International Journal of Algebra, Vol. 3, 2009, no. 13, 629 - 637

On Finite Groups Having Perfect Order Subsets

Ashish Kumar Das

Department of Mathematics, North-Eastern Hill University
Permanent Campus, Shillong-793022, Meghalaya, India
akdas@nehu.ac.in

Abstract

A finite group G is said to be a POS-group if for each x in G the cardinality of the set $\{y \in G | o(y) = o(x)\}$ is a divisor of the order of G. In this paper we study some of the properties of arbitrary POS-groups, and construct a couple of new families of nonabelian POS-groups. We also prove that the alternating group A_n, $n \geq 3$, is not a POS-group.

Mathematics Subject Classification: 20D60, 11A41, 11Z05

Keywords: finite groups, semidirect product, divisibility, primes

1 Introduction

Throughout this paper G denotes a finite group, $o(x)$ the order of a group element x, and $|X|$ the cardinality of a set X. Also, given a positive integer n and a prime p, $\operatorname{ord}_p n$ denotes the largest nonnegative integer k such that $p^k | n$. As in [3], the order subset (or, order class) of G determined by an element $x \in G$ is defined to be the set $\operatorname{OS}(x) = \{y \in G | o(y) = o(x)\}$. Clearly, $\forall x \in G$, $\operatorname{OS}(x)$ is a disjoint union of some of the conjugacy classes in G. The group G is said to have perfect order subsets (in short, G is called a POS-group) if $|\operatorname{OS}(x)|$ is a divisor of $|G|$ for all $x \in G$.

The object of this paper is to study some of the properties of arbitrary POS-groups, and construct a couple of new families of nonabelian POS-groups. In the process, we re-establish the facts that there are infinitely many nonabelian POS-groups other than the symmetric group S_3, and that if a POS-group has its order divisible by an odd prime then it is not necessary that 3 divides the order of the group (see [3], [4] and [6]). Finally, we prove that the alternating group A_n, $n \geq 3$, is not a POS-group (see [4], Conjecture 5.2).

2 Some necessary conditions

Given a positive integer n, let C_n denote the cyclic group of order n. Then, we have the following characterization for the cyclic POS-groups.

Proposition 2.1. *C_n is a POS-group if and only if $n = 1$ or $n = 2^\alpha 3^\beta$ where $\alpha \geq 1,\ \beta \geq 0$.*

Proof. For each positive divisor d of n, C_n has exactly $\phi(d)$ elements of order d, where ϕ is the Euler's phi function. So, C_n is a POS-group if and only if $\phi(d)|n\ \forall\, d|n$, *i.e.* if and only if $\phi(n)|n$; noting that $\phi(d)|\phi(n)\ \forall\, d|n$. Elementary calculations reveal that $\phi(n)|n$ if and only if $n = 1$ or $n = 2^\alpha 3^\beta$ where $\alpha \geq 1,\ \beta \geq 0$. Hence, the proposition follows. □

The following proposition plays a very crucial role in the study of POS-groups (abelian as well as nonabelian).

Proposition 2.2. *For each $x \in G$, $|\operatorname{OS}(x)|$ is a multiple of $\phi(o(x))$.*

Proof. Define an equivalence relation $\sim$ by setting $a \sim b$ if a and b generate the same cyclic subgroup of G. Let $[a]$ denote the equivalence class of a in G under this relation. Then, $\forall x \in G$ and $\forall a \in \operatorname{OS}(x)$, we have $[a] \subset \operatorname{OS}(x)$, and $|[a]| = \phi(o(a)) = \phi(o(x))$. Hence it follows that $|\operatorname{OS}(x)| = k \cdot \phi(o(x))$ for all $x \in G$, where k is the number of distinct equivalence classes that constitute $\operatorname{OS}(x)$. □

As an immediate consequence we have the following generalization to the Proposition 1 and Corollary 1 of [3].

