A GENERALIZATION OF POST' S THEOREM

MATHEMATICS

1970

SovietRxiv

Abstract

Full Text

UDC 519.44

MATHEMATICS

S. A. RUSAKOV

A GENERALIZATION OF POST' S THEOREM

(Presented by Academician V. M. Glushkov on 29 I 1970)

§ 1. As is known, Lagrange's theorem for finite n-groups is in general irreversible already for $n = 2$. Therefore it is very important to find those classes of finite n-groups for which the converse of Lagrange' s theorem holds at least for a certain kind of divisor of the order of the n-group.

In the present paper we study the "saturation"of Abelian n-groups (see Definition 3) by subgroups; the results obtained by us generalize a well-known result of E. Post ([2], p. 284) on the existence of subgroups in cyclic n-groups, expressed by the following theorem:

Let $\mathfrak{G}$ be a cyclic n-group of order $g = rs$, where r is the largest divisor of g relatively prime to $n-1$. Then $\mathfrak{G}$ has at least one element and exactly one subgroup of those and only those orders γ for which $\gamma = \delta s$, where δ is an arbitrary divisor of r.

§ 2. We give the definitions and notation used in the paper.

Let $\mathfrak{G}$ be a set on which an n-ary operation σ_n is defined ([1], p. 5), where $n \geq 2$ is the arity of the operation, and let $\sigma_n(x_1 x_2 \dots x_n)$ be the value of the n-ary operation σ_n applied to the elements $x_1, x_2, \dots, x_n$ of $\mathfrak{G}$. Then we have

Definition 1 (cf. ([3], p. 158; ([2], p. 213). The set $\mathfrak{G}$ is called an n-**group** if the following postulates are satisfied:

1. The operation σ_n is associative, i.e., for any elements $x_1, x_2, \dots, x_n, x_{n+1}, \dots, x_{2n-1}$ of $\mathfrak{G}$ the equality

   $$\sigma_n(\sigma_n(x_1 x_2 \dots x_n) x_{n+1} \dots x_{2n-1}) = \sigma_n(x_1 x_2 \dots x_j \sigma_n(x_{j+1} \dots x_{j+n}) \dots x_{2n-1}),$$

   where $j = 1, 2, \dots, n-1$, holds.

2. The law of single-valued and unrestricted invertibility holds, i.e., for any elements $a_1, a_2, \dots, a_{i-1}, a_{i+1}, \dots, a_n, a$ belonging to $\mathfrak{G}$, each of the equations

   $$\sigma_n(a_1 a_2 \dots a_{i-1} x_i a_{i+1} \dots a_n) = a \quad (i = 1, 2, \dots, n)$$

   is always solvable in $\mathfrak{G}$ with respect to x_i, and uniquely.

The concept of a subgroup for n-groups with $n > 2$ is introduced in the same way as for $n = 2$.

We shall denote the cardinality of any set $\mathfrak{S}$ (in particular, of an n-group $\mathfrak{G}$) by $|\mathfrak{S}|$. If $\mathfrak{S} = \mathfrak{G}$, then $|\mathfrak{G}|$ will be called the order of the n-group $\mathfrak{G}$. If $|\mathfrak{G}|$ is finite, the n-group $\mathfrak{G}$ is also called finite.

Let Γ be the set of all nonempty subsets composed of elements of the n-group $\mathfrak{G}$. On this set we define an n-ary operation ω_n in the following way. Let $\mathfrak{M}_i \in \Gamma$ $(i = 1, 2, \dots, n)$. Then by

$$\omega_n(\mathfrak{M}_1 \mathfrak{M}_2 \dots \mathfrak{M}_n)$$

we shall understand the set of all elements of $\mathfrak{G}$, each of which is equal to $\sigma_n(m_1 m_2 \dots m_n)$, where $m_i \in \mathfrak{M}_i$ and m_i takes an arbitrary value from $\mathfrak{M}_i$. It is clear that some of $\mathfrak{M}_1, \mathfrak{M}_2, \dots, \mathfrak{M}_n$, or possibly all of them, may consist of a single element. If $\mathfrak{M}_i = \{m_i\}$ $(i = 1, 2, \dots, n)$, then obviously

