Comm. Korean Math. Soc. 10 (1995), No. 2, pp. 275–284

ON GROUP EXTENSIONS AND REPRESENTATIONS

EUNMI CHOI

ABSTRACT. In this paper various G-module structures on M and all possible extensions of M by G will be studied, whence equivalence classes of extensions of M by G and those of extensions which are compatible with the given G-module structure of M will be determined explicitly. Further the difference between extensions and compatible extensions will be pointed out.

1. Introduction

Let G be a finite group and M be an (additive) abelian group. A group extension of M by G is a short exact sequence $(i,j) : 0 \to M \xrightarrow{i} E \xrightarrow{j} G \to 1$ such that $i(M) \subset E$. The purpose of this paper is to study various G-module structures on M and all possible extensions of M by G, whence is to determine equivalence classes of extensions of M by G and those of extensions which are compatible with the given G-module structure of M, precisely. Further the difference between extensions and compatible extensions will be pointed out. In doing this, the second cohomology group $H^2(G,M)$ will play important role; the connection $H^2(G,M)$ with group representation will be also discussed. Some results in this paper may be known or suspect to be true to many mathematicians; the aim here is to describe and record in print explicitly the results.

Received September 30, 1994.
AMS subject classfication: 20.
Key words: group extension, group representation.

2. Extensions of groups

Throughout the paper, G refers to a finite group and M refers to an (additive) abelian group. A homomorphism $\psi : G \to \mathrm{Aut}(M)$ of G into the automorphism group is an action of G on M. We remark an easy lemma.

LEMMA 1. *If an action $\psi : G \to Aut(M)$ is given, then M can be made into a G-module by defining $gm = -\psi(g)(m)$ for $g \in G$, $m \in M$. Conversely, a G-module structure on M gives an action of G on M. On the other hand, a group extension $0 \to M \to E \to G \to 1$ determines an action ψ of G on M, and this action furnishes M with a G-module structure.*

Two extensions E_1 and E_2 of M by G are said to be *equivalent* provided that there is a homomorphism $\alpha : E_1 \to E_2$ which renders the following commutative diagram:

$$\begin{array}{ccccccccc} 0 & \to & M & \xrightarrow{i} & E_1 & \xrightarrow{j} & G & \to & 1 \\ & & \| & & \downarrow \alpha & & \| & & \\ 0 & \to & M & \xrightarrow{i'} & E_2 & \xrightarrow{j'} & G & \to & 1 \end{array}$$

Here, α is an isomorphism and this forms an equivalence relation. Thus we may speak about the equivalence class of group extensions and will denote it by $\{E\}$. Note that equivalent extensions are isomorphic, but isomorphic extensions need not be equivalent (see Remark 2).

Let M be a given G-module. We say that an extension $0 \to M \to E \to G \to 1$ is *compatible* with the G-module structure of M if the G-module structure obtained from the extension following Lemma 1 coincides with the given module structure of M. Any extension which is equivalent to a compatible extension of M by G is also a compatible extension; this yields the set of all equivalence classes of compatible extensions, which is denoted by $\mathcal{E}(G, M)$. The sets $\mathcal{E}(G, M)$ and $\{E\}$ are strongly related to the second cohomology group $H^2(G, M)$, in the following way.

LEMMA 2. *Let M be a G-module. Then $H^2(G, M) \cong \mathcal{E}(G, M)$. If the given module structure M of G is trival then $H^2(G, M) \cong \{E\}$. Further, if E is a split extension then $H^2(G, M) = \{0\}$.*

Indeed, over a split extension $0 \to M \to E \to G \to 1$, E is a semidirect product $M \times G$ and 2-cocycles arise over the extension are trivial.

3. Group extensions of cyclic groups

In this section we consider various G-module structures on M and group extensions of M by G. Note that for a prime p, $\mathrm{Aut}(Z_p)$ is isomorphic to Z_p^*, where Z_p^* is the multiplicative cyclic group of order $p-1$.

THEOREM 1. *Let* $M = Z_p$ *and* $G = \langle z \mid z^p = 1 \rangle$. *Let* $E_1 = \langle x \mid x^{p^2} = 1 \rangle$ *and* $E_2 = Z_p \oplus Z_p$.

