Research Journal of Pure Algebra -1(1), Apr. - 2011, Page: 2-5

RJPA Available online through www.rjpa.info

A NOTE ON WEISENER THEOREM[1]

Rulin Shen*

Department of Mathematics, Hubei University for Nationalities, Enshi, Hubei, P. R. China, 445000

***E-mail:** rulinshen@gmail.com*

(Received on: 25-01-11; Accepted on: 23-02-11)

ABSTRACT

Let $\pi(n)$ be the prime divisor set of n and called that n is a $\pi(n)$-number. Denote by n_π the greatest divisor of n whose prime divisor set is π. Let G be a finite group. Weisener Theorem states that the number w(n) of elements whose orders are multiples of n is either zero, or a multiple of $|G|_{\pi(|G|)\backslash\pi(n)}$. In this paper we classify groups satisfied w(n) is 0 or a $\pi(|G|)\backslash\pi(n)$ -number.

Keywords: *Weisener theorem, number of elements, finite groups.*

MR (2000): *20D60, 20D06.*

---

1. INTRODUCTION AND LEMMAS:

A fundamental result of Frobenius states that in a finite group the number of elements which satisfy the equation $x^n=1$, where n divides the order of the group, is divisible by n. This theorem and several generalizations were obtained by Frobenius at the turn of the 1900s. These results have stimulated a great amount of interest in counting solutions of equations in groups. Afterwards, Weisener gave a theorem about quantitative relations of numbers of elements (see Theorem 3, [6]). Let G be a finite group of order $|G|$. Let $o(g)$ denote the order of $g(\in G)$. Let $W(n)=\{x\in G: n\,|o(x)\}$ where a, b means a divides b and let $w(n)=|W(n)|$. Clearly, $w(1)=|G|$. Let $\pi(n)$ be the prime divisor set of n and called that n is a $\pi(n)$-number (we also assume that 1 is a π-number). Denote by n_π the greatest divisor of n whose prime divisor set is π. Let G be a finite group. Weisener theorem states that the number $w(n)$ of elements whose orders are multiples of n is either zero, or a multiple of $|G|_{\pi(|G|)\backslash\pi(n)}$. In this paper we classify groups satisfied $w(n)$ is a $\pi(|G|)\backslash\pi(n)$-number. We prove

Theorem: Suppose that $w(n)$ is 0, or a $\pi(|G|)\backslash\pi(n)$-number for all n. Then G is one of the following groups

(a) Z_2;

(b) Frobenius groups $K: Z_2$, where Sylow subgroup of K is of order a Fermat prime or isomorphic to Z_3^2;

(c) Frobenius groups Z_2^k: H, where H is cyclic and Sylow subgroup of H is of order a Mersenne prime.

(d) Simple groups $PSL_2(2^2)$, $PSL_2(2^4)$, $PSL_2(2^8)$ and $PSL_2(2^{16})$.

***Corresponding author: Rulin Shen*, *E-mail: rulinshen@gmail.com**

Next we will cite some lemmas. On the set $\pi(|G|)$ we define a graph $GK(G)$, called prime graph, whose vertices set is $\pi(|G|)$ with the following adjacency relation: vertices r and s in $\pi(|G|)$ are joined by edge if and only if rs is the order of some element of G. Denote the connected components of the graph by $\{\pi_i, i=1,\ldots,s:=s(G)\}$, $s(G)$ is said to the number of connected components of G and if $2\in\pi(G)$, denote the component containing 2 by π_1 always. The structure of the group which the number of connected components of prime graph is more than 1 is due to Gruenberg and Kegel as follows. Recall that a 2-Frobenius group G is ABC, where A and AB are normal subgroups of G, AB and BC are Frobenius group with kernel A, B and complements B, C respectively.

Lemma: 1 If a finite group G has the disconnected prime graph, then one of the following statements holds:

(1) $s(G)=2$ and G is a Frobenius group or 2-Frobenius.

(2) there exists a non-abelian simple group S such that $S\leq H=G/N\leq Aut(S)$, where N is the maximal normal soluble subgroup of G. Furthermore, N and H/S are $\pi_1(G)$-subgroups, the prime graph GK(S) is disconnected.

In [2] and [5] the prime graph components of non-abelian simple groups are given.

Lemma: 2 If $\pi(G)=\{p, q\}$ with p, q both odd primes, and G has no element of order pq, then G is a Frobenius group or a 2-Frobenius group.

Lemma: 3 Let $G=ABC$ be a 2-Frobenius group as above. Suppose that AC is a p-group. Then exp (AC) $\geq p^2$.

