

GROUPS OF TYPE $\backslash(CS\backslash)$

E. I. Shatylo

1970

SovietRxiv

View the original and related papers at <https://sovietrxiv.org/items/ru-197001.79322>

Source: Math-Net.Ru and CyberLeninka. Machine translation. Verify with the original.

Abstract

Full Text

UDC 519.44

MATHEMATICS

E. I. SHATYLO

GROUPS OF TYPE CS

(Presented by Academician V. I. Glushkov, 24 VI 1969)

The imposition of one or another restriction on one or another system of subgroups of an arbitrary group often leads to classes of groups whose structure can be described by specifying generators and defining relations. Classical examples of such an approach to the study of groups are the investigation of Miller and Moreno ⁽¹⁾, devoted to finite nonabelian groups all of whose proper subgroups are abelian, and the investigation of O. Yu. Schmidt ⁽²⁾, devoted to finite non-nilpotent groups all of whose proper subgroups are nilpotent. A description of the structure of Miller-Moreno groups and Schmidt groups (the latter are also called groups of type S) down to specifying generators and defining relations was obtained by Redei ^(3,4). All proper subgroups of Schmidt groups are nilpotent and, consequently, decompose into direct products of their Sylow p -subgroups. It is clear that, by imposing on the proper subgroups the condition of decomposability into one or another (generally speaking, no longer direct) product of their Sylow p -subgroups, one can obtain various extensions of the class of Schmidt groups.

Here one may use, in particular, the decompositions introduced by S. N. Chernikov into *uniform products* (i.e., into products in which the cyclic subgroups generated pairwise by any two distinct factors are permutable), who at one time posed the problem of studying periodic groups decomposable into a uniform product of their Sylow p -subgroups. An article by V. P. Shunkov ⁽⁵⁾ is devoted to this problem.

The present article is devoted to a question proposed to the author by S. N. Chernikov, concerning the structure of finite groups not decomposable into a uniform product of their Sylow p -subgroups, under the condition that all their proper subgroups are decomposable into products of this kind. For brevity, let us call such groups *groups of type CS* , or, more shortly, CS -groups. By virtue of the definition formulated here, the class of CS -groups includes all Schmidt groups, except for those among them which decompose into a uniform product of their Sylow p -subgroups. It is not difficult to verify that Schmidt groups of this kind are exhausted by groups of orders pq^n with generators A and B and defining relations:

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

The study of groups of type CS has been carried by the author to the specification of generators and defining relations (see Theorems 3 and 4).

1°. Let $\mathfrak{H}$ be some group (in multiplicative notation), $\mathfrak{R}$ some ring with identity, and φ a fixed multiplicative homomorphism from $\mathfrak{H}$ into $\mathfrak{R}$:

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

Obviously, one multiplicative homomorphism always exists—it is the trivial homomorphism, mapping any element α of $\mathfrak{H}$ to the identity of the ring $\mathfrak{R}$. With this notation, the following proposition, established by Rédei ⁽³⁾, holds.

(*) The set of all pairs (α, a) ($\alpha \in \mathfrak{H}$, $a \in \mathfrak{R}$) forms, with respect to multiplication

$$(\alpha, a)(\beta, b) = (\alpha \cdot \beta, a + \alpha\varphi \cdot b), \quad (2)$$

a group. This group is called the skew product $\mathfrak{H}\mathfrak{R}$ of the first kind. Below, such a product is established for a cyclic group $\mathfrak{H}$ and a finite ring $\mathfrak{R}$ related to one another in a definite way.

Let p and q be two distinct prime numbers, m some natural number, u_m the least natural number for which $p^{u_m} \equiv 1 \pmod{q^m}$, $\mathfrak{H}(q^m)$ a cyclic group of order q^m , $K(p^u)$ a finite field with p^u elements, and $K^*(p^u)$ its multiplicative group (cyclic of order $p^u - 1$).

Lemma 1. Let α be a generating element of the cyclic group $\mathfrak{H} = \mathfrak{H}(q^m)$, and let r be an element of order q^m of the multiplicative group $K^*(p^{u_m})$ of the finite field $K(p^{u_m})$, related in the indicated way to the group $\mathfrak{H} = \mathfrak{H}(q^m)$. Then there exists a nontrivial skew product of the first kind $\mathfrak{G}_1 = \mathfrak{H}\mathfrak{R}$ —a group that is the set of pairs of the form (α^i, a) ($i = 0, 1, \dots, q^m - 1$), where $a \in K(p^{u_m})$, multiplied according to the rule

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

corresponding to the multiplicative homomorphism $\varphi : \alpha\varphi = r$.

This proposition follows directly from proposition (*).

