On the order equations of finite groups

Rulin Shen

Department of Mathematics, Hubei University for Nationalities, Enshi, Hubei, P. R. China
E-mail: shenrulin@hotmail.com

Abstract  In this paper, we give definitions of the $\varphi$-element and $\varphi$-subgroup by the order equation of finite groups, then investigate some properties of the $\varphi$-subgroup.

Key Words  $\varphi$-elements, $\varphi$-subgroup, Sylow subgroups

MSC 2010  20D05, 20D06

1 Introduction and Definition

The orders of elements of finite group $G$ and numbers of the same order elements of $G$ are very important for investigating the structure of group. Assume that $|G| = n$, it is well known that the order of element in $G$ divides the order $n$ of $G$. Thus by the partition of elements of same order we can obtain the order equation

$$n = s_0\varphi(1) + s_1\varphi(n_1) + \cdots + s_t\varphi(n_t),$$

where $s_0 = 1$ and $n_i|\|G|$, $s_i \geq 1$, $\varphi$ is Euler totient function, $1 \leq i \leq t$. Clearly, if group $G$ is isomorphic to $\overline{G}$, then their order equations are complete same, but the inverse of it is not true. For instance, the abelian group $Z_4 \times Z_4$ and the metacyclic group $T$, which $T = \langle a, b \rangle$ and has relations $a^4 = b^4 = 1, bab^{-1} = a^{-1}$, have the same order equation $16 = \varphi(1) + 3\varphi(2) + 6\varphi(4)$, obviously, $Z_4 \times Z_4$ is not isomorphic to $T$. In the following, the group $G$ is always finite.

Definition.  Assume that the order equation of group $G$ is $|G| = 1 + s_1\varphi(n_1) + \cdots + s_t\varphi(n_t)$. If $s_i = 1$ in the order equation of group $G$, and order of element $x$ is $n_i$, then called $x$ a $\varphi$-element of $G$ with order $n_i$. Denote the subgroup $H$ is generated by $X = \{x|x$ is a $\varphi$-element of $G\}$, called $H$ the $\varphi$-subgroup of $G$.

Clearly, the identity 1 is $\varphi$-element. By above definition, in the other words, the element $x$ is a $\varphi$-element if and only if $x$ satisfied the property: if $o(y) = o(x)$ for any other $y \in G$, then $\langle x \rangle = \langle y \rangle$.  

Citation:  Rulin Shen, On the order equations of finite groups, South Asian J Math, 2016, 6(1), 38-42.
2 Main results

**Theorem 1.** Suppose that \( H \) is the \( \varphi \)-subgroup of \( G \), then \( H \) is a cyclic characteristic subgroup and the generator of \( H \) is a \( \varphi \)-element.

**Proof.** Assume that \( H = \langle X \rangle = \langle x | x \varphi \rangle \) is \( \varphi \)-element of \( G \), it is easily shown that \( H \) is a characteristic subgroup of \( G \). Since, for every \( x \in X \) and any \( \alpha \in \text{Aut}(G) \), and \( \alpha \) preserve the order of elements, then we have \( (x)\alpha = \langle x^\alpha \rangle = \langle x \rangle \). In the following we will show that \( H \) is cyclic. Let \( p_1, p_2, \ldots, p_k \) be distinct primes such that 
\[
\{p_1, p_2, \ldots, p_k\} = \{p | p \text{ is prime divisor of the order of some } x \in X\}
\]

Then \( o(x) = p_1^{e_1(x)}p_2^{e_2(x)} \cdots p_k^{e_k(x)} \) for each \( x \in X \).

