**Доклады Академии наук СССР**
1970. Том 190, № 5

УДК 519.44 *МАТЕМАТИКА*

Е. И. ШАТЫЛО

# ГРУППЫ ТИПА CS

*(Представлено академиком В. М. Глушковым 24 VI 1969)*

Наложение тех или иных ограничений на ту или иную систему подгрупп произвольной группы нередко приводит к классам таких групп, описание строения которых удается довести до выделения образующих элементов и указания определяющих соотношений. Классическими примерами такого подхода к изучению групп являются: исследование Миллера и Морено ([1]), посвященное конечным неабелевым группам, все истинные подгруппы которых абелевы, и исследование О. Ю. Шмидта ([2]), посвященное конечным ненильпотентным группам, все истинные подгруппы которых нильпотентны. Описание строения групп Миллера и Морено и групп Шмидта (последние также называют группами типа $S$) до выделения образующих элементов и указания определяющих соотношений довел Редеи ([3, 4]). Все истинные подгруппы групп Шмидта нильпотентны и, значит, разлагаются в прямые произведения своих силовских $p$-подгрупп. Понятно, что, налагая на истинные подгруппы условие разложимости в то или иное (вообще говоря, уже непрямое) произведение своих силовских $p$-подгрупп, можно получить те или иные расширения класса групп Шмидта.

Здесь можно воспользоваться, в частности, введенными С. Н. Черниковым разложениями в равномерные произведения (т. е. в произведения, в которых попарно перестановочны циклические подгруппы любых двух различных множителей), поставившим в свое время задачу изучения периодических групп, разложимых в равномерное произведение своих силовских $p$-подгрупп. Этой задаче посвящена статья В. П. Шункова ([5]).

Настоящая статья посвящена вопросу, предложенному автору С. Н. Черниковым, о строении конечных групп, неразложимых в равномерное произведение своих силовских $p$-подгрупп, при условии разложимости всех их истинных подгрупп в произведения такого рода. Краткости ради такие группы назовем группами типа $CS$, или, короче, $CS$-группами. В силу сформулированного здесь определения, в класс $CS$-групп попадут все группы Шмидта, за исключением тех из них, которые разложимы в равномерное произведение своих силовских $p$-подгрупп. Нетрудно убедиться, что группы Шмидта такого рода исчерпываются группами порядков $pq^n$ с образующими элементами $A$ и $B$ и определяющими соотношениями:

$$A^p = B^{q^n} = 1, \quad B^{-1}AB = A^s, \quad \text{где } s^q \equiv 1 \pmod p,$$
$$B^{-q}A^{-1}B^qA = 1.$$

Изучение групп типа $CS$ доведено автором до выделения образующих элементов и указания определяющих соотношений (см. теоремы 3 и 4).

1°. Пусть $\mathfrak{H}$ — некоторая группа (в мультипликативной записи), $\mathfrak{R}$ — некоторое кольцо с единицей и $\varphi$ — фиксированный мультипликативный гомоморфизм $\mathfrak{H}$ в $\mathfrak{R}$:

$$(\alpha\cdot\beta)\varphi = \alpha\varphi\cdot\beta\varphi \quad (\alpha \in \mathfrak{H},\ \alpha\varphi \in \mathfrak{R}). \tag{1}$$

Очевидно, один мультипликативный гомоморфизм всегда существует — это тривиальный гомоморфизм, отображающий любой элемент $\alpha$ из $\mathfrak{H}$ в единицу кольца $\mathfrak{R}$. При таких обозначениях имеет место следующее установленное Редеи ([3]) предложение.

(*) Множество всех пар $(\alpha, a)$ $(\alpha \in \mathfrak{H},\ a \in \mathfrak{R})$ образует относительно умножения

$$(\alpha, a)(\beta, b) = (\alpha \cdot \beta, a + \alpha\varphi \cdot b) \tag{2}$$

группу. Эта группа называется к о с ы м  п р о и з в е д е н и е м $\mathfrak{H}\mathfrak{R}$ п е р в о г о  р о д а. Ниже такого рода произведение устанавливается для определенным образом связанных между собой циклической группы $\mathfrak{H}$ и конечного кольца $\mathfrak{R}$.

