Сибирский математический журнал
Ноябрь—декабрь, 2008. Том 49, № 6

УДК 512.544

ОЦЕНКА ПОРЯДКА ГРУППЫ, ПОРОЖДЕННОЙ КОНЕЧНЫМ СКРУЧЕННЫМ ПОДМНОЖЕСТВОМ

В. В. Беляев, А. Л. Мыльников

Аннотация. Доказано, что группа, порожденная конечным скрученным подмножеством, конечна и ее порядок ограничен некоторой функцией, зависящей только от порядка скрученного подмножества.

Ключевые слова: скрученное подмножество, скрученная подгруппа.

Следуя [1], приведем определение скрученного подмножества.

Определение 1. Подмножество K из группы G называется *скрученным*, если $1 \in K$ и для любых элементов x, y из K элемент $xy^{-1}x$ принадлежит K.

Основной вопрос, который рассматривается в данной работе, состоит в следующем: *конечна ли группа, порожденная конечным скрученным подмножеством*? При положительном ответе на данный вопрос сразу же возникают другие вопросы, а именно: *можно ли дать оценку порядка группы, зная порядок скрученного подмножества, порождающего данную группу*? *Насколько точна данная оценка*?

Получены следующие результаты, отвечающие на указанные вопросы.

Теорема 1. *Пусть G — группа и K — конечное скрученное подмножество группы G такое, что $G = \langle K \rangle$. Тогда G — конечная группа и $|G| \leq 2^{|K|-1}$.*

Теорема 2. *Пусть G — группа и K — конечное скрученное подмножество группы G такое, что $G = \langle K \rangle$. Тогда следующие условия эквивалентны:*
(I) $|G| = 2^{|K|-1}$;
(II) *G — элементарная абелева 2-группа и $K \setminus \{1\}$ — базис группы G.*

Конечность группы, порожденной конечным скрученным подмножеством, изначально доказана вторым автором, но впоследствии первым автором предложено усиление данного результата в виде теорем 1, 2 настоящей работы. Основные идеи доказательств теорем 1, 2 принадлежат первому автору, а их детальное изложение с учетом замечаний первого автора проведено вторым автором данной работы.

Доказательство теоремы 1. Нам потребуется следующая

Лемма 1.1 [1, лемма 2.1]. *Пусть G — группа и K — скрученное подмножество G. Тогда для любого элемента x из K подгруппа $\langle x \rangle$ содержится в K.*

Пусть G — группа и K — конечное скрученное подмножество G такое, что $G = \langle K \rangle$. Введем некоторые понятия, необходимые для доказательства теорем 1, 2. Пусть $E := \{e \in K : |e| = 2\}$, $B := \{b \in K : |b| > 2\}$. Тогда $|E| = m$, $|B| = n$ для некоторых натуральных чисел m, n. Ясно, что $K \setminus \{1\} = E \cup B$ и $E \cap B = \varnothing$. Проиндексируем натуральными числами элементы из E и B

следующим образом: $E = \{w_1, \dots, w_m\}$, $B = \{w_{m+1}, \dots, w_{m+n}\}$, где для любого номера $i > m$ если $i - m$ — нечетное число, то $w_{i+1} = w_i^{-1}$.

Введем на множестве $K \setminus \{1\}$ бинарное отношение $\preceq$. Для любых w_i, w_j из $K \setminus \{1\}$ полагаем $w_i \preceq w_j$, если $i \le j$. В том случае, когда для элементов w_i, w_j справедливо $w_i \preceq w_j$ и $w_i \ne w_j$, будем писать $w_i \prec w_j$. Легко видеть, что отношение $\preceq$ является отношением линейного порядка на множестве $K \setminus \{1\}$.

Пусть $g \in G \setminus \{1\}$ и Ω_g — множество слов $v_1 \dots v_s$ таких, что $g = v_1 \dots v_s$ и $v_i \in K \setminus \{1\}$, $i = 1, \dots, s$. С помощью отношения $\preceq$ введем бинарное отношение $\underset{g}{\le}$ на Ω_g. Пусть $u_1 \dots u_r, v_1 \dots v_s \in \Omega_g$, т. е. $g = u_1 \dots u_r = v_1 \dots v_s$, где $u_i, v_j \in K \setminus \{1\}$. Полагаем $u_1 \dots u_r \underset{g}{\le} v_1 \dots v_s$, если выполняется одно из следующих условий:

(a) существует номер k такой, что $u_k \prec v_k$ и для любого номера $i < k$ справедливо равенство $u_i = v_i$.

