Сибирский математический журнал
Сентябрь—октябрь, 2006. Том 47, № 5

УДК 512.544

НИЛЬПОТЕНТНОСТЬ КОММУТАНТА КОНЕЧНОЙ ПЕРЕКРУЧЕННОЙ ГРУППЫ

А. Л. Мыльников

Аннотация: Исследуются конечные группы, в которых любое подмножество, содержащее 1 и замкнутое относительно операции $x \circ y = xy^{-1}x$, является подгруппой. Доказано, что коммутант такой группы нильпотентен, откуда вытекает, что ступень разрешимости такой группы не превосходит трех.

Ключевые слова: скрученное подмножество, скрученная подгруппа, перекрученная подгруппа.

Следуя [1], приведем

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

В 1998 г. Ашбахер в работе [2] показал, что скрученные подмножества связаны с инволютивными автоморфизмами группы, однако он оперировал не со скрученными подмножествами, а со *скрученными подгруппами*, которые согласно [2] определяются следующим образом: подмножество K из группы G называется *скрученной подгруппой*, если $1 \in K$ и $xyx \in K$ для любых x, y из K. Нетрудно показать, что в конечных группах понятия «скрученное подмножество» и «скрученная подгруппа» совпадают. Отметим также, что несколько иначе, чем в [2], связь между скрученными подмножествами и инволютивными автоморфизмами излагается в работе автора [3].

Понятно, что в произвольной группе любая ее подгруппа является скрученным подмножеством, но обратное в общем случае не выполняется. В связи с этим естественно возникает **вопрос**: *каково строение групп, у которых любое скрученное подмножество является подгруппой?*

Определение 2. Группа называется *перекрученной*, если в ней любое скрученное подмножество является подгруппой.

В данной работе продолжается исследование конечных перекрученных групп, начатое в [1]. Получен следующий результат.

Теорема 1. *Коммутант конечной перекрученной группы нильпотентен.*

Ввиду лемм 1.1, 1.2 (см. ниже) и [4, с. 15, теорема 15] из теоремы 1 получаем

Следствие 1. *Конечная перекрученная группа разрешима, и ее ступень разрешимости не превосходит трех.*

Автор выражает глубокую благодарность профессору В. В. Беляеву, под руководством которого была выполнена эта работа.

1. Известные результаты

В данном разделе для удобства читателя мы приводим некоторые известные результаты, используемые при доказательстве теоремы 1.

Лемма 1.1 [1, следствие 2.4]. *Любая секция перекрученной группы является перекрученной группой.*

По теореме 2 из [1] и теореме 7 из [4] получаем следующее утверждение.

Лемма 1.2. *Для конечной нильпотентной группы G нечетного порядка следующие условия эквивалентны:*
(1) *G — перекрученная группа;*
(2) *G — модулярная группа (т. е. решетка подгрупп группы G модулярна);*
(3) *$\langle X, Y\rangle = XY = YX$ для любых подгрупп X, Y группы G.*

Лемма 1.3 [1, теорема 1]. *Для конечной группы G следующие условия эквивалентны:*
1) *G — перекрученная группа;*
2) *$G = O_2(G) \times O(G)$, где $O_2(G)$ — циклическая группа, а $O(G)$ — конечная перекрученная группа нечетного порядка.*

Лемма 1.4 [5, с. 188, теорема 3.16]. *Пусть абелева q-группа A действует на q'-группе X. Тогда $X = \langle C_X(A_0) \mid A/A_0$ циклическая$\rangle$.*

Лемма 1.5 [3, лемма 2.6]. *Если H — неабелева группа, то $G := H \times H$ не является перекрученной.*

Лемма 1.6 [4, с. 33, предложение 1.7]. *Пусть G — конечная модулярная p-группа. Совокупность всех элементов периода p образует в ней характеристическую абелеву подгруппу.*

Лемма 1.7 [6, с. 211, теорема 12.5.2]. *Конечная p-группа, содержащая только одну подгруппу порядка p, является циклической или обобщенной группой кватернионов.*

Лемма 1.8 [5, с. 74, теорема 4.4]. *Пусть $G = PQ$, где P — элементарная абелева нормальная p-подгруппа из G и $|Q| = q$, где $p \neq q$ и p, q простые. Допустим, что $C_G(P) = P$ и P — минимальная нормальная подгруппа из G.*

Тогда если V/F — точный G-модуль, в котором F — поле характеристики, отличной от p и q, то $C_V(Q) \neq 0$.

Лемма 1.9 [5, с. 94, теорема 6.12]. *Полупростая ассоциативная алгебра A/F над полем F является прямой суммой своих минимальных двусторонних идеалов, каждый из которых является простым кольцом.*

Из леммы 1.4 вытекает следующее утверждение.

Лемма 1.10. *Пусть $G = A \leftthreetimes B$, где A — элементарная абелева p-группа, B — элементарная абелева q-группа и p, q — различные простые числа, причем $m(B) \geq 2$. Тогда существует элемент b из B такой, что $C_A(b) \neq 1$.*

2. Вспомогательные результаты

В данном разделе доказываются вспомогательные результаты, необходимые для доказательства теоремы 1.

Лемма 2.1. *Пусть $G = A \rtimes \langle b \rangle$ — конечная группа, где A — элементарная абелева p-группа, $|b| = q^n$, $p \neq q$ и b действует неприводимо на A. Пусть R — подкольцо $\operatorname{End} A$, порожденное φ_b таким, что $\varphi_b(a) = b^{-1}ab$ для любого a из A. Тогда справедливы следующие утверждения:*

(1) R — поле;

(2) $A = \{\varphi(a) \mid \varphi \in R\}$ для любого a из $A \setminus \{1\}$;

(3) если элемент b^q действует неприводимо на подгруппе A, то кольцо R порождается эндоморфизмом φ_b^q.