(1) (i) *There are exactly* $p-1$ *nonequivalent group extensions of the form* $0 \to M \to E_1 \to G \to 1$.

(2) (ii) *There is unique group extension of the form* $0 \to M \to E_2 \to G \to 1$.

PROOF. Since $\langle x^p \rangle$ is the only subgroup of E_1 of order p, we may consider an exact sequence

$$(1) \qquad (i_r, j_s): \ 0 \to M \xrightarrow{i_r} E_1 \xrightarrow{j_s} G \to 1$$

for each $1 \leq r,\ s \leq p-1$, where i_r and j_s are homomorphisms such that $i_r(\bar{1}) = x^{pr}$ and $j_s(x) = z^s$. It is easy to show that (i_r, j_s) is equivalent to the extension (i_k, j_1), where $k \equiv rs \pmod{p}$. Assume that (i_r, j_1) and (i_k, j_1) are equivalent. There is a homomorphism $\alpha: E_1 \to E_1$ which commutes the diagram:

$$\begin{array}{ccccccccc} 0 & \to & M & \xrightarrow{i_r} & E_1 & \xrightarrow{j_1} & G & \to & 1 \\ & & \| & & \downarrow \alpha & & \| & & \\ 0 & \to & M & \xrightarrow{i_k} & E_1 & \xrightarrow{j_1} & G & \to & 1 \end{array}$$

Let $\alpha(x) = x^a$ for some $a \in Z$. Then $a \equiv 1 \pmod{p}$ and $ra \equiv k \pmod{p}$. This yields that $r \equiv k \pmod{p}$ and $i_r = i_k$. Therefore there are $p-1$ non-equivalent extensions

$$(2) \qquad (i_1, j_1),\ (i_2, j_1),\ \cdots,\ (i_{p-1}, j_1),$$

as is required. For second part, let $i : M \to E_2$ and $j : E_2 \to G$ be homomorphisms such that $i(\bar{1}) = (\bar{1}, \bar{0})$ and $j(\bar{a}, \bar{b}) = z^b$. Then i and j yield a group extension

$$(3) \qquad (i,j) : \ 0 \ \to \ M \ \to \ E_2 \ \to \ G \ \to 1.$$

Suppose that there is another group extension $(i', j') : \ 0 \ \to \ M \ \xrightarrow{i'} \ E_2 \ \xrightarrow{j'} \ G \ \to 1$. If we consider $E_2 = Z_p \oplus Z_p$ as a 2-dimensional vector space over a field Z_p, then $\mathrm{im}(i') = \ker(j')$ is an 1-dimensional subspace of E_2 generated by $i'(\bar{1}) = u$. Let v be an element of E_2 such that $j'(v) = z$. Then $v \notin \mathrm{im}(i')$ and $E_2 = Z_p u \oplus Z_p v$. This yields an automorphism $\alpha : \ E_2 \to E_2$ such that $\alpha(\bar{1}, \bar{0}) = u$ and $\alpha(\bar{0}, \bar{1}) = v$. Since $\alpha i(\bar{1}) = u = i'(\bar{1})$ and $j'\alpha(\bar{a}, \bar{b}) = j'(au + bv) = z^b = j(\bar{a}, \bar{b})$, the group extension (i', j') is equivalent to (i, j). This completes the proof.

A simple outline of the following theorem was remarked in [6, *p.*156] by using relations to the second cohomology group. Here, we shall discuss it more precisely by finding all possible extensions explicitly.

