Bull. Korean Math. Soc.
Vol. 16, No. 1, 1979

ON SCHUR MULTIPLIERS OF SOME FINITE GROUPS

BY WAN SOON KIM

1. Introduction

The purpose of this paper is to determine the Schur multipliers of some finite groups. The Schur multiplier of a finite group G over an algebraically closed field k will be denoted by $M(G)$. Our main theorems are as follows.

THEOREM 1. *Let G be a finite group, and let $M(G)$ be the Schur multiplier of G over an algebraically closed field k. Suppose that $G=CH$, where C is a cyclic normal subgroup and H is a cyclic subgroup. Then*

$$|M(G)| \leq |Z(G):C\cap H|.$$

In paricular, if $Z(G)=C\cap H$ then G has a trivial Schur multiplier.

THEOREM 2. *Let $C=<a>$ be a cyclic group of order p^m for an odd prime p and some integer $m>0$ and let $H=<\alpha>$, where α is an automorphism of C of order p^n for some integer $n \geq 0$.*

Let G be the semidirect product of C by H. Then

(1) $Z(G)=<a^{p^n}>$, and

(2) $M(G)$ is a cyclic p-group whose order is $\leq p^{m-n}$.

Our study on the order of the Schur multiplier is motivated by the fact that some properties of a finite group G can be derived from the order of $M(G)$. Actually $M(G)$ is the second cohomology group $H^2(G, k^*)$, where k^* is a trivial G-module. The Schur multiplier of a group G is related to central extensions of G.

In section 2 we will state two propositions which play the central role for the proof of Theorem 1.

In section 3 we will prove Theorem 1 and Theorem 2. In order to prove Theorem 2 we need the fundamental theorem on primitive root modulo m. At the end of this section we deal with some examples as applications of Theorem 1 and Theorem 2.

All groups in this paper are assumed to be finite. Let G be a finite group. Denote the order of G by $|G|$ and the center of G by $Z(G)$.

Let $x^y = y^{-1}xy$ and $[x, y] = x^{-1}y^{-1}xy$. Let H and K be subgroups of G. We denote by $[H, K]$ the commutator subgroup which is generated by the elements $[h, k]$ for all $h \in H$ and $k \in K$. We denote the commutator subgroup $[G, G]$ of G by G'.

2. Preliminary results

Let G be a finite group and let k be an algebraically closed field. Any function $\alpha: G \times G \to k^*$ satisfying

$$\alpha(x, yz)\,\alpha(y, z) = \alpha(x, y)\,\alpha(xy, z) \text{ for all } x, y, z \in G,$$

is called a factor set of G, where $k^* = k - \{0\}$. Two factor sets α and β of G are said to be equivalent if there is a function $c: G \to k^*$ such that

$$\alpha(x, y) = \beta(x, y) c(x) c(y) c(xy)^{-1} \text{ for all } x, y \in G.$$

For any factor set α of G, let $\{\alpha\}$ be the equivalence class containing α. The set $M(G)$ of all equivalence classes of factor sets forms an abelian group via a multiplication defind by

$$\{\alpha\}\{\beta\} = \{\alpha\beta\}.$$

This group is called *the Schur multiplier* of G *over* k.

PROPOSITION 1 [Schur]. *Let G be a finite group and $M(G)$ be the Schur multiplier of G over k. Then there is a central extension Γ of G with kernel $M(G)$.*

Proof. The proof can be found in [2, Theorem 25.5].

We define a *Schur representation group* for G to be a central extension whose kernel is isomophic to $M(G)$.

PROPOSITION 2 [Schur]. *Let Γ be a finite central extension of G with kernel A.*

(1) *If A is contained in the commutator subgroup Γ', then A is isomorphic to a subgroup of $M(G)$.*

(2) *Assume that $|A| = |M(G)|$. Then $A \subseteq \Gamma'$ if and only if Γ is a Schur representation group for G.*

Proof. The proof can be found in [5, Corollary 11.20].

By the above two propositions we see that Γ is a Schur representation group for G if and only if $G \cong \Gamma / A$ for some $A \subseteq Z(\Gamma) \cap \Gamma'$ such that $|A| = |M(G)|$.

3. Main theorems

In this section our main theorems will be proved. We will make use of the following two Lemmas in proving the Theorem 1.

LEMMA 1. *Let G be a group. Then for any element x, y and z of G, the following equalities hold.*

(i) $[xy, z]=[x, z]^y[y, z]=[x, z][[x, z], y][y, z]$.

(ii) $[x, yz]=[x, z][x, y]^z=[x, z][x, y][[x, y], z]$.

Proof. These can be proved by easy computations.

LEMMA 2. *Let G be a group and let $G=AH$, where A is an abelian normal subgroup and $H=\langle y\rangle$ is a cyclic subgroup. Then*

(i) $G'=[G, G]=[A, H]\subseteq A$.

