УДК 512.542

Д. В. Грицук
канд. физ.-мат. наук, доц., зав. каф. прикладной математики и информатики
Брестского государственного университета имени А. С. Пушкина
e-mail: dmitry.gritsuk@gmail.com

ВЛИЯНИЕ СТРОЕНИЯ ХОЛЛОВОЙ ПОДГРУППЫ КОНЕЧНОЙ π-РАЗРЕШИМОЙ ГРУППЫ НА ПРОИЗВОДНУЮ π-ДЛИНЫ

Пусть G – π-разрешимая группа. Тогда она обладает субнормальным рядом $1 = G_0 \subset G_1 \subset \dots \subset G_{m-1} \subset G_m = G$, факторы G_{i+1}/G_i которого являются либо π'-группами, либо абелевыми π-группами. Наименьшее число абелевых π-факторов среди всех таких субнормальных рядов π-разрешимой группы G называется производной π-длиной π-разрешимой группы. Приводится обзор оценок производной π-длины конечной π-разрешимой группы с заданной π-холловой подгруппой.

GRITSUK D. V.

INFLUENCE OF THE STRUCTURE OF THE HALL SUBGROUP OF THE FINITE π-SOLVABLE GROUP ON THE DERIVATIVE π-LENGTH

Let G is a π-solvable group. Then it has a subnormal series рядом $1 = G_0 \subset G_1 \subset \dots \subset G_{m-1} \subset G_m = G$ whose factors G_{i+1}/G_i are either π'-groups or abelian π-groups. The smallest number of Abelian π-factors among all such subnormal series of a π-solvable group G is called the derivative of the π-length of the π-solvable group. This article provides an overview of estimates for the derivative of the π-length of a finite π-solvable group with a given π-Hall subgroup.

Введение

Рассматриваются только конечные группы. Все используемые понятия и обозначения соответствуют [1], [2].

Пусть π – некоторое подмножество множества простых чисел $\mathbb{P}$. Дополнение к π во множестве $\mathbb{P}$ обозначается через π'. Символом π обозначается также функция, определенная на множестве всех натуральных чисел $\mathbb{N}$ следующим образом: $\pi(a)$ – множество простых чисел, делящих натуральное число a. Для группы G и ее подгруппы H считаем, что $\pi(G) = \pi(|G|)$ и $\pi(G:H) = \pi(|G:H|)$ Зафиксируем множество простых чисел π. Если $\pi(m) \subseteq \pi$, то натуральное число m называется π-числом. Группа G называется π-группой, если $\pi(G) \subseteq \pi$, и π'-группой, если $\pi(G) \subseteq \pi'$. В этом случае $\pi(G) \cap \pi' = \emptyset$.

Напомним, что субнормальным рядом группы G называется цепочка подгрупп

$$1 = G_0 \subset G_1 \subset \dots \subset G_{m-1} \subset G_m = G, \tag{1}$$

такая, что G_i нормальна в G_{i+1} для любого i. Фактор-группы G_{i+1}/G_i называются факторами субнормального ряда (1).

Группа называется π-разрешимой, если она обладает субнормальным рядом (1), факторы которого являются либо разрешимыми π-группами, либо π'-группами.

Пусть G – π-разрешимая группа. Тогда она обладает субнормальным рядом (1), факторы которого являются либо π'-группами, либо абелевыми π-группами. Наименьшее число абелевых π-факторов среди таких субнормальных рядов группы G называется производной π-длиной π-разрешимой группы G и обозначается через $l_\pi^a(G)$. Если $\pi(G) = \pi$, то значение $l_\pi^a(G)$ совпадает со значением производной длины группы G. Данное понятие было предложено в 2006 г. В. С. Монаховым [3].

Начальные свойства производной π-длиной π-разрешимой группы были получены Д. В. Грицуком, В. С. Монаховым и О. А. Шпырко в работе [4]. В частности, в данной работе доказано, что

$$l_\pi(G) \le l_\pi^n(G) \le l_\pi^a(G),$$

где $l_\pi(G)$ и $l_\pi^n(G)$ – π-длина и нильпотентной π-длины π-разрешимой группы G соответственно.

В данной статье приводится обзор оценок производной π-длины конечной π-разрешимой группы G в зависимости от строения ее π-холловой подгруппы.

Производная π-длина π-разрешимой группы с заданной π-холловой подгруппой

Первые исследования производной π-длины в зависимости от строения π-холловой подгруппы проведены в работе [4]. Как обычно, X' и $Z(X)$ – коммутант и центр группы X соответственно.