$$\omega_n(m_1 m_2 \dots m_n) = \sigma_n(m_1 m_2 \dots m_n).$$

Definition 2 ([3], p. 165). A subgroup $\mathfrak{H}$ of an n-group $\mathfrak{G}$ is called **invariant** in $\mathfrak{G}$ if, for any element $x \in \mathfrak{G}$, the equality

$$\omega_n(x\mathfrak{H} \dots \mathfrak{H}) = \omega_n(\underbrace{\mathfrak{H} \dots \mathfrak{H}}_{i-1} x \underbrace{\mathfrak{H} \dots \mathfrak{H}}_{n-i}) \quad (i = 2, \dots, n)$$

holds. If

$$\omega_n(x\mathfrak{H} \dots \mathfrak{H}) = \omega_n(\mathfrak{H} \dots \mathfrak{H}x),$$

then $\mathfrak{H}$ is called a **semi-invariant** subgroup of the n-group $\mathfrak{G}$.

Definition 3 (cf. [2]), p. 217). An n-group $\mathfrak{G}$ will be called **Abelian** if, for any elements $x_1, x_2, \dots, x_n$ of $\mathfrak{G}$, the value $\sigma_n(x_1 x_2 \dots x_n)$ does not change under any permutation of these elements.

§ 3. We shall also need the following theorems.

Theorem 1 (cf. [3]), p. 163). Let $\mathfrak{H}$ be some subgroup of an arbitrary n-group $\mathfrak{G}$, and let $a_1, a_2, \dots, a_{k-1}, a_{k+l}, \dots, a_n$ be fixed elements of the n-group $\mathfrak{G}$, where $k \geqslant 1$, $l \geqslant 1$. If in

$$\omega_n(a_1 a_2 \dots a_{k-1} \underbrace{\mathfrak{H} \dots \mathfrak{H}}_{l} a_{k+l} \dots a_n)$$

one of the elements a_i $(i = 1, 2, \dots, k-1, k+l, \dots, n)$ is replaced by the variable element x, then, for distinct x, two such obtained subsets of the n-group $\mathfrak{G}$ either coincide or have not a single common element; such subsets have the same cardinality and, taken together, exhaust the entire n-group $\mathfrak{G}$. If, moreover, $\mathfrak{G}$ is finite, then the cardinality of each such subset is equal to $|\mathfrak{H}|$.

Theorem 2 ([3], p. 165). If $\mathfrak{H}$ is a semi-invariant subgroup for an n-group $\mathfrak{G}$, then all subsets of the n-group $\mathfrak{G}$ of the form $\omega_n(x\mathfrak{H}\dots\mathfrak{H})$ form an n-group with respect to the operation ω_n.

We shall call such an n-group the factor group for $\mathfrak{G}$ with respect to $\mathfrak{H}$, and denote it by $\mathfrak{G}/\mathfrak{H}$. In what follows we shall consider only finite n-groups.

§ 4. We now state the results obtained by us.

Theorem 3. A nonempty subset $\mathfrak{H}$ of a finite n-group $\mathfrak{G}$ is an n-subgroup if and only if $\mathfrak{H}$ is a subset on which the n-ary operation σ_n is defined.

The proof is carried out by the same method as for $n = 2$.

Theorem 4. Let the factor group $\mathfrak{G}/\mathfrak{N}$ for a finite n-group $\mathfrak{G}$ with respect to $\mathfrak{N}$ possess some subgroup $\mathfrak{B}$. Then $\mathfrak{G}$ contains such a subgroup $\mathfrak{B}$ that $|\mathfrak{B}| = |\mathfrak{N}|\,|\overline{\mathfrak{B}}|$.

Proof. On the basis of Theorem 1, the n-group $\mathfrak{G}$ can be represented as

$$\mathfrak{G} = \omega_n(x_1\mathfrak{N}\dots\mathfrak{N}) + \omega_n(x_2\mathfrak{N}\dots\mathfrak{N}) + \dots + \omega_n(x_\rho\mathfrak{N}\dots\mathfrak{N}), \tag{1}$$

where $|\omega_n(x_i\mathfrak{N}\dots\mathfrak{N})| = |\mathfrak{N}|$, $i = 1, 2, \dots, \rho$. Now considering in (1) each summand as a separate element, we obtain, by Theorem 2, the factor group $\mathfrak{G}/\mathfrak{N}$. Since $\overline{\mathfrak{B}} \subseteq \mathfrak{G}/\mathfrak{N}$, we have

$$\overline{\mathfrak{B}} = \omega_n(y_1\mathfrak{N}\dots\mathfrak{N}) + \omega_n(y_2\mathfrak{N}\dots\mathfrak{N}) + \dots + \omega_n(y_\tau\mathfrak{N}\dots\mathfrak{N}), \tag{2}$$

where $y_1, y_2, \dots, y_\tau$ are among $x_1, x_2, \dots, x_\rho$, and $\tau = |\overline{\mathfrak{B}}|$.

