

Конечные группы с минимальной системой образующих максимально возможной длины

Я. Г. БЕРКОВИЧ (Ростов на Дону)

Пусть $|G| = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ -каноническое разложение порядка конечной группы G ; $\lambda = \lambda(G) = \alpha_1 + \dots + \alpha_k$. Если B -минимальная система образующих группы G , то из теоремы Лагранжа следует $|B| \leq \lambda$.

Определение. G назовем Λ -группой, если она обладает минимальной системой образующих длины $\lambda = \lambda(G)$.

Цель заметки — классифицировать Λ -группы. Наше доказательство совершенно элементарно. Для удобства основные цитируемые в тексте результаты собраны в лемме.

Лемма. 1. Пусть M и N -нормальные делители группы G . Тогда $G/M \cap N$ изоморфна подгруппе из $G/M \times G/N$.

2. (О. Гельдер). Если порядок группы свободен от квадратов, она сверхразрешима.

3. (У. Бернсайд). Если силовская p -подгруппа группы G лежит в центре своего нормализатора, то G имеет инвариантное p -дополнение.

4. Группа автоморфизмов группы простого порядка p циклическая порядка $p-1$.

5. Циклическая группа тогда и только тогда является Λ -группой, когда ее порядок свободен от квадратов.

Скажем, что подгруппа H дополняема в группе G , если $G = FH$ и $F \cap H = 1$ для некоторой подгруппы F группы G .

Основная теорема. Следующие свойства конечной группы G эквивалентны:

- (а) G — Λ -группа.
- (б) G сверхразрешима и все ее силовские подгруппы элементарные абелевы.
- (в) G изоморфна подгруппе прямого произведения групп, порядки которых свободны от квадратов.
- (г) Все подгруппы дополняемы в G .

Доказательство. (а) $\Rightarrow$ (б). Пусть $B = \{x_1, \dots, x_\lambda\}$ -минимальная система образующих Λ -группы G , $\lambda = \lambda(G)$. Очевидно,

- (i) Любое подмножество множества B порождает Λ -группу.
- (ii) Эпиморфные образы Λ -группы G являются Λ -группами.

Доказательство. Пусть R -нормальная подгруппа группы G , $\bar{G} = G/R$, $\bar{x}_i = x_i R$. Перенумеруем x_i так, что $\{\bar{x}_1, \dots, \bar{x}_t\}$ -минимальная система образующих группы $\bar{G}$. Тогда $G = \langle x_1, \dots, x_t \rangle R$, $\lambda(\langle x_1, \dots, x_t \rangle) = t$ по (i), при этом $\{x_1, \dots, x_t\}$ -минимальная система образующих A -группы $\langle x_1, \dots, x_t \rangle$. Как отмечалось,

$$t \leq \lambda(\bar{G}) = \lambda(G) - \lambda(R) \leq \lambda(\langle x_1, \dots, x_t \rangle) + \lambda(R) - \lambda(R) = \lambda(\langle x_1, \dots, x_t \rangle) = t.$$

Поэтому $\lambda(\bar{G}) = t$ и $\bar{G}$ — A -группа, что и требовалось доказать.

$$(iii) \quad \Phi(G) = 1.$$

Доказательство. Положим в (ii), $R = \varphi(G)$, и пусть в обозначениях доказательства (ii), $\bar{G} = \langle \bar{x}_1, \dots, \bar{x}_t \rangle$. Тогда

$$G = \langle x_1, \dots, x_t, \Phi(G) \rangle = \langle x_1, \dots, x_t \rangle,$$

откуда $t = \lambda$. Так как $\lambda = t \leq \lambda(\bar{G}) \leq \lambda$, то $\lambda(\bar{G}) = \lambda(G)$, $G = \bar{G}$, так что $\varphi(G) = 1$.

(iv) Если G содержит неединичный разрешимый нормальный делитель, то G разрешима.

Это тотчас же следует из (ii) по индукции.

(v) Группа G разрешима.

