DEMONSTRATIO MATHEMATICA
Vol. XIV No 2 1981

Czesław Bagiński

SOME REMARKS ON FINITE p-GROUPS

This paper contains some results concerning finite p-groups. We investigate p-groups of the property W introduced by J.Ambrosiewicz in [2]. We give some results on p-groups of order p^{p+2} and p-groups of exponent p^p.

We start with the definition of the property W for p-groups.

Definition (J.Ambrosiewicz). We shall say that a p-group G has the property W if $K_n \neq \emptyset$ implies $K_nK_n \leqslant G$, where $K_n = \{x \in G: o(x) = p^n\}$ and $AB = \{ab: a \in A, b \in B\}$. The symbol $o(x)$ denotes the order of x.

In [1] it was proved that all regular p-groups have this property. In [3] a unique group of the order 2^4 was found which is not a W-group. This group is of the smallest order which does not have the property W. The first theorem and example show that the above observations can be generalized. In the second theorem we prove that the class of W-groups of exponent p^2 is closed under operation of direct product. The proof that this fact is not valid for different exponents will be given in a separate paper. We also prove two propositions concerning p-groups of the exponent not grater than p^p.

In the paper symbols and terminology are standard.

Theorem 1. If G is a p-group of the order less than p^{p+2}, then G has the property W.

Proof. Let G be a group satisfying the assumption of the theorem. If the order of G is less than p^{p+1} or class of nilpotency of G is less than p, then G is regular ([4].III.10.2.). So, according to the result of [1] mentioned above, we may assume $G = p^{p+1}$ and $c(G) = p$. Moreover let us assume $p > 3$. For $p = 2$ the theorem is simple; for $p = 3$ see [3].

If $\langle K_i \rangle = H < G$, then $K_i K_i = H$ follows from the regularity of H. Let $\langle K_i \rangle = G$. Lemma III.14.2 ([4]) implies $|G/G'| = p^2$ (i.e, $d(G) = 2$) and by lemma III.14.14. ([4]) $\exp G = p$. Since G/G' cannot be cyclic, p'th power of each element of G belongs to G'. Then only K_1 and K_2 are non-empty. Let us choose two elements x,y from K_i such that $G = \langle x,y \rangle$. It is clear that $G = \langle x \rangle \langle y,G' \rangle$. This means that each element of G is of the form $x^m y^n c$ $(c \in G',\ 0 < m,n \leqslant p^2)$.

For $(m,p) = (n,p) = 1$ $o(x^m) = o(y^n c) = p^i$. Indeed, $c(\langle y,G' \rangle) \leqslant p-1$ and by regularity of $\langle y,G' \rangle$ $(y^n c)^p = y^{np}$. If $p|m$ or $p|n$, then $o(x^m y^n c) = p^i$ or $x^m y^n c \in G'$. But $\langle y,G' \rangle \subset K_i K_i$ and for $p \neq 2$ $K_i \subset K_i K_i$. Hence the theorem is proved.

The following example shows that for each odd prime p there exist a group of the order p^{p+2} which has not the property W.

E x a m p l e . Let G be a group generated by elements $a, a_1, a_2, \dots, a_p$ which satisfy the following relations

$$(1)\quad \begin{cases} a^p = a_1^p = \dots = a_{p-1}^p = a_p^{p^2} = 1 \ (p - \text{fixed odd prime number}) \\ [a_i, a_j] = 1, \quad 1 \leqslant i,j \leqslant p \\ [a,a_1] = [a,a_p] = a_2,\ [a,a_2] = a_3, \dots, [a,a_{p-2}] = a_{p-1} \\ [a,a_{p-1}] = a_p^{-p}. \end{cases}$$

The subgroup A generated by the elements $a_1, a_2, \dots, a_p$ is abelian, its order is equal to p^{p+1} and $|G : A| = p$. Hence G is of the order p^{p+2}. We will show that G is generated by elements of the order p and $K_1 K_1 \neq G$.