Let \( x, y \in X \). Then we may write \( x = x_1x_2 \cdots x_k \) and \( y = y_1y_2 \cdots y_k \) such that \( o(x_i) = p_i^{e_i} \) and \( o(y_i) = p_i^{f_i} \) for \( 1 \leq i \leq k \). Since \( \langle x \rangle \leq G \) and \( \langle y \rangle \leq G \), we have \( \langle x_i \rangle \leq G \) and \( \langle y_i \rangle \leq G \). Furthermore, \( \langle x_i, x_j \rangle = \langle x_i \rangle \times \langle x_j \rangle \), \( \langle y_i, y_j \rangle = \langle y_i \rangle \times \langle y_j \rangle \), and \( \langle x_i, y_j \rangle = \langle x_i \rangle \times \langle y_j \rangle \) for \( i \neq j \). Clearly, either \( e_i \leq f_i \) or \( f_i \leq e_i \) for each \( i \), without loss of generality, we assume that \( e_i \leq f_i \) for some \( i \). Then \( x' = x_1x_2 \cdots x_{i-1}y_i^{p_i^{j-i}}x_i+1 \cdots x_k \) has order \( o(x) \). In fact
\[
o(x^{p_i^{j-i}}) = \frac{o(y_i)}{o(x_i)} = \frac{p_i^{j-i}}{p_i^{j-i}} = p_i^{e_i} = o(x_i)
\]

Denote \( y_i^{p_i^{j-i}} \) by \( g_i \), since \( \langle y_i \rangle < G \), it also \( g_i \leq G \), but \( (o(x_i), o(g_i)) = 1(i \neq j) \), we have \( \langle x_i \rangle \cap \langle g_i \rangle = 1 \), so that \( x_jg_ix_j^{-1}g_i^{-1} = (x_jg_jx_j^{-1}g_i^{-1})x_j = x_jg_jx_j^{-1}g_i \in \{x_j \} \cap \{g_i \} = 1 \), hence \( x_jg_i = g_ix_j \), it implies that \( y_i^{p_i^{j-i}} \) commutes with every one of \( x_1, \ldots, x_i, x_{i+1}, \ldots, x_k \), thus \( o(x') = o(x) \). Obviously, since \( x \) is \( \varphi \)-element, hence \( \langle x' \rangle = \langle x \rangle \). It follows that \( \langle x_i \rangle = \langle y_i^{p_i^{j-i}} \rangle \) and so \( x_i \in \langle y \rangle \). Duplicate the above calculation, finally, it implies that
\[
\langle x, y \rangle = \langle x_{i_1} \rangle \times \langle x_{i_2} \rangle \times \cdots \times \langle x_{i_t} \rangle \times \langle y_{i_{t+1}} \rangle \times \cdots \times \langle y_{i_k} \rangle
\]

where \( i_1, \ldots, i_k \) is a permutation of \( 1, 2, \ldots, k \) such that \( e_{i_t} \geq f_{i_t} \) for \( 1 \leq t \leq l \) and \( e_{i_t} < f_{i_t} \) for \( l+1 \leq t \leq k \). The above argument implies that \( H \cong Z_{p_1} \times \cdots \times Z_{p_k} \). Thus \( H \) is cyclic. Clearly, \( |H| = p_1^{e_1}p_2^{e_2} \cdots p_k^{e_k} \). Suppose that \( H = \langle h \rangle \), if \( g \in G \) and \( o(g) = o(h) = |H| \), since \( o(x) = p_1^{e_1(x)}p_2^{e_2(x)}p_k^{e_k(x)} \) for all \( x \in X \) and
\[
o(g^{p_1^{m_1-e_1(x)}p_2^{m_2-e_2(x)} \cdots p_k^{m_k-e_k(x)}}) = o(x),
\]

hence \( x \in \langle g \rangle \), then \( \langle X \rangle \leq \langle g \rangle \), that is \( H \leq \langle g \rangle \), but \( |H| = |\langle g \rangle| \), so that \( \langle g \rangle = H = \langle h \rangle \). Thus \( g \) is the \( \varphi \)-element. \[ \square \]