Доказательство. Пусть уже доказано, что все A -группы, чей порядок меньше $|G|$, разрешимы, а G неразрешима. Тогда G полупростая по (iv). Положим $H = \langle x_1, \dots, x_{\lambda-1} \rangle$. Тогда $|G:H| = p$, где p -простое число. По (i) H является A -группой, и поэтому по индукции сверхразрешима. По (iv) имеем $\bigcap_{x \in G} xHx^{-1} = 1$. Отсюда следует, что G изоморфна подгруппе симметрической группы S_p степени p , и поэтому p^2 не делит $|G|$ и p -наибольший простой делитель $|G|$. Так как H сверхразрешима, то $Q \in \text{Syl}_q(H)$ нормальна в H , где q -наибольший простой делитель $|H|$. Предположим, что $|Q| > q$. Положим $F = \langle x_2, \dots, x_\lambda \rangle$. Предыдущее рассуждение дает $|G:F| = p$, так что $|F| = |H|$. Так как G — A -группа, то

$$\lambda(\langle x_2, \dots, x_{\lambda-1} \rangle) = \lambda - 2 = \lambda(H) - 1 = \lambda(F) - 1,$$

и поэтому $H \cap F = \langle x_2, \dots, x_{\lambda-1} \rangle$. По предположению $|Q| > q$; поэтому q делит $|H \cap F|$. Пусть $Q_0 \in \text{Syl}_q(H \cap F)$. Так как $H \cap F$ сверхразрешима, Q_0 нормальна в $H \cap F$. Если $Q_0 < Q$, то $N_G(Q_0) \cong \langle H \cap F, Q, \bar{Q} \rangle$, где $\bar{Q} \in \text{Syl}_q(F)$, и поэтому $H_G(Q_0) \cong \langle H, F \rangle = G$, то есть Q_0 нормальна в G , вопреки полупростоте группы G . Итак, $|Q| = q^*$). Тогда $H = A\lambda Q$ -полупрямое произведение q' -холловской подгруппы A в H с $Q \in \text{Syl}_q(H)$, $|Q| = q$. Аналогично $F = A \cdot \bar{Q}$. Положим $C = C_A(Q)$, $D = C_A(\bar{Q})$. Тогда C нормальна в H , а D нормальна в F . Поэтому $C \cap D$ нормальна в $\langle H, F \rangle = G$, и $C \cap D = 1$ ввиду полупростоты группы G . Но A/C изоморфна подгруппе циклической группы порядка $p-1$ по лемме (п. 4). То же самое верно и для A/D . По п. 1 леммы A абелева, и ее порядок свободен от кубов. Пусть $R \in \text{Syl}_r(A)$, $N = N_G(R)$. Если $N \leq H$ или $N \leq F$, то R лежит

*) Т. к. $Q \leq H \cap F$.

в центре N , и G имеет по п. 3 леммы инвариантное r -дополнение. Пусть $N \not\leq H$, $N \not\leq F$. Тогда $A < N$, $|G:A| = qp$. Так как G полупростая, $N < G$, так что $|N| = |A|p$ или $|A|q$. Пусть $|N| = |A|p$. Рассмотрим подгруппу RP , где $P \in \text{Syl}_p(N)$. Если P нормальна в RP , то R лежит в центре N , и тогда G имеет инвариантное r -дополнение по п. 3 леммы. Если P неинвариантна в RP , то по теореме Силова $r^2 \equiv 1 \pmod{p}$, а так как $r < p$, то $r = 2$, $p = 3$, $r \neq q \neq p$, и отсюда следует $q > p$ противоречие. Пусть $|N| = |A|q$. Если $Q \in \text{Syl}_q(N)$ нормальна в RQ , то снова по п. 3 леммы G имеет инвариантное r -дополнение. Пусть Q неинвариантна в RQ . Тогда, как и выше, $r = 2$, $q = 3$, $|G| = 2 \cdot 3p$ или $|G| = 4 \cdot 3p$. В первом случае G разрешима по п. 2 леммы. Во втором случае $P \in \text{Syl}_p(G)$ неинвариантна в G , и поэтому по теореме Силова $p = 5$, $G = A_5$. Получается противоречие, так как A_5 не является A -группой. Итак, для любого простого делителя r числа $|A|$ группа G имеет инвариантное r -дополнение. Поэтому $G = A \cdot B$, где $|B| = |G:A| = qp$, и поэтому G разрешима. А это противоречит предположению. Утверждение (v) доказано.

