J. Korean Math. Soc. 26(1989), No. 2, pp. 291-300

A CHARACTERIZATION OF SOME FINITE GROUPS WITH IRREDUCIBLE CHARACTERS OF PRIME DEGREE

SEUNG AHN PARK

1. Introduction

Let G be a finite group. Let $\mathrm{Irr}(G)$ be the set of all irreducible characters of a finite group G over the complex number field and let $\mathrm{c.d.}(G)$ be the set of all degrees of irreducible characters in $\mathrm{Irr}(G)$. In [2] and [3], I. M. Isaacs and D. S. Passman have determined the structure of G with $\mathrm{c.d.}(G)=\{1, m\}$, $m>1$. We say that a finite group G is of type

$$\mathrm{d.t.}(G)=\begin{Bmatrix}1 & m\\ a & b\end{Bmatrix},$$

if G satisfies the following conditions:

(i) $\mathrm{c.d.}(G)=\{1, m\}$, and
(ii) G has exactly a linear characters and exactly b irreducible characters of degree m.

The purpose of this paper is to characterize all the finite groups G of type

$$\mathrm{d.t.}(G)=\begin{Bmatrix}1 & p\\ a & b\end{Bmatrix}$$

where p is a prime and $1\leq b\leq p+1$. In fact, we will explicitly determine G.

In section 2 we will prove theorems on the properties of some special groups. These theorems will be useful in proving our main theorems. We will prove our main theorems in section 3.

The notation and the terminology in this paper are standard, and they are taken fromi [8].

Received March 2, 1989.
*This reseach has been supported by Ministry of Education.

Let G be a group. If X is a subset of G, $\langle X\rangle$ denotes a subgroup generated by X. If $x, y\in G$, then x^y and $[x, y]$ denote $y^{-1}xy$ and $x^{-1}y^{-1}xy$, respectively. The commutator subgroup and the center of G are denoted by G' and $Z(G)$, respectively.

The cyclic group of order n, the dihedral group of order $2n$ and the quaternion group of order 8 are denoted by C_n, D_{2n} and Q_8, respectively. Thus

$$C_n=\langle x\,|\,x^n=1\rangle,\quad D_{2n}=\langle x, y\,|\,x^n=y^2=1,\quad x^y=x^{-1}\rangle,$$
$$Q_8=\langle x, y\,|\,x^4=y^4=1, x^2=y^2, x^y=x^{-1}\rangle.$$

2. Properties of some special groups

In this section we will prove several theorems on the properties of some special groups.

Let r be a prime and let m be a positive integer. Then there exists a Galois field F with r^m elements. The additive group F^+ is an elementary abelian r-group of order r^m and its multiplicative group F^* is a cyclic group of order r^m-1.

Suppose that p is a fixed prime factor of r^m-1. Then $1+dp=r^m$ for some positive integer d. Let θ be a fixed element of F^* such that $F^*=\langle\theta\rangle$ and let $\xi=\theta^d$. Then $\langle\xi\rangle$ is a unique subgroup of F^* of order p. The map

$$\phi(\theta)\,:\,F^+\longrightarrow F^+,\quad \phi(\theta)\,(\alpha)=\theta\alpha$$

is an automorphism of F^+, and $\phi : F^*\longrightarrow \mathrm{Aut}(F^+)$ is a homomorphism of F^* into the automorphism group $\mathrm{Aut}(F^+)$. Thus $\phi(F^*)$ is a cyclic subgroup of $\mathrm{Aut}(F^+)$ of order r^m-1 and $\phi(\langle\xi\rangle)$ is a cyclic subgroup of $\phi(F^*)$ of order p.

Let $p=\langle y\rangle$ be a cyclic group of order $p^n, n\geq 1$. Then the homomorphism $T : P\longrightarrow \mathrm{Aut}(F^+)$ given by

$$T(y^i)=\phi(\xi^i)$$

defines an action of P on F and we have $T(P)=\phi(\langle\xi\rangle)$.