THEOREM 2. *Let $M = Z_p$ and $G = \langle z \mid z^p = 1 \rangle$ as in Theorem 1. Then the only action of G on M is the trivial action. Further, there are p equivalence classes of extensions of M by G, and $H^2(G, M) \cong Z_p$.*

PROOF. Since $\mathrm{Aut}(M) \cong Z_p^*$ and $\gcd(p, p-1)=1$, we have $\mathrm{Hom}(G, \mathrm{Aut}(M)) \cong \{0\}$; this isomorphism follows from the fact that $\mathrm{Hom}(Z_m, Z_n) \cong Z_d$, where $d = \gcd(m, n)$. Thus there is only a trivial action and a trivial G-module structure on M. Let $0 \to M \to E \to G \to 1$ be any extension of M by G. Then E is an abelian group of order p^2, hence any extension of M by G is compatible with the trivial G-module structure of M. Further E is isomorphic to either $E_1 = \langle x \mid x^{p^2} = 1 \rangle$ or $E_2 = Z_p \oplus Z_p$. E_1 is not isomorphic to E_2 so that the group extension (i, j) in (3) is not equivalent to any extension of the form (i_r, j_1) in (2) for all $1 \leq r \leq p-1$. Therefore, there are exactly p nonequivalent group extensions

$$(i_1, j_1), \ \cdots, \ (i_{p-1}, j_1), \ (i, j)$$

of M by G. In particular, this implies that $|H^2(G, M)| = p$ by Lemma 2, so that $H^2(G, M) \cong Z_p$. This completes the proof.

For more generalization of Theorem 2, the next two theorems will be devoted to the case that M and G are two cyclic groups of different prime orders.

THEOREM 3. *Let $M = Z_p$ and $G = \langle z | \ z^q = 1 \rangle$, where p and q are distinct primes. Suppose that q does not divide $p-1$. Then the only G-module structure of M is the trivial one and there is exactly one equivalence class of extensions of M by G. In particular $H^2(G, M) = \{0\}$, where M is the trivial G-module.*

PROOF. Since $\gcd(q, p-1) = 1$, the first statement follows from the same reason for Theorem 1. Consider the extension E of M by G. Then G-module structure of M furnished by this extension must be trivial, so that E is an abelian group of order pq. Hence $E = \langle x \rangle \times \langle y \rangle = \langle xy \rangle$, where x and y are of order p and q respectively. And every extension of M by G is compatible with the trivial G-module structure of M. For each r and s with $1 \leq r \leq p-1$ and $1 \leq s \leq q-1$, consider an exact sequence of M by G (i_r, j_s) : $0 \ \to M \ \xrightarrow{i_r} \ E \ \xrightarrow{j_s} \ G \ \to 1$ where i_r and j_s are homomorphisms defined by

$$i_r(\bar{1}) = x^r; \quad j_s(x) = 1, \quad j_s(y) = z^s. \tag{4}$$

Since $\langle x \rangle$ is the unique subgroup of E of order p, these are the all extensions of M by G. Moreover by assigning the relations

$$\alpha(x) = x^k, \quad \text{where} \quad kr \equiv 1 \pmod{p}, \quad \text{and} \quad \alpha(y) = y^s$$

to $\alpha : E \ \to E$, we can show that (i_r, j_s) is equivalent to (i_1, j_1). This proves Theorem 3.

THEOREM 4. *Let M and G be as in Theorem 3. Suppose that q does divide $p-1$. Then there are exactly q distinct G-module structures of M. For each G-module structure of M, there is exactly one equivalence class of compatible extensions of M by G. In particular, for each G-module structure of M we have $H^2(G, M) = \{0\}$. There are however exactly q equivalence classes of extensions of M by G.*

PROOF. Since $\gcd(p-1,q)=q$ and Z_p^* is cyclic of order $p-1$, there is a unique subgroup H of Z_p^* of order q, and $\mathrm{Hom}(G,\mathrm{Aut}(M)) \cong \mathrm{Hom}(G,Z_p^*) \cong H$. Set $H=\langle \bar{t} \rangle$ where $\bar{t}^q=\bar{1}$. Then $\mathrm{Hom}(G,\mathrm{Aut}(M)) = \{\psi_0,\psi_1,\cdots,\psi_{q-1}\} \cong \langle \bar{t} \rangle$ where each homomorphism $\psi_k : G \to \mathrm{Aut}(M)$ is given by $(\psi_k(z))(\bar{1}) = \bar{t}^k = \overline{(t^k)}$ for $0 \le k \le q-1$. Thus every ψ_k gives rise to a G-module structure on M, and there are q distinct G-module structures on M. We consider the following two cases.