To this aim we need some calculations. By the relations (1) we have

$$(2)\quad \begin{cases} a^{-1}a_1a = a_1a_2^{-1} \\ a^{-2}a_1a^2 = a_1a_2^{-2}a_3 \\ \dots\dots\dots\dots\dots\dots \\ a^{-(p-1)}a_1a^{p-1} = a_1^{\binom{p-1}{0}}a_2^{-\binom{p-1}{1}}a_3^{\binom{p-1}{2}}\dots a_{p-1}^{(-1)^{p-2}\binom{p-1}{p-2}}(a_p^{-p})^{\binom{p-1}{p-1}} \end{cases}$$

so

$$(3)\quad \left(a^{-(p-1)}a_1a^{p-1}\right)\left(a^{-(p-2)}a_1a^{p-2}\right)\dots\left(a^{-1}a_1a\right)a_1 =$$

$$= a^{\sum_{k=0}^{p-1}\binom{k}{0}}\, a_2^{-\sum_{k=1}^{p-1}\binom{k}{1}}\, a_3^{\sum_{k=2}^{p-1}\binom{k}{2}}\dots a_{p-1}^{\sum_{k=p-2}^{p-1}\binom{k}{p-2}}\, a_p^{-p} =$$

$$= a_1^{\binom{p}{1}}a_2^{-\binom{p}{2}}a_3^{\binom{p}{3}}\dots a_{p-1}^{-\binom{p}{p-1}}a_p^{-p} = a_p^{-p}.$$

Similarly

$$(4)\quad \left(a^{-(p-1)}a_pa^{p-1}\right)\left(a^{-(p-2)}a_pa^{p-2}\right)\dots\left(a^{-1}a_pa\right)a_p = a_p^{\binom{p}{1}}a_2^{-\binom{p}{2}}a_3^{\binom{p}{3}}\dots$$

$$\dots a_{p-1}^{-\binom{p}{p-1}}a_p^{-p} = 1$$

and for $1 < i < p$

$$\left(a^{-(p-1)}a_ia^{p-1}\right)\left(a^{-(p-2)}a_ia^{p-2}\right)\dots\left(a^{-1}a_ia\right)a_i =$$

$$= a_i^{\binom{p}{1}}a_{i+1}^{-\binom{p}{2}}\dots a_{p-1}^{(-1)^{p-i-1}\binom{p}{p-i}}\left(a_p^{-p}\right)^{(-1)^{p-1}\binom{p}{p-i+1}} = 1.$$

Let now $g \in A$. Then $g = \prod_{j=1}^{p} a_j^{n_j}$ and (1)-(4) implies

$$(5)\quad (ag)^p = a^p a^{-(p-1)} g a^{p-1} \dots (a^{-1}ga)g = \prod_{i=1} \left(a^{-(p-i)} g a^{p-i}\right) =$$

$$= \prod_{i=1}^{p} \left(a^{-(p-i)}\left(\prod_{j=1}^{p} a_j^{n_j}\right)a^{p-i}\right) = \prod_{j=1}^{p}\left(\prod_{i=1}^{p}\left(a^{-(p-i)} a_j^{n_j} a^{p-i}\right)\right) =$$

$$= \prod_{i=1}^{p}\left(a^{-(p-i)} a_1^{n_1} a^{p-i}\right)\cdot \prod_{j=2}^{p}\left(\prod_{i=1}^{p}\left(a^{-(p-i)} a_j^{n_j} a^{p-i}\right)\right) =$$

$$= \prod_{i=1}^{p}\left(a^{-(p-i)} a_1^{n_1} a^{p-i}\right).$$

Therefore $o(ag) = p$ if and only if $n_1 \equiv 0 (\mathrm{mod}\, p)$ i.e. when $g \in B$ where B is the subgroup generated by the elements $a_2, a_3, \dots, a_p$. Similarly it can be proved by means of (1)-(4) that for $m \not\equiv 0(\mathrm{mod}\, p)$ $o(a^m g) = p$ if and only if $g \in B$.