Пусть $p$ и $q$ — два различных простых числа, $m$ — какое-нибудь натуральное число, $u_m$ — наименьшее натуральное число, для которого $p^{u_m} \equiv 1 \pmod{q^m}$, $\mathfrak{H}(q^m)$ — циклическая группа порядка $q^m$, $K(p^u)$ — конечное поле из $p^u$-элементов и $K^*(p^u)$ — его мультипликативная группа (циклическая порядка $p^u - 1$).

Л е м м а 1. *Пусть $\alpha$ — образующий элемент циклической группы $\mathfrak{H} = \mathfrak{H}(q^m)$ и $r$ — элемент порядка $q^m$ мультипликативной группы $K^*(p^{u_m})$ конечного поля $K(p^{u_m})$, связанного указанным образом с группой $\mathfrak{H} = \mathfrak{H}(q^m)$. Тогда существует нетривиальное косое произведение первого рода $\mathfrak{G}_1 = \mathfrak{H}\mathfrak{R}$ — группа, которая является множеством пар вида $(\alpha^i, a)$ $(i = 0, 1, \ldots, q^m - 1)$, где $a \in K(p^{u_m})$, перемножаемых по правилу*

$$(\alpha^i, a)(\alpha^k, b) = (\alpha^{i+k}, a + r^i \cdot b), \tag{3}$$

*отвечающая мультипликативному гомоморфизму $\varphi$: $\alpha\varphi = r$.*

Это предложение непосредственно вытекает из предложения (*).

Л е м м а 2. *Пусть $\Psi(x)$ — неприводимый многочлен из разложения многочлена $(x^{q^m} - 1) / (x^{q^{m-1}} - 1)$ на неприводимые множители над полем $K(p)$. Пусть $M$ — множество всевозможных пар $(i, f(x))$, где $i$ — целое число и $f(x)$ — многочлен с коэффициентами из поля $K(p)$, из которых любые две различные удовлетворяют условию*:

$$\text{либо } i \not\equiv k \pmod{q^m}, \quad \text{либо } f(x) \not\equiv g(x) \pmod{\Psi(x)}. \tag{4}$$

*Тогда относительно умножения, определяемого правилом*

$$(i, f(x))(k, g(x)) = (i + k, f(x) + x^i g(x)), \tag{5}$$

*множество $M$ образует группу $\mathfrak{G}_2$, и эта группа изоморфна группе $\mathfrak{G}_1 = \mathfrak{H}\mathfrak{R}$ леммы* 1.

Если обозначить через $\overline{K(p)[x]}$ поле классов кольца многочленов с коэффициентами из поля $K(p)$ по $\operatorname{mod} \Psi(x)$, то отмечаемый здесь изоморфизм между $\mathfrak{G}_1$ и $\mathfrak{G}_2$ можно описать как соответствие, сопоставляющее произвольному элементу $(\alpha^i, a)$ из $\mathfrak{G}_1$ тот элемент $(i, f(x))$ из $\mathfrak{G}_2$, для которого $a$ и $\overline{f(x)}$ — отвечающие один другому элементы изоморфных полей $K(p^{u_m})$ и $\overline{K(p)[x]}$.

Л е м м а 3. *Пусть неприводимый многочлен $\Psi(x)$ (см. лемму 2) имеет вид*

$$\Psi(x) = x^{u_m} - c_{u_m - 1} x^{u_m - 1} - \ldots - c_0. \tag{6}$$

*Тогда группа $\mathfrak{G}_2$ леммы 2 (а следовательно, и группа $\mathfrak{G}_1$) изоморфна абстрактной группе $\mathfrak{G}_3$ с образующими элементами $P_0, P_1, \ldots, P_{u_m - 1}, Q$ и определяющими соотношениями*:

$$\begin{gathered}
P_0^p = P_1^p = \ldots = P_{u_m-1}^p = Q^{q^m} = 1, \\
P_i P_j = P_j P_i, \\
Q^{-1} P_i Q = P_{i+1} \quad (i = 0, 1, \ldots, u_m - 2), \\
Q^{-1} P_{u_m-1} Q = P_1^{c_0} P_0^{c_1} \ldots P_{u_m-1}^{c_{u_m-1}}.
\end{gathered} \tag{7}$$

Один из изоморфизмов между группами $\mathfrak{G}_2$ и $\mathfrak{G}_3$ определяется соответствием

$$(0, x^i) \leftrightarrow P_i \quad (i = 0, 1, \ldots, u_m - 1),$$
$$(-1, 0) \leftrightarrow Q.$$

Леммы 1, 2 и 3 являются естественными обобщениями теорем 5, 6 и 7 из ([3]), и доказательства их повторяют доказательства соответствующих теорем.

