Доклады Академии Наук СССР
1938. Том XX, № 2—3

МАТЕМАТИКА

С. А. ЧУНИХИН

О СИЛОВСКИХ ПОДГРУППАХ ПРОСТОЙ ГРУППЫ

(Представлено академиком И. М. Виноградовым 9 V 1938)

1. В работе «Über einige Sätze der Gruppentheorie» (1) я доказал следующую теорему:

Теорема I. *Пусть $\mathfrak{H}$ — подгруппа индекса k группы $\mathfrak{G}$ и пусть $\mathfrak{K}$ — подгруппа $\mathfrak{H}$, содержащая коммутант $\mathfrak{H}$. Если в $\mathfrak{H}$, но не в $\mathfrak{K}$, содержится элемент A, порядок которого взаимно прост с k и такой, что для любого λ все элементы $\mathfrak{H}$, сопряженные с A^λ в $\mathfrak{G}$, принадлежат системе $\mathfrak{K}A^\lambda$, то $\mathfrak{G}$ является непростой группой.*

В настоящей работе с помощью этой теоремы устанавливается одно свойство силовских подгрупп у простых групп. Другое приложение этой же теоремы было указано также L. Weisner'ом (2).

2. Пусть $\mathfrak{G}$ группа порядка $p^\beta n$, p — простое число и не делит n. Пусть $\mathfrak{P}$—одна из силовских подгрупп порядка p^β и пусть $\mathfrak{P}$ является абелевой группой. Мы предположим также, что $p-1$ взаимно просто с n. Докажем следующие леммы.

Лемма I. *Пусть A порядка p^m является элементом фундаментального базиса группы $\mathfrak{P}$. Пусть α не делится на p и пусть $m_1 < \beta$ и $m_1 < m$. Тогда равенство*

$$A^{\alpha p^{m_1}} = X^{p^\beta} \tag{1}$$

невозможно для всякого элемента X группы $\mathfrak{P}$.

Доказательство. Допустим, что существует элемент X, входящий в $\mathfrak{P}$ и удовлетворяющий равенству (1). Выразим X через элементы фундаментального базиса $\mathfrak{P}$:

$$X = A^y B,$$

где B — элемент $\mathfrak{P}$, уже независящий от A. Таким образом имеем:

$$A^{\alpha p^{m_1}} = A^{yp^\beta} B^{p^\beta}$$

или

$$A^{p^{m_1}(\alpha - yp^{\beta - m_1})} = B^{p^\beta}. \tag{2}$$

Здесь $\beta - m_1 > 0$ по условию.

Левая сторона равенства (2) отлична от единицы, так как $m_1 < m$ и $\alpha - yp^{\beta - m_1} \not\equiv 0 \pmod p$.

Поэтому равенство (2) невозможно, если $B^p = E$. Однако, равенство (2) невозможно также и в случае, когда $B^{p^\beta} \neq E$, так как любая отличная от единицы степень элемента A не может быть выражена через остальные элементы фундаментального базиса. Таким образом лемма I доказана.

Лемма II. *Пусть элемент A порядка p^m является единственным элементом фундаментального базиса группы $\mathfrak{P}$, имеющим этот порядок. Тогда все элементы $\mathfrak{P}$, сопряженные с A в $\mathfrak{G}$, имеют следующий вид: $A^x B$, где $x \equiv 1 \pmod p$, а B является элементом $\mathfrak{P}$, не зависящим от A, или единицей.*

Доказательство. Известно ([3]), что элементы центра силовской подгруппы, сопряженные во всей группе, уже сопряжены в нормализаторе этой силовской подгруппы, т. е. из $G^{-1}AG \subset \mathfrak{P}$, $G \subset \mathfrak{G}$ следует $G^{-1}AG = C^{-1}AC$, где $C^{-1}\mathfrak{P}C = \mathfrak{P}$. Если $C^{-1}AC$ отлично от A, то элемент C не содержится в $\mathfrak{P}$ (так как в данном случае группа $\mathfrak{P}$ является абелевой). Выразим элемент $C^{-1}AC$, входящий в $\mathfrak{P}$, через элементы фундаментального базиса группы $\mathfrak{P}$. Необходимо, очевидно, рассмотреть лишь случай, когда $C^{-1}AC$ отлично от A. Возможны следующие три случая:

1) $C^{-1}AC = A^x$. Как было мной показано раньше ([4]), элемент центра силовской подгруппы, принадлежащей числу p, не может быть сопряженным со своей, отличной от него самого, степенью, если только $p-1$ взаимно просто с порядком всей группы. Следовательно, имеем $x \equiv 1 \pmod{p^m}$.