Let now $\mathfrak{B}$ be the collection of all elements of the n-group $\mathfrak{G}$ of the form $\sigma_n(y_j v_1 \dots v_{n-1})$, where $j = 1, 2, \dots, \tau$ and $v_1, \dots, v_{n-1}$ are arbitrary elements of $\mathfrak{N}$. Then it is obvious that

$$\sigma_n(y_j v_1 \dots v_{n-1}) \in \omega_n(y_j\mathfrak{N}\dots\mathfrak{N}). \tag{3}$$

Let us show that $\mathfrak{B}$ is a subgroup of the n-group $\mathfrak{G}$. Indeed, let

$$\sigma_n(z_1 v_1' \dots v_{n-1}'), \quad \sigma_n(z_2 v_1'' \dots v_{n-1}''), \quad \dots, \quad \sigma_n(z_n v_1^{(n)} \dots v_{n-1}^{(n)})$$

be arbitrary elements of $\mathfrak{B}$, where $z_1, z_2, \dots, z_n$ are among the elements $y_1, y_2, \dots, y_\tau$. Then, taking equality (3) into account, we obtain

$$\sigma_n(\sigma_n(z_1 v_1' \dots v_{n-1}'), \sigma_n(z_2 v_1'' \dots v_{n-1}''), \dots, \sigma_n(z_n v_1^{(n)} \dots v_{n-1}^{(n)})) = z \in \mathfrak{N} =$$

$$= \omega_n(\omega_n(z_1\mathfrak{N}\dots\mathfrak{N})\omega_n(z_2\mathfrak{N}\dots\mathfrak{N})\dots\omega_n(z_n\mathfrak{N}\dots\mathfrak{N})).$$

Since $\overline{\mathfrak{B}}$ is a subgroup of the factor group $\mathfrak{G}/\mathfrak{N}$, it follows that $\mathfrak{N} \in \overline{\mathfrak{B}}$, and, consequently, $\mathfrak{N} = \omega_n(y_\lambda \mathfrak{N} \dots \mathfrak{N})$ $(1 \leqslant \lambda \leqslant \tau)$. Hence $z \in \mathfrak{B}$, and by Theorem 3, $\mathfrak{B}$ will be a subgroup of the n-group $\mathfrak{G}$. Further, since each summand in (2) has $|\mathfrak{N}|$ elements from $\mathfrak{G}$ and these summands have no common elements, we have $|\mathfrak{B}| = |\mathfrak{N}|\tau = |\mathfrak{N}|\,|\overline{\mathfrak{B}}|$. The theorem is proved.

The definitions and notation we use, relating to the degree and order of an element of an n-group, can be found in ([2]), p. 282.

Theorem 5. *An Abelian n-group $\mathfrak{G}$ of order $g = rs$, where $(r, s) = 1$ and $(r, n-1) = 1$, has a subgroup of order δs, where δ is an arbitrary divisor of r.*

Proof. Suppose that the theorem is false. Then, among all Abelian n-groups satisfying the condition of the theorem, choose an n-group $\mathfrak{G}$ of least order g for which the theorem does not hold. Since for $g = 1$ the theorem holds, we have $g > 1$.

We shall subsequently consider the following possibilities:

1. In $\mathfrak{G}$ there is at least one element of first order. Let a be an element of first order of the n-group $\mathfrak{G}$, i.e. $\sigma_n(aa \dots a) = a$. Then the $(n-1)$-term sequence $\{a, a, \dots, a\}$ is the identity of the n-group $\mathfrak{G}$ (see ([2]), p. 214). On the set $\mathfrak{G}$ we define a binary operation σ_2 as follows:

$$\sigma_2(x_1 x_2) = x_1 x_2 = \sigma_n(x_1 x_2 a \dots a), \tag{4}$$

where x_1 and x_2 are arbitrary elements of $\mathfrak{G}$.

