Bull. Korean Math. Soc. **35** (1998), No. 4, pp. 719–726

CONJUGACY CLASSES OF SUBGROUPS OF SPLIT METACYCLIC GROUPS OF PRIME POWER ORDER

HYO-SEOB SIM

ABSTRACT. In this paper, we consider conjugacy of subgroups of some split metacyclic groups of odd prime power order to determine the numbers of conjugacy classes of subgroups of those groups. The study was motivated by the linear isomorphism problem of metacyclic primitive linear groups.

1. Introduction

Let $G = GL(n, q)$ be the general linear group of degree n over the field of q elements. As is well known from the representation theory of cyclic groups, there is a unique conjugacy class of irreducible cyclic subgroups of order $q^n - 1$ in G, which are called *Singer cycles*. Let $Y = \langle y \rangle$ be such a Singer cycle. Then the normalizer $H = N_G(Y)$ is a split extension of Y by a cyclic group $X = \langle x \rangle$ of order n, where $x^{-1}yx = y^q$. Thus, if π denotes the set of prime divisors of n, we have $H = PQ$, where P is a Hall π-subgroup of H and Q the Hall π'-subgroup of Y. In [3], it was shown that if n is a power of an odd prime, the conjugacy classes of metacyclic primitive subgroups of G are completely determined by the conjugacy classes of P-conjugacy classes of subgroups of P and the irreducible subgroups of Q. In this point of view, the study of the conjugacy problem of split metacyclic p-groups has importance.

Let P now be *any* finite split metacyclic p-group for an odd prime p. Such a group P is a semidirect product of two cyclic subgroups A and B, that is, $P = A \ltimes B$.

Received February 12, 1998.

1991 Mathematics Subject Classification: 20D15, 20G40.

Key words and phrases: metacyclic p-groups, conjugate subgroups, primitive linear groups.

This work was supported by KOSEF research grant 96-0701-03-01-3.

Let C and D be arbitrary subgroups of A and B, respectively. Let $\mathcal{D}(C, B/D)$ be the (additive) group of all derivations from C to B/D, and $\mathcal{I}(C, B/D)$ the subgroup of $\mathcal{D}(C, B/D)$ consisting of the inner derivations (for the related terminology and the general background, see p. 304–305 in [2]). The corresponding factor group $\mathcal{D}(C, B/D)/\mathcal{I}(C, B/D)$ is the first cohomology group $H^1(C, B/D)$ of C with coefficients in B/D.

For every derivation δ in $\mathcal{D}(C, B/D)$, we define

$$[C, D, \delta] := \{\, cb : c\delta = bD,\ c \in C \,\}.$$

Then $[C, D, \delta]$ is a subgroup U such that $UB = CB$ and $U \cap B = D$. On the other hand, all subgroups of P can be realized in this way. In fact, for every subgroup U there exist subgroups C in A and D in B and a derivation δ in $\mathcal{D}(C, B/D)$ such that $U = [C, D, \delta]$. We also note that such a realization of a given subgroup is unique.

Let $A = \langle a \rangle$ and $B = \langle b \rangle$. Then $b^a = b^q$ for some positive integer q with $q^{|A|} \equiv 1 \bmod |B|$. For any $\delta \in \mathcal{D}(C, B/D)$, we define δ^a as the function which maps c to $(c\delta)^a$, for every $c \in C$. Note that $\delta \mapsto \delta^a$ is an automorphism of $\mathcal{D}(C, B/D)$ with δ^a the qth multiple, $q\delta$, of δ. So the map induces a natural action of A on $\mathcal{D}(C, B/D)$. This shows that $\mathcal{D}(C, B/D)$ is an A-module. Since $\mathcal{I}(C, B/D)$ is evidently an A-submodule, the quotient $H^1(C, B/D)$ is also an A-module.

Then we will show that the following theorem.

THEOREM 1.1. *Let $h(C, D)$ be the order of $H^1(C, B/D)$ for subgroups C of A and D of B, and let $|q \bmod d|$ be the smallest positive integer i such that $q^i \equiv 1 \bmod d$. There exist exactly*

$$\sum_{C \le A, D \le B} \sum_{d \mid h(C,D)} \frac{\phi(d)}{|q \bmod d|}$$

conjugacy classes of the subgroups of P.

