Kangweon-Kyungki Math. Jour. 2 (1994), pp. 39–43

EXTRA-SPECIAL p-GROUPS WITH ITS AUTOMORPHISMS

JOONG SANG SHIN

1. Introduction. Let p be a prime. Let D be the dihedral group of order 8 and let Q be the quaternion group.

It is well known that a nonabelian p-group of order p^3 is isomorphic to one of the groups $M_3(p)$, $M(p)$, D or Q, where

$$M_3(p) = \langle x, y \mid x^{p^2} = y^p = 1, \quad x^y = x^{1+p} \rangle$$

and

$$M(p) = \langle x, y, z \mid x^p = y^p = x^p = 1, \ [x, y] = z, \ [x, z] = [y, z] = 1 \rangle$$

Any automorphism of D (resp. Q) induces the identity automorphism on the center $Z(D)$ of D (resp. $Z(Q)$) and the automorphism group $\mathrm{Aut}(D)$ (resp. $\mathrm{Aut}\,(Q)$) is isomorphic to D (resp. Σ_4 the symmetric group of degree 4).

An automorphism of a group G is *p'-automorphism* if its order is not divisible by p.

We are interested in relating the action of p'-automorphisms of a p-group G to their induced actions on certain subgroups and factor groups of G.

In this paper, we study actions of p'-automorphisms of $M_3(p)$ and $M(p)$ to obtain some results(Theorems2.6–2.9).

Notations and terminologies not described are conferred to [1], we denote by $[x, y]$ the commutator of x and y.

2. Results. Let G be a group. The*Frattini subgroup* $F(G)$ is the intersection of all the maximal subgroups of G. If the inverse image of $Z(G/Z(G))$ is G, then G is *of class at most 2.* A p-group G is *special* if either G is elementary abelian or G is of class 2 and $G' = Z(G) = F(G)$ is elementary abelian. A special p-group G is *extra-special* if G has class 2 and the commutator subgroup G' is of order p. If G is a p-group, we denote by $\Omega_i(G)$ the subgroup of G generated by its elements of order dividing p^i.

Received January 4, 1994. Revised March 2, 1994

REMARK 2.1. Let G be a group. Then subgroups $F(G)$ and $\Omega_i(G)$ are characteristic subgroups of G.

We are necessary the following lemmas.

LEMMA 2.2. *Let G be a group. Let $x, y \in G$ and suppose $z = [x, y]$ commutes with both x and y. Then $[x^i, y^j] = z^{ij}$ for all i, j.*

Proof. [1, Lemma 2.2.2].

LEMMA 2.3. *Let G be a p-group of class at most 2 with p odd. Then*

(i) $x^p = 1$ for all $x \in \Omega_1(G)$

(ii) If $G/Z(G)$ is elementary abelian, $(xy)^p = x^p y^p$ for all x, y in G.

Proof. [1, Lemma 5.3.9].

LEMMA 2.4. *A nonabelian p-group G of order p^3 is extra-special and is isomorphic to one of the groups $M_3(p)$, $M(p)$, D or Q.*

Proof. [1, Lemma 5.5.1]

LEMMA 2.5. *Let*

$$M_3(p) = \langle\, x, y \mid x^{p^2} = y^p = 1, \quad x^y = x^{1+p} \,\rangle$$

Then

$$Z(M_3(p)) = \langle x^p \rangle \quad \text{and} \quad \Omega_1(M_3(p)) = \langle x^p \rangle \times \langle y \rangle.$$

Proof. [1, Theorem 5.4.3]

Now we obtain our results.

THEOREM 2.6. *Let p be an odd prime and let*

$$G = M_3(p) = \langle\, x, y \mid x^{p^2} = y^p = 1, \quad x^y = x^{1+p} \,\rangle$$

Let σ be a p'-automorphism of the p-group G which induces the identity automorphism on $Z(G)$. Then σ is the identity automorphism of G.

Proof. Set $z = x^p$. Then $G' = F(G) = Z(G) = \langle z \rangle$ by Lemma 2.4 and Lemma 2.5 and $G/Z(G)$ is elementary abelian by Lemma 2.3.

By the assumption we have $\sigma(z) = z$ and $\sigma(x) = x^i y^j$ for some integer i and j. Now it follows from Lemma 2.3 that

$$z = \sigma(z) = \sigma(x^p) = \sigma(x)^p = (x^i y^j)^p = x^{pi} y^{pj} = x^{pi} = z^i.$$

Hence we have $i \equiv 1 (\mathrm{mod}\, p)$ and so $\sigma(x) = cxy^j$ for some c in $Z(G)$.

Note that $\Omega_1(G) = \langle z \rangle \times \langle y \rangle = Z(G) \times \langle y \rangle$ by Lemma 2.5 and that $\Omega_1(G)$ is invariant under σ (cf. Remark 2.1). Thus we have $\sigma(y) = dy^k$ for some $d \in Z(G)$ and for some integer k. Now from the relation $x^y = x^{1+p} = zx$, we have

$$(cxy^j)^{dy^k} = \sigma(zx) = zcxy^j$$

and so

$$cz^k xy^j = czxy^j.$$

Thus $k \equiv 1 (\mathrm{mod}\, p)$ and so $\sigma(y) = dy$.

Let σ be of order n. Then $(n, p) = 1$ by the assumption. Since $y = \sigma^n(y) = d^n y$, it follows that $d = 1$ and $\sigma(y) = y$. Hence we have

$$x = \sigma^n(x) = c^n xy^{nj} = x(cy^j)^n$$

and so $(cy^j)^n = 1$.