Case 1. Suppose that M is furnished with a G-module structure by ψ_0. The action should be trivial, hence by the same arguments as that in Theorem 3, every extension of M by G which is compatible with the trivial G-module structure of M is equivalent to the extension

$$(5) \qquad (i,j): \quad 0 \to M \xrightarrow{i} E_0 \xrightarrow{j} G \to 1$$

where $E_0=\langle x \rangle \times \langle y \rangle$, $x^p=y^q=1$, and i and j are homomorphisms defined by $i(\bar{1})=x$; $j(x)=1$ and $j(y)=z$. Thus there is exactly one class of extensions which are compatible with the trivial G-module structure on M.

Case 2. Suppose that M is furnished with a G-module structure by ψ_k, $1 \le k \le q-1$. E is a nonabelian group of order pq, and has a normal subgroup of order p, say $\langle x \rangle$. Let t be a fixed integer such that $t \not\equiv 1 \pmod p$ and $t^q \equiv 1 \pmod p$. Then E contains an element y to be

$$E = \langle\, x,y \mid x^p=1,\ y^q=1,\ x^y=x^t \,\rangle.$$

Thus there are exactly $(p-1)(q-1)$ extensions. Indeed they are of the form $(i_r,j_s): \quad 0 \to M \xrightarrow{i_r} E \xrightarrow{j_s} G \to 1$, where i_r and j_s $(1 \le r \le p-1,\ 1 \le s \le q-1)$ are defined by the same way as in (4).

Suppose that the extension (i_r,j_s) is compatible with the G-module structure of M furnished by fixed ψ_k, for $1 \le k \le q-1$. Let a be an integer such that $as \equiv 1 \pmod q$, $1 \le a \le q-1$. Then $j_s(y^a)=z$ and the compatibility yields $i_r(\psi_k(z)(\bar{1})) = (i_r(\bar{1}))^{y^a}$. This implies that $a=k$ and $ks \equiv 1 \pmod q$. Therefore, for each ψ_k, there are exactly $(p-1)$ extensions

$$(i_1,j_s),\ \cdots,\ (i_{p-1},j_s)$$

of M by G which are compatible with ψ_k, where $ks \equiv 1 \pmod{p}$. Moreover, these extensions are equivalent to each other: that is, a map $\alpha : E \to E$, $\alpha(x) = x^r$, $\alpha(y) = y$, $(1 \leq r \leq p-1)$ shows that every (i_r, j_s) is equivalent to (i_1, j_s). Hence, there is exactly one equivalence class of extensions of M by G which are compatible with the G-module structure of M furnished by ψ_k.

Assume that two extensions (i_1, j_s) and (i_1, j_l) for some $1 \leq s, l \leq q-1$ are equivalent. Then there is an automorphism $\alpha : E \to E$ which makes the diagram commute:

$$\begin{array}{ccccccccc} 0 & \to & M & \xrightarrow{i_1} & E & \xrightarrow{j_s} & G & \to & 1 \\ & & \| & & \downarrow \alpha & & \| & & \\ 0 & \to & M & \xrightarrow{i_1} & E & \xrightarrow{j_1} & G & \to & 1 \end{array}$$

The commutivity defines $\alpha(x) = x$ and $\alpha(y) = x^a y^b$, where a is any integer and b is a positive integer with $bl \equiv s \pmod{q}$. Since $x^y = x^t$ and $x^{t^b} = x^t$ so that $t^b \equiv t \pmod{p}$. Since $\bar{t} \in Z_p^*$, i.e., $\langle t \rangle$ is of order q, this guarantees $q \mid b-1$. Therefore, $b \equiv 1 \pmod{q}$, and $l \equiv s \pmod{q}$, thus $l = s$. Hence the extensions (i_1, j_s) and (i_1, j_l) are identical. This shows that the $(q-1)$ extensions

$$(i_1, j_1),\ (i_1, j_2), \cdots, (i_1, j_q)$$

are non-equivalent. Moreover, the extension (i, j) is not equivalent to any of the (i_r, j_s). Thus there are exactly q equivalent classes of extensions of M by G. This completes the proof of Theorem 4.