Note that the converse of the theorem is not true, the elementary abelian \( p \)-group is an example. By above if \( a, b \) are both \( \varphi \)-elements and their orders are not equal, then \( ab = ba \) and \( ab \) is also a \( \varphi \)-elements. Conversely, if \( x \) is \( \varphi \)-element with order \( o(x) \) and \( d | o(x) \), then the \( \varphi \)-element with order \( d \) maybe not exist. For instance, the dihedral group \( D_{12} \), the order equation is \( 12 = \varphi(1) + 7\varphi(2) + \varphi(3) + \varphi(6) \). Clearly, \( 2|6 \), while there is not the \( \varphi \)-element with order \( 2 \). Furthermore, the order of \( ab \) of \( \varphi \)-elements \( a \) and \( b \) is the least common multiple \( [o(a), o(b)] \) of them. If consider the construct of \( \varphi \)-elements in abelian group \( G \), then we obtain the following result:
Theorem 2. Let G be an abelian group, then the following conditions are equivalent mutually

1. There exists a $\varphi$-element with order $m$.
2. Let $m_1, m_2, \ldots, m_t$ be the invariant factors of $G$, then $(m, m_i) = 1$ for $1 \leq i \leq t - 1$.
3. Let $\pi$ be the set of prime divisors of $m$, then $G$ has a cyclic $\pi$-Hall subgroup.
4. $G$ has the unique cyclic subgroup of order $m$.

Proof. (1) $\Rightarrow$ (2). Since $G$ is abelian, we may write $G \cong Z_{m_1} \times Z_{m_2} \times \cdots \times Z_{m_t}$ and $m_i | m_{i+1}$ for $1 \leq i \leq t - 1$, and suppose that $m_1 = p_1^{e_1} s_1, m_2 = p_1^{e_1} s_2, \ldots, m_t = p_1^{e_1} s_t$ for $e_1 \leq e_2 \leq \cdots \leq e_t$. Denote $f(n)$ by the total number of order $n$'s elements in $G$ and, by the set $\{x | G: x^n = 1\}$, obviously $f(1) = 1$ and, we have $f(pq) = f(p)f(q)$ for $(p, q) = 1$. In fact, we may assume $p$ and $q$ are both primes, then $pG = \{g^p | g \in G\}$ is a subgroup of $G$ and, furthermore, either $p^s (Z_{p^s} \times Z_{q^s}) \cong p^s Z_{p^s} \times p^s Z_{q^s}$, $e_{ij}$ with $1 \leq i \leq t - 1$ and $1 \leq j \leq k$. For $e_{ij} < s(i+1)$, $1 \leq i \leq t - 1$ and $1 \leq j \leq k$. Denote $f(n)$ by the total number of order $n$'s elements in $G$ and, by $E(n)$ the set $\{x | G: x^n = 1\}$, obviously $f(1) = 1$ and, we have $f(pq) = f(p)f(q)$ for $(p, q) = 1$. Thus $f(p^n) = \frac{|G|}{|p^n|} - f(p^n - 1)$ for $s \geq 1$. Applying the same way above and $E(p^n) \cap E(q^n) = 1$, we have $f(p^n q^n) = f(p^n)f(q^n)$. Therefore if $p, q$ are not prime, then $(p, q) = 1$, the formula is also right. Now we assume $m = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$. Then $f(m) = f(p_1^{e_1})f(p_2^{e_2})\cdots f(p_t^{e_t})$. In the following we discuss $f(p_i^{e_i})$ with $s_i \neq 0$ by different cases.

Case 1: If $e_{i+1} = s_i < e_{i+1}$ for $1 < i < t$, then $e_{i+1} \leq s_i - 1 < e_{i+1}$. Thus

$$f(p_i^{e_i}) = p_i^{e_i + (s_i - 1)} - p_i^{e_i + e_{i+1}} = p_i^{e_i + s_i + (t - 1)s_i - 1}.$$
Thus if \( f(p_i^{e_i}) = p_i^{s_i-1}(p_i - 1) \), then \( t = 1 \). We get the result that if there is order \( p_i^{e_i} \) \( \phi \)-element, then \( e_1 = e_2 = \cdots = e_{(t-1)i} = 0 \) from above. That is, it is only \( e_1 \neq 0 \). Consequently, \((m, m_i) = 1 \) for \( 1 \leq i \leq t - 1 \).