Доказательство. (1) Ясно, что R — конечное коммутативное кольцо. Пусть $\psi \in R$. Покажем, что либо $\psi = 0$, либо ψ — автоморфизм A. Предположим, что ψ не является автоморфизмом. Тогда $\operatorname{Ker}\psi \neq 0$. Очевидно, что $\operatorname{Ker}\psi \leq A$. Так как для любого x из $\operatorname{Ker}\psi$ имеем $\psi(\varphi_b(x)) = \varphi_b(\psi(x)) = \varphi_b(0) = 0$, то $\varphi_b(\operatorname{Ker}\psi) \subseteq \operatorname{Ker}\psi$ и, следовательно, $\operatorname{Ker}\psi$ — нормальная подгруппа в G. Поскольку A — минимальная нормальная подгруппа в G, имеем $\operatorname{Ker}\psi = A$, т. е. $\psi = 0$.

Таким образом, R не содержит делителей нуля и, значит, является полем.

(2) Пусть $a \in A \setminus \{0\}$ и $L := \{\psi(a) \mid \psi \in B\}$; L — подгруппа в A, так как для любых φ, ψ из B по определению сложения в $\operatorname{End} A$ будет $\varphi(a) + \psi(a) = (\varphi + \psi)(a) \in L$.

Далее, L — нормальная подгруппа в G, так как $(\psi(a))^b = (\varphi_b\psi)(a) \in L$ для любого ψ из B. Тогда в силу минимальной нормальности A получаем, что $L = A$.

(3) Пусть $H := A \rtimes \langle b^q \rangle$ и L — подкольцо $\operatorname{End} A$, порожденное φ_b^q. Нетрудно видеть, что для подгруппы H выполнены все условия леммы 2.1. Тогда из п. (2) данной леммы вытекает, что $|L| = |A|$. Понятно, что $L \subseteq R$. Поскольку согласно п. (2) данной леммы $|R| = |A|$, имеем $L = R$. Доказательство леммы 2.1 завершено.

Лемма 2.2. *Пусть $G = A \rtimes \langle b \rangle$ — конечная группа нечетного порядка, где $A = A_1 \times \dots \times A_q$ — абелева группа, $|b| = q^n$, q простое и $A_i^b = A_{i+1}$, $A_q^b = A_1$, причем $A_1 \neq 1$, $i = 1, \dots, q-1$. Тогда G не является перекрученной группой.*

Доказательство. Следуя [1], подгруппоид, порожденный некоторым подмножеством $M \cup 1$ из группы G с помощью бинарной операции $x \circ y = xy^{-1}x$, будем обозначать через $Tw(M)$.

Рассмотрим $K := Tw(A_1, b)$. Ясно, что $G = \langle K \rangle$.

Покажем, что $K \neq G$. Доказательство этого утверждения разбивается на ряд этапов.

(i) Пусть $x \in K$. Тогда для x возможны случаи:

(1) $x = b_1 a_1 \dots b_s a_s b_s \dots a_1 b_1$;

(2) $x = b_1 a_1 \dots b_s a_s b_{s+1} a_s b_s \dots a_1 b_1$ для некоторого $s \geq 0$,

где в обоих случаях $a_i \in A_1$, $b_i \in \langle b \rangle$.

Пусть M — множество элементов из K, которые представимы в виде (1) или (2). Несложно проверить, что M замкнуто относительно операции $x \circ y = xy^{-1}x$ и, значит, является скрученным подмножеством, так как $1 \in M$. Поскольку $A_1 \cup b \subseteq M \subseteq K$, получаем, что $M = K$, и утверждение (i) доказано.

(ii) Пусть $x \in K \cap A$. Тогда если для x выполнен случай (1) из (i), то x представим в виде $x = \big(a_1^{b_1^{-1}} a_1^{b_1}\big) \dots \big(a_{s-1}^{b_{s-1}^{-1}} a_{s-1}^{b_{s-1}}\big) a_s$, если — случай (2), то в виде $x = \big(a_1^{b_1^{-1}} a_1^{b_1}\big) \dots \big(a_{s-1}^{b_{s-1}^{-1}} a_{s-1}^{b_{s-1}}\big)$, где в обоих случаях $a_i \in A_1$, $b_i \in \langle b \rangle$.

В случае (1) из (i) с помощью вставок вида $\hat{b}^{-1}\hat{b}$ для подходящего $\hat{b}$ из $\langle b\rangle$ элемент x приводится к слову следующего вида:

$$x = a_1^{b_1^{-1}} \dots a_{s-1}^{b_{s-1}^{-1}} b^* a_s b^* a_{s-1}^{b_{s-1}} \dots a_1^{b_1},$$

где $b^*, b_i \in \langle b\rangle$. Так как G — группа нечетного порядка и $x \in A$, то $b^* = 1$. Теперь легко получаем искомое разложение.

Если для x выполнен случай (2), рассуждения аналогичны предыдущим.