Proof: Without loss of generality, we assume that A is elementary abelian p-group and C is of order p. We regard BC acts on the vector space A. Since p does not divide $|B|$ and B acts nontrivially, A has a basis that is permuted semi-regularly by C. This means that all orbits have size $|C|$ (see Theorem 15.16, [1]. Let $x_1, x_2,\ldots,x_p$ be one C-orbit of basis vectors. Then the subgroup of A generated by the $\{x_1, x_2\ldots x_p\}$ is elementary of order p^p, and a basis is permuted transitively by C. The p-group generated by $\{x_1, x_2\ldots x_p\}$ and C, therefore, is isomorphic to the wreath product of a cyclic group Z_p by itself. That wreath product has exponent p^2. More specifically, let c generate C. Then the element $x_i c$ has order p^2.

2. Proof of Theorem: Let $\pi_e(G)$ be the set of order of elements of G and $\pi(|G|)=\{p_1, p_2, \ldots, p_m\}$. Denote by s_i the number of elements of order i. Suppose that $|G|=p_1^{u1} p_2^{u2}\ldots p_m^{um}$ and n is a maximal order in $\pi_e(G)$. And let $|G|_{\pi(n)}= p_1^{u1} p_2^{u2}\ldots p_l^{ul}$. Since $w(n)$ is a $\{p_{l+1}, p_{l+2}, \ldots, p_m\}$-number and $\varphi(n) \mid w(n)$ with φ Euler function, we have n is a square-free number, that is a multiple of some primes. Thus every order of non-unit elements is a multiple of primes. Now if there is odd prime order p which is not maximal in $\pi_e(G)$. Without loss of generality, we assume that $p = p_1$. Then we have the following identity formula

$$p_2^{t2}\ldots p_m^{tm} = w(p) = s_p+w(pr_1)+w(pr_2)+\ldots +w(pr_h),$$

where $\{ r_1, r_2, \ldots, r_h\} \subseteq \pi(|G|)\backslash\{p_1\}$. So $W(pr_i)$ has no element of order 2p for $i=1,2,\ldots, h$. In fact, otherwise w(2p) is odd, but w(p) and $w(pr_i)$ is even for $r_i\neq 2$ since $2 \mid p-1 \mid \varphi(p) \mid w(p)$ and $w(pr_i)$. This contradicts above equality. Therefore, odd prime p is disconnected to 2 in the prime graph of G, that is 2 is a component of $GK(G)$. By Lemma 1 we divide into three cases to discuss.

Case 1: *G is a Frobenius group.* Suppose that K and H are kernel and complement of G, respectively. Then H is one of square-free order since Sylow subgroup of H is a cyclic group of order prime.

If $2 \mid |H|$, then $|H|=2$ since $s(G)=2$. In addition, since K is nilpotent, suppose that $\pi(K) = \{p_1, p_2\ldots p_k\}$,

© 2011, RJPA. All Rights Reserved

then $w(p_1 p_2 \ldots p_k)=2^t$, i.e.,

$$(p_1^{t1}-1)(p_2^{t2}-1)\ldots(p_k^{tk}-1)=2^t. \quad (*1)$$

Denote by r_n the primitive prime divisor of q^n-1 if $r_n \mid q^n-1$, but r_n cannot divide q^i-1 for every i<n. By Zsigmondy theorem [7] there exists r_n always except the cases $(n, q)=(6,2)$ and $(n, q)=(2,2^k-1)$ with nature number k.. If $t_i \geq 3$, then there primitive prime divisor of $p_i^{t_i}-1$, and hence (*1) has no solution. If $t_i=2$, then $p_i^2-1=2^{t0}$, that is $(p_i+1)(p_i-1)=2^{t0}$, and so $p_i=3$. If $t_i=1$, then p_i is a Fermat prime. Therefore Sylow subgroup of K is isomorphic to Z_3^2 or Z_p with p a Fermat prime.

If $2 \mid |K|$, then K is elementary abelian 2-group and H is of square-free order. Hence H is cyclic or a metacyclic group with generated relations $\langle a, b: a^m=b^n=1, a^b=a^r\rangle$, where $((r-1)m,n)=1$, $r^m\equiv 1 \pmod n$ and $|H|=mn$ (see 10.1.10, [4]). If H is cyclic, then every prime divisor of $|H|$ is a Mersenne prime. If H is meta-cyclic, obviously, $(m, n)=1$ and $\langle a\rangle$ is normal in H. Since for every element x of $\langle a\rangle$, $\langle x\rangle$ is normal in H, we have every element of order prime in $\langle a\rangle$ commutes with all elements of order prime in $\langle b\rangle$. In fact, otherwise there exists an element $x_0\in\langle a\rangle$ and $y_0\in\langle b\rangle$ such that $\langle x_0\rangle\langle y_0\rangle$ is a Frobenius group by Lemma 2, then K: $\langle x_0\rangle\langle y_0\rangle$ is a 2-Frobenius group. Now we regard as K is a $\langle x_0\rangle\langle y_0\rangle$-module. By 8.3.5 of [3] we know that $C_K(\langle y_0\rangle)\neq 1$, it implies that 2 is connected to an odd prime in the prime graph of G, a contradiction. Since orders of a, b are both square-free, we have $ab=ba$, hence H is abelian, a contradiction.