We shall show that with respect to this operation $\mathfrak{G}$ is a 2-group. Indeed, taking (4) into account, we have $(x_1 x_2)x_3 = \sigma_n(\sigma_n(x_1 x_2 a \dots a)x_3 a \dots a)$ and $x_1(x_2 x_3) = \sigma_n(x_1 \sigma_n(x_2 x_3 a \dots a)a \dots a)$, where x_1, x_2, and x_3 are arbitrary elements of $\mathfrak{G}$.

By postulate 1 of Definition 1 and taking into account that $\mathfrak{G}$ is an Abelian n-group, we obtain that

$$\sigma_n(\sigma_n(x_1 x_2 a \dots a)x_3 a \dots a) = \sigma_n(x_1 \sigma_n(x_2 x_3 a \dots a)a \dots a).$$

Therefore $(x_1 x_2)x_3 = x_1(x_2 x_3)$, i.e. associativity holds for the binary operation.

Since the equation $\sigma_n(x b_1 a \dots a) = b$ (b_1 and b are arbitrary elements of the n-group $\mathfrak{G}$) is always uniquely solvable in $\mathfrak{G}$ with respect to x, the equation $x b_1 = b$ is also uniquely solvable in $\mathfrak{G}$ with respect to x. The same assertion is valid for the equation $b_1 y = b$. Consequently, $\mathfrak{G}$ is a 2-group.

We now show that for any elements $x_1, x_2, \dots, x_n$ of $\mathfrak{G}$ the equality

$$x_1 x_2 \dots x_n = \sigma_n(x_1 x_2 \dots x_n) \tag{5}$$

holds.

Indeed, from equality (4) it follows that

$$\begin{aligned} x_1x_2x_3 \dots x_n &= (\dots((x_1x_2)x_3)\dots)x_{n-1})x_n \\ &= \sigma_n(\sigma_n(\dots(\sigma_n(\sigma_n(x_1x_2a\dots a)x_3a\dots a)\dots)x_{n-1}a\dots a)x_{na}\dots a) \\ &= \sigma_n(x_1x_2\underbrace{a\dots a}_{n-2}x_3\underbrace{a\dots a}_{n-2}\dots x_{n-1}\underbrace{a\dots a}_{n-2}x_n\underbrace{a\dots a}_{n-2}), \end{aligned}$$

and, as is easy to show, the number of all a' s occurring under the sign σ_n is $(n-1)(n-2)$. Since $\mathfrak{G}$ is an Abelian n-group, we have

$$x_1x_2\dots x_n = \sigma_n(x_1x_2\dots x_n\underbrace{a\dots a}_{(n-1)(n-2)}) = \sigma_n(x_1x_2\dots x_{na}\dots a\dots a\dots a).$$

Here the last displayed occurrence consists of two blocks of a' s, each containing $n-1$ terms:

$$\sigma_n(x_1x_2\dots x_n\underbrace{a\dots a}_{n-1}\dots\underbrace{a\dots a}_{n-1}).$$

Since the $(n-1)$-term sequence $\{a, a, \dots, a\}$ is the identity of the n-group $\mathfrak{G}$, it follows that $x_1x_2\dots x_n = \sigma_n(x_1x_2\dots x_n)$.

It is not difficult to show that the 2-group $\mathfrak{G}$ is also Abelian. Therefore $\mathfrak{G}$, as an Abelian 2-group of order $g = rs$, has a subgroup $\mathfrak{H}$ of order δs, where δ is an arbitrary divisor of r. We shall show that $\mathfrak{H}$ is a subgroup of the n-group $\mathfrak{G}$. Indeed, let $h_1, h_2, \dots, h_n$ be arbitrary elements of $\mathfrak{H}$. Then $h_1h_2\dots h_n \in \mathfrak{H}$. Hence, from equality (5) we conclude that $\sigma_n(h_1h_2\dots h_n) \in \mathfrak{H}$, i.e. by Theorem 3, $\mathfrak{H}$ is a subgroup of the n-group $\mathfrak{G}$. We have a contradiction.