(iii) Пусть t целое, $0 \le t < q$ и x — элемент из A, представимый в виде $x = \big(a_1^{b_1^{-1}} a_1^{b_1}\big) \dots \big(a_{s-1}^{b_{s-1}^{-1}} a_{s-1}^{b_{s-1}}\big)$, где $a_i \in A_1$, $b_i = b^{k_i}$ и для любых i,j справедливо $k_i \equiv k_j \equiv t (\operatorname{mod} q)$. Тогда x представим в виде $x = b^m a_1^{c_1} \dots a_s^{c_s} b^{-m} b^{-m} a_1^{c_1^{-1}} \dots a_s^{c_s^{-1}} b^m$, где $c_i \in \langle b\rangle$, $a_i^{c_i}, a_i^{c_i^{-1}} \in A_1$ и $0 \le m \le \frac{q-1}{2}$. По условию $k_i = t + m_i q$, где m_i целое. Тем самым

$$\begin{aligned} x &= \big(a_1^{b_1^{-1}} a_1^{b_1}\big) \dots \big(a_{s-1}^{b_{s-1}^{-1}} a_{s-1}^{b_{s-1}}\big) \\ &= b^t\big(b^{m_1 q} a_1 b^{-m_1 q} \dots b^{m_s q} a_s b^{-m_s q}\big) b^{-t} b^{-t} (b^{-m_1 q} a_1 b^{m_1 q} \dots b^{-m_s q} a_s b^{m_s q}) b^t. \end{aligned}$$

Если $t \le \frac{q-1}{2}$, то, полагая $m = t$ и $c_i = b^{-m_i q}$, получаем требуемое.

Таким образом, далее можно считать, что $\frac{q-1}{2} < t < q$. Тогда

$$\begin{aligned} x = (b^{q-t} b^{-q} (b^{m_1 q} a_1 b^{-m_1 q} \dots b^{m_s q} a_s b^{-m_s q}) b^q b^{t-q}) (b^{t-q} b^q (b^{-m_1 q} a_1 b^{m_1 q} \\ \dots b^{-m_s q} a_s b^{m_s q}) b^{-q} b^{q-t}) = b^{q-t} (b^{m_1 q - q} a_1 b^{-m_1 q + q} \\ \dots b^{m_s q - q} a_s b^{-m_s q + q}) b^{t-q} b^{t-q} (b^{-m_1 q + q} a_1 b^{m_1 q + q} \dots b^{-m_s q + q} a_s b^{m_s q + q}) b^{q-t}. \end{aligned}$$

Нетрудно видеть, что $0 < q - t \le \frac{q-1}{2}$.

Так как $b^{m_i q - q} a_i b^{-m_i q + q}, b^{-m_i q + q} a_i b^{m_i q - q} \in A_1$, то, полагая $m = q - t$ и $c_i = b^{-m_i q + q}$, получаем искомое разложение x.

(iv) $|K \cap A| \ne |A|$.

Из (ii) и (iii) вытекает, что любой x из $K \cap A$ представим в виде

$$\begin{aligned} x = a\big[b^{m_1} a_1^{v_1} \dots a_s^{v_s} b^{-m_1} b^{-m_1} a_1^{v_1^{-1}} \dots a_s^{v_s^{-1}} b^{m_1}\big] \dots \big[b^{m_k} (a_1^*)^{w_1} \\ \dots (a_l^*)^{w_l} b^{-m_k} b^{m_k} (a_1^*)^{w_l^{-1}} \dots (a_l^*)^{w_l^{-1}} b^{-m_k}\big], \end{aligned}$$

где $a, a_i, a_j^* \in A_1$; $v_i, w_j \in \langle b\rangle$; $a_i^{v_i}, a_i^{v_i^{-1}}, (a_j^*)^{w_j}, (a_j^*)^{w_j^{-1}} \in A_1$, $i = 1, \dots, s$, $j = 1, \dots, l$; $0 < m_t \le \frac{q-1}{2}$, $t = 1, \dots, k$ и $m_i < m_j$ при $i < j$.

Значит, $|K \cap A| \le |A_1|^{(\frac{q-1}{2}+1)}$. Очевидно, что $|A| = |A_1|^q$. Нетрудно видеть, что $\frac{q-1}{2} + 1 < q$. Таким образом, $|K \cap A| < |A|$, и утверждение (iv) доказано.

Далее, из (iv) следует, что $K \ne G$, и лемма 2.2 доказана.

Лемма 2.3. *Пусть $G = A \leftthreetimes \langle c\rangle$ — конечная группа, где A — элементарная абелева p-группа, $|c| = r^m$, $p \ne r$, p, r простые. Допустим, что c действует неприводимо на A. Тогда справедливо одно из следующих утверждений:*

(1) c^r действует неприводимо на A;

(2) c^r действует тождественно на A;

(3) $A = A_1 \times \dots \times A_r$, где A_1 — минимальная c^r-инвариантная подгруппа группы A и $A_{i+1} := A_i^c$, $i = 2, \dots, r$.

Доказательство. Допустим, что c^r действует приводимо и нетождественно на A. Покажем, что тогда G удовлетворяет утверждению (3) леммы 2.3.

Пусть A_1 — минимальная c^r-инвариантная подгруппа из A. В силу исходного предположения имеем $A_1 \neq A$. Дальнейший анализ разбивается на ряд этапов.

(i) $C_A(c^r) = 1$.

Допустим противное, т. е. пусть $C_A(c^r) \neq 1$. Так как $C_A(c^r)$ — c-инвариантная подгруппа, ввиду неприводимого действия элемента c на A имеем $A = C_A(c^r)$, что противоречит предположению нетождественности действия c^r на A.

(ii) $A = A_1 \times \dots \times A_s$, где $1 < s \leq r$ и $(A_i)^c = A_{i+1}$, $i = 1, \dots, s-1$.

Справедливость данного утверждения вытекает из того, что A — минимальная c-инвариантная подгруппа, $A_1 \neq A$ и A_1 — минимальная c^r-инвариантная подгруппа.