Thus we can consider the semidirect product

$$G_n(p, d, r^m)=\{(y^i, \alpha)\,|\,\alpha\in F,\ \ 0\leq i\leq p^n-1\}$$

of F and P with respect to this P-action on F. It is a nonabelian group of order $(1+dp)p^n$, whose multiplication is given by

$$(y^i, \alpha)\ \ (y^j, \beta)=(y^{i+j},\ \ \xi^j\alpha+\beta).$$

If we consider P and F as subgroups of $G_n(p, d, r^m)$, then P is a Sylow p-subgroup and F is an abelian normal p-complement.

The subgroup

$$G(p, d, r^m) = \{ \begin{bmatrix} \xi & 0 \\ \alpha & 1 \end{bmatrix} | \alpha \in F, \ 0 \leqq i \leqq p-1 \}.$$

of the general linear group $GL(2, F)$ is a Frobenaus group of order with a Frobienius complement H and a Frobenius kernel K, where

$$K = \{ \begin{bmatrix} 1 & 0 \\ \alpha & 1 \end{bmatrix} | \alpha \in F \}, \quad H = \{ \begin{bmatrix} \xi^i & 0 \\ 0 & 1 \end{bmatrix} | 0 \leqq i \leqq p-1 \}.$$

And K is isomorphic to F and H is cyclic of order p.

Let $P = \langle y \rangle$ be a cyclic group of ordr p^n, $n \geq 1$. Then the map $K \times P \longrightarrow K$, $(x, y^i) \longrightarrow x^{y^i}$ defined by

$$\begin{bmatrix} 1 & 0 \\ \alpha & 1 \end{bmatrix}^{y^i} = \begin{bmatrix} 1 & 0 \\ \xi^i \alpha & 1 \end{bmatrix}$$

is an action of P on K, and the group $G_n(p, d, r^m)$ is indeed isomorphic to the semidirect proiduct of K by P with respect to this P-action on K. In particular we have

$$G_1(p, d, r^m) \cong G(p, d, r^m).$$

THEOREM 2.1. *Let* $G = G_n(p, d, r^m)$. *Then*

$$\text{d. t. } (G) = \begin{Bmatrix} 1 & p \\ p & p^{n-1}d \end{Bmatrix}.$$

Proof. The group G has an abelian normal subgroup $F\langle y^p \rangle$ of index p. Hence $\chi(1) \mid p$ for all $\chi \in \mathrm{Irr}(G)$, by Ito's theorem. Since G is not abelian, this implies c. d. $(G) = \{1, p\}$. Moreover, we have $G' = F$, $|G : G'| = p$. Therefore, the assertion holds.

Assume that m is the order of r modulo p, that is, $m = \mathrm{ord}_p\, r$. Thus m is the smallest positive integer such that $r^m \equiv 1 \pmod{p}$, and if $r^k \equiv 1 \pmod{p}$ then $m \mid k$.

THEOREM 2.2. *Let* p *and* r *be primes such that*

$$1 + dp = r^m, \quad m = ord_p r.$$

(1) *The only normal subgroups of* $G = G_n(p, d, r^m)$ *contained in the normal* p*-complement* F *are* $\{0\}$ *and* F.

(2) *Let* G *be a finite group such that*

$$G = AP, \quad A \cap P \{1\},$$

where A *is an elementary abelian normal subgroup of order* r^m, $P = \langle y \rangle$

is cyclic of order p^n, $n \geq 1$ *and* $C_P(x) = \langle y^p \rangle$ *for all* $x \in A - \{1\}$.
Then $G \cong G_n(p, d, r^m)$.

Proof. (1) The abelian normal p-complement F is an elementary abelian r-group of order r^m.

Let B be a nontrivial normal subgroup of G contained in F. Then B is an elementary abelian r-group of order r^k, where $1 \leq k \leq m$. And for each non-identity element x of B, the conjugacy class containing x is of size p. Hence

$$|B| \equiv 1 \pmod{p}, \text{ and } m \mid k.$$

Thus $k=m$ and $B=F$.

