Доклады Академии Наук СССР
1948. Том LX. № 8

МАТЕМАТИКА

Ю. А. ГОЛЬФАНД

О ГРУППАХ, ВСЕ ПОДГРУППЫ КОТОРЫХ СПЕЦИАЛЬНЫЕ

(Представлено академиком О. Ю. Шмидтом 9 IV 1948)

Неспециальные группы, все подгруппы которых специальные (по терминологии С. А. Чунихина, „группа типа S"), были изучены О. Ю. Шмидтом (1), установившим следующие основные свойства этих групп: если Γ — группа типа S, то:

I. Γ имеет инвариантную силовскую подгруппу Σ порядка q^β, фактор-группа Γ/Σ циклическая порядка p^α (p простое число).

II. Если P — элемент порядка p^α, то P^p лежит в центре группы Γ.

III. Если Φ — наибольший нормальный делитель группы Γ, заключенный в Σ, то индекс $(\Sigma:\Phi)=q^b$, где b — показатель числа q по модулю p.

IV. Элемент P перестановочен со всеми элементами подгруппы Φ.

V. Если Σ — абелева группа, то она элементарная, порядка q^b („случай Miller-Moreno").

В настоящей заметке значительно уточняется структура групп типа S. Введенные в I—V обозначения: Γ, Σ, Φ, P и b в дальнейшем сохраняются.

Теорема 1. *Если группа Σ неабелева, то Φ будет одновременно ее центром, коммутантом и подгруппой Фраттини.*

Обозначим через Z, K и F центр, коммутант и подгруппу Фраттини группы Σ. Тогда $Z, K, F\subseteq\Phi$. С другой стороны, Γ/K неспециальная группа и, следовательно, группа типа S. Но Σ/K абелева группа. Из свойств V и III следует $K=F=\Phi$. Пусть T — централизатор Φ в Σ. $T\Phi$ характеристическая подгруппа группы Σ, не содержащаяся в Φ, ибо, если S — элемент из Σ, не лежащий в Φ, то коммутатор $[P, S]=P^{-1}S^{-1}PS$ лежит в T (IV), но не в Φ. Поэтому $T\Phi=\Sigma$, откуда, по известному свойству подгруппы Фраттини (2), $T=\Sigma$, и, значит, $Z=\Phi$.

Теорема 2. *Если группа Σ неабелева, то Φ элементарная группа. При $q\neq 2$ порядки всех элементов группы Σ равны q. При $q=2$ порядки элементов группы Σ не превосходят 4, но не могут быть все равны 2.*

Пусть $x, y\in\Sigma$. Ввиду $\Phi=K=Z=F$

$$[x, y]^q=[x, y^q]=1.$$

Поэтому порядки всех элементов группы Φ равны q.

Пусть $q\neq 2$. x элемент из Σ, не лежащий в Φ. Допустим, что $x^q\neq 1$. $y=P^{-1}xP\neq x$, но, ввиду IV, $x^q=y^q$. Пусть $S=xy^{-1}$.

$$S^q=(xy^{-1})^q=x^q y^{-q}[y^{-1}x]^{\frac{1}{2}q(q-1)}=1. \qquad (1)$$

Элементы $S_i=P^{-i}SP^i$ $(0\leqslant i<b)$ порождают группу Σ. Но порядок

S_i равен q, и, ввиду (1), порядок произведения двух элементов из Σ не превосходит порядков сомножителей. Поэтому порядки всех элементов группы Σ равны q. При $q=2$ это рассуждение не проходит. Но, если $x \in \Sigma$, то $x^2 \in \Phi$, и $x^4=1$. Все элементы группы Σ не могут быть порядка 2, ибо Σ неабелева группа.

Теорема 3. *При заданных p, q и α существует единственная группа Γ_0 типа S максимального порядка $p^\alpha q^{\beta_0}$, где*

$$\beta_0=\begin{cases} b & \text{при } b\equiv 1 \\ \frac{3}{2}b & \text{при } b\equiv 0 \end{cases} \pmod 2.$$

Все остальные группы типа S порядка $p^\alpha q^\beta$ изоморфны фактор-группам группы Γ_0 по ее центральным нормальным делителям.

Рассмотрим случай $q\neq 2$. Пусть группа Ω задана соотношениями:

a) $P^{p^\alpha}=Q^q=1$, $\quad X^{p^t}=Z^t=1$

b) $P^p \rightleftarrows Q$, $\quad X^p \rightleftarrows Z$

$$\text{c)}\ \prod_{i=0}^{b}(P^{-i}QP^i)^{\alpha_i}=1, \tag{2}$$

d) $P^{-i}QP^i \rightleftarrows [P^{-j}QP^j,\ P^{-k}QP^k]$ $\quad (0\leqslant i<b,\ 0\leqslant j<k<b)$.