(iii) Пусть Ω — множество минимальных c^r-инвариантных подгрупп из A. Тогда

(1) для любых X, Y из Ω либо $X = Y$, либо $X \cap Y = 1$;

(2) $A = \bigcup X$, где $X \in \Omega$;

(3) для любого X из Ω $|X| = |A_1| = p^l$ для некоторого l.

Утверждение (1) — очевидное свойство минимальных c^r-инвариантных подгрупп из A.

Докажем (2) и (3). Заметим, что $A_1 \in \Omega$. Пусть $x \in A_1 \setminus \{1\}$ и $y \in A$. Так как c действует неприводимо на A, по лемме 2.1 $A = \{\psi(x) \mid \psi \in R\}$, где R — подкольцо $\operatorname{End} A$, порожденное эндоморфизмом φ_c, который определен следующим образом: $\varphi_c(z) = c^{-1}zc$, $z \in A$. Отсюда следует существование такого φ из R, что $y = \varphi(x)$. Значит, $y \in \varphi(A_1)$. Поскольку $(\varphi(A_1))^{c^r} = \varphi(A_1^{c^r})$, нетрудно видеть, что $\varphi(A_1) \in \Omega$. В силу леммы 2.1 R — поле и, значит, φ — биекция, откуда $|A_1| = |\varphi(A_1)|$.

Итак, для любого $y \in A$ существует $M \in \Omega$ такая, что $y \in M$ и $|M| = |A_1|$. Таким образом, (2) доказано, откуда в силу (1) получаем, что для любого $M \in \Omega$ справедливо $|M| = |A_1|$, и, следовательно, (3) также доказано.

(iv) G удовлетворяет утверждению (3).

Из (ii) и (iii) вытекает, что $|A| = p^{ls}$. Так как по (iii) Ω образует расщепление A и $|X| = p^l$ для любого $X \in \Omega$, то $|\Omega| = \frac{p^{ls}-1}{p^l-1} = (p^l)^{s-1} + \dots + p^l + 1$.

Далее, Ω разбивается на орбиты под действием c, причем, как нетрудно видеть, порядок каждой орбиты равен r. Значит, $|\Omega| \equiv 0 (\operatorname{mod} r)$.

Таким образом, $(p^l)^{s-1} + \dots + p^l + 1 = wr$ для некоторого натурального w.

Из (i) следует, что $C_{A_1}(c^r) = 1$. Значит, $A_1 \setminus \{1\}$ под действием c^r разбивается на орбиты так, что порядок каждой орбиты делится на r. Так как $|A_1| = p^l$, то $p^l = 1 + vr$ для некоторого натурального v, откуда $(1+vr)^{s-1} + \dots + (1+vr) + 1 = wr$. Раскрывая скобки, получаем $(1 + v_1 r) + \dots + (1 + v_{s-1} r) + 1 = wr$ для некоторых натуральных $v_1, \dots, v_{s-1}$, тем самым $s = dr$ для некоторого d.

Заметим, что $s \leq r$. Следовательно, $s = r$, и лемма 2.3 доказана.

Из лемм 2.2 и 2.3 вытекает

Следствие 2.4. *Пусть $G = A \leftthreetimes \langle c \rangle$ — конечная неабелева перекрученная группа нечетного порядка, где A — элементарная абелева p-группа, $|c| = r^m$, $p \neq r$, p, r простые. Допустим, что c действует неприводимо на A.*

Тогда либо c^r также действует неприводимо на A, либо c^r действует тождественно на A.

3. Нильпотентность коммутанта конечной перекрученной группы

В данном разделе излагается доказательство теоремы 1. Везде далее под G понимается минимальный контрпример к теореме 1, A — минимальная нормальная подгруппа из G и $\overline{G} := G/A$.

Изучение контрпримера G разбивается на ряд этапов.

(1) A — единственная минимальная нормальная подгруппа из G.

Допустим, что G имеет две различные минимальные нормальные подгруппы A и B. Тогда $A \cap B = 1$. Следовательно, G изоморфно вкладывается в группу $G^* := G/A \times G/B$. По лемме 1.1 G/A и G/B — перекрученные группы, откуда в силу минимальности G получаем, что $(G/A)'$ и $(G/B)'$ нильпотентны. Тогда $(G^*)'$ нильпотентен, а значит, G' нильпотентен, что противоречит выбору G.

(2) G имеет нечетный порядок.

Допустим противное, т. е. пусть G имеет четный порядок. Тогда по лемме 1.3 $G = O_2(G) \times O(G)$, где $O_2(G)$ циклическая. В силу (1) получаем, что $O(G) = 1$, откуда G абелева, что противоречит выбору контрпримера.

(3) G разрешима.

Следует из (2) и теоремы Фейта — Томпсона [7].

(4) A — элементарная абелева p-группа для некоторого простого p.

Следует из (3) и того, что A — минимальная нормальная подгруппа в G.

(5) Пусть $\overline{N} := (\overline{G})'$. Тогда группа $\overline{N}$ нильпотентна и не является p-группой.

Из минимальности G следует нильпотентность $\overline{N}$.

Покажем, что $\overline{N}$ не является p-группой. Допустим противное, т. е. что $\overline{N}$ — p-группа. Тогда полный прообраз N группы $\overline{N}$ является p-группой. Так как G' содержится в N, получаем, что G' — p-группа, откуда G' нильпотентен, что противоречит выбору контрпримера G.

(6) $G = A \leftthreetimes H$ для некоторой неабелевой подгруппы H из G и $C_G(A) = A$.

Из (5) следует, что $\overline{N}$ содержит минимальную нормальную в $\overline{G}$ элементарную абелеву q-подгруппу $\overline{B}$, где q — простое число, отличное от p.