Corollary 2.3. *If G is a POS-group then, for every prime divisor p of $|G|$, $p - 1$ is also a divisor of $|G|$. In particular, every nontrivial POS-group is of even order.*

Proof. By Cauchy's theorem (see [7], page 40), G has an element of order p. So, G being a POS-group, $\phi(p) = p - 1$ divides $|G|$. □

A celebrated theorem of Frobenius asserts that if n is a positive divisor of $|G|$ and $X = \{g \in G | g^n = 1\}$, then n divides $|X|$ (see, for example, Theorem 9.1.2 of [5]). This result enables us to characterize the 2-groups having perfect order subsets.

Proposition 2.4. *A 2-group is a POS-group if and only if it is cyclic.*

Proof. By Proposition 2.1, every cyclic 2-group is a POS-group. So, let G be a POS-group with $|G| = 2^m$, $m \geq 0$. For $0 \leq n \leq m$, let $X_n = \{g \in G \,|\, g^{2^n} = 1\}$. Clearly, $X_{n-1} \subset X_n$ for $1 \leq n \leq m$. We use inductuion to show that $|X_n| = 2^n$

for all n with $0 \leq n \leq m$. This is equivalent to saying that G is cyclic. Now, $|x_0| = 1 = 2^0$. So, let us assume that $n \geq 1$. Since G is a POS-group, and since $X_n - X_{n-1} = \{g \in G \mid o(g) = 2^n\}$, we have, using Proposition 2.2,

$$|X_n| - |X_{n-1}| = |X_n - X_{n-1}| = 0 \text{ or } 2^t \tag{2.1}$$

for some t with $n-1 \leq t \leq m$. By induction hypothesis, $|X_{n-1}| = 2^{n-1}$, and, by Frobenius' theorem, 2^n divides $|X_n|$. Hence, from (2.1), it follows that $|X_n| = 2^n$. This completes the proof. □

The possible odd prime factors of the order of a nontrivial POS-group are characterized as follows

Proposition 2.5. *Let G be a nontrivial POS-group. Then, the odd prime factors (if any) of $|G|$ are of the form $1+2^k t$, where $k \leq \text{ord}_2 |G|$ and t is odd, with the smallest one being a Fermat's prime.*

Proof. Let p be an odd prime factor of $|G|$. Then, by Corollary 2.3,

$$p-1 \text{ divides } |G| \implies \text{ord}_2(p-1) \leq \text{ord}_2 |G|,$$

which proves the first part. In particular, if p is the smallest odd prime factor of $|G|$ then $p-1 = 2^k$, for some $k \leq \text{ord}_2 |G|$. Thus $p = 1+2^k$ is a Fermat's prime; noting that k is a power of 2 as p is a prime. □

We now determine, through a series of propositions, certain necessary conditions for a group to be a POS-group.

Proposition 2.6. *Let G be a nontrivial POS-group with $\text{ord}_2 |G| = \alpha$. If $x \in G$ then the number of distinct odd prime factors in $o(x)$ is at the most α. In fact, the bound gets reduces by $(k-1)$ if $\text{ord}_2 o(x) = k \geq 1$.*

Proof. If $o(x)$ has r distinct odd prime factors then $2^r | \phi(o(x))$, and so $r \leq \alpha$. In addition, if $\text{ord}_2 o(x) = k \geq 1$ then $2^{r+k-1} | \phi(o(x))$, and so $r \leq \alpha - (k-1)$. □

Proposition 2.7. *If $|G| = 2k$ where k is an odd positive integer having at least three distinct prime factors, and if all the Sylow subgroups of G are cyclic, then G is not a POS-group.*

Proof. By ([7], 10.1.10, page 290), G has the following presentation:

$$G = \langle x, y | x^m = 1 = y^n, xyx^{-1} = y^r \rangle$$

where $0 \leq r < m$, $r^n \equiv 1 \pmod{m}$, m is odd, $\gcd(m, n(r-1)) = 1$, and $mn = 2k$. Clearly, at least one of m and n is divisible by two distinct odd primes. So, $o(x)$ or $o(y)$ is divisible by at least two distinct odd primes. The result now follows from Proposition 2.6. □