(2) \( \Rightarrow \)(3). Assumed that \( m = p_1^{m_1}p_2^{m_2} \cdots p_k^{m_k} \), clearly, \( m||G| \), without loss of generality, we can let \( e_j > 0 \) for \( 1 \leq j \leq k' \) and \( k' \leq k \), then \( \pi = \{p_1, p_2, \cdots, p_{k'}\} \). Since \((m, m_i) = 1 \), so \( e_{ij} = 0 \) for \( 1 \leq i \leq t - 1 \), and thus the \( \pi \)-Hall subgroup \( H \) of \( G \) is isomorphic to \( Z_{p_1^{e_1}} \times Z_{p_2^{e_2}} \times \cdots \times Z_{p_{k'}^{e_{k'}}} \). Therefore, it is cyclic.

(3) \( \Rightarrow \)(4). Obviously, \( m|||H| \), thus there is unique cyclic subgroup \( H_m \) of order \( m \) in \( H \). If there exists other subgroup \( H'_m \) with order \( m \) of \( G \), then \( H'_m \leq H_m \) since \( \pi \)-Hall subgroup \( H \) is unique by \( G \)'s commutativity.

(4) \( \Rightarrow \)(1). Supposed that \( H_m \) is unique cyclic subgroup with order \( m \). Then there is an element \( x \) such that \( o(x) = m \). If \( o(y) = m \) for any other \( y \in G \), clearly, \( \langle x \rangle = \langle y \rangle \). So that element \( x \) is the \( \phi \)-element of order \( m \).

By the theorem above, we know that commutative \( p \)-group which is not cyclic has only a \( \phi \)-element 1. If \( p \) is any prime factor of \(|G| \) in abelian group \( G \), \( p|m \) and there is order \( m \)'s \( \phi \)-element, then \( G \) is cyclic group. Also assume \( H \) is the hole of abelian group \( G \), and \( m_1, m_2, \cdots, m_t \) is invariant factor of \( G \), it is easily to check that \( G/H \cong |H|/(Z_{m_1} \times Z_{m_2} \times \cdots \times Z_{m_t}) \). Consider the existence of \( \phi \)-element in general groups, we have obtained a sufficient condition.

**Theorem 3.** Assume that the Hall subgroup \( H \) of \( G \) is cyclic normal, then the generated elements of \( H \) are \( \phi \)-elements.

**Proof.** Supposed that \( H = \langle a \rangle \) and \( o(a) = m(m > 0) \). Since \( H \) is a Hall subgroup, so \((m, |G:H|) = 1 \). Now if there is other element \( x \in G \) such that \( o(x) = o(a) = m \), then \( x \in H \). In fact, let \(|G:H| = l \), then \( x^m = 1 \) and \((xH)^l = H \) since \( H \leq G \). Thus it imply \( x^l \in H \) by \( x^lH = H \). By above \((m, l) = 1 \), there exist integers \( r, s \) such that \( rm + sl = 1 \), so \( x = x^1 = x^{rm+sl} = (x^m)^r(x^l)^s \in H \).

Therefore, the generated elements of \( H \) are \( \phi \)-elements. □

Above we give a necessary condition, but what is the equivalent condition of \( \phi \)-subgroup in finite groups? it need us to further study. In the following, we discuss the relations between hole and Sylow subgroup, and give an equivalent condition which \( p \)-element become a \( \phi \)-element.