2) $C^{-1}AC = A^x B$, *где $B \neq E$ зависит лишь от тех элементов фундаментального базиса группы $\mathfrak{P}$, порядки которых меньше p^m.*

Так как, очевидно, $B^{p^{m-1}} = E$, то имеем:

$$C^{-1}A^{p^{m-1}}C = A^{xp^{m-1}}.$$

Но это последнее равенство возможно лишь тогда, когда $x \equiv 1 \pmod p$, так как здесь мы имеем предыдущий случай.

3) $C^{-1}AC = A^x B_1 B_2$, *где $B_1 \neq E$ зависит лишь от тех элементов фундаментального базиса, порядки которых больше p^m, а B_2 зависит лишь от тех элементов фундаментального базиса, порядки которых меньше p^m, или равно E.*

Прежде всего ясно, что наивысшая степень каждого элемента фундаментального базиса, входящего в B_1, делится на p, так как в противном случае порядок правой стороны равенства $C^{-1}AC = A^x B_1 B_2$ был бы больше порядка p^m левой стороны, что невозможно. Поэтому B_1 можно представить в следующей форме $B_1 = D^p$, где D опять элемент группы $\mathfrak{P}$.

Из равенства $C^{-1}AC = A^x D^p B_2$ получаем:

$$C^{-1}A^{p^{m-1}}C = A^{xp^{m-1}}D^{p^m}, \tag{3}$$

так как $B_2^{p^{m-1}} = E$. Пусть теперь C^d — наименьшая степень элемента C, перестановочная с $A^{p^{m-1}}$. Число d является, очевидно, делителем порядка C и, следовательно (элемент C не содержится в $\mathfrak{P}$, как было уже выше отмечено),

$$d \text{ взаимно просто с } p-1. \tag{4}$$

Из равенства (3) последовательно получаем:

$$C^{-2}A^{p^{m-1}}C^2 = A^{x^2p^{m-1}}D^{xp^m}C^{-1}D^{p^m}C$$

$$\cdots\cdots\cdots\cdots\cdots\cdots$$

$$\cdots\cdots\cdots\cdots\cdots\cdots$$

$$C^{-d}A^{p^{m-1}}C^d = A^{x^d p^{m-1}}D^{x^{d-1}p^m}\underbrace{C^{-1}D^{x^{d-2}p^m}C}\ldots\underbrace{C^{-(d-1)}D^{p^m}C^{d-1}}$$

Подчеркнутые члены в последнем равенстве являются элементами группы $\mathfrak{P}$, так как C перестановочен с $\mathfrak{P}$. Последнее равенство можно представить в следующей форме:

$$C^{-d} A^{p^{m-1}} C^{d} = A^{x^d p^{m-1}} D_1^{p^m}, \tag{5}$$

где D_1 также элемент группы $\mathfrak{P}$.

Из равенства (5) получаем

$$A^{p^{m-1}(x^d-1)} = D_2^{p^m}. \tag{6}$$

Здесь $D_2 = D_1^{-1}$ также является элементом $\mathfrak{P}$. Согласно лемме I равенство (6) возможно лишь в случае, когда $x^d \equiv 1 \pmod p$. Это же сравнение может иметь решение [на основании условия (4)] лишь в случае, когда $x \equiv 1 \pmod p$.

Лемма II доказана.

Лемма III. *Пусть A является тем же самым элементом, что и в случае леммы* II. *Тогда все элементы $\mathfrak{P}$, сопряженные с A^λ в $\mathfrak{G}$, имеют следующий вид:*

$A^x B$, где $x \equiv \lambda \pmod p$, а B является элементом $\mathfrak{P}$, не зависящим от A, или единицей.

Доказательство. Пусть $C^{-1}A^\lambda C \subset \mathfrak{P}$, $C^{-1}\mathfrak{P}C = \mathfrak{P}$. Отсюда следует $C^{-1}A^\lambda C = (C^{-1}AC)^\lambda$. Но $C^{-1}AC \subset \mathfrak{P}$, так как $C^{-1}\mathfrak{P}C = \mathfrak{P}$. Согласно лемме II имеем в этом случае $C^{-1}AC = A^x B$, $x \equiv 1 \pmod p$, а B — элемент $\mathfrak{P}$, не зависящий от A. Таким образом получаем: $C^{-1}A^\lambda C = (A^x B)^\lambda = A^{x\lambda} B^\lambda$ и, очевидно, $x\lambda \equiv \lambda \pmod p$, а B^λ не зависит от A. Лемма III доказана.