As $a_2, a_3, \dots, a_{p-1}$ belong to G' and G' is contained in the Frattini subgroup of G, G is generated by the elements a, a_1, a_p. Hence the elements a, a_1, aa_p generate the group G too and by (5) $o(a) = o(a_1) = o(aa_p) = p$.

Now we will show that the element $a_1 a_p$ from $A \setminus B$ does not belong to $K_1 K_1$. Since $a_1 a_p$ is of the order p^2, $a_1 a_p$ cannot be expressed as a product of two elements of order p from A because A is abelian. If $o(a^n g_1) = o(a^n g_2) = p$, then $g_1, g_2 \in B$ and $(a^n g_1)(a^m g_2) = a^{n+m}(a^{-m} g_1 a^m) g_2 \in A$ if and only if $n + m \equiv 0(\mathrm{mod}\, p)$. But $(a^{-m} g_1 a^m) g_2$ belongs to B. Thus $a_1 a_p \notin K_1 K_1$.

In the further part of the paper we consider only finite p-groups for p odd.

P r o p o s i t i o n 2. If G is a p-group of exponent p^n, where $n \leqslant p$, then there exists i, $1 \leqslant m \leqslant n$, such that $\langle K_m \rangle = G$.

P r o o f . We proceed by induction on the order of G. If G is cyclic, then the proposition is clear. So we can assume that G is not cyclic. According to Burnside's basis theorem, there exist at least $p + 1$ maximal subgroups $M_1, \dots, M_k$, $k \geqslant p+1$. Each M_i is of exponent less than p^{p+1} and

$|M_i| < |G|$. Then by induction M_i is generated by elements of the order p^m for some m, $1 \leqslant m \leqslant n$, i.e. $M_i = \langle K_m \cap M_i \rangle$. The number of maximal subgroups M_i of G is grater than the number of sets K_m. Then at least two subgroups M_i, M_j must be generated by elements from this same set K_m, that is $M_i = \langle K_m \cap M_i \rangle$ and $M_j = \langle K_m \cap M_j \rangle$. Hence $G = \langle M_i \cup M_j \rangle = \langle (M_i \cap K_m) \cap (M_j \cap K_m) \rangle = \langle K_m \rangle$.

P r o p o s i t i o n 3. G is a p-group of exponent p^n, where $n \leqslant p$, and for each i, $1 \leqslant i \leqslant n$, $i \neq m$, $\langle K_i \rangle \neq G$ then $K_m K_m = G$.

P r o o f . Since for $i \neq m$ $\langle K_i \rangle \neq G$, each subgroup $\langle K_i \rangle$ is contained in any maximal subgroup M_i. We have not more than $n-1$ subgroups M_i, $i \neq m$, containing all sets K_i except K_m. By inequality $n-1 < p$, $\bigcup_{i \neq m} M_i \neq G$. Let x be any element from $G \setminus \bigcup_{i \neq m} M_i$. Since for $i \neq m$ $K_i \subset \bigcup_{i \neq j} M_i$, $x \in K_m$.

Now let y be any element of a group G. If $y \in K_m$, then $K_m \subset K_m K_m$ yields $y \in K_m K_m$. Suppose $y \in K_{i_1}$, $i_1 \neq m$. Therefore $xy \in K_{i_2}$, $i_2 \neq i_1$; otherwise $y \in K_{i_1}$. But then $x = (xy)y^{-1} \subset K_{i_1} K_{i_1} \subset \bigcup_{i \neq m} M_i$. If $xy \in K_m$ then $y = x^{-1}(xy) \in K_m K_m$. By the same argument $x^2 y \in K_{i_3}$, $i_3 \neq i_1, i_2$. Really, if $x^2 y \in K_{i_2}$ then $(x^2 y) y^{-1} \in K_{i_2} K_{i_2} \subset \bigcup_{i \neq m} M_i$; if $x^2 y \in K_{i_1}$ then $x = (x^2 y)(y^{-1} x^{-1}) \in K_{i_1} K_{i_1} \subset \bigcup_{i \neq m} M_i$. Hence there is k, $k < n$, such that $x^k y \in K_m$. Since $n \leqslant p$ implies $x^k \in K_m$, we have $y = x^{-k}(x^k y) \in K_m K_m$.

