* К вопросу Д. И. Молдаванского о p-отделимости подгрупп свободной группы // Сибирский математический журнал. 2004. Т. 45, № 3. С. 505—509.
2. Коуровская тетрадь. Нерешенные вопросы теории групп. 15-е изд. Новосибирск : Новосиб. гос. ун-т, 2002. 172 с.
3. *Магнус В., Каррас А., Солитэр Д.* Комбинаторная теория групп. М. : Наука, 1974. 455 с.
4. *Романовский Н. С.* О финитной аппроксимируемости свободных произведений относительно вхождения // Известия АН СССР. Сер. математическая. 1969. Т. 33, № 6. С. 1324—1329.
5. *Allenby R., Gregorac R.* On locally extended residually finite groups // Lecture Notes Math. 1973. Vol. 319. P. 9—17.
6. *Hall M.* Coset representations in free groups // Trans. Amer. Math. Soc. 1949. Vol. 67. P. 421—432.
7. *Meskin S.* Nonresidually finite one-relator groups // Trans. Amer. Math. Soc. 1972. Vol. 164. P. 105—114.
8. *Sokolov E. V.* On the cyclic subgroup separability of the free product of two groups with commuting subgroups // Int. J. Algebra Comput. 2014. Vol. 24, № 5. P. 741—756.
9. *Stebe P.* Residual finiteness of a class of knot groups // Comm. Pure Appl. Math. 1968. Vol. 21. P. 563—583.

УДК 519.688

Е. В. Соколов

АЛГОРИТМЫ ПОЛУЧЕНИЯ ОБЩЕГО СЕКРЕТНОГО КЛЮЧА, ИСПОЛЬЗУЮЩИЕ ГРУППЫ С ТОЖДЕСТВАМИ

Приводятся обобщения двух известных криптографических алгоритмов получения общего секретного ключа, использующие в качестве базовой произвольную группу, удовлетворяющую нетривиальному тождеству определенного вида.

Ключевые слова: криптография с открытым ключом, проблема поиска сопрягающего элемента, проблема поиска разложения элемента.