Lemma 2. Let $\Psi(x)$ be an irreducible polynomial from the factorization of the polynomial $(x^{q^m} - 1)/(x^{q^{m-1}} - 1)$ into irreducible factors over the field $K(p)$. Let M be the set of all possible pairs $(i, f(x))$, where i is an integer and $f(x)$ is

a polynomial with coefficients in the field $K(p)$, of which any two distinct ones satisfy the condition:

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

Then, with respect to multiplication defined by the rule

$$(i, f(x))(k, g(x)) = (i + k, f(x) + x^i g(x)), \quad (5)$$

the set M forms a group $\mathfrak{G}_2$, and this group is isomorphic to the group $\mathfrak{G}_1 = \mathfrak{H}\mathfrak{R}$ of Lemma 1.

If one denotes by $\overline{K(p)[x]}$ the field of residue classes of the polynomial ring with coefficients in the field $K(p)$ modulo $\Psi(x)$, then the isomorphism between $\mathfrak{G}_1$ and $\mathfrak{G}_2$ noted here may be described as the correspondence that assigns to an arbitrary element (α^i, a) of $\mathfrak{G}_1$ that element $(i, f(x))$ of $\mathfrak{G}_2$ for which a and $f(x)$ are corresponding elements of the isomorphic fields $K(p^{u_m})$ and $\overline{K(p)[x]}$.

Lemma 3. Let the irreducible polynomial $\Psi(x)$ (see Lemma 2) have the form

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

Then the group $\mathfrak{G}_2$ of Lemma 2 (and consequently also the group $\mathfrak{G}_1$) is isomorphic to the abstract group $\mathfrak{G}_3$ with generating elements $P_0, P_1, \dots, P_{u_m-1}, Q$ and defining relations:

$$P_0^p = P_1^p = \dots = P_{u_m-1}^p = Q^{q^m} = 1,$$

$$P_i P_j = P_j P_i,$$

$$Q^{-1} P_i Q = P_{i+1} \quad (i = 0, 1, \dots, u_m - 2),$$

$$Q^{-1} P_{u_m-1} Q = P_1^{c_0} P_0^{c_1} \dots P_{u_m-1}^{c_{u_m-1}}. \quad (7)$$

One of the isomorphisms between the groups $\mathfrak{G}_2$ and $\mathfrak{G}_3$ is determined by the correspondence

$$(0, \alpha^i) \leftrightarrow P_i \quad (i = 0, 1, \dots, u_m - 1),$$

$$(-1, 0) \leftrightarrow Q.$$

Lemmas 1, 2, and 3 are natural generalizations of Theorems 5, 6, and 7 from (3), and their proofs repeat the proofs of the corresponding theorems.

Theorem 1. Let $\mathfrak{G}$ be a finite group decomposable into the semidirect product $\mathfrak{G} = \mathfrak{P}\lambda\{Q\}$, where $\mathfrak{P}$ is an elementary abelian group and $Q^{q^m} = 1$, and no power Q^{q^k} different from the identity is contained in the center of the group $\mathfrak{G}$. Then the group $\mathfrak{G}$ contains a subgroup $\mathfrak{H}$, isomorphic to the wreath product $\mathfrak{H}\mathfrak{A}$, where $\mathfrak{H} = \mathfrak{H}(q^m)$ is cyclic of order q^m and $\mathfrak{A} = K(p^{u_m})$.

In the proof of the theorem the following is used.

Lemma 4. If $\mathfrak{G} = \mathfrak{P}\lambda\{Q\}$ is the decomposition of the group $\mathfrak{G}$ from Theorem 1 and Q^i is a power of the element Q with exponent q^i ($i = 0, 1, \dots, q^m - 1$), then for any i there exists in the set $\mathfrak{P}$ an invariant subgroup $\overline{\mathfrak{P}}_{q^i}$ in $\mathfrak{G}$ such that the center of the group $\{\overline{\mathfrak{P}}_{q^i}, Q\}$ is equal to the identity.

2°. We proceed to the consideration of CS -groups.

Theorem 2. Every CS -group $\mathfrak{G}$ has order of the form $p^k q^l$, where p and q are distinct prime numbers, and is a semidirect product of its Sylow subgroups, the non-invariant one of which is cyclic.

Lemma 5. The factor group of a CS -group $\mathfrak{G}$ by the Frattini subgroup $\Phi(\mathfrak{P})$ of an invariant Sylow p -subgroup is itself a CS -group.

A CS -group $\mathfrak{G} = \mathfrak{P}\lambda\{Q\}$ with a non-invariant cyclic Sylow subgroup $\{Q\}$, in which no power Q^{q^k} of the element Q different from the identity is contained in the center of the group $\mathfrak{G}$, will be called a $\overline{CS}$ -group.

Theorem 3. A group $\mathfrak{G}$ of order divisible by the primes p, q , and with an elementary abelian Sylow p -subgroup is a $\overline{CS}$ -group if and only if it has one of the following three types.