Пусть T — полный прообраз $\overline{B}$ в группе G. Тогда $T = A \leftthreetimes B$, где B — силовская q-подгруппа группы T и B — элементарная абелева группа.

Покажем, что $Z(T) = 1$. Допустим, что $Z(T) \neq 1$. Так как $T \lhd G$, то $Z(T) \lhd G$. Тогда ввиду (1) $A \leq Z(T)$, тем самым $T = A \times B$. Следовательно, $B \lhd G$, что противоречит (1). Итак, $Z(T) = 1$. Из нормальности T в G и того, что B — силовская q-подгруппа группы T, по лемме Фраттини имеем $G = N_G(B)T = N_G(B)A$. Так как $N_G(B) \cap A \leq Z(T)$, то $N_G(B) \cap A = 1$.

Таким образом, $G = A \leftthreetimes H$, где $H := N_G(B)$. В силу минимальности контрпримера G подгруппа H неабелева.

Так как $C_H(A) \lhd G$ и $A \cap C_H(A) = 1$, ввиду (1) имеем $C_H(A) = 1$. Следовательно, $C_G(A) = A$, и (6) доказано.

(7) $O_p(G) = A$.

Ясно, что $A \subseteq O_p(G)$. Имеем $Z(O_p(G)) \neq 1$. Так как $Z(O_p(G)) \lhd G$, то по (1) $A \leq Z(O_p(G))$. Следовательно, $O_p(G) \leq C_G(A)$, откуда ввиду (6) получаем, что $A = O_p(G)$.

(8) H' — p'-группа.

Допустим, что H' не является p'-группой. Так как H' нильпотентен, существует нормальная в H' p-подгруппа M. Тогда $MA \lhd G$ и MA — p-группа. Значит, $MA \leq O_p(G)$. Так как $A \neq MA$, получаем противоречие с (7).

(9) H — группа Миллера — Морено.

Пусть Y — собственная подгруппа из H и $M := \langle Y, A\rangle$. Понятно, что $A \leq F(M)$, где $F(M)$ — подгруппа Фиттинга группы M. Так как по (6) $C_G(A) = A$ и $F(M)$ нильпотентна, то $F(M)$ — p-группа.

Очевидно, что M — собственная подгруппа из G и, значит, M' нильпотентна, откуда $M' \leq F(M)$. Следовательно, M' — p-группа.

Понятно, что $Y' \leq M'$ и, значит, Y' является p-группой, но в силу (8) Y' — p'-группа. Следовательно, $Y' = 1$, откуда Y абелева. Утверждение (9) доказано.

(10) Для любого x из $Z(H) \setminus \{1\}$ $\quad C_A(x) = 1$.

Пусть существует x из $Z(H)\setminus\{1\}$ такой, что $C_A(x) \neq 1$. Ясно, что $C_A(x) \lhd G$. Значит, согласно (1) $A \leq C_A(x)$. Следовательно, $C_G(A) \neq A$, что противоречит (6).

(11) Любая собственная нормальная p'-подгруппа из H является циклической.

Предположим противное, т. е. что в H имеется собственная нормальная p'-подгруппа T, которая не является циклической. В силу (9) T абелева. Тогда для некоторого простого q из $\pi(T)$, отличного от p, существует нормальная в H нециклическая элементарная абелева q-подгруппа F из T.

Далее анализ ситуации разбивается на ряд этапов.

(11.1) $H = F\langle h\rangle$ для некоторого $h \in H$.

Так как F — нециклическая элементарная абелева q-подгруппа, в силу леммы 1.10 существует x из $F \setminus \{1\}$ такой, что $C_A(x) \neq 1$. Из (10) получаем, что $x \notin Z(H)$. Тогда по (9) существует элемент h из H такой, что $H = F\langle h\rangle$.

(11.2) Существуют элемент f и подгруппа N из F такие, что $C_A(N) \neq 1$ и $F = \langle f\rangle \times N$.

Вытекает из нецикличности F и леммы 1.4.

(11.3) Существует нетривиальная f-инвариантная подгруппа Q из $C_A(N)$ такая, что $Q \lhd AF$ и $\langle Q, f\rangle$ неабелева.

Существование нетривиальной f-инвариантной подгруппы Q следует из того, что $C_A(N) \lhd AF$ и $C_A(N) \neq 1$. Очевидно, что $Q \lhd AF$.

Покажем теперь, что $\langle Q, f\rangle$ неабелева. Допустим противное, т. е. что $\langle Q, f\rangle$ абелева. Тогда $Q \leq C_A(F)$ и $C_A(F) \neq 1$. Так как $F \lhd H$, то $C_A(F) \lhd G$. Значит, по (1) $C_A(F) = A$, откуда $C_G(A) \neq A$, что противоречит (6). Таким образом, $\langle Q, f\rangle$ неабелева, и утверждение (11.3) доказано.

(11.4) Пусть $M := \{x \in F : [Q, x] \neq 1\}$. Тогда

(a) существует x из M такой, что $[Q^h, x] = 1$;

(b) существует y из M^h такой, что $[Q, y] = 1$, где h — элемент из H, удовлетворяющий п. (11.1)

Докажем (a), утверждение (b) доказывается аналогично. Понятно, что $M = F \setminus N$. Допустим противное: для любого $x \in M$ справедливо $[Q^h, x] \neq 1$. Напомним, что $F \lhd H$. Значит, $M^h = \{x \in F : [Q^h, x] \neq 1\}$. Тогда $M \subseteq M^h$, откуда $M^h = M$. Ввиду того, что $N = F \setminus M$, имеем $N^h = N$, тем самым $N \lhd H$.