(vi) Если G содержит два различных минимальных нормальных делителя, то (a) $\Rightarrow$ (б).

Это тотчас же следует из п. 1 леммы.

Поэтому далее можем считать, что G содержит единственный минимальный нормальный делитель R . Положим $|R| = p^n$.

(vii) $n = 1$.

Доказательство. Пусть $\bar{G} = G/R$, $\bar{x}_i = x_i R$, и x_i перенумерованы так, что $\langle \bar{x}_1, \dots, \bar{x}_t \rangle$ -минимальная система образующих для $\bar{G}$. Тогда $G = \langle x_1, \dots, x_t \rangle R$. Так как R -минимальная нормальная подгруппа в G , $\lambda(\langle x_1, \dots, x_t \rangle) = t < \lambda$ то $R \not\leq \langle x_1, \dots, x_t \rangle$, и поэтому $\langle x_1, \dots, x_t \rangle$ максимальна в G . Поэтому $\langle x_1, \dots, x_t, x_{t+1} \rangle = G$, откуда $\lambda(R) = 1$, и $|R|$ -простое число, что и требовалось.

Мы имеем $G = A \cdot R$ и $C_A(R) = 1$, так как R -единственная минимальная нормальная подгруппа в G , а $C_A(R)$ нормальна в G . Но тогда подядок группы G свободен от квадратов по пп. 4 и 5 леммы. Это завершает, в силу п. 2 леммы, доказательство импликации (a) $\Rightarrow$ (б).

(a) $\Rightarrow$ (в). Приведенное выше рассуждение доказывает и эту импликацию.

(в) $\Rightarrow$ (б). Это очевидно.

(в) $\Rightarrow$ (г). Это — известная теорема Ф. Холла [1].

(б) $\Rightarrow$ (a). Пусть это уже доказано для групп, чей порядок меньше $|G|$. Пусть p -наибольший простой делитель $|G|$, R -нормальная подгруппа порядка p в G . Пусть F - p' -холловская подгруппа в G . По теореме Машке о полной приводимости в $P \in \text{Syl}_p(G)$ имеется подгруппа P_1 , инвариантная относительно F , и такая, что $P = P_1 \times R$. Положим $H = FP_1$. По индукции H имеет минимальную систему образующих $\{x_1, \dots, x_{\lambda-1}\}$. Положим $R = \langle x_\lambda \rangle$. Покажем, что $\{x_1, \dots, x_{\lambda-1}, x_\lambda\}$ -минимальная система образующих для G . Очевидно, из этой системы нельзя удалить x_λ , так как $\{x_1, \dots, x_{\lambda-1}\} = H < G$. Предположим, что $\langle x_2, \dots, x_\lambda \rangle = G$. Тогда $GR = \langle \bar{x}_2, \dots, \bar{x}_{\lambda-1} \rangle$. Поэтому $G = \langle x_2, \dots, x_{\lambda-1} \rangle R$ и $\langle x_2, \dots, x_{\lambda-1} \rangle$ максимальна в G . Но это неверно, так как $\langle x_2, \dots, x_{\lambda-1} \rangle < H < G$. Это завершает доказательство теоремы.

Следствие 1. *Подгруппы A -группы являются A -группами.*

Следствие 2. *Центральное произведение двух A -групп является A -группой.*

В самом деле, пусть $G = H * F$ -центральное произведение двух A -групп H и F . Тогда $G = H \times F/R$. Так как $H \times F$ — A -группа по теореме, то G по (ii) из доказательства теоремы является A -группой.

Цитированная литература

- [1] P. HALL, Complemented groups, *J. London Math. Soc.*, 12 (1937), 201—204.

344006, Ростов-на-Дону, Энгельса 111, кв. 18
Беркович Яков Гильевич

(Поступило 4. VII. 1984 г.)