Теорема 1 [4]. *Пусть G – π-разрешимая группа, G_π – ее π-холлова подгруппа.*

1. Если G_π абелева, то $l_\pi^a(G) \le 1$.

2. Если $(G_\pi)' \subseteq Z(G_\pi)$, то $l_\pi^a(G) \le 3$.

Напомним, что группой Шмидта называют ненильпотентную группу, в которой все собственные подгруппы нильпотентны. Свойства групп Шмидта перечислены, например, в [2, III.5]. Группа называется дедекиндовой, если все ее подгруппы нормальны.

Следствие 1.1. *Если в π-разрешимой группе G_π-холлова подгруппа дедекиндова, то $l_\pi(G) \le 1$ и $l_\pi^a(G) \le 2$.*

Следствие 1.2. *Если в π-разрешимой группе G π-холлова подгруппа является группой Шмидта, то $l_\pi^a(G) \le 3$.*

Напомним, что метабелевой называют группу, у которой коммутант абелев.

Теорема 2 [4]. *Пусть G – π-разрешимая группа с метабелевой π-холловой подгруппой. Если $2 \notin \pi$, то $l_\pi^a(G) \le 3$.*

В работе [5] исследована производная π-длина конечной π-разрешимой группы со сверхразрешимой π-холловой подгруппой. Доказана следующая теорема.

Теорема 3 [5]. *Если G – π-разрешимая группа, у которой коммутант π-холловой подгруппы нильпотентен, то $l_\pi^a(G) \le 1 + max_{r\in\pi} l_r^a(G)$.*

Дополнением к подгруппе H в группе G называется такая подгруппа K, что $G = HK$ и $H \cap K = 1$. Ю. М. Горчаков [6] показал, что дополняемость всех подгрупп равносильна дополняемости подгрупп простых порядков.

Группа, у которой все подгруппы дополняемы, называется вполне факторизуемой. В 1937 г. Ф. Холл [7] установил, что конечные группы, в которых дополняемы все подгруппы, исчерпываются сверхразрешимыми группами с элементарными абелевыми силовскими подгруппами.

Следствие 3.1. *Если G – π-разрешимая группа, π-холлова подгруппа которой вполне факторизуема, то $l_\pi^a(G) \le 2$.*

Следствие 3.2. *Если G – π-разрешимая группа со сверхразрешимой π-холловой подгруппой, то $l_\pi^a(G) \le 1 + max_{r\in\pi} l_r^a(G)$.*

Следствие 3.3. *Если G – π-разрешимая группа, у которой π-холлова подгруппа является группой Миллера – Морено, то $l_\pi^a(G) \le 2$.*

В 2014 г. получены оценки производной π-длины $l_\pi^a(G)$ группы G в зависимости от строения подгруппы G_π или M, где M – максимальная подгруппа из G_π [8].

Теорема 4 [8]. *Пусть G – π-разрешимая группа и G_π – π-холлова подгруппа в G. Тогда справедливы следующие утверждения:*

1) если G_π является группой Миллера – Морено, то $l_\pi^a(G) \le 2$;

2) если G_π является группой Шмидта, то $l_\pi^a(G) \leq 3$.

Теорема 5 [8]. *Пусть G – π-разрешимая группа в G, G_π – π-холлова подгруппа и M – максимальная подгруппа в G_π. Тогда справедливы следующие утверждения:*

1) если подгруппа M абелева, то $l_\pi^a(G) \leq 3$;

2) если подгруппа M абелева и холлова, то $l_\pi^a(G) \leq 2$;

3) если подгруппа M нильпотентна, то

$$l_\pi^a(G) \leq max_{r\in\pi} d(G_r) \cdot \left(1 + max_{r\in\pi} l_r(G)\right);$$

4) если подгруппа M нильпотентна и холлова, то

$$l_\pi^a(G) \leq 1 + max_{r\in\pi(M)} l_r(G) \cdot max_{r\in\pi} d(G_r).$$

Теорема 6 [8]. *Пусть G – π-разрешимая группа, G_π – π-холлова подгруппа и M – максимальная подгруппа из G_π. Тогда справедливы следующие утверждения:*

1) если M – группа Миллера – Морено, то $l_\pi^a(G) \leq 4$; в частности, если M холлова, то $l_\pi^a(G) \leq 3$;

2) если M – группа Шмидта, то $l_\pi^a(G) \leq 5$; в частности, если M холлова, то $l_\pi^a(G) \leq 4$.

В работе [9] исследовано влияние 2-максимальной подгруппы π-холловой подгруппы π-разрешимой группы на оценки производной π-длины.