Теорема 1. *Пусть $\tilde{\mathfrak{G}}$ — конечная группа, разложимая в полупрямое произведение $\tilde{\mathfrak{G}} = \mathfrak{P}\lambda\{Q\}$, где $\mathfrak{P}$ — элементарная абелева группа и $Q^{q^m} = 1$, причем ни одна отличная от единицы степень $Q^{q^k}$ не содержится в центре группы $\tilde{\mathfrak{G}}$. Тогда группа $\tilde{\mathfrak{G}}$ содержит подгруппу $\mathfrak{G}$, изоморфную косому произведению $\mathfrak{H}\mathfrak{R}$, где $\mathfrak{H} = \mathfrak{H}(q^m)$ — циклическая порядка $q^m$ и $\mathfrak{R} = K(p^{u_m})$.*

При доказательстве теоремы используется

Лемма 4. *Если $\tilde{\mathfrak{G}} = \mathfrak{P}\lambda\{Q\}$ — разложение группы $\tilde{\mathfrak{G}}$ из теоремы 1 и $Q^{q^i}$ — степень элемента $Q$ с показателем $q^i$ $(i = 0, 1, \ldots, q^m - 1)$, то для любого $i$ в множителе $\mathfrak{P}$ существует такая инвариантная в $\tilde{\mathfrak{G}}$ подгруппа $\mathfrak{P}_{q^i}$, что центр группы $\{\mathfrak{P}_{q^i}, Q\}$ равен единице.*

2⁰. Переходим теперь к рассмотрению $CS$-групп.

Теорема 2. *Всякая $CS$-группа $\mathfrak{G}$ имеет порядок вида $p^k q^l$, где $p$ и $q$ — различные простые числа, и является полупрямым произведением своих силовских подгрупп, неинвариантная из которых циклична.*

Лемма 5. *Фактор-группа $CS$-группы $\mathfrak{G}$ по подгруппе Фраттини $\Phi(\mathfrak{P})$ инвариантной силовской $p$-подгруппы сама является $CS$-группой.*

$CS$-группу $\mathfrak{G} = \mathfrak{P}\lambda\{Q\}$ с неинвариантной циклической силовской подгруппой $\{Q\}$, в которой ни одна отличная от единицы степень $Q^{q^k}$ элемента $Q$ не содержится в центре группы $\mathfrak{G}$, будем называть $\overline{CS}$-группой.

Теорема 3. *Группа $\mathfrak{G}$ с порядком, делящимся на простые числа $p$, $q$, и с элементарной абелевой силовской $p$-подгруппой тогда и только тогда является $CS$-группой, когда она имеет один из следующих трех типов.*

1. *$\mathfrak{G}$ — группа Миллера — Морено порядка $p^{u_1}q$, где $u_1 > 1$ — наименьшее натуральное число, для которого $p^{u_1} \equiv 1 \pmod q$.*

2. *$\mathfrak{G}$ — группа порядка $p^2 q^m$ с разложением $\mathfrak{G} = (\{P_1\} \times \{P_2\})\lambda\{Q\}$, где*

$$P_1^p = P_2^p = Q^{q^m} = 1,$$
$$Q^{-1}P_1Q = P_1^{h_1}, \quad Q^{-1}P_2Q = P_2^{h_2}, \tag{8}$$
$$h_1, h_2 \in K(p), \quad h_1 \neq h_2, \quad h_1^q = h_2^q,$$

*причем хотя бы одно из чисел $h_1$ и $h_2$ является первообразным корнем степени $q^m$ из единицы в простом поле $K(p)$. Число $m \geqslant 1$ здесь не превосходит наибольшего показателя $n$ степени $q$, делящей $p - 1$.*

3. *$\mathfrak{G}$ — группа порядка $p^q q^{n+1}$, где $n \geqslant 1$ — наибольший показатель степени числа $q$, делящей $p - 1$, причем образующие элементы $P_0, P_1, \ldots, P_{q-1}, Q$ группы $\mathfrak{G}$ удовлетворяют соотношениям:*

$$P_0^p = P_1^p = \ldots = P_{q-1}^p = Q^{q^{n+1}} = 1,$$
$$Q^{-1}P_iQ = P_{i+1} \quad (i = 0, 1, \ldots, q - 2), \tag{9}$$
$$Q^{-1}P_{q-1}Q = P_0^h,$$

*где $h$ — первообразный корень степени $q^n$ из единицы в $K(p)$.*

Назовем группы типов 1, 2 и 3 соответственно $\overline{CS}_1$-, $\overline{CS}_2$- и $\overline{CS}_3$-группами. Существование $\overline{CS}$-группы с заданными простыми делителями ее порядка устанавливается ниже в теореме 5.