4. Cohomology groups and group representations

As was remarked, studying group extension is related to studying group representation. This section is devoted to the subject. For convenience, we assume that M is a multiplicative group. When we say a group extension $1 \to M \xrightarrow{i} E \xrightarrow{j} G \to 1$ *central*, we mean $i(M) = M$ is contained in the center of E. We may consider the equivalence class of central group extensions. The next theorem shows connections between the class of group extensions, $H^2(G, M)$ and representations.

THEOREM 5. *Let F be a field and G acts trivially on F. Let M be a cyclic group such that a primitive $|M|$-th root of unity is contained in F^*. Then there are bijective correspondences between the following 4 classes:*

(1) (i) *equivalence class of central cyclic group extensions* $1 \to M \to E \to G \to 1$.
(2) (ii) *second cohomology group* $H^2(G, F^*)$ *arises from a central cyclic group extension by* G.
(3) (iii) *equivalence class of twisted group algebra* $F \circ G$.
(4) (iv) *equivalence class of projectively equivalent projective representations of* G.

PROOF. The terminologies appeared in (iii) and (iv) can be found in [2] or [3]. Any equivalent central cyclic group extensions $1 \to M \to E \to G \to 1$ provide cohomologous 2-cocycles, say α_1, α_2 in $Z^2(G, M)$. Since $\mathrm{Hom}(M, F^*)$ is a cyclic group with a generator, say χ, we may consider a transgression map

$$\mathrm{tra} : \mathrm{Hom}(M, F^*) \to H^2(G, F^*), \quad \text{where } \mathrm{tra}(\chi) = \overline{\chi\alpha_i}.$$

Write $\overline{\chi\alpha_i}$ by $\overline{f_i}$ in $H^2(G, F^*)$. Since $\chi\alpha_1$ is cohomologous to $\chi\alpha_2$ in $Z^2(G, F^*)$, $\overline{f_1} = \overline{f_2}$. Conversely, let f be a 2-cocycle in $\overline{f} \in H^2(G, F^*)$ arising from a central cyclic group extension of M by G. Without lose of generality, we may consider $f(g, x) \in M$ for all $g, x \in G$, i.e., $f \in Z^2(G, M)$. Define a set $E = M \times G$ with multiplication $(m_1, g)(m_2, x) = \big(m_1 m_2 f(g, x),\ gx\big)$. Then E is a group extension which affords the 2-cocycle f. Suppose that $f' \in Z^2(G, F^*)$ be cohomologous to f. Then $f(g, x) = t(g)t(x)t(gx)^{-1} f'(g, x)$ for some map $t : G \to M$ with $t(1_G) = 1_M$. Define $E' = M \times G$ by $(m_1, g)(m_2, x) = \big(m_1 m_2 f'(g, x),\ gx\big)$. Then a map $\alpha : E \to E'$ defined by $\alpha(m, g) = (mt(g), g)$ is a homomorphism and yields the commutativity of two extensions E and E'. This proves the equivalence of (i) and (ii).

Consider a twisted group algebra with an F-basis $\{a_g \mid g \in G\}$ where $a_g a_x = f(g, x) a_{gx}$ for $f(g, x) \in F^*$. The associativity of a_g implies that f is a 2-cocycle. Two equivalent twisted group algebras yield two cohomologous 2-cocycles, and vice versa; this shows the equivalence of

(ii) and (iii). Write F^fG for a twisted group algebra corresponding to f and write V for a F^fG-module. Then $P : G \to GL(V)$ defined by $P(g)v = gv$ $(g \in G,\ v \in V)$ and $P(g)P(x) = f(g,x)P(gx)$ is a projective (f)-representation of G. Suppose we have two equivalent twisted group algebras $F^{f_1}G$ and $F^{f_2}G$ for $f_1,\ f_2 \in Z^2(G,F^*)$. Then f_1 is cohomologous to f_2. Let P_1 be a f_1-representation on V. Then there is a f_2-representation on V which is projectively equivalent to P_1 (see [3. p.72, 77]). The converse direction is clear, so that this gives the equivalence of (iii) and (iv). This completes the proof.