Теорема 7 [9]. *Пусть G – π-разрешимая группа, G_π – π-холлова подгруппа и M – 2-максимальная подгруппа в G_π. Справедливы следующие утверждения.*

1. Если подгруппа M абелева, то

$$l_\pi^n(G) \leq 3 \text{ и } l_\pi^a(G) \leq 4.$$

2. Если подгруппа M нильпотентна, то

$$l_\pi^n(G) \leq 1 + max_{r\in\pi}\, l_r\,(G) \text{ и } l_\pi^a(G) \leq max_{r\in\pi}\, d\,(G_r)\left(1 + max_{r\in\pi}\, l_r\,(G)\right).$$

Напомним, что число n свободно от m-х степеней, если p^m не делит n для всех простых p. При $m = 2$ говорят, что n свободно от квадратов, при $m = 3$ – от кубов. В работе [10] исследовались оценки производной π-длины π-разрешимой группы, у которой порядок π-холловой подгруппы свободен от n-ых степеней.

Теорема 8 [10]. *Пусть G – π-разрешимая группа.*

1) Если порядок π-холловой подгруппы свободен от кубов, то справедливы следующие утверждения:

a) если $2 \notin \pi$, то $l_\pi^a(G) \leq 2$;

b) если $2 \in \pi$, то $l_\pi^a(G) \leq 3$.

2) Если порядок π-холловой подгруппы свободен от квадратов, то G разрешима и $l_\pi^a(G) \leq 2$.

Теорема 9. *Пусть G – π-разрешимая группа, а G_π – π-холлова подгруппа.*

1. Если G_π изоморфна симметрической группе S_3, то $l_\pi^a(G) \leq 2$.

2. Если G_π изоморфна знакопеременной группе A_4, то $l_\pi^a(G) \leq 2$.

3. Если G_π изоморфна симметрической группе S_4, то $l_\pi^a(G) \leq 3$.

<u>Доказательство.</u> Очевидно, что фактор-группа $G_\pi N/N$ является π-холловой подгруппой фактор-группы G/N. По теореме 2.4 [1]

$$G_\pi N/N \cong G_\pi/(G_\pi \cap N).$$

Если $F(G) = 1$, то $O_{\pi'}(G) \neq 1$. По индукции $l_\pi\,(G/O_{\pi'}(G)) \leq 1$. Так как

$$l_\pi\,(G/O_{\pi'}(G)) = l_\pi\,(G) \leq 1,$$

то $l_\pi(G) \leq 1$. Поэтому можно считать, что $F(G) \neq 1$.

Пусть $K = G_\pi \cap F(G)$. Так как $K \subseteq F(G)$, то K является нильпотентной группой. Тогда возможны шесть случаев.

Случай, когда $G_\pi \cong S_3$ и $K = 1$. Тогда

$$G_\pi F(G)/F(G) \cong S_3,$$

и по индукции $l_\pi^a(G/F(G)) \leq 1$. Так $F(G)$ является π'-группой, то $l_\pi^a(G/F(G)) = l_\pi^a(G)$ и $l_\pi(G) \leq 1$. Случаи, когда $K = 1$, а π-холлова подгруппа G_π изоморфна либо A_4, либо S_4 доказываются аналогично.

Если $G_\pi \cong S_3$ и $K \cong Z_3$, то $K = O_3(G) = G_3$. Причем G_3 циклическая, поэтому $C_G(K) = K$. По теореме 2.8 [1] фактор-группа G/K изоморфна подгруппе группы автоморфизмов K, являющейся циклической группой порядка 2. Значит, G является $\{2,3\}$-подгруппой и $G = G_\pi$. Следовательно, $l_\pi(G) = 1$.

Если $G_\pi \cong A_4$ и $K = E_4$, то $K = O_2(G) = E_4$ и $C_G(K) = K$. Так как фактор-группа G/K изоморфна подгруппе автоморфизмов группы $GL(2,2)$, то $G/K \cong Z_3$. Из того, что $G/K \cong Z_3$ получаем, что $G \cong A_4$. Значит, $l_\pi(G) = 1$.

Если $G_\pi \cong S_4$ и $K = E_4$, то $K = O_2(G) = E_4$. Так как фактор-группа G/K изоморфна подгруппе группы $GL(2,2)$, то $G/K \cong S_3$. Из того, что $G/K \cong S_3$, получаем, что $G \cong S_4$. Поэтому $l_\pi(G) = 1$.