**Theorem 4.** Let \( p \) be a prime divisor of \(|G| \). Then \( x \) is a \( p \)-element and \( \phi \)-element if and only if \( x \in H_{P_1} \cap H_{P_2} \cap \cdots \cap H_{P_l} \), where \( H_{P_i} \) denote the \( \phi \)-subgroup of the Sylow \( p \)-subgroup \( P_i \) of \( G \) for \( i = 1, 2, \cdots, l \).

**Proof.** Let \( x \) be a \( \phi \)-element and \( p \)-element. Then \( x \) must be in some Sylow \( p \) subgroup \( P_m \), where \( m \) is chosen in the set \( \{1, 2, \cdots, l\} \). Obviously, \( x \) is also \( \phi \)-element of group \( P_m \), that is, \( x \in H_{P_m} \). Now
assume that \( y \in G \) and \( o(y) = o(x) \), but \( P_1, P_2, \ldots, P_l \) are relative conjugacy because of Sylow subgroups, and \( P_1 \cong P_2 \cong \cdots \cong P_l \), so there exists \( x_i \in P_i(i \neq m) \) such that \( o(x_i) = o(x) \). Thus we have \( \langle x_i \rangle = \langle x \rangle \), it is forced to \( x \in P_i, i = 1, 2, \ldots, l \). Therefore, \( x \in H_{P_1} \cap H_{P_2} \cap \cdots \cap H_{P_l} \).

Conversely, if \( x \in H_{P_1} \cap H_{P_2} \cap \cdots \cap H_{P_l} \), clearly, \( x \in H_{P_i}(i = 1, 2, \cdots, l) \). Let \( y \in G \) and \( o(y) = o(x) \), then \( y \) be in some Sylow \( p \) subgroup \( P_{l'}(1 \leq l' \leq l) \), but \( x \in P_{l'} \), thus we have \( \langle x \rangle = \langle y \rangle \). Consequently, \( x \) is a \( \varphi \)-element of \( G \).

This theorem tell us that, if \( p \)-element \( x \) is \( \varphi \)-element then the \( x \) is determined by the \( \varphi \)-subgroups of its Sylow \( p \)-subgroups completely. If Sylow \( p \)-subgroup \( P \) of \( G \) is unique, Obviously, \( \varphi \)-elements of \( P \) is also one of \( G \) by above. Note that not all \( \varphi \)-elements of the group \( G \) are determined by the \( \varphi \)-subgroup of Sylow subgroups of \( G \). For instance, the Dihedral group \( D_{12} = \langle a, b \rangle \) with relations \( a^6 = 1, b^2 = 1, abab = 1 \) has the \( \varphi \)-element \( a \) with order 6, but there is unique Sylow 2-subgroup \( P_2 \cong Z_2 \times Z_2 \) and Sylow 3-subgroup \( P_3 \cong Z_3 \) in \( D_{12} \). Clearly the \( \varphi \)-subgroup of \( P_2 \) is the trivial and one of \( P_3 \) is isomorphic to \( Z_3 \), so that the \( \varphi \)-element \( a \) is not characterized by Sylow subgroups. Further, how to characterize the \( \varphi \)-element which is not \( p \)-element, it is an interesting problem. But if the \( G \) is solvable, we know that \( \pi \)-Hall subgroup must exist and mutually conjugate, and every \( \pi \)-element must belong to some \( \pi \)-Hall subgroup. Using same method of proof in Theorem 4, we may get the following theorem.

**Theorem 5.** Assume that \( G \) is solvable, and let \( H = \langle x \rangle \) be the \( \varphi \)-subgroup of \( G \) and \( o(x) = m \). Let \( \pi \) be the set of all prime divisor of \( m \). Then \( x \) is a \( \varphi \)-element if and only if \( x \in H_{Q_1} \cap H_{Q_2} \cap \cdots \cap H_{Q_l} \), where \( H_{Q_i} \) is the \( \varphi \)-subgroup of a \( \pi \)-Hall subgroup \( Q_i \) of \( G \) for \( i = 1, 2, \cdots, l \).

**References**