Proposition 2.8. *Let* $|G| = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \dots p_k^{\alpha_k}$ *where* $\alpha_1, \alpha_2, \dots, \alpha_k$ *are positive integers and* $2 = p_1 < p_2 < \cdots < p_k$ *are primes such that* $p_k - 1 = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \dots p_{k-1}^{\alpha_{k-1}}$, $k \geq 2$. *If* G *is a POS-group then the Sylow* p_k*-subgroup of* G *is cyclic.*

Proof. Note that G has a unique Sylow p_k-subgroup, say P, so that every element of G, of order a power of p_k, lies in P. Let m_i denote the number of elements of G of order $p_k{}^i$, $1 \leq i \leq \alpha_k$. Then, by Proposition 2.2, $\phi(p_k{}^i)|m_i$. So,

$$m_i = p_k{}^{i-1}(p_k - 1)x_i$$

for some integer $x_i \geq 0$. If G is a POS-group then we have

$$x_i | p_k{}^{\alpha_k - i + 1} \tag{2.2}$$

whenever $x_i \neq 0$, $1 \leq i \leq k$. Now,

$$\begin{aligned} \sum_{i=1}^{\alpha_k} m_i &= |P| - 1 = p_k{}^{\alpha_k} - 1 \\ \Rightarrow \sum_{i=1}^{\alpha_k} p_k{}^{i-1} \times (x_i - 1) &= 0 \end{aligned} \tag{2.3}$$

This gives

$$\begin{aligned} x_1 &\equiv 1 \pmod{p_k} \\ \Rightarrow x_1 &= 1, \qquad \text{by (2.2)}. \end{aligned}$$

But, then (2.3) becomes

$$\sum_{i=2}^{\alpha_k} p_k{}^{i-1} \times (x_i - 1) = 0.$$

Repeating the above process inductively, we get

$$\begin{aligned} x_1 = x_2 &= \cdots = x_{\alpha_k} = 1 \\ \Rightarrow m_{\alpha_k} &= p_k{}^{\alpha_k - 1}(p_k - 1) \neq 0. \end{aligned}$$

This means that P is cyclic. □

In view of Proposition 2.7 the following corollary is immediate.

Corollary 2.9. *If* $|G| = 42 \times 43^r$, $r \geq 1$, *then* G *is not a POS-group.*

Finally, we have

Proposition 2.10. *Let G be a nontrivial POS-group. Then, the following assertions hold:*

(a) *If* $\operatorname{ord}_2|G| = 1$ *then either* $|G| = 2$*, or* 3 *divides* $|G|$*.*

(b) *If* $\operatorname{ord}_2|G| = \operatorname{ord}_3|G| = 1$ *then either* $|G| = 6$*, or* 7 *divides* $|G|$*.*

(c) *If* $\operatorname{ord}_2|G| = \operatorname{ord}_3|G| = \operatorname{ord}_7|G| = 1$ *then either* $|G| = 42$*, or there exists a prime* $p \geq 77659$ *such that* $43^2 p$ *divides* $|G|$*.*

Proof. We have already noted that $|G|$ is even. So, let

$$|G| = {p_1}^{\alpha_1} \times {p_2}^{\alpha_2} \times \cdots {p_k}^{\alpha_k}$$

where $k \geq 1$, $2 = p_1 < p_2 < \cdots < p_k$ are primes, and $\alpha_1, \alpha_2, \ldots, \alpha_k$ are positive integers. Now, for all $i = 1, 2, \ldots, k$, we have $\gcd(p_i, p_i - 1) = 1$. So, in view of Corollary 2.3 we have the following implications:

$$\begin{aligned} &k \geq 2,\ \alpha_1 = 1 \implies (p_2 - 1)|2 \implies p_2 = 3, \\ &k \geq 3,\ \alpha_1 = \alpha_2 = 1 \implies (p_3 - 1)|6 \implies p_3 = 7, \\ &k \geq 4,\ \alpha_1 = \alpha_2 = \alpha_3 = 1 \implies (p_4 - 1)|42 \implies p_4 = 43. \end{aligned}$$