Для $l_\pi^a(G) = 1$ известно, что

$$d(G_\pi) \leq l_\pi^a(G) \leq l_\pi(G) \cdot d(G_\pi).$$

Поэтому, если $G_\pi \cong S_3$ или $G_\pi \cong A_4$, то $l_\pi^a(G) \leq 2$. Если $G_\pi \cong S_4$, то $l_\pi^a(G) \leq 3$.

Теорема доказана.

Напомним, что t-группой называют группу, в которой каждая субнормальная подгруппа нормальна. Строение разрешимых t-групп описал В. Гашюц [11]. В частности, разрешимая t-группа сверхразрешима. $\mathfrak{N}$ – класс всех нильпотентных групп, $G^{\mathfrak{N}}$ – $\mathfrak{N}$-корадикал группы G, т. е. пересечение всех нормальных подгрупп группы G, фактор-группы по которым принадлежат $\mathfrak{N}$. Известно, что если G является t-группой, то $G^{\mathfrak{N}}$ – абелева холлова подгруппа нечетного порядка, все подгруппы из $G^{\mathfrak{N}}$ – нормальны в G, $G^{\mathfrak{N}}$ – дедекиндова.

Теорема 10. *Если π-холлова подгруппа π-разрешимой группы является t-группой, то $l_\pi^a(G) \leq 3$.*

Доказательство. Так как G_π является разрешимой t-группой, то $G_\pi = [A]B$, где $A = G_\pi^{\mathfrak{N}}$ – абелева холлова подгруппа нечетного порядка, B – дедекиндова группа.

Если $A = 1$, то G_π дедекиндова и, следовательно, $l_\pi^a(G) \leq 2$.

Рассмотрим случай, когда $A \neq 1$. Так как фактор-группа G/N является t-группой для произвольной неединичной нормальной подгруппы группы G [11], то для доказательства теоремы можем воспользоваться индукцией по порядку группы G. Поэтому для $l_\pi(G)$ можно считать, что

$$\Phi(G) = O_{\pi'}(G) = 1,$$

а подгруппа Фиттинга $F(G) = O_\pi(G)$ является единственной минимальной нормальной p-подгруппой в G и $C_G(F(G)) = F(G)$. Так как $G_\pi^{\mathfrak{N}}$ – абелева холлова подгруппа, то $F(G) = G_\pi^{\mathfrak{N}}$. Из того, что π-холлова подгруппа группы $G/F(G)$ является дедекиндовой, получаем, что $l_\pi(G/F(G)) \leq 1$. Так как $F(G) = O_\pi(G)$, то

$$l_\pi(G/F(G)) = l_\pi(G) - 1.$$

Поэтому $l_{\pi}(G) \leq 2$.

Для $l_{\pi}^{a}(G/F(G))$ можно считать, что в G только одна минимальная нормальная подгруппа, $O_{\pi'}(G) = 1$,

$$F(G) = O_p(G) = F(O_{\pi}(G))$$

для некоторого простого $p \in \pi$ и $C_G(F(G)) \subseteq F(G)$. Так как $G_{\pi}^{\mathfrak{N}}$ – абелева и холлова подгруппа, то $G_{\pi}^{\mathfrak{N}}$=F(G). Так как $G/F(G)$ имеет дедекиндову холлову подгруппу $G_{\pi}/F(G)$, то $l_{\pi}^{a}(G/F(G)) \leq 2$. $F(G) = G_{\pi}^{\mathfrak{N}}$ – абелева холлова подгруппа нечетного порядка, поэтому $d(F(G)) \leq 1$. Следовательно, $l_{\pi}^{a}(G) \leq 3$.

Теорема доказана.

Обобщенным коммутантом группы G называется наименьшая нормальная подгруппа N группы G, такая, что G/N является группой с абелевыми силовскими подгруппами. Очевидно, что обобщенный коммутант совпадает с $\mathfrak{A}$-корадикалом группы G, где $\mathfrak{A}$ – класс всех разрешимых групп с абелевыми силовскими подгруппами.

Теорема 11. *Пусть G – π-разрешимая группа, у которой обобщенный коммутант π-холловой подгруппы нильпотентен. Тогда*

$$l_{\pi}^{a}(G) \leq |\pi(G_{\pi})| - 1 + max_{p\in\pi} l_{p}^{a}(G).$$

Доказательство. Применим индукцию к порядку группы G. Условия теоремы переносятся на фактор-группы, поэтому получаем, что

$$O_{\pi'}(G) = O_{p'}(G) = 1,$$

в G существует единственная минимальная нормальная подгруппа,

$$F(G) = O_p(G) = F(O_{\pi}(G))$$

для некоторого простого $p \in \pi$ и $C_G(F(G)) \subseteq F(G)$.