1. $\mathfrak{G}$ is a Miller-Moreno group of order $p^{u_1} q$, where $u_1 > 1$ is the least natural number for which $p^{u_1} \equiv 1 \pmod{q}$.
2. $\mathfrak{G}$ is a group of order $p^2 q^m$ with decomposition $\mathfrak{G} = (\{P_1\} \times \{P_2\})\lambda\{Q\}$, where

$$P_1^p = P_2^p = Q^{q^m} = 1,$$

$$Q^{-1}P_1Q = P_1^{h_1}, \quad Q^{-1}P_2Q = P_2^{h_2}, \quad (8)$$

$$h_1, h_2 \in K(p), \quad h_1 \neq h_2, \quad h_1^q = h_2^q,$$

and at least one of the numbers h_1 and h_2 is a primitive root of degree q^m from unity in the prime field $K(p)$. The number $m \geq 1$ here does not exceed the greatest exponent n of the power of q dividing $p - 1$.

3. $\mathfrak{G}$ is a group of order $p^q q^{n+1}$, where $n \geq 1$ is the greatest exponent of the power of the number q dividing $p-1$, and the generating elements $P_0, P_1, \dots, P_{q-1}, Q$ of the group $\mathfrak{G}$ satisfy the relations:

$$P_0^p = P_1^p = \dots = P_{q-1}^p = Q^{q^{n+1}} = 1,$$

$$Q^{-1}P_iQ = P_{i+1} \quad (i = 0, 1, \dots, q-2), \quad (9)$$

$$Q^{-1}P_{q-1}Q = P_0^h,$$

where h is a primitive root of degree q^n from unity in $K(p)$.

We shall call groups of types 1, 2, and 3 respectively $\overline{CS}_1$ -, $\overline{CS}_2$ -, and $\overline{CS}_3$ -groups. The existence of a $\overline{CS}$ -group with prescribed prime divisors of its order is established below in Theorem 5.

Theorem 4. If the factor group $\mathfrak{G}/\Phi(\mathfrak{P})$ of a $\overline{CS}$ -group $\mathfrak{G}$ by the Frattini subgroup $\Phi(\mathfrak{P})$ of an invariant Sylow p -subgroup $\mathfrak{P}$, and $\mathfrak{G}$, is a $\overline{CS}_2$ - or $\overline{CS}_3$ -group, then $\Phi(\mathfrak{P}) = 1$, and therefore the group $\mathfrak{G}$ itself will be a $\overline{CS}_2$ - or $\overline{CS}_3$ -group. If, however, the factor group $\mathfrak{G}/\Phi(\mathfrak{P})$ is a $\overline{CS}_1$ -group, then $\mathfrak{G}$ is a group of type S .

Theorem 5. For an arbitrary pair of distinct primes p and q there exist $\overline{CS}$ -groups with a cyclic noninvariant Sylow q -subgroup (p -subgroup). All $\overline{CS}$ -groups of order $p^\alpha q^\beta$ are exhausted either by groups of type S ($\overline{CS}_1$ -groups), or by groups of types $\overline{CS}_2$ and $\overline{CS}_3$.

Remark. Every $\overline{CS}$ -group is a semidirect product $\mathfrak{G} = \mathfrak{P}\lambda\Omega$ of its Sylow p - and q -subgroups $\mathfrak{P}$ and Ω , the second (noninvariant) of which is cyclic. Let $\Omega = \{Q\}$ and $Q^{q^m} = 1$. Take natural numbers k and $m_1 = k + m$, and in the defining relations of the group $\mathfrak{G}$ replace the element Q by the element Q_1 ($Q_1^{q^{m_1}} = 1$), and introduce additional relations requiring the commutativity of the element $Q_1^{q^m}$ with every element of $\mathfrak{P}$. Then the group $\mathfrak{G}$ will pass into the group

$$\mathfrak{G}_1 = \mathfrak{P}\lambda\{Q_1\},$$

satisfying the condition

$$\mathfrak{G}_1/\{Q_1^{q^m}\} \cong \mathfrak{G}.$$

Starting from an initial $\overline{CS}$ -group $\mathfrak{G}$ of order $p^l q^m$, we obtain in this way an infinite series of $\overline{CS}$ -groups with orders $p^l q^{k+m}$ ($k \geq 0$). If the group $\mathfrak{G}$ was a group of type $\overline{CS}_i$ ($i = 1, 2, 3$), then an arbitrary group from the corresponding series will be called a $\overline{CS}_i$ -group. The totality of groups of this kind exhausts all $\overline{CS}$ -groups with orders divisible by the chosen primes p and q and with an invariant Sylow p -subgroup.

Corollary. CS -groups that are not groups of type S are exhausted by CS_2 - and CS_3 -groups.

Institute of Mathematics
Academy of Sciences of the Ukrainian SSR
Kiev

Received
12 VI 1969

REFERENCES

1. G. Miller, H. Moreno, Trans. Am. Math. Soc., **4**, 388 (1903).
2. O. Yu. Shmidt, Matem. sborn., **31**, 366 (1924).
3. L. Redei, Comm. Math. Helv., **20**, 225 (1947).
4. L. Redei, Public. Math., **4**, 303 (1956).
5. V. P. Shunkov, DAN, **154**, 542 (1964).

Note: Figure translations are in progress. See original paper for figures.

Source: Math-Net.Ru and CyberLeninka. Machine translation. Verify with the original.