Suppose we have a 2-cocycle $f \in Z^2(G,F^*)$ of finite order l. Then F contains a primitive l-th root of unity ζ. Consider a finite multiplicative group $G(f) = \{\zeta^i a_g |\ g \in G,\ i \in Z\} \subseteq F^fG$. Let $A(f) = \{\zeta^i a_1 |\ i \in Z\} \cong \langle\zeta\rangle$. The group $G(f)$ is called an f-covering group and yields a central cyclic group extension

$$1 \to A(f) \to G(f) \xrightarrow{j} G \to 1, \tag{6}$$

where $j(\zeta^i a_g) = g$. For this definition, we may refer to [5] or [3].

COROLLARY. *Any 2-cocycle yielded by the extension (6) is cohomologous to f.*

EXAMPLE. For an explicit example of the situation in Theorem 5, related to the extension (6), let $G = \{1, x, y, xy\}$ and F be a field containing a primitive 2-th root of unity. Consider $D_4 = \langle c, d |\ c^4 = d^2 = 1,\ d^{-1}cd = c^{-1}\rangle$. Then $D_4/\langle c^2\rangle \cong G$ and

$$1 \to \langle c^2\rangle \to D_4 \xrightarrow{j} G \to 1 \tag{7}$$

is a central cyclic group extension. Choose a transversal $\{r_g |\ g \in G\}$ of $\langle c^2\rangle$ in D_4. Then $j(r_g) = g$ for any $g \in G$ and a section $\lambda : G \to D_4$ of j can be defined by $\lambda(g) = r_g$. We may consider $r_x = c$, $r_y = d$ and $r_{xy} = cd$, so that $j(r_x r_y) = j(r_x)j(r_y) = cd = j(r_{xy})$, and hence $r_x r_y = f(x,y)r_{xy}$ for $f(x,y) \in \langle c^2\rangle$. For any $\chi \in \mathrm{Hom}(\langle c^2\rangle, F^*)$, we consider $\chi f(g,h) = \pm 1 \in F^*$ for all $g, h \in G$. We may use the same notation f for χf. Then $f \in Z^2(G,F^*)$ of order 2.

Let T be a representation of D_4. Define a map T_1 on G by $T_1(g) = T(r_g)$ for $g \in G$. Then $T_1(g)T_1(h) = T(r_g r_h) = f(g,h)T_1(gh)$. Thus T_1 is a projective representation of G, which can be lifted to T.

In this case, $|G(f)| = 8$ and $|A(f)| = 2$. Further the twisted group algebra F^fG with basis r_g $(g \in G)$ is not commutative, so that $G(f)$ is identical with D_4. Thus the extension yielded by f like (6) is equivalent to the original extension (7).

REMARK. 1. If $G(f) = A(f) \times G$ is a direct product then $\{\zeta^i a_g |\ g \in G\} = \{\zeta^i g | g \in G\}$. Hence we may consider $a_g = g$, this implies $f(g,h) = 1$ for all $g, h \in G$. The converse is also true.

2. Of course, $D_n = \langle c, d |\ c^n = d^2 = 1,\ dc = c^{-1}d\rangle$ is a semi-direct product $\langle c\rangle \times \langle d\rangle$. Thus D_n is a split extension of $\langle c\rangle$ by $\langle d\rangle$, and it gives a trivial 2-cocycle. When $n = 4$, this extension is not equivalent to (7).

References

1. Babakhanian, A., *Cohomological method in group theory*, Marcel Dekker, New York, 1972.
2. Choi, E. M, *Projective representations, abelian F-groups and central extensions*, J. Algebra **159** (1993), 242-256.
3. Karpilovsky, G., *Projective representations of finite groups*, Marcel Dekker, New York/Basel, 1985.
4. Lyndon, R. C., *The cohomology theory of group extensions*, Duke Math. J. **15** (1948), 271-292.
5. Reynolds, W. F., *Noncommutators and the number of projective characters of a finite group*, Proc. Symp. Pure Math. **47** (1982), 71-74.
6. Rotman, J. J., *An introduction to homological algebra*, Academic Press, 1979.
7. Tahara, K. I., *On second cohomology groups of semi-direct products*, Math. Z. **129** (1972), 365-379.

HanNam University
Ojungdong, Taejon