Если H нильпотентна, то в силу того, что $N \lhd H$, имеем $N \cap Z(H) \neq 1$. Тогда согласно (10) получаем, что $C_A(N) = 1$, что противоречит (11.2).

Таким образом, H ненильпотентна. Тогда ввиду (9) $H = F \leftthreetimes \langle h \rangle$, где F — q-группа, $\langle h \rangle$ — r-группа, q, r — различные простые числа и F — минимальная нормальная в H подгруппа. Так как N — подгруппа из F и N нормальна в H, выводим, что $F = N$; противоречие с (11.2). Полученное противоречие доказывает (11.4).

(11.5) Существует подгруппа T из G такая, что $T = R \times R$, где R — некоторая неабелева подгруппа из G.

Рассмотрим $T := \langle Q, Q^h, x, y \rangle$, где x, y удовлетворяют соответственно утверждениям (a) и (b) из (11.4). Ясно, что $\langle x, y \rangle = \langle x \rangle \times \langle y \rangle$.

Докажем, что $Q \cap Q^h = 1$. Допустим противное, т. е. что $Q \cap Q^h \neq 1$. Так как Q, Q^h — минимальные f-инвариантные подгруппы из A, то $Q^h = Q$. Следовательно, $Q \lhd G$, и, значит, по (1) $A = Q = C_A(N)$, что противоречит (6).

Таким образом, $T = (Q \times Q^h) \leftthreetimes (\langle x \rangle \times \langle y \rangle) = (Q \leftthreetimes \langle x \rangle) \times (Q^h \leftthreetimes \langle y \rangle)$, $Q\langle x \rangle$ и $Q^h \langle y \rangle$ неабелевы.

Заметим, что x может быть выбран так, что $x = f x_1$ для некоторого $x_1 \in N$. Тем самым $Q\langle x \rangle \cong Q\langle f \rangle$, так как $[x_1, Q] = 1$.

Аналогично $y = f^h (y_1)^h$, где $y_1 \in N$. Таким образом, $Q^h \langle y \rangle \cong Q\langle f \rangle$, так как $[(y_1)^h, Q^h] = 1$. Значит, полагая $R := Q\langle x \rangle$, получаем требуемое.

Из леммы 1.5 получаем, что T не является перекрученной. Поэтому по лемме 1.1 G не является перекрученной и получаем противоречие с выбором контрпримера, которое доказывает (11).

(12) H не является нильпотентной.

Допустим, что H нильпотентна. Так как по (9) H — группа Миллера — Морено, то в силу (8) H — q-группа, где $q \neq p$. Из лемм 1.1, 1.2, 1.6 следует, что $\Omega_1(H)$ — элементарная абелева q-группа. Тогда по (11) $\Omega_1(H)$ циклическая. Применяя лемму 1.7, получаем, что H циклическая; противоречие с (9), и (12) доказано.

(13) $H = \langle b \rangle \leftthreetimes \langle c \rangle$, где $|b| = q$, $|c| = r^m$, $q \neq p$, q, r — различные простые числа и $[b, c^r] = 1$.

В силу (9) и (12) имеем $H = B \leftthreetimes \langle c \rangle$, где B — элементарная абелева q-группа, $|c| = r^m$, q, r — различные простые числа и $[B, c^r] = 1$. Ввиду (8) B — p'-группа. Тогда по (11) B циклическая, и (13) доказано.

(14) $|c| = r$.

Допустим противное, т. е. что $c^r \neq 1$. Понятно, что $c^r \in Z(H)$. Значит, в силу (10) получаем $C_A(c^r) = 1$, откуда вытекает, что $p \neq r$.

Далее анализ разбивается на ряд этапов.

(14.1) Элемент c^r действует неприводимо на A.

Пусть Q — минимальная c^r-инвариантная подгруппа из A. Тогда Q^b также является минимальной c^r-инвариантной подгруппой из A. Из следствия 2.4 следует, что Q, Q^b c-инвариантны, т. е. $(Q^b)^c = Q^b$.

С другой стороны, $(Q^b)^c = Q^{b^t}$, где $b^c = b^t$, причем $t^r \equiv 1 (\operatorname{mod} q)$ и $t \not\equiv 1 (\operatorname{mod} q)$. Тогда $Q^{b^{t-1}} = Q$ и, значит, $Q^b = Q$. Таким образом, $Q \lhd G$, и по (1) имеем $Q = A$.

(14.2) $C_A(b) \neq 1$.

Пусть R — подкольцо $\mathrm{End}\,A$, порожденное эндоморфизмом φ_c, который определен следующим образом: $\varphi_c(a) = c^{-1}ac$, $a \in A$. Ввиду (14.1) c и c^r действуют неприводимо на A. Тогда по лемме 2.1 R — поле, причем R порождается φ_c^r. Значит, $\varphi_c = \sum\limits_i \alpha_i \varphi_c^{ri}$ для некоторых $0 \le \alpha_i < p$.

Пусть $a \in A \setminus \{1\}$. Тогда $\varphi_c(a^b) = [\varphi_c(a)]^{b^t}$, где $b^c = b^t$, причем $t^r \equiv 1 (\mathrm{mod}\, q)$ и $t \not\equiv 1 (\mathrm{mod}\, q)$. С другой стороны,

$$\varphi_c(a^b) = \Big(\sum_i \alpha_i \varphi_c^{ri}\Big)(a^b) = \Big[\Big(\sum_i \alpha_i \varphi_c^{ri}\Big)(a)\Big]^b = [\varphi_c(a)]^b,$$

так как $[b, c^r] = 1$. Таким образом, $[\varphi_c(a)]^{b^t} = [\varphi_c(a)]^b$, откуда $[\varphi_c(a)]^b = \varphi_c(a)$. Значит, $C_A(b) \neq 1$, и (14.2) доказано.