2. The order of any element of the n-group $\mathfrak{G}$ is different from 1.

Let b be an arbitrary element of the n-group $\mathfrak{G}$, and let $\mathfrak{B}$ be the cyclic subgroup generated by this element. By Lagrange' s theorem for n-groups ([2], p. 222), $g_1 = |\mathfrak{B}|$ is a divisor of g. Since $(r, s) = 1$, we may write g_1 as follows: $g_1 = r_1s_1$, where r_1 and s_1 divide r and s, respectively. Then $(r_1, s_1) = 1$. Therefore $\mathfrak{B}$ contains an element, and consequently also a subgroup, of order s. Indeed, let us require that $(b^{[\theta]})^{[s_1]} = b^{[\theta]}$, where θ is, for the moment, an unknown number. On the basis of relation 2 (see ([2], p. 282)) we have

$$b^{[(n-1)\theta s_1+\theta+s_1]} = b^{[\theta]}.$$

Since the order of the element b is the number g_1, it follows, according to E. Post' s assertion ([2], p. 283), that the congruence

$$(n-1)\theta s_1 + \theta + s_1 - \theta \equiv 0 \pmod{g_1}$$

holds. Hence it follows that

$$s_1(n-1)\theta \equiv -s_1 \pmod{g_1}. \tag{6}$$

According to the hypothesis of the theorem, $(r, n-1) = 1$. Therefore $(s_1(n-1), g_1) = s_1$, and hence the congruence (6) has in all s_1 distinct solutions

$$t,\ t + r_1, \ldots,\ t + (s_1 - 1)r_1,$$

where t is a solution of the congruence

$$(n-1)\theta \equiv -1 \pmod{r_1}.$$

Now consider the class of numbers congruent to t modulo r_1. Let c be an arbitrary positive number belonging to this class. Then

$$c = g_1 q + g_2, \quad \text{where } 0 \geq g_2 < g_1,$$

and therefore

$$(b^{[g_1 q + g_2]})^{[s_1]} = b^{[g_1 q + g_2]}.$$

Hence, and from the fact that g_1 is the order of the element b, follows the equality

$$(b^{[g_2]})^{[s_1]} = b^{[g_2]},$$

i.e., in $\mathfrak{B}$ there exists an element $b_1 = b^{[g_2]}$, and consequently also a subgroup $\mathfrak{S}$ of order s_1. If $s_1 = 1$, then in $\mathfrak{G}$ there would exist an element b_1 of first order, contrary to the case under consideration. Therefore we shall assume $s_1 > 1$, i.e. $|\mathfrak{S}| > 1$. In view of the abelianness of the n-group $\mathfrak{G}$, we conclude that $\mathfrak{S}$ is an invariant subgroup.

Consider the factor group $\mathfrak{G}/\mathfrak{S}$. It is easy to show that $\mathfrak{G}/\mathfrak{S}$ is an abelian n-group. Since

$$|\mathfrak{G}/\mathfrak{S}| = r\frac{s}{s_1} < g$$

and

$$\left(r, \frac{s}{s_1}\right) = 1,$$

the theorem is true for $\mathfrak{G}/\mathfrak{S}$, i.e. $\mathfrak{G}/\mathfrak{S}$ contains a subgroup $\mathfrak{H}$ of order

$$\delta\frac{s}{s_1},$$

where δ is an arbitrary divisor of r. Then, on the basis of Theorem 4, we conclude that $\mathfrak{G}$ contains a subgroup $\mathfrak{H}$ of order δs. We have again obtained a contradiction. Thus the theorem is completely proved.

From Theorem 5 follows the following

Corollary 1. *An abelian n-group $\mathfrak{G}$ of order $g = rs$, where r is the greatest divisor of g relatively prime to $n-1$, possesses a subgroup of order δs, where δ is an arbitrary divisor of r.*

Proof. Since r is the greatest divisor of g relatively prime to $(n-1)$, we have $(r, s) = 1$, and on the basis of Theorem 5 we conclude that $\mathfrak{G}$ possesses a subgroup of order δs, where δ is an arbitrary divisor of r.

Corollary 1 generalizes E. Post' s theorem ([2], p. 284) on the existence of subgroups in cyclic n-groups.

Gomel Laboratory
Institute of Mathematics
Academy of Sciences of the BSSR

Received
12 XII 1969

References

[1] V. D. Belousov, *Foundations of the Theory of Quasigroups and Loops*, Moscow, 1967.
[2] E. L. Post, Trans. Am. Math. Soc., 48, No. 2, 208 (1940).
[3] A. K. Sushkevich, *Theory of Generalized Groups*, Kharkov–Kiev, 1937.

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