(ii) *A mapping $f: A\to G$ defined by $f(a)=[a, y]$ is a homomorphism of A onto G'. In particular, $A/A\cap Z(G)\cong G'$.*

Proof. (i) Since A is normal in G and G/A is abelian, we have

$$[A, H]\subseteq[G, G]\subseteq A.$$

Each element of G is of the form ah, where $a\in A$ and $h\in H$. By assumption A is an abelian normal subgroup and H is an abelian subgroup. Using this fact and Lemma 1, we can show that the equality

$$[ah, bk]=[a^h, k][h, b^k]$$

holds for any $a, b\in A$ and $h, k\in H$. This yields that $G'=[G, G]=[A, H]$. Now the assertion (i) holds.

(ii) First $f(ab)=[ab, y]=[a, y]^b[b, y]$ for any elements a and b of A. Since $[A, H]\subseteq A$ by (i) and A is abelian, we have $[a, y]^b=[a, y]$. Hence $f(ab)=[a, y][b, y]=f(a)f(b)$. Thus f is a homomorphism of A into G'.

To show that f is onto it suffices to prove $f(A)=[A, H]$. Obviously, we have $f(A)\subseteq[A, H]$. Let a be an element of A. Then for any positive integer n, the equality $[a, y^{n+1}]=[a, y][a^y, y^n]$ holds. Hence, by induction on n, we can show that $[a, y^n]\in f(A)$. Moreover, $[a, h^{-1}]=[hah^{-1}, h]^{-1}$ for any $a\in A$ and $h\in H$. Therefore, it follows that $[A, H]\subseteq f(A)$. Hence $f(A)=[A, H]$ and f is onto.

Since A is abelian and H is generated by y, the kernel of f is

$$\begin{aligned}\ker f&=\{a\in A\mid [a, y]=1\}\\ &=\{a\in A\mid [a, g]=1 \text{ for all } g \text{ in } G\}=A\cap Z(G).\end{aligned}$$

Hence from the first isomorphism theorem it follows that $A/A\cap Z(G)\cong G'$. This completes the proof of Lemma 2.

THEOREM 1. *Let G be a finite group and let $M(G)$ be the the Schur multiplier of G. Suppose that $G=CH$, where C is a cyclic normal subgroup and H is a cyclic subgroup. Then*

$$|M(G)|\leq|Z(G):C\cap H|.$$

In particuler if $Z(G)=C\cap H$, then G has a trivial Schur multiplier.

Proof. By assumption $C\cap H\subseteq C\cap Z(G)\subseteq Z(G)$. By Lemma 2 we have $C/(C\cap Z(G))\cong G'$. Hence $|G'|=|C:C\cap Z(G)|\leq|C:C\cap H|$.

Let Γ be a Schur representation group for G with kernel A such that $A\subseteq Z(\Gamma)\cap\Gamma'$ and $|A|=|M(G)|$. Since $G\cong\Gamma/A$ and $A\subseteq\Gamma'$, we obtain $G'\cong\Gamma'/A$. Thus $|G'|\cdot|A|=|\Gamma'|$. Moreover, Γ has a normal subgroup $L\supseteq A$ and a subgroup $M\supseteq A$ such that $L/A\cong C$, $M/A\cong H$ and $LM=\Gamma$. Since L/A is cyclic and A is contained in $Z(\Gamma)$, it is easy to show that L is abelian. Similarly, M is abelian. Since $\Gamma=LM$, this implies that $A\subseteq L\cap M\subseteq Z(\Gamma)$.

The group Γ/L is isomorpic to a group $M/L\cap M$, by the correspondence theorem. Moreover, $M/L\cap M$ is isomorphic to a factor group of a cyclic group M/A. Hence Γ/L is a cyclic group. If we set $\Gamma/L=\langle Ly\rangle$, then $\Gamma=L\langle y\rangle$. Thus we can apply Lemma 2 to conclude that $\Gamma'\cong L/L\cap Z(\Gamma)$.

Now, the above results yield

$$|G'||M(G)|=|G'||A|=|\Gamma'|=|L:L\cap Z(\Gamma)|$$
$$\leq|L:L\cap M|=|C:C\cap H|,$$
$$|G'|=|C:C\cap Z(G)|.$$

Therefore, we obtain

$$|M(G)|\leq|C\cap Z(G):C\cap H|\leq|Z(G):C\cap H|.$$

In particular, if $Z(G)=C\cap H$ then G has a trivial Schur multiplier.

This completes the proof of Theorem 1.

COROLLARY 1. *Let G be a finite cyclic group. Then G has a trivial Schur multiplier.*

Proof. By setting $C=H=G$ in Theorem 1 we obtain the assertion.

THEOREM 2. *Let $C=\langle a\rangle$ be a cyclic group of order p^m for an odd prime p and some integer $m>0$ and let $H=\langle\alpha\rangle$, where α is an automorphism of C of order p^n for some integer $n\geq 0$.*

Let G be the semidirect product of C by H. Then

(1) $Z(G)=\langle a^{p^n}\rangle$, *and*

(2) $M(G)$ *is a cyclic p-group whose order is* $\leq p^{m-n}$.