Далее, так как $C_A(b) \lhd G$, согласно (1) $A = C_A(b)$ и, значит, $C_G(A) \neq A$, что противоречит (6). Полученное противоречие доказывает (14).

(15) Существует элемент e из $A \setminus \{1\}$ такой, что $[e, c] = 1$.

Данное утверждение вытекает из леммы 1.8, если $p \neq r$. В случае $p = r$ оно вытекает из того, что A является нормальной подгруппой в $A\langle c\rangle$.

(16) Пусть B — подкольцо $\mathrm{End}\,A$, порожденное эндоморфизмом φ_b, определенным следующим образом: $\varphi_b(a) = b^{-1}ab$, $a \in A$. Тогда $A = \{\psi(e) \mid \psi \in B\}$, где e — элемент, существование которого утверждается в (15).

Пусть $Q = \{\psi(e) \mid \psi \in B\}$. Множество Q является подгруппой в A, так как для любых φ, ψ из B по определению сложения в $\mathrm{End}\,A$ будет $\varphi(e) + \psi(e) = (\varphi + \psi)(e) \in Q$. Подгруппа Q b-инвариантна, так как $(\psi(e))^b = (\varphi_b\psi)(e) \in Q$ для любого эндоморфизма ψ из B. Подгруппа Q c-инвариантна, поскольку $(\psi(e))^c = \psi^*(e)$ для любого эндоморфизма ψ из B, где $\psi^* \in B$ и ψ^* определяется следующим образом: если $\psi = \sum\limits_i \alpha_i \varphi_b^i$, то $\psi^* = \sum\limits_i \alpha_i \varphi_b^{ti}$, где t такое число, что $b^c = b^t$, $0 \le \alpha_i < p$.

Таким образом, $Q \lhd G$, и по (1) имеем $Q = A$.

(17) Введем на A бинарную операцию $*$, определенную следующим образом: для любых x, y из A полагается $x * y := (\varphi\psi)(e)$, где φ, ψ из B такие, что $x = \varphi(e)$, $y = \psi(e)$. Тогда $R := \langle A, +, *\rangle$ является кольцом, изоморфным B.

Из (16) следует, что операция $*$ определена для любых x, y из A.

Рассмотрим отображение $\tau : B \to R$, определенное следующим образом: $\tau(\psi) := \psi(e)$ для любого ψ из B. Покажем, что τ — изоморфизм между B и R.

Легко проверить справедливость следующих свойств: для любых x, y из B

$$\tau(x + y) = \tau(x) + \tau(y), \quad \tau(x * y) = \tau(x) * \tau(y).$$

Таким образом, τ — гомоморфизм из B в R. Остается показать биективность τ, для чего в силу конечности B и R достаточно показать лишь взаимную однозначность τ или, что эквивалентно, $\mathrm{Ker}\,\tau = 0$.

Из определения B следует, что B — коммутативное кольцо.

Пусть φ из B такой, что $\varphi(e) = 0$. Согласно (16) для любого a из A существует ψ из B такой, что $a = \psi(e)$. Тогда $\varphi(a) = \varphi(\psi(e)) = \psi(\varphi(e)) = \psi(0) = 0$. Значит, $\varphi = 0$ и $\mathrm{Ker}\,\tau = 0$. Утверждение (17) доказано.

(18) Пусть $\tau_c : R \to R$ — отображение, определенное следующим образом: $\tau_c(a) = c^{-1}ac$ для любого a из R. Тогда τ_c — автоморфизм кольца R и $|\tau_c| = r$.

Линейность и биективность τ_c очевидны. Покажем, что $\tau_c(x*y)=\tau_c(x)*\tau_c(y)$ для любых x,y из R.

Пусть $x,y\in R$ и $\varphi,\psi\in B$ такие, что $x=\varphi(e)$, $y=\psi(e)$. Так как B порождается φ_b, то φ и ψ можно представить в следующем виде: $\varphi=\sum\limits_i\alpha_i\varphi_b^i$, $\psi=\sum_j\beta_j\varphi_b^j$ для некоторых $0\le\alpha_i,\beta_j<p$. Так как $c^{-1}b^ic=b^{it}$ для некоторого t и $c^{-1}ec=e$, то $\tau_c(\varphi_b^i(e))=\varphi_b^{it}(e)$. Тогда

$$\begin{aligned}\tau_c(x*y)&=\tau_c\Big(\Big(\sum_i\alpha_i\varphi_b^i\Big)\Big(\sum_j\beta_j\varphi_b^j\Big)(e)\Big)=\tau_c\Big(\Big(\sum_i\sum_j\alpha_i\beta_j\varphi_b^{i+j}\Big)(e)\Big)\\&=\sum_i\sum_j\alpha_i\beta_j\tau_c\big(\varphi_b^{i+j}(e)\big)=\sum_i\sum_j\alpha_i\beta_j\varphi_b^{(i+j)t}(e)=\sum_i\sum_j\alpha_i\beta_j\big(\varphi_b^{it}(e)*\varphi_b^{jt}(e)\big)\\&=\sum_i\sum_j\alpha_i\beta_j\big(\tau_c\big(\varphi_b^i(e)\big)*\tau_c\big(\varphi_b^j(e)\big)\big)=\Big(\sum_i\alpha_i\tau_c\big(\varphi_b^i(e)\big)\Big)*\Big(\sum_j\beta_j\tau_c\big(\varphi_b^j(e)\big)\Big)\\&=\tau_c\Big(\sum_i\alpha_i\varphi_b^i(e)\Big)*\tau_c\Big(\sum_j\beta_j\tau_c\varphi_b^j(e)\Big)=\tau_c(x)*\tau_c(y)\end{aligned}$$

и, следовательно, τ_c — автоморфизм кольца R.