However,

$$k \geq 5, \alpha_1 = \alpha_2 = \alpha_3 = \alpha_4 = 1 \implies (p_5 - 1)|1806$$

which is not possible for any prime $p_5 > 43$. Hence, the theorem follows from Corollary 2.9 and the fact that $p = 77659$ is the smallest prime greater than 43 such that $p - 1$ divides $2 \times 3 \times 7 \times 43^r$, $r > 1$. □

Remark 2.11. Using Proposition 2.7 and the celebrated theorem of Frobenius one can, in fact, show that if $|G| = 42 \times 43^r \times 77659$, $r \leq 3$, then G is not a POS-group. The proof involves counting of group elements of order powers of 43.

We have enough evidence in support of the following conjecture; however, a concrete proof is still eluding.

Conjecture 2.12. *If G is a POS-group such that* $\operatorname{ord}_2|G| = \operatorname{ord}_3|G| = \operatorname{ord}_7|G| = 1$ *then* $|G| = 42$*.*

3 Some examples

Recall (see [7], page 27) that if H and K are any two groups, and $\theta : H \longrightarrow \mathrm{Aut}(K)$ is a homomorphism then the Cartesian product $H \times K$ forms a group under the binary operation

$$(h_1, k_1)(h_2, k_2) = (h_1 h_2, \theta(h_2)(k_1)k_2), \tag{3.1}$$

where $h_i \in H$, $k_i \in K$, $i = 1, 2$. This group is known as the *semidirect product* of H with K (with respect to θ), and is denoted by $H \ltimes_\theta K$. Such groups play a very significant role in the construction of nonabelian POS-groups.

The following proposition gives a partial characterization of POS-groups whose orders have exactly one distinct odd prime factor.

Proposition 3.1. *Let G be a POS-group with $|G| = 2^\alpha p^\beta$ where α and β are positive integers, and p is a Fermat's prime. If $2^\alpha < (p-1)^3$ then G is isomorphic to a semidirect product of a group of order 2^α with the cyclic group C_{p^β}.*

Proof. Since p is a Fermat's prime, $p = 2^{2^k} + 1$ where $k \geq 0$. Let $X_n = \{g \in G \,|\, g^{p^n} = 1\}$ where $0 \leq n \leq \beta$. Then, using essentially the same argument as in the proof of Proposition 2.4 together with the fact that the order of 2 modulo p is 2^{k+1}, we get $|X_n| = p^n$ for all n with $0 \leq n \leq \beta$. This implies that G has a unique (hence normal) Sylow p-subgroup and it is cyclic. Thus, the proposition follows. □

Taking cue from the above proposition, we now construct a couple new families of nonabelian POS-groups which also serve as counter-examples to the first and the third question posed in section 4 of [3].

Theorem 3.2. *Let p be a Fermat's prime. Let α, β be two positive integers such that $2^\alpha \geq p - 1$. Then there exists a homomorphism $\theta : C_{2^\alpha} \to \mathrm{Aut}(C_{p^\beta})$ such that the semidirect product $C_{2^\alpha} \ltimes_\theta C_{p^\beta}$ is a nonabelian POS-group.*

Proof. Since p is a Fermat's prime, $p = 2^{2^k} + 1$ where $k \geq 0$. Also, since the group $U(C_{p^\beta})$ of units in the ring C_{p^β} is cyclic and has order $p^{\beta-1} \times 2^{2^k}$, there exists a positive integer z such that

$$z^{2^{2^k}} \equiv 1 \pmod{p^\beta}, \text{ and } z^{2^{2^k-1}} \equiv -1 \pmod{p^\beta}.$$

Moreover, we may choose z in such a way that

$$z^{2^{2^k}} \not\equiv 1 \pmod{p^{\beta+1}}$$

(for, otherwise, z may be replaced by $z + p^\beta$). Let the cyclic groups C_{2^α} and C_{p^β} be generated by a and b respectively. Define an automorphism f :