C o r o l l a r y 4. Let G be a p-group such as in Proposition 3. If for each i,j, $i \neq j$, $\langle K_i \rangle \cap K_j \subset M_i$, where M_i is a maximal subgroup of K_i then G has the property W. It is not difficult to construct a irregular p-group which satisfy assumptions of corollary 4.

If G is of exponent p^2 we can prove something more.

L e m m a 5. If G is of exponent p^2 then $K_1K_1 = G$ or $K_2K_2 = G$.

P r o o f . Suppose $K_1K_1 \neq G$. Since $K_1 \subset K_1K_1$, there exists y in K_2 such that $y \notin K_1K_1$. Then $xK_1 \subset K_2$. Indeed, if for some $y \in K_1$ $xy \in K_1$, then $x = (xy)y_{-1}^{-1} \in K_1K_1$. Hence $K_1 \subset x^{-1}K_2 \subset K_2K_2$ and by $G = K_1 \cup K_2 \cup \{1\}$, $K_2 \subset K_2K_2$, we have $K_2K_2 = G$.

L e m m a 6. If G is of exponent p^n, then for each i, $1 \leqslant i \leqslant n$, $G = \bigcup_{j=1}^{n} K_jK_i$ /($G = \bigcup_{j=1}^{n} K_iK_j$).

P r o o f . If $x \notin K_iK_i$ then $xK_i \cap K_i = \emptyset$ i.e. for each $y \in K_i$ there is $z \in K_j$ $(i \neq j)$ such that $xy = z$. Hence $x = zy^{-1} \in K_jK_i$.

T h e o r e m 7. If G_1 and G_2 are p-groups of exponent less than p^3 and have the property W, then the direct product of these groups has the property W.

P r o o f . If G_1 or G_2 is of exponent p then the theorem is clear. Let us assume that G_1 and G_2 are of exponent p^2. Let $X_i = G_1 \cap K_i$, $Y_i = G_2 \cap K_i$. Then by Lemma 1.6 $G_1 = X_2X_2 \cup X_2X_1$ and $G_2 = Y_2Y_2 \cup Y_1Y_2$. Now for $a \notin X_2X_2$ and $b \notin Y_2Y_2$ we have $a = x_2x_1$ and $b = y_1y_2$, where $x_i \in X_i$, $y_i \in Y_i$. Hence $ab = x_2y_1x_1y_2$ and $x_2y_1, x_1y_2 \in K_2$. The other cases are evident. Therefore $K_2K_2 = G$. It is obvious that $K_1K_1 \leqslant G$.

As it is easy to see, we did not use the assumption that $(K_2 \cap G_i)(K_2 \cap G_i)$ is a subgroup of G_i. Thus the following corollary is true.

C o r o l l a r y 8. The direct product of two groups G_1 and G_2 of exponent p^2 has the property W if and only if $(G_i \cap K_1)(G_i \cap K_1) \leqslant G_i$.

REFERENCES

[1] E. A m b r o s i e w i c z : O kwadratach zbiorów elementów jednakowego rzędu. Doctoral Thesis, Institute of Mathematics, Technical University of Warsaw, Warsaw 1978.

[2] J. A m b r o s i e w i c z : O pewnej własności grup, Zeszyty Nauk.-Dydakt. Filii UW, Białystok, Nauki Mat.-Przyr. t.II, z.7, 1974.

[3] J. A m b r o s i e w i c z : Grupy rzędu p^4, Zeszyty Nauk.-Dydakt. Filii UW, Białystok (in print).

[4] B. H u p p e r t : Endliche Gruppen. Berlin 1967.

[5] П. Л а к а т о ш : О структуре сплетения циклических групп простово порядка, Publ. Math. 22 (1975) 293-305.

INSTITUTE OF MATHEMATICS, UNIVERSITY OF WARSAW, BIAŁYSTOK BRANCH
Received June 22nd, 1979.