(2) By assumption the automorphism $T(y)$ of A defined by

$$T(y)(x) = x^y$$

is of order p. On the other hand, $\mathrm{Aut}(A)$ is of order

$$r^{m(m-1)/2}(r^m-1)(r^{m-1}-1)\cdots(r-1).$$

Let p^e be the highest power of p dividing r^m-1. Then it is the highest power of p which divides $\mathrm{Aut}(A)$ since $m = \mathrm{ord}_p r$. Hence Sylow p-subgroups of $\mathrm{Aut}(A)$ are of order p^e.

We will identify A with the additive group F, where $F = GF(r^m)$. The group $\mathrm{Aut}(A)$ has a cyclic subgroup of order r^m-1 and so it has a cyclic subgroup of order p^e. Hence any Sylow p-subgroup of $\mathrm{Aut}(A)$ is cyclic, and every cyclic subgroup of order p is conjugate in $\mathrm{Aut}(A)$ to $\langle \phi(\xi) \rangle$, where ξ is a fixed element of F^* of order p and $\phi(\xi)$ is defined by

$$\phi(\xi)(\alpha) = \xi\alpha, \quad \alpha \in F.$$

In particular $\langle T(y) \rangle$ is conjugate to $\langle \phi(\xi) \rangle$ in $\mathrm{Aut}(A)$. Therefore, G is isomorphic to $G_n(p, d, r^m)$.

It is easy to prove the following proposition.

PROPOSITION 2.3. *Let* p *and* r *be primes such that*

$$1 + dp = r^m$$

for some positive integers d *and* m.

(1) *If* $1 \leq d \leq p+1$, *then* $m = \mathrm{ord}_p r$.

(2) *Suppose that* $m = \mathrm{ord}_p r$. *Then the following hold.*

(i) $m \mid (p-1)$, *and if* $p=2$ *then* $m=1$.

(ii) *If* p *is odd and* $m>1$, *then* $(r-1) \mid d$.

In particular if p *is odd,* $d=2$ *and* $m>1$ *then* $r=3$ *and* $m \geq 3$.

3. A characterization of some finite groups

Let G be a finite group of type

$$\text{d. t. } (G)=\begin{bmatrix}1 & p\\ a & b\end{bmatrix},$$

where p is a prime and a and b are positive integers. Then G is a nonabelian group such that

$$|G:G'|=a, \quad |G|=a+bp^2.$$

Since G has an irreducible character of degree p, we have $p\mid |G|$ by Ito's theorem. Therefore, we have $p\mid (a+bp^2)$ and $p\mid a$. We also have $a\mid bp^2$ by Lagrange's theorem.

Set $a=pc$. Specially, if b is a prime then c is one of the integers $1, p, b, bp$, and so the integer a is one of the integers p, p^2, bp, bp^2.

Now we will characterize the group G under a certain restriction on a and b.

THEOREM 3.1. *Let p be an odd prime and let G be a finite group of type*

$$\text{d. t. } (G)=\begin{Bmatrix}1 & p\\ a & b\end{Bmatrix}$$

where $1\leq b\leq p+1$.

(I) *If $a=p$, then p is an odd prime such that $1+bp=r^m$ for some prime r, and $G\cong G(p, b, r^m)$.*

(II) *If $a=p^2$, then one of the following holds.*

(1) $b=p-1$, and $G\cong M(p^3)$ *or* $G\cong E(p^3)$, where
$M(p^3)=\langle x, y\mid x^{p^2}=y^p=1,\ x^y=x^{-1}\rangle$,
$E(p^3)=\langle x, y, z\mid x^p=y^p=z^p=1,\ [x, y]=z,\ [x, z]=[y, z]=1\rangle$.

(2) p is a Mersenne prime of the form $p=2^m-1$, $b=p$, and
$G\cong G(p, 1, 2^m)\times C_p$ or $G\cong G_2(p, 1, 2^m)$

(III) *If $a=bp$, $b\neq 1$ and $b\neq p$, then p is a Mersenne prime of the form $p=2^m-1$, and*

$$G\cong G(p, 1, 2^m)\times C_b.$$

(IV) *The integer a can not be equal to bp^2.*

Proof. Since c. d. $(G)=\{1, p\}$, the group G is nonabelian and G has an abelian normal p-complement A. Let P be a Sylow p-subgroup

of G. Then

$$G=AP, \quad A\cap P=\{1\}.$$

and we have $|G:N_G(P)|\equiv 1 \pmod{p}$ by Sylow's theorem.