$C_{p^\beta} \to C_{p^\beta}$ by setting $f(b) = b^z$; noting that $\gcd(z, p) = 1$. Consider now the homomorphism $\theta : C_{2^\alpha} \to \mathrm{Aut}(C_{p^\beta})$ defined by $\theta(a) = f$. Let $(a^x, b^y) \in C_{2^\alpha} \ltimes C_{p^\beta}$. we may write $x = 2^r m$, $y = p^s n$, where $0 \le r \le \alpha$, $0 \le s \le \beta$, $2 \nmid m$, and $p \nmid n$. It is easy to see that

$$\theta(a^x)(b^y) = b^{yz^x}. \tag{3.2}$$

So, in $C_{2^\alpha} \ltimes_\theta C_{p^\beta}$, we have, by repeated application of (3.1) and (3.2),

$$(a^x, b^y)^{2^{\alpha-r}} = (1, b^\gamma) \tag{3.3}$$

where

$$\gamma = y \times \frac{z^{2^\alpha m} - 1}{z^{2^r m} - 1}. \tag{3.4}$$

Now, put $c = \mathrm{ord}_p\, m$. Then, $m = p^c u$ for some positive integer u such that $p \nmid u$. Therefore, using elementary number theoretic techniques, we have, for all $r \ge 2^k$,

$$z^{2^r m} = (z^{2^{2^k}})^{2^{r-2^k} p^c u} \equiv 1 \pmod{p^{\beta+c}} \quad \text{but} \quad \not\equiv 1 \pmod{p^{\beta+c+1}}.$$

On the other hand, if $r < 2^k$ then

$$z^{2^r m} \not\equiv 1 \pmod{p};$$

otherwise, since z has order 2^{2^k} modulo p, we will have

$$2^{2^k} | 2^r m \implies 2^k \le r.$$

Thus, we have

$$\gamma = \begin{cases} p^{\beta+c+s} v, & \text{if } r < 2^k, \\ p^s w, & \text{if } r \ge 2^k, \end{cases}$$

where v and w are two positive integers both coprime to p. This, in turn, means that

$$o((a^x, b^y)^{2^{\alpha-r}}) = \begin{cases} 1, & \text{if } r < 2^k, \\ p^{\beta-s}, & \text{if } r \ge 2^k. \end{cases} \tag{3.5}$$

Putting $o(a^x, b^y) = t$, we have

$$(a^x, b^y)^t = (1, 1) \implies a^{tx} = 1 \implies 2^\alpha | 2^r tm \implies 2^{\alpha-r} | t,$$

since m is odd. Thus, $2^{\alpha-r} | o(a^x, b^y)$. hence, from 3.5, we have

$$o(a^x, b^y) = \begin{cases} 2^{\alpha-r}, & \text{if } r < 2^k, \\ 2^{\alpha-r} p^{\beta-s}, & \text{if } r \ge 2^k. \end{cases} \tag{3.6}$$

This enables us to count the number of elements of $C_{2^\alpha} \ltimes_\theta C_{p^\beta}$ having a given order, and frame the following table:

Orders of group elements	Cardinalities of corresponding order subsets
1	1
$2^{\alpha-r}$, $(0 \leq r < 2^k)$	$2^{\alpha-r-1}p^{\beta}$
$2^{\alpha-r}$, $(2^k \leq r < \alpha)$	$2^{\alpha-r-1}$
$p^{\beta-s}$, $(0 \leq s < \beta)$	$p^{\beta-s-1}(p-1)$
$2^{\alpha-r}p^{\beta-s}$, $(2^k \leq r < \alpha,\ 0 \leq s < \beta)$	$2^{\alpha-r-1}p^{\beta-s-1}(p-1)$

It is now easy to see from this table that $C_{2^\alpha} \ltimes_\theta C_{p^\beta}$ is a nonabelian POS-group. This completes the proof. □

Remark 3.3. For $p = 5$, taking $z = -1$ in the proof of the above theorem, we get another class of nonabelian POS-groups, namely, $C_{2^\alpha} \ltimes_\theta C_{5^\beta}$ where $\alpha \geq 2$ and $\beta \geq 1$. In this case we have the following table:

Orders of group elements	Cardinalities of corresponding order subsets
1	1
2^{α}	$2^{\alpha-1}5^{\beta}$
$2^{\alpha-r}$, $(1 \leq r < \alpha)$	$2^{\alpha-r-1}$
$5^{\beta-s}$, $(0 \leq s < \beta)$	$2^2 5^{\beta-s-1}$
$2^{\alpha-r}5^{\beta-s}$, $(1 \leq r < \alpha,\ 0 \leq s < \beta)$	$2^{\alpha-r+1}5^{\beta-s-1}$

Remark 3.4. The argument used in the above theorem also enables us to show that the semidirect product $C_6 \ltimes_\theta C_7$ is a nonabelian POS-group where the homomorphism $\theta : C_6 \to \mathrm{Aut}(C_7)$ is given by $(\theta(a))(b) = b^2$ (here a and b are generators of C_6 and C_7 respectively). In this case the element orders are $1, 2, 3, 6, 7, 14$ and the cardinalities of the corresponding order subsets are $1, 1, 14, 14, 6, 6$.

In ([3], Theorem 1), it has been proved, in particular, that if $C_{p^a} \times M$ is a POS-group then $C_{p^{a+1}} \times M$ is also a POS-group where $a \geq 1$ and p is a prime such that $p \nmid |M|$. Moreover, as mentioned in the proof of Theorem 1.3 of [4], the group M need not be abelian. This enables us to construct yet another family of nonabelian POS-groups.

Proposition 3.5. *Let M be a nonabelian group of order 21. Then, $C_{2^a} \times M$ is a POS-group for each $a \geq 1$.*

Proof. In view of the above discussion, it is enough to see that $C_2 \times M$ is a POS-group. In fact, the element orders and the cardinalities of the corresponding order subsets of $C_2 \times M$ are same as those mentioned in Remark 3.4 □

Finally, we settle Conjecture 5.2 of [4] regarding A_n.

Proposition 3.6. *For $n \geq 3$, the alternating group A_n is not a POS-group.*

Proof. It has been proved in [2] and also in [1] that every positive integer, except $1, 2, 4, 6$, and 9, can be written as the sum of distinct odd primes. Consider now a positive integer $n \geq 3$. It follows that either n or $n-1$ can be written as the sum $p_1+p_2+\cdots+p_k$ where $p_1, p_2, \ldots, p_k$ are distinct odd primes ($k \geq 1$). Clearly, for such n, the number of elements of order $p_1p_2\ldots p_k$ in A_n is $\dfrac{n!}{p_1p_2\ldots p_k}$ which does not divide $|A_n| = \dfrac{n!}{2}$. This completes the proof. □

References

[1] J. L. Brown, Jr., *Generalization of Richert's Theorem*, Amer. Math. Monthly, **83**(8) (1976), 631–634.

[2] R. E. Dressler, *A Stronger Bertrand's Postulate with an Application to Partitions*, Proc. Amer. Math. Soc.**33**(2) (1972), 226–228.

[3] C. E. Finch and L. Jones, *A curious connection between Fermat numbers and finite groups*, Amer. Math. Monthly **109** (2002), 517–524.

[4] C. E. Finch and L. Jones, *Nonabelian groups with perfect order subsets*, JP J. Algebra Number Theory Appl. **3**(1) (2003), 13–26. See also: *Corrigendum to: "Nonabelian groups with perfect order subsets" [JP J. Algebra Number Theory Appl.* **3***(1) (2003), 13–26]*, JP J. Algebra Number Theory Appl. **4**(2) (2004), 413–416.

[5] M. Hall, *Theory of Groups*, Macmillan, New York, 1959.

[6] S. Libera and P. Tlucek, *Some perfect order subset groups*, Pi Mu Epsilon Journal, **11** (2003), 495–498.

[7] D. J. S. Robinson, *A course in the Theory of Groups* (Second Edition), Graduate Text in Mathematics **80**, Springer, New York, 1996.

Received: May, 2009