(b) если (a) не выполняется, то $r \le s$.

Нетрудно видеть, что отношение $\underset{g}{\le}$ является отношением линейного порядка на множестве Ω_g. В том случае, когда $u_1 \dots u_r \underset{g}{\le} v_1 \dots v_s$ и существует номер k такой, что $u_k \ne v_k$, будем писать $u_1 \dots u_r \underset{g}{<} v_1 \dots v_s$.

Лемма 1.2. *Пусть g — элемент из $G \setminus \{1\}$. Тогда существуют элементы $u_1, \dots, u_s$ из $K \setminus \{1\}$ такие, что $g = u_1 \dots u_s$ и $u_i \prec u_j$ при $i < j$.*

Доказательство. Пусть $u_1 \dots u_s$ — слово минимальной длины в алфавите $K \setminus \{1\}$ из Ω_g. Заметим, что порядок множества слов в алфавите $K \setminus \{1\}$ длины s не превосходит величины $(|K| - 1)^s$, в частности, это множество конечно. Значит, существует наименьшее в смысле отношения $\underset{g}{\le}$ слово в множестве слов длины s. Обозначим его через $u_1 \dots u_s$. Покажем, что оно удовлетворяет заключению леммы 1.2.

Допустим противное, т. е. пусть существует номер $k < s$ такой, что $u_k \succeq u_{k+1}$, а для любых номеров i, j, удовлетворяющих неравенству $i < j < k$, справедливо $u_i \prec u_j$. Поскольку $u_1 \dots u_s$ — слово минимальной длины в алфавите $K \setminus \{1\}$ из Ω_g, ввиду леммы 1.1 получаем, что $u_i \ne u_{i+1}$ для любого номера $i = 1, \dots, s-1$. Следовательно, $u_k \succ u_{k+1}$.

Заметим, что $u_{k+1} \ne u_k^{-1}$. Действительно, в противном случае $u_1 \dots u_s = v_1 \dots v_{s-2}$, где $v_i = u_i$ при $i < k$ и $v_i = u_{i+2}$ при $i \ge k$. Ясно, что $v_1 \dots v_{s-2} \in \Omega_g$ и длина слова $v_1 \dots v_{s-2}$ меньше длины слова $u_1 \dots u_s$, что противоречит выбору слова $u_1 \dots u_s$.

Далее, $u_1 \dots u_s = u_1 \dots u_{k-1} u_{k+1}^{-1} (u_{k+1} u_k u_{k+1}) u_{k+2} \dots u_s = v_1 \dots v_s$, где при $i \ne k, k+1$ справедливо $v_i = u_i$, $v_k = u_{k+1}^{-1}$, $v_{k+1} = u_{k+1} u_k u_{k+1}$. В силу леммы 1.1 $v_k, v_{k+1} \in K$. Ясно, что $v_k \ne 1$.

Заметим, что $v_{k+1} \ne 1$. Действительно, в противном случае $u_k u_{k+1} = u_{k+1}^{-1}$. Тогда $u_1 \dots u_s = e_1 \dots e_{s-1}$, где при $i < k$ имеем $e_i = u_i$, $e_k = u_{k+1}^{-1}$, и при $i > k$ будет $e_i = u_{i+1}$. Ясно, что $e_1 \dots e_{s-1} \in \Omega_g$ и длина слова $e_1 \dots e_{s-1}$ меньше длины слова $u_1 \dots u_s$, что противоречит выбору $u_1 \dots u_s$.

Итак, $v_{k+1} \ne 1$. Следовательно, $v_1 \dots v_s \in \Omega_g$. Поскольку $u_{k+1} \ne u_k^{-1}$ и $u_{k+1} \prec u_k$, то $u_{k+1}^{-1} \prec u_k$. Значит, $v_1 \dots v_s \underset{g}{<} u_1 \dots u_s$, что противоречит выбору $u_1 \dots u_s$. Полученное противоречие доказывает лемму 1.2.