The p-group P acts on an abelian p'-group A by conjugation, and so we have

$$A=C_A(P)\times[A,P]$$

by [8, Theorem 2.5.17]. Moreover, if P is abelian then

$$G'=[G,G]=[A,P].$$

This can be proved by using the following identities:

$$[xy,u]=[x,u]^y\,[y,u], \quad [u,xy]=[u,y][u,x]^y.$$

In the following proof we will use the above results and the fact that p is odd.

(I) Assume that $a=p$. Then

$$|G|=p(1+bp), \quad |G'|=1+bp.$$

The Sylow p-subgroup P is cyclic of order p and $A=G'$. Hence we have

$$A=C_A(P)\times[A,P], \quad [A,P]=G'=A$$

and it follows that

$$C_A(P)=\{1\}, \quad C_G(P)=P, \quad Z(G)=\{1\}.$$

Moreover,

$$C_G(x)=A, \quad C_P(x)=\{1\}$$

for all $x\in A-\{1\}$.

The factor group $N_G(P)/P$ is isomorphic to a subgroup of $\mathrm{Aut}(P)$, and $\mathrm{Aut}(P)$ is a cyclic group of order $p-1$. Hence it follows that

$$|G:N_G(P)|\ |N_G(P):P|=|G:P|\equiv 1 \pmod{p}.$$

This implies that $|N_G(P):P|\equiv 1 \pmod{p}$. Hence $N_G(P)=P$ and $P\cap P^x=\{1\}$ for all $x\in G-P$.

Therefore, G is a Frobenius group with Frobenius complement P and Frobenius kernel A.

Let r be a prime factor of $1+bp$. Then A has an element x of order r. Consider the conjugacy class $\mathfrak{B}_x$ of G containing x. Then

$$\mathfrak{B}_x\subseteq A, \quad |\mathfrak{B}_x|=|G:C_G(x)|=|G:A|=p.$$

Suppose that $b=1$. Then $A=\mathfrak{B}_x\cup\{1\}$ and A is an elementary abelian r-group of order $1+p$. This implies that $r=2$ and $1+p=2^m$. Suppose that $1<b\leq p+1$. Then the only positive divisors d of $1+bp$ with $d\equiv 1 \pmod{p}$ are 1 and $1+bp$. Hence $\mathfrak{B}_x\cup\{1\}$ is not a subgroup of A. Thus there exist two distinct elements $u,v\in\mathfrak{B}_x$ such

that $uv \in A - \mathfrak{B}_x$, and $w=uv$ is of order r. Continuing the above argument, we can show that there exist b elements $x_1, x_2, \ldots, x_b$ in A such that

$$A=\{1\} \cup \mathfrak{B}_{x_1} \cup \mathfrak{B}_{x_2} \cup \ldots \cup \mathfrak{B}_{x_b}.$$

This implies that A is indeed an elementary abelian r-group and, by Proposition 2.3, we have

$$|A|=1+bp=r^m, \quad m=\mathrm{ord}_p r,$$

Therefore, $G \cong G(p, b, r^m)$ by Theorem 2.2.

(II) Assume that $a=p^2$. Then

$$|G|=p^2(1+b), \quad |G'|=1+b.$$

Suppose that $p|(b+1)$. Then $b=p-1$, and G is a nonabelian group of order p^3 with $|G'|=p$. Two groups $M(p^3)$ and $E(p^3)$ are the only nonabelian groups of order p^3, and their commutator subgroups are cyclic of order p. Hence $G \cong M(p^3)$ or $G \cong E(p^3)$.