Пусть N – обобщенный коммутант π-холловой подгруппы G_{π}. Так как N является нильпотентной группой, то p'-холлова подгруппа $N_{p'}$ из N нормальна в G_{π} и, следовательно,

$$N_{p'} \subseteq C_G(F(G)) \subseteq F(G).$$

Поэтому $N_{p'} = 1$ и N является p-группой. Так как N обобщенный коммутант π-холловой подгруппы G_{π}, то силовская r-подгруппа G_rN/N абелева для всех $r \in \pi$. По теореме 2.4 [1] $G_qN/N \cong G_q$ для всех $q \in \pi\backslash\{p\}$.

Таким образом, силовские q-подгруппы в группе G абелевы для всех $q \in \pi\backslash\{p\}$. Из определения производной q-длины получаем, что $l_{q}^{a}(G) \leq 1$ для всех $q \in \pi\backslash\{p\}$. Поэтому $\max_{t\in\pi} l_{t}^{a}(G) = l_{p}^{a}(G)$.

Так как в $G_{\pi\backslash\{p\}}$ все силовские абелевы, то

$$l_{\pi\backslash\{p\}}^{a}(G) \leq |\pi(G_{\pi\backslash\{p\}})| = |\pi(G_{\pi})| - 1.$$

Из свойств производной π-длины следует, что

$$l_{\pi}^{a}(G) \leq l_{\pi\backslash\{p\}}^{a}(G) + l_{p}^{a}(G),$$

поэтому

$$l_{\pi}^{a}(G) \leq |\pi(G_{\pi})| - 1 + \max_{p\in\pi} l_{p}^{a}(G).$$

Теорема доказана.

Заключение

Получение новых оценок производной π-длины конечной π-разрешимой группы имеет важное значение не только для теории конечных групп и их классов, а и в современной криптографии. В частности, полученные оценки будут полезны при получении новых шифров и новых криптосистем с высокой эффективностью и криптостойкостью.

Найденные оценки производной π-длины конечной π-разрешимой группы могут стать основой для создания новых методов современной теории защиты информации и теории кодирования.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Монахов, В. С. Введение в теорию конечных групп и их классов / В. С. Монахов. – Минск : Выш. шк., 2006. – 207 с.

2. Huppert, B. Endliche Gruppen I / B. Huppert. – Berlin ; Heidelberg ; New York. – 1967. – 792 s.

3. Монахов, В. С. Конечные группы с полунормальной холловой подгруппой / В. С. Монахов // Мат. заметки. – 2006. – Т. 80, № 4. – С. 573–581.

4. Грицук, Д. В. О производной π-длине π-разрешимой группы / Д. В. Грицук, В. С. Монахов, О. А. Шпырко. // Вестн. БГУ. Сер. 1. – 2012. – № 3. – С. 90–95.

5. Monakhov, V. S. On derived π-length of a finite π-solvable group with supersolvable π-Hall subgroup / V. S. Monakhov, D. V. Gritsuk // Algebra and Discrete Mathematics. – 2013. – Vol. 16, nr 2. – P. 233–241.

6. Горчаков, Ю. М. Примитивно факторизуемые группы / Ю. М. Горчаков // Учен. зап. Перм. ун-та. – 1960. – № 17. – С. 15–31.

7. Hall, Ph. Complemented group / Ph. Hall // J. London Math. Soc. – 1937. – Vol. 12. – P. 201–204.

8. Монахов, В. С. О производной π-длине конечной π-разрешимой группы с заданной π-холловой подгруппой / В. С. Монахов, Д. В. Грицук // Тр. Ин-та математики и механики Урал. отд-ния РАН. – 2013. – Т. 18, № 3. – С. 215–223.

9. Грицук, Д. В. Конечные π-разрешимые группы с заданными свойствами 2-максимальных π-подгрупп / Д. В. Грицук, А. А. Трофимук // Вестн. Брест. гос. техн. ун-та. Физика, математика, информатика. – 2017. – № 5 (107). – С. 69–72.

10. Грицук, Д. В. Оценки производной π-длины π-разрешимой группы, у которой π-холловы подгруппы свободны от n-ых степеней / Д. В. Грицук, А. А. Трофимук, Т. А. Артюшеня // Вестн. Витеб. гос. ун-та им. П. М. Машерова. – 2018. – № 1 (98). – С. 11–15.

11. Gaschutz, W. Gruppen in denen das normalteilersein transitiv ist / W. Gaschutz // J. Reine Angew. Math. – 1957. – Vol. 198. – P. 87–92.

Рукапіс паступіў у рэдакцыю 16.10.2020