Case 2: *G is a 2-Frobenius group.* Suppose that G is ABC, where A and AB are normal subgroups of G, AB and BC are Frobenius group with kernel A, B and complements B, C respectively. Since B and C are both cyclic and B is of odd order, we have $2 \mid |AC|$. Hence AC is a 2-group since $s(G)=2$. By Lemma 3 we have $exp(AC) \geqslant 4$, a contradiction.

Case 3: *There exists a non abelian simple group S such that $S\leq H=G/N\leq Aut(S)$, where N is the maximal normal soluble subgroup of G.* Since N and H/S are $\pi_1(G)$-groups, N is a 2-group. In addition, since Sylow 2-subgroup of G is an elementary abelian group, we have $G\cong N{:}S^*$, where $S\leq S^*\leq Aut(S)$. Since the prime graph $GK(S)$ is disconnected and 2 is a component of $GK(S)$, by papers [2] and [5] it is easy to check that S is $L_2(2^f)$, $L_3(2^f)$ or $Sz(2^{2m+1})$. Since centralizers of field automorphisms of them have an element of order 2, we have $S^*=S$. Furthermore, the exponents of Sylow 2-subgroups of $L_3(2^f)$ and $Sz(2^{2m+1})$ are more than 2, so S^* is $L_2(2^f)$.

Now suppose that T is a Frobenius subgroup of S of order $2(2^f-1)$. Then $N: T$ is a 2-Frobenius group. By Lemma 3, the exponent of Sylow 2-subgroup of $N: T$ is more than 2, a contradiction. Therefore $N=1$.
Since $w(2^f-1)=s\{2^f-1\}=\varphi(2^f-1\times 2^{f-1}\times(2^f+1)$, we have

$$\pi(\varphi(2^m-1))\subseteq\pi(2^m+1)\cup\{2\}, \quad (*2)$$

and similarly we have

$$\pi(\varphi(2^m+1))\subseteq\pi(2^m-1)\cup\{2\}. \quad (*3)$$

Suppose that p is an odd prime divisor of f. Let r_p and r_{2p} are primitive prime divisors of 2^p-1 and $2^{2p}-1$, respectively. Then $p \mid r_p-1$ and $2p \mid r_{2p}-1$. Also since $r_p-1 \mid \varphi(2^f-1)$ and $r_{2p}-1 \mid \varphi(2^f+1)$, we have $p \mid (\varphi(2^f-1),\varphi(2^f+1))$. On the other hand, by (*2), (*3), $(\varphi(2^f-1), \varphi(2^f+1))$ has only prime divisor 2 since $(2^f-1, 2^f+1)=1$. Thus f is a power of 2, say, 2^n. Denote by F_n the Fermat number $2^{2n}+1$. If $1\leq n\leq 4$, it is easy to check that $PSL_2(2^{2n})$ is satisfied the conditions of Theorem. If n=5, then $17449 \mid \varphi(2^{32}+1)$, but does not divide $2^{32}-1=3\times5\times17\times257\times65537$, a contradiction. If $n\geq 6$, then $2^{2n}-1=F_0 F_1\ldots F_{n-1}$. Thus $F_5 \mid 2^{2^{\wedge}n}-1$. Since $F_5=641\times6700417$, we have $3 \mid \varphi(F_5) \mid \varphi(2^{2^{\wedge}n}-1)$, and hence $3 \mid 2^{2^{\wedge}n}+1$ by the (*2), a contradiction.

© 2011, RJPA. All Rights Reserved

REFERENCES:

[1] Isaacs, I. M., Character theory of finite group, Acdemic Prees, NewYork, San Francisco, London, 1976.

[2] Kondratev A.S., Prime graph components finite simple groups, Mat. sbornik, 180, No.6(1989), 787-797.

[3] Kurzweil Hans, Stellmacher Bernd, The theory of finite groups: an introduction, Springer-Verlag New York, Inc., 2004.

[4] Robinson D.J.S, A course in the theory of groups, Springer-Verlag, New York, 1982.

[5] Williams J.S. , Prime Graph Components of Finite Groups, J.Alg., 1981, 69: 487-513.

[6] Weisne L., On the number of elements of a group, which have a power in a given conjugate set, Bull. Amer. Math. Soc. 31, (1925), 492-496.

[7] Zsigmondy K., Zur Theorie der Potenzreste, Monatsh.Math.Und Phys. 3(1892), 265-284.

[1] ***Project supported by the NNSF of China (No.11026195) and the foundation of Educational Department of Hubei Province in China (No.Q20111901).***

****

© 2011, RJPA. All Rights Reserved