Now suppose that $(b+1, p)=1$. Then P is of order p^2 and it is either elementary abelian or cyclic. And we have $A=G'$. Hence

$$A=C_A(P) \times [A, P], \quad [A, P]=G'=A,$$

and if follows that

$$C_A(P)=\{1\}, \quad C_G(P)=P, \quad Z(G) \subseteq P.$$

Since $1 \leq b \leq p+1$, it follows that

$$|G : N_G(P)|=1+p, \quad N_G(P)=P, \quad p=b$$

And we have

$$|\mathfrak{B}_x|=|G : C_G(x)|=p, \quad A=\mathfrak{B}_x \cup \{1\}$$

for any $x \in A-\{1\}$. Hence A is an elementary abelian r-group of order $1+p$. Thus $r=2$, $1+p=2^m$.

Since P is abelian, we have

$$P \cap C_G(x)=(P \cap C_G(x))^y=P \cap C_G(x^y),$$

$$C_G(A)=C_G(x), \quad C_G(A)=C_G(x)=Z(G), \quad |Z(G)|=p$$

for any $x \in A\{1\}$ and $y \in P$.

If P is elementary abelian, then there exists a subgroup $\langle y \rangle$ of P of order p such that

$$P=\langle y \rangle \times Z(G), \quad G=A\langle y \rangle \times Z(G).$$

Hence, by Theorem 2.2, we have

$$G=A\langle y \rangle \cong G(p, 1, 2^m) \times C_p.$$

If P is cyclic of order p^2 and $P=\langle y \rangle$, then $Z(G)=\langle y^p \rangle$ and so $G \cong G_2(p, 1, 2^m)$ by Theorem 2.2.

(III) Assume that $a=bp$, $b\neq 1$, $b\neq p$. Then

$$|G|=pb(1+p), \quad |G'|=1+p.$$

The Sylow p-subgroup P is cyclic of order p, and so

$$A=C_A(P)\times[A,P], \quad [A,P]=G'\subseteq A.$$

Hence the following hold.

$$C_G(P)=P\times Z(G), \quad Z(G)=C_A(P), \quad |Z(G)|=b,$$
$$A=G'\times Z(G), \quad G=G'P\times Z(G).$$

Thus by the similar arguments to those in (II) we can show that G' is an elementary abelian group of order $1+p$, where $1+p=2^m$ for some m. Therefore, by Theorem 2.2, we have

$$G=G'P\times Z(G)\cong G(p,1,2^m)\times C_b$$

(IV) Assume that $a=bp^2$. Then $|G|=2bp^2$ and $|G'|=2$. Thus we have $G'\subseteq Z(G)$.

Suppose that $b=p$. Then P is of order p and $G=G'P$. Thus P is normal in G and G/P is abelian. But this implies that $G'\subseteq P$, which is a contradiction.

Now suppose that $b\neq p$. Then $G=AP$ and P is abelian of order p^2, Hence

$$A=C_A(P)\times[A,P], \quad [A,P]=G'\subseteq Z(G).$$

and $A\subseteq Z(G)$. Thus P is normal in G and G/P is abelian, and so $G'\subseteq P$. But this is a contradiction.

In Theorem 3.1, if $b=1$ then a must be either p or p^2. And if b is prime then a must be one of the integers p, pbp, bp^2. Hence the following theorem follows from Theorem 3.1 and Proposition 2.3.

THEOREM 3.2. *Let p be an odd prime and let G be a finite group of type*

$$\text{d. t. } (G)=\begin{Bmatrix}1 & p\\ a & b\end{Bmatrix}.$$

(1) *If $b=1$, then p is a Mersenne prime of the form $p=2^m-1$, $a=p$ and $G\cong G(p,1,2^m)$.*

(2) *If $b=2$, then one of the following holds.*

(i) *p is a prime such that $1+2p=r$ for some odd prime r, $a=p$, and $G\cong G(p,2,r)$.*

(ii) *p is an odd prime such that $1+2p=3^m$, $m\geq 3$, $a=p$, and $G\cong G(p,2,3^m)$.*

(iii) $p=3$, $a=p^2$, *and* $G\cong M(3^3)$ *or* $G\cong E(3^3)$.

(iv) p *is a Mersenne prime of the form* $p=2^m-1$, $n=2p$, and $G\cong G(p, 1, 2^m)\times C_p$.