Proof. (1) Note that the action of α is completely determined by its effect on a and that a^{α} is a generator of C. Let $a^{\alpha}=a^t$ for some integer t. Then t is relatively prime to p^m and the order of t modulo p^m is p^n. And an easy computation shows that

$$Z(G)=\{a^i\in C \mid (a^i)^{\alpha}=a^i\}=\{a^i\in C \mid i(t-1)\equiv 0 \pmod{p^m}\}.$$

Since p is an odd prime there exists an integer g which is a primitive root modulo p^e for each positive integer $e\leq m$ [6, Theorem 3.18]. Hence $t=g^j$ for some integer j. Since the order of g modulo p^m is $\varphi(p^m)$ and the order of g^j is p^n, we have $\dfrac{\varphi(p^m)}{(j,\varphi(p^m))}=p^n$. Hence $(j,\varphi(p^m))=\varphi(p^{m-n})$. This yields that $g^j\equiv 1 \pmod{p^{m-n}}$ and $g^j\not\equiv 1 \pmod{p^{m-n+1}}$. Thus we have $p^n(t-1)=p^n(g^j-1)\equiv 0 \pmod{p^m}$, and $p^s(t-1)=p^s(g^j-1)\not\equiv 0 \pmod{p^m}$. for all integers $0\leq s<n$. From this fact it follows that $Z(G)=\langle a^{p^n}\rangle$.

(2) From Theorem 1, $|M(G)|\leq|Z(G)|$. By (1), $Z(G)=\langle a^{p^n}\rangle$ is contained in $C=\langle a\rangle$ which is a cyclic group of order p^m. Thus the order of $Z(G)$ is p^{m-n}. Hence $|M(G)|\leq|Z(G)|=p^{m-n}$.

On the other hand, by assumption G is a p-group which is generated by two elements and three relations on these generators. Hence $M(G)$ is a cyclic p-group by [4, Satz 23.10, and Satz 25.2].

This completes the proof of Theorem 2.

In case $p=2$, there exist a primitive root modulo p^m only if p^m is 2 or 4. Thus Theorem 2 holds if $m\leq 2$ by the same argument as before, but it may not hold if $m>2$. For example, let

$$D=\langle a,b \mid a^{2^{m-1}}=b^2=1,\ a^b=a^{-1}\rangle,$$

be the dihedral group of order 2^m, $m>2$. Then $Z(D)=\langle a^{2^{m-2}}\rangle$, and Theorem 2 does not hold.

COROLLARY 1. *Let* $Q=\langle a,b \mid a^{2^{m-1}}=b^2=c,\ c^2=1, a^b=a^{-1}\rangle$ *be the generalized quaternion group of order* 2^m.

Then the group Q has a trivial Schur multiplier.

Proof. Since $Z(Q)=\langle b^2\rangle=\langle a\rangle\cap\langle b\rangle$, this follows from Theorem 1.

COROLLARY 2. *Let* $D_n=\langle a,b \mid a^n=b^2=1,\ a^b=a^{-1}\rangle$ *be the dihedral group of order* $2n$. *Then*

(1) *if n is odd, D_n has a trivial Schur multiplier, and*

(2) *if n is even,* $|M(D_n)|=2$.

Proof. (1) The center $Z(D_n)$ is trivial. Hence the assertion (1) follows from Theorem 1.

(2) Since $Z(D_n)=\langle a^{\frac{n}{2}}\rangle$, we have $|M(D_n)|\leq|Z(D_n)|=2$ by Theorem 1. On the other hand, let

$$D_{2n}=\langle a,b\,|\,a^{2n}=b^2=1,\ a^b=a^{-1}\rangle$$

be the dihedral group of order $4n$. Then it can be easily shown that $D_n\cong D_{2n}/Z(D_{2n})$. This means that D_{2n} is a central extension of D_n with kernel $Z(D_{2n})$. Moreover, since $Z(D_{2n})\subseteq D_{2n}'$, we can use Proposition 2 in section 2 to obtain that $2=|Z(D_{2n})|\leq|M(D_n)|$.

Therefore, we conclude that $|M(D_n)|=2$.

References

1. Curtis, C. W. and Reiner, I., *Representation theory of finite groups*, Wiley, New York, 1962.
2. Dornhoff, L., *Group representation theory Part A*, Marcel Dekker, New York, 1971.
3. Gorenstein, D., *Finite groups, Harper and Row*, New york, 1968.
4. Huppert, B., *Endliche Gruppen* I., Springer, Berlin, 1967.
5. Issacs, I. M., *Character theory of finite group*, Academic Press, New York, 1976.
6. McCoy, N. H., *The theory of numbers*, Macmillian, London, 1965.
7. Schur, I., *Über die Darstellung der endlichen Gruppen durch gebrochene lineare Substitutionen*, J. reine angew. Math. **127** (1964), 20–50.
8. Schur, I., *Untersuchungen über die Darstellung der endlichen Gruppen durch gebrochene lineare Substitutionen*, J. reine angew. Math. **132** (1907), 85–137.
9. Tahara, K., *On the second cohomology groups of semidirect products*, Math. Z. **129** (1972), 365–379.

Sogang University