Символ $\rightleftarrows$ обозначает перестановочность элементов. α_i — коэффициенты фиксированного, не приводимого в поле Галуа порядка q уравнения

$$f(x)=x^b+\alpha_{b-1}x^{b-1}+\ldots+\alpha_0, \tag{3}$$

которому удовлетворяет p-й корень из 1. $\alpha_b=1$.

С помощью шрейеровской теории расширений групп легко установить следующие свойства групп Ω:

1) Порядок Ω равен $p^\alpha q^{\frac{1}{2}b(b+1)}$.

2) Элементы $Q_i=P^{-i}QP^i$ $(0\leqslant i<b)$ порождают нормальный делитель $\Delta\subset\Omega$ порядка $q^{\frac{1}{2}b(b+1)}$.

3) Элементы $K_{ij}=[Q_i,\ Q_j]$ $(0\leqslant i<j<b)$ порождают коммутант Λ группы Δ. Λ элементарная абелева группа порядка $q^{\frac{1}{2}b(b-1)}$.

Во всякой группе Γ типа S и порядка $p^\alpha q^\beta$ можно выбрать два образующих элемента P и Q, удовлетворяющих соотношениям (2). Пусть P — элемент Γ порядка p^α, Q — элемент из Σ, не лежащий в Φ. Ввиду II P производит в Σ автоморфизм порядка p. Поэтому должно выполняться соотношение:

$$\prod_{i=0}^{b}(P^{-i}QP^i)^{\beta_i}=F_0,$$

где β_i — коэффициенты уравнения типа (3), а $F_0\in\Phi$. Заменяя элемент P некоторой его степенью, можно добиться равенств $\beta_i=\alpha_i$ $(0\leqslant i\leqslant b)$. Так как $f(1)\neq 0 \pmod q$, то можно решить сравнение

$$t\,f(1)\equiv -1 \pmod q.$$

Заменим элемент Q на QF_0^i. Элементы, полученные после наших замен, обозначим снова P и Q. Легко проверить, что они удовлетворяют соотношение (2, с). Остальные соотношения выполняются ввиду теорем 1 и 2 и свойства II. Но $\{P, Q\}$ неспециальная группа, и, значит $\{P, Q\}=\Gamma$.

Из теоремы Дика ([4]), следует, что

$$\Gamma \simeq \Omega / \theta, \tag{4}$$

причем легко установить, что $\theta \subseteq \Lambda$. При изоморфизме (4) Δ / θ отображается на Σ, а Λ / θ на Φ.

Элемент P производит в группе Λ автоморфизм порядка p. Поэтому Λ разбивается в прямое произведение допустимых подгрупп, порядки которых равны q^b или q. Обозначим через θ_0 объединение всех прямых множителей первого типа. Элемент P производит тождественный автоморфизм в фактор-группе Λ / θ_0. Из IV следует, что $\theta_0 \subseteq \theta$. С другой стороны, нетрудно установить, что

$$\Gamma_0 = \Omega / \theta_0$$

будет группой типа S. Всякая другая группа типа S и порядка $p^\alpha q^\beta$ будет фактор-группой Γ_0 по центральному нормальному делителю, ибо $\Phi_0 = \Lambda / \theta_0$ лежит в центре Γ_0.

Остается вычислить порядок группы Γ_0. Порядок θ_0 равен q^{kb} (k — целое число). С другой стороны, порядок Φ_0 меньше, чем q^b, ибо в группе Γ_0 элементы K_{ij}, ввиду IV, удовлетворяют соотношениям:

$$K_{ij} = K_{mn} \text{ при } n-m=j-i,$$

и, значит, Φ_0 имеет не более, чем $b-1$ независимых образующих порядка q. Значит, порядок Φ_0 равен q^γ, где γ — остаток от деления числа $\frac{1}{2} b(b-1)$ на b. Отсюда непосредственно следует утверждение теоремы.

При $q=2$ доказательство проводится в основном так же, но соотношения (2, а) заменяются соотношениями

$$\text{a}')\ P^{p^\alpha} = Q^4 = 1 \tag{2}$$

и, кроме того, добавляются еще соотношения

$$\text{e})\ [Q, P^{-i} Q P^i] = 1 \quad (0 \leqslant i < b). \tag{2}$$

Интересно отметить, что при $b \equiv 1 \pmod 2$ возможен только „случай Miller-Moreno".

Поступило
7 IV 1948

ЦИТИРОВАННАЯ ЛИТЕРАТУРА

[1] О. Ю. Шмидт, Математическ. сб., 31, 3—4, 366 (1924); Тр. семинара по теории групп (1938). [2] H. Zassenhaus, Lehrbuch der Gruppentheorie, 1, 1937. [3] O. Schreier, Monatsh. Math. Phys., 34 (1926); Hamb. Abh., 4 (1926). [4] А. Г. Курош, Теория групп, 1944.