В силу (14) $|\tau_c|=r$, и (18) доказано.

(19) R — конечное коммутативное полупростое кольцо.

Из определения B следует, что B — конечное коммутативное кольцо. Тогда по (18) получаем, что и R является таковым.

Покажем, что R — полупростое кольцо, т. е. нильпотентный радикал N кольца R равен 0. Предположим противное: $N\neq 0$. Покажем, что N — нормальная подгруппа из G. Так как N — подкольцо R, то N является подгруппой в A. Так как N — идеал, то $N^b=\varphi_b(e)*N\subseteq N$ и, значит, N b-инвариантна.

В силу единственности нильпотентного радикала и того, что по (18) элемент c индуцирует автоморфизм τ_c кольца R, заключаем, что N c-инвариантна. Таким образом, $N\lhd G$, откуда ввиду (1) $N=A$. Значит, $R=N$, т. е. для любого x из R существует натуральное n такое, что $x^n=0$. Но, с другой стороны, $1(e)\in R$ и $(1(e))^n\neq 0$ для любого натурального n. Получили противоречие, которое доказывает (19).

(20) R — поле.

Допустим противное, т. е. что R не является полем.

Пусть $\{R_1,\dots,R_s\}$ — множество минимальных идеалов из R. По (19) и лемме 1.9 $R=R_1\oplus\dots\oplus R_s$. Так как R — коммутативное кольцо, то R_i — поле.

В силу предположения о том, что R не является полем, имеем $s>1$. По (18) $|\tau_c|=r$. Рассмотрим $\{\tau_c^i(R_1)\mid i=1,\dots,r\}$. Ясно, что $\tau_c^i(R_1)\in\{R_1,\dots,R_s\}$ для любого i. Рассмотрим $Q:=\langle\tau_c^i(R_1)\mid i=1,\dots,r\rangle\le A$. Очевидно, что Q c-инвариантна. Так как R_i — идеал для любого i, то $\varphi_b(e)*R_i\subseteq R_i$ и тем самым Q b-инвариантна. Таким образом, $Q\lhd G$, откуда в силу (1) $Q=A$.

Так как $s>1$, то $R_1\neq\tau_c(R_1)$.

Множество $A_i:=\tau_c^i(R_1)$ — подгруппа в A. Таким образом, $A=A_1\times\dots\times A_r$, где $A_i^c=A_{i+1}$ и $A_r^c=A_1$, $i=1,\dots,r-1$. По лемме 2.2 $(A_1\times\dots\times A_r)\leftthreetimes\langle c\rangle$ не является перекрученной группой, так что по лемме 1.1 G не является перекрученной. Получили противоречие с выбором контрпримера G, которое доказывает (20).

(21) G не является перекрученной.

В силу (20) R — поле, которое является расширением своего простого подполя F.

Далее, ввиду [8, с. 232] существует нормальный базис $W := \{w_i \mid i = 1, \dots, m(A)\}$ расширения R над F (определение нормального базиса расширения R над F см. в [8, с. 232]). Так как по (19) $|\tau_c| = r$, то $\tau_c(w_i) \neq w_i$ для некоторого w_i из W.

Пусть $v_j := \tau_c^j(w_i)$, $j = 1, \dots, r$. Имеем $\{v_j\} \subseteq W$ и, значит, $\langle v_j \mid j = 1, \dots, r\rangle = \langle v_1\rangle \times \dots \times \langle v_r\rangle$. Таким образом, в G имеется подгруппа $T := (\langle v_1\rangle \times \dots \times \langle v_r\rangle) \leftthreetimes \langle c\rangle$, где $v_i^c = v_{i+1}$ и $v_r^c = v_1$. По лемме 2.2 T не является перекрученной. Следовательно, по лемме 1.1 G не является перекрученной, и (21) доказано.

В силу (21) получаем противоречие с выбором контрпримера G, которое доказывает теорему 1.

ЛИТЕРАТУРА

1. *Мыльников А. Л.* Конечные перекрученные группы // Математические системы. Красноярск: Краснояр. гос. аграр. ун-т., 2005. Вып. 3. С. 53–58.
2. *Aschbacher M.* Near subgroups of finite groups // J. Group Theory. 1998. V. 1, N 2. P. 113–129.
3. *Мыльников А. Л.* Конечные минимальные неперекрученные группы // Вестн. Красноярск. гос. ун-та. 2005. Т. 1. С. 71–76.
4. *Судзуки М.* Строение группы и строение структуры ее подгрупп. М.: Изд-во иностр. лит., 1960.
5. *Gorenstein D.* Finite groups. New York: Harper and Row, 1968.
6. *Холл М.* Теория групп. М.: Изд-во иностр. лит., 1962.
7. *Feit W., Tompson J.* Solvability of groups of odd order // Pacif. J. Math. 1963. V. 13, N 3. P. 775–1029.
8. *Ван дер Варден Б. Л.* Алгебра. М.: Наука, 1979.

Статья поступила 16 июня 2005 г.

Мыльников Андрей Леонидович
Красноярский гос. университет, факультет математики и информатики,
пр. Свободный, 79, Красноярск 660041
mylnand@yandex.ru