Теорема 4. *Если фактор-группа* $\mathfrak{G}/\Phi(\mathfrak{P})$ $\overline{CS}$*-группы* $\mathfrak{G}$ *по подгруппе Фраттини* $\Phi(\mathfrak{P})$ *инвариантной силовской* $p$*-подгруппы* $\mathfrak{P}$ *и* $\mathfrak{G}$ *является* $\overline{CS}_2$*- или* $\overline{CS}_3$*-группой, то* $\Phi(\mathfrak{P}) = 1$, *а потому сама группа* $\mathfrak{G}$ *будет* $\overline{CS}_2$*- или* $\overline{CS}_3$*-группой. Если же фактор-группа* $\mathfrak{G}/\Phi(\mathfrak{P})$ *является* $CS_1$*-группой, то* $\mathfrak{G}$ *является группой типа* $S$.

Теорема 5. *Для произвольной пары различных простых чисел* $p$ *и* $q$ *существуют* $\overline{CS}$*-группы с циклической неинвариантной силовской* $q$*-подгруппой* ($p$*-подгруппой*). *Все* $\overline{CS}$*-группы порядка* $p^\alpha q^\beta$ *исчерпываются либо группами типа* $S$ ($\overline{CS}_1$*-группами*), *либо группами типов* $\overline{CS}_2$ и $\overline{CS}_3$.

Примечание. Каждая $CS$-группа является полупрямым произведением $\mathfrak{G} = \mathfrak{P}\lambda\mathfrak{Q}$ своих силовских $p$- и $q$-подгрупп $\mathfrak{P}$ и $\mathfrak{Q}$, вторая (неинвариантная) из которых — циклическая. Пусть $\mathfrak{Q} = \{Q\}$ и $Q^{q^m} = 1$. Возьмем натуральные числа $k$ и $m_1 = k + m$ и заменим в определяющих соотношениях группы $\mathfrak{G}$ элемент $Q$ элементом $Q_1 (Q_1^{q^{m_1}} = 1)$ и введем дополнительные соотношения, требующие перестановочности элемента $Q_1{}^{q^m}$ с каждым элементом из $\mathfrak{P}$. Тогда группа $\mathfrak{G}$ перейдет в группу $\mathfrak{G}_1 = \mathfrak{P}\lambda\{Q_1\}$, удовлетворяя условию $\mathfrak{G}1 / \{Q_1^{q^m}\} \cong \mathfrak{G}$. Отправляясь от первоначальной $\overline{CS}$-группы $\mathfrak{G}$ порядка $p^l q^m$, получим на этом пути бесконечную серию $CS$-групп с порядками $p^l q^{k+m}$ $(k \geqslant 0)$. Если группа $\mathfrak{G}$ была группой типа $\overline{CS}_i$ $(i = 1, 2, 3)$, то произвольную группу из соответствующей ей серии будем называть $CS_i$-группой. Совокупностью групп такого рода исчерпываются все $CS$-группы с порядками, делящимися на взятые простые числа $p$ и $q$ с инвариантной силовской $p$-подгруппой.

Следствие. *$CS$-группы, не являющиеся группами типа* $S$, *исчерпываются* $CS_2$*- и* $CS_3$*-группами.*

Институт математики
Академии наук УССР
Киев

Поступило
12 VI 1969

ЦИТИРОВАННАЯ ЛИТЕРАТУРА

[1] G. Miller, H. Moreno, Trans. Am. Math. Soc.. **4**, 388 (1903). [2] О. Ю. Шмидт, Матем. сборн., **31**, 366 (1924). [3] L. Redei, Comm. Math. Helv., **20**, 225 (1947). [4] L. Redei, Public. Math., 4, 303 (1956). [5] В. П. Шунков, ДАН, **154**, 542 (1964).