Теорема II. *Пусть $\mathfrak{G}$ — простая группа порядка $p^\delta n$, p — простое число и не делит n, $p-1$ и n взаимно просты. Пусть $\mathfrak{P}$ — одна из подгрупп Силова порядка p^δ. Пусть $\mathfrak{P}$ является абелевой группой. Тогда число элементов фундаментального базиса $\mathfrak{P}$, имеющих один и тот же порядок, всегда больше единицы.*

Доказательство. Пусть A порядка p^m является единственным элементом этого порядка среди элементов фундаментального базиса группы $\mathfrak{P}$. Пусть $\mathfrak{K}$ — подгруппа $\mathfrak{P}$, порожденная элементом A^p и всеми отличными от A элементами фундаментального базиса $\mathfrak{P}$. Группа $\mathfrak{K}$, очевидно, не содержит элемент A.

Согласно леммам II и III всякий элемент из $\mathfrak{P}$, сопряженный с A^λ в $\mathfrak{G}$, имеет вид $A^x B$, где $x \equiv \lambda \pmod p$, а B — элемент $\mathfrak{P}$, не зависящий от A (или E). Таким образом $x = \lambda + tp$, и мы имеем $A^x B = A^\lambda A^{tp} B$. Элементы B и A^{tp} входят, очевидно, в $\mathfrak{K}$, следовательно, $A^x B$ входит в систему $A^\lambda \mathfrak{K}$. Мы видим, что для элемента A выполняются условия теоремы I (если положить $\mathfrak{H} = \mathfrak{P}$) и группа $\mathfrak{G}$ в этом случае является непростой. Полученное противоречие доказывает теорему II.

3. Частным случаем теоремы II является следующая теорема L. Weisner'а (2):

Пусть группа $\mathfrak{G}$ имеет абелеву силовскую подгруппу $\mathfrak{P}$ порядка p^α и типа $(n_1, n_2, \ldots, n_r)$, где $n_1 > n_2 \geqslant n_3 \geqslant \ldots \geqslant n_r$.

Если $p-1$ взаимно просто с порядком $\mathfrak{G}$, то группа $\mathfrak{G}$ имеет нормальный делитель индекса p.

4. Подобным образом можно рассмотреть и общий случай, когда группа $\mathfrak{P}$ не является абелевой. Мы получаем следующие результаты. Пусть $\mathfrak{P}$ порядка p^δ является подгруппой Силова у простой группы $\mathfrak{G}$ порядка $p^\delta n$. Пусть $p-1$ и n взаимно просты.

Пусть $\mathfrak{Q}$ порядка p^{η} является центром группы $\mathfrak{P}$. Пусть $\mathfrak{Q}$ имеет тип $(p^{\lambda_1}, p^{\lambda_2}, \ldots p^{\lambda_r})$, где $\lambda_1 \geqslant \lambda_2 \geqslant \ldots \geqslant \lambda_r$. Введем следующие обозначения:

1) если $1 < i < r$, то ω_i равно наименьшему из чисел $\lambda_{i-1} - \lambda_i$ и $\lambda_i - \lambda_{i+1}$;

2) если $i = 1$, то $\omega_1 = \lambda_1 - \lambda_2$;

3) если $i = r$, то $\omega_r = \lambda_{r-1} - \lambda_r$;

4) если $r = 1$, то $\omega_1 = \lambda_1$.

Теорема III. *Для каждого значения i выполняется неравенство* $\omega_i \leqslant \delta - \eta$.

Математический институт
им. В. А. Стеклова.
Академия Наук СССР.
Москва.

Поступило
16 V 1938.

ЦИТИРОВАННАЯ ЛИТЕРАТУРА

[1] Serge Tchounikhin, Math. Ann., **112** (1935). [2] L. Weisner, Duke Math. Journ., **2**, № 4 (1936). [3] W. Burnside, Theory of Groups of Finite Order, sec. ed., 155. [4] Serge Tchounikhin, Math. Ann., **112** (1935).