Приступим к доказательству теоремы 1. Пусть Ω — множество слов $v_1 \dots v_s$, где $v_i \in K \setminus \{1\}$ и $v_i \prec v_j$ при $i < j$. Поскольку все v_i попарно различны, нетрудно видеть, что длина любого слова $v_1 \dots v_s$ из Ω не превосходит величины $|K \setminus \{1\}| = |K| - 1$. Тогда порядок множества Ω равен порядку множества непустых подмножеств множества $K \setminus \{1\}$, т. е. числу $2^{|K|-1} - 1$.

В силу леммы 1.2 для любого элемента g из $G \setminus \{1\}$ существует слово $v_1 \dots v_s$ из Ω такое, что $g = v_1 \dots v_s$. Таким образом, $|G \setminus \{1\}| \leq 2^{|K|-1} - 1$, откуда $|G| \leq 2^{|K|-1}$.

Доказательство теоремы 2. Нетрудно видеть, что из (II) следует (I).

Покажем, что из (I) следует (II). Анализ ситуации разбивается на ряд этапов.

(1) *Пусть Ω — множество всех наборов $(v_1, \dots, v_s)$ элементов из $K \setminus \{1\}$ таких, что $v_i \prec v_j$ при $i < j$. Тогда для любого элемента g из $G \setminus \{1\}$ существует единственный набор $(u_1, \dots, u_t)$ из Ω такой, что $g = u_1 \dots u_t$.*

Нетрудно видеть, что порядок множества Ω равен порядку множества непустых подмножеств множества $K \setminus \{1\}$, т. е. $|\Omega| = 2^{|K|-1} - 1 = |G| - 1$.

В силу леммы 1.2 для любого элемента g из $G \setminus \{1\}$ существует набор $(u_1, \dots, u_t)$ из Ω такой, что $g = u_1 \dots u_t$. Значит, в силу того, что $|\Omega| = |G \setminus \{1\}|$, для любого элемента g из $G \setminus \{1\}$ существует единственный набор $(u_1, \dots, u_t)$ из Ω такой, что $g = u_1 \dots u_t$.

(2) *Для любого элемента x из K имеет место неравенство $|x| \leq 2$.*

Допустим, что существует элемент x из K такой, что $|x| > 2$. Очевидно, $x \in K \setminus \{1\}$. Можно считать, что $x \prec x^{-1}$. Следовательно, $(x, x^{-1}) \in \Omega$.

Из леммы 1.2 и п. (1) вытекает, что для любого набора $(u_1, \dots, u_s)$ из Ω справедливо $u_1 \dots u_s \neq 1$. Но $(x, x^{-1}) \in \Omega$ и $xx^{-1} = 1$. Получаем противоречие, которое доказывает (2).

(3) *Пусть $u, v \in K$. Тогда $uv = vu$.*

Допустим противное, т. е. что существуют элементы u, v из K такие, что $uv \neq vu$. Ввиду (2) u, v — инволюции. Ясно, что $w := u^v \in K$. Перенумеровав при необходимости элементы множества E, без уменьшения общности рассуждений можно считать, что $u \prec v \prec w$.

Рассмотрим $z := uv$. Ясно, что $z = vw$. Поскольку, как нетрудно видеть, $(u, v), (v, w) \in \Omega$, получаем противоречие с (1), которое доказывает п. (3).

(4) *Группа G — элементарная абелева 2-группа, и $K \setminus \{1\}$ — базис G.*

Из (2) и (3) вытекает, что G — элементарная абелева 2-группа. Поскольку $|G| = 2^{|K \setminus \{1\}|}$, легко видеть, что $K \setminus \{1\}$ — базис G.

П. (4), а вместе с ним и теорема 2 доказаны.

ЛИТЕРАТУРА

1. *Мыльников А. Л.* Конечные перекрученные группы // Сиб. мат. журн. 2007. Т. 48, № 2. С. 369–375.

Статья поступила 16 мая 2006 г., окончательный вариант — 9 февраля 2008 г.

Беляев Виссарион Викторович
Московский физико-технический институт, кафедра высшей математики,
Институтский пер., 9, Долгопрудный Московской обл. 141700
V.v.belyaev@list.ru

Мыльников Андрей Леонидович
Институт фундаментальной подготовки Сибирского федерального университета,
кафедра высшей математики 1, пр. Свободный, 79, Красноярск 660041
mylnand@yandex.ru