On the other hand, cy^j is an element of $\Omega_1(G)$. Thus its order is 1 or p. Now it follows that $cy^j = 1$ and $\sigma(x) = x$. Hence σ is the identity automorphism of G.

THEOREM 2.7. *Let p be an odd prime and let*

$$G = M(p) = \langle\, x, y, z \mid x^p = y^p = z^p = 1,\ [x, y] = z,\ [x, z] = [y, z] = 1 \,\rangle$$

Let q be a prime divisor of p-1 and r be a fixed integer such that $1 < r < p$ and $r^q \equiv 1 (\mathrm{mod}\, p)$. Then the automorphism τ of G defined by

$$\tau(x) = x^r, \quad \tau(y) = y^{r^{q-1}}, \quad \tau(z) = z$$

is an automorphism of order q, which induces the identity automorphism on $Z(G)$.

Proof. By definition of $M(p)$, $\Omega_1(G) = G$. Since G is extra-special, we have $G' = F(G) = Z(G) = \langle z \rangle$. Now since $[x, y] = z$ and $z \in Z(G)$, it follows from Lemma 2,2 that $[x^i, y^j] = z^{ij}$ for all i and j.

The multiplicative group $Z^* = \{1, 2, ..., p-1\}$ is a cyclic group of order $p-1$ and so for each prime divisor q of $p-1$ there exists a unique subgroup of order q. Hence there exists an integer r which satisfies the given condition.

Now it is easy to show that, for given r under the condition, the given τ is an automorphism of order q which induces the identity automorphism on $Z(G)$.

THEOREM 2.8. *Let τ be an automorphism of $M(3)$ of order 2 which induces the identity automorphism on $Z(M(3))$. Then there exist elements $x, y, z \in M(3)$ such that*

$$M(3) = \langle x, y, z \mid x^3 = y^3 = z^3 = 1,\ [x,y] = z,\ [x,z] = [y,z] = 1 \rangle$$

and

$$\tau(x) = x^{-1}, \quad \tau(y) = y^{-1}, \quad \tau(z) = z.$$

proof. Let

$$M(3) = \langle x, y, z \mid x^3 = y^3 = z^3 = 1,\ [x,y] = z,\ [x,z] = [y,z] = 1 \rangle$$

Let

$$\tau(x) = x^a y^b z^c \quad \text{and} \quad \tau(y) = x^r y^s z^t$$

where a, b, c, r, s and t are integers. Since τ is an automorphism of $M(3)$ of order 2 which induces the identity automorphism on $Z(M(3))$, we have

$$\tau^2(x) = x \quad \text{and} \quad z = \tau(z) = [\tau(x), \tau(y)].$$

From these facts, it is easy to show that

$$\tau(x) = x^{-1}z^t \quad \text{and} \quad \tau(y) = y^{-1}z^t,\ t = -1, 0, 1.$$

By changing generators if necessary, we may assume that

$$\tau(x) = x^{-1} \quad \text{and} \quad \tau(y) = y^{-1}.$$

In fact if $\tau(x) = x^{-1}z$ and $\tau(y) = y^{-1}z$ then we choose xz, yz and z as generators of $M(3)$ and other case is similar. By Theorem 2.7, τ is an automorphism of $M(3)$ of order 2 which induces the identity automorphism on $Z(M(3))$.

THEOREM 2.9. *Let G be a group which contains a normal subgroup F and an element u such that*

(i) $F \cong M(3)$ and

(ii) u is an element of order 2^n such that $u \notin C_G(F)$, $u^2 \in C_G(F)$ and $u \in C_G(Z(F))$.

Then there exist elements $x, y, z \in F$ such that

$$F\langle u \rangle = \langle x, y, z, u \mid x^3 = y^3 = z^3 = u^{2^n} = 1,\ x^u = x^{-1},\ y^u = y^{-1},\ [x,z] = [y,z] = [u,z] = 1,\ [x,y] = z \rangle$$

Furthermore,

$$Z(F\langle u \rangle) = \langle z \rangle \times \langle u^2 \rangle = \langle zu^2 \rangle.$$

Proof. The conjugation on F by u is an automorphism of F of order 2 which induces the identity automorphism on $Z(F)$. By Theorem 2.8, there exist elements $x, y, z \in F$ such that

$$F = \langle x, y, z \mid x^3 = y^3 = z^3 = 1,\ [x, y] = z,\ [x, z] = [y, z] = 1 \rangle$$

and

$$x^u = x^{-1},\ y^u = y^{-1} \text{ and } z^u = z.$$

Since $u^2 \in C_G(F)$ and $u \notin C_G(F)$, it is clear that $Z(F\langle u \rangle) = \langle z \rangle \times \langle u^2 \rangle = \langle zu^2 \rangle$. Thus the assertion holds.

REMARK. *Using Theorem 2.9, we can find all groups whose degrees of irreducible complex characters are primes ([4], [5]).*

References

[1] D. Gorenstein, *Finite groups*, Chelsea, New York, 1980.

[2] B. Huppert, *Endliche gruppen I*, Springer-Verlag, Berlin, 1967.

[3] B. Huppert and N. Blackburn, *Finite groups II, III*, Springer-Verlag, Berlin, 1982.

[4] J.S. Shin, *A characterization of finite groups whose degrees of irreducible characters are 1,2 and 3*, Sc-Gang University (1986).

[5] J.S. Shin, *Properties of finite groups whose degrees of irreducible characters are primes*, J. of K.M.S. **31** (1994).

[6] M. Suzuki, *Group theory I, II*, Springer–Verlag, New York, 1982, 1986.

Department of Mathematics
Kyung won University
Sung nam,461-200, Korea