(3) *If* b *is an odd prime such that* $b<p$, *then one of the following holds.*

(i) p *is a prime such that* $1+bp=2^m$, $a=p$, *and* $G\cong G(p, b, 2^m)$.

(ii) p *is a Mersenne prime of the form* $p=2^m-1$, $a=bp$, *and* $G\cong G(p, 1, 2^m)\times C_b$.

(4) *If* $b=p$, *then* p *is a Mersenne prime of the form* $p=2^m-1$, $a=p^2$, *and*

$$G\cong G(p, 1, 2^m)\times C_p \text{ or } G\cong G_2(p, 1, 2^m)$$

The next theorem deals with the case when $p=2$, and and this has been essentially proved in Theorem 3. 1.

Note that there are exactly nine isomorphism classes of nonabelian groups of order 16 (*cf.* [1, §§113-118]). Among them there are six groups whose commutator subgroups are cyclic of order 2, and three groups

$$D_{16},\qquad S_{16}=\langle x\,|\,x^8=y^2=1,\ x^y=x^3\rangle,$$
$$Q_{16}=\langle x, y\,|\,x^8=y^4=1,\ x^4=y^2,\ x^y=x^{-1}\rangle$$

are groups whose commutator subgroups are of order 4.

Note that if $1+2b=r$ for some odd prime then

$$G_2(2, b, r)\cong\langle x, y\,|\,x^r=y^4=1,\ x^y=x^{-1}\rangle,\ G(2, b, r)\cong D_{2r}.$$

THEOREM 3. 3. *Let* G *be a finite group of type*

$$\text{d. t. }(G)=\begin{Bmatrix}1 & 2\\ a & b\end{Bmatrix}.$$

(1) *If* $b=1$, *then one of the following holds.*

(i) $a=2$, *and* $G\cong D_6$.

(ii) $a=4$, *and* $G\cong D_8$ *or* $G\cong Q_8$.

(2) *If* $b=2$, *then one of the following holds.*

(i) $a=2$, *and* $G\cong D_{10}$.

(ii) $a=4$, *and* $G\cong D_6\times C_2=D_{12}$.

(iii) $a=4$, *and* $G\cong\langle x, y\,|\,x^3=y^4=1,\ x^y=x^{-1}\rangle$.

(iv) $a=8$, *and* G *is a nonabelian group of order* 16 *such that* G' *is cyclic of order* 2. *There are six such groups.*

(3) *If* $b=3$, *then one of the following holds.*

(i) $a=2$, *and* $G\cong D_{14}$.

(ii) $a=4$, *and* G *is a nonabelian group of order* 16 *such that* G' *is cyclic of order* 4. *Thus*

$$G\cong D_{16},\ G\cong Q_{16} \text{ or } G\cong S_{16}.$$

(iii) $a=6$, *and* $G\cong D_6\times C_3$.

(iv) $a=12$, *and* $G\cong D_8\times C_3$ *or* $G\cong Q_8\times C_3$.

References

1. Burnside, W., *The theory of groups of finite order*, 2nd ed., Dover, New York, 1955.
2. Isaacs, I. M. and D. S. Passman, *Groups with representations of bounded degree*, Canada J. Math., **16**(1964), 299–309.
3. Isaacs, I. M. and D. S. Passman, *A characterization of groups in terms of the degree of their characters* I, II, pacific J. Math., **15**(1965), 877–903; **24**(1968), 467–510.
4. Iaacs, I. M. and D. S. Passman, *Finite groups with small character degrees and large prime divisors*, I, II, Pacific J. Math., **23**(1967), 273–280; **29**(1969), 311–324.
5. Isaacs, I. M., *Groups having at most three irreducible character degrees*, Proc. Amer. Math. Soc., **21**(1969), 185–188.
6. Isaacs, I. M., *Character degrees and derived lenth of a solvable group*, Canada J. Math., **27**(1975), 146–151.
7. Isaacs, I. M., *Character correspondences in solvable groups*, Advances in Math., **43**, (1982), 284–306.
8. Suzuki, M., *Group theory* I, II, Springer-Verlag, New York, 1982, 1986.

Sogang University
Seoul 121–742, Korea