Let p^α be the order of A and let p^β be the p-part of $q - 1$. Since p is an odd prime, we see that $p^{\alpha+\beta}$ is the p-part of $q^{|A|} - 1$. In view of our motivation, we are only interested in the case when $|B| = p^{\alpha+\beta}$,

that is, A acts on B faithfully by conjugation. Note that $h(C,D)$ is the minimum of $|C|, |D|, |B|/|C|$ and $|B|/|D|$ in this case.

The following two results improve the above result under some extra restriction.

THEOREM 1.2. *Suppose that A acts on B faithfully by the conjugation and $|A|$ divides $p(q-1)$. Then $[C,D,\delta_1]$ is conjugate to $[C,D,\delta_2]$ by an element in P if and only if $\delta_1 + \mathcal{I}(C,B/D) = \delta_2 + \mathcal{I}(C,B/D)$; so there exists a one to one correspondence between the set of all conjugacy classes of subgroups of P and $H^1(P) := \{(C,D,\Delta) \mid C \leq A,\ D \leq B,\ \Delta \in H^1(C,B/D)\}$.*

THEOREM 1.3. *Under the assumptions of* Theorem 1.2, *there exist exactly*

$$(\beta - \alpha + 1)(p^{\alpha+1} - 1)/(p-1) + 4\sum_{i=0}^{\alpha-1} p^i(\alpha - i)$$

conjugacy classes of subgroups of P.

2. Basic facts

We first state the following useful fact without proof.

LEMMA 2.1. *Let p be an odd prime, let m, n be nonnegative integers and let r be an integer.*

(i) *If $r \equiv 1 \bmod p$, then $|r \bmod p^n| = p^n/\gcd(p^n, r-1)$.*

(ii) *If $r^{p^m} \equiv 1 \bmod p^n$, then $1 + r + \cdots + r^{p^m-1} \equiv p^m \bmod p^n$.*

Let G be a metacyclic group and K a cyclic normal subgroup with cyclic quotient. Then G has a cyclic subgroup S such that $G = SK$. Such a factorization $G = SK$ is called a *metacyclic factorization*. In particular, if $S \cap K = 1$, the metacyclic factorization is called *split*. A metacyclic group is *split* if it has a split metacyclic factorization.

We now collect some basic properties of metacyclic groups; we will use this facts without always pinpointing the references. For the proof, see [1] for example.

LEMMA 2.2. *Let G be a metacyclic group with a metacyclic factorization $G = SK$. Let $S = \langle x \rangle$, $K = \langle y \rangle$. Let r be an integer such that $y^x = y^r$. Define $s := |r \bmod |K||$ and $t := |K|/\gcd(|K|, r-1)$. Then*
(i) $G' = \langle y^{r-1} \rangle$;
(ii) $Z(G) = C_S(K)C_K(S) = \langle x^s, y^t \rangle$;
(iii) $|S/C_S(K)| = s$;
(iv) $|G'| = t$.

LEMMA 2.3. *Let P be a metacyclic p-group for odd p and let $P = SK$ be a metacyclic factorization. Then $P' \cong S/C_S(K)$.*

Proof. Since S is a finite p-group, $r^{p^i} \equiv 1 \bmod p$ for some nonnegative integer i. Fermat's Little Theorem yields $r \equiv 1 \bmod p$. By Lemma 2.1, we have $s = t$, so the result follows from (iii) and (iv) of the above lemma. □

3. Conjugacy of subgroups

We now turn to the conjugacy problem of the subgroups of our split metacyclic group $P = AB$. Keeping the notation in the introduction, we shall need the following elucidation of a result observed in [3]:

LEMMA 3.1. *$[C, D, \delta_1]$ is conjugate to $[C, D, \delta_2]$ by an element in P if and only if $\delta_1 + \mathcal{I}(C, B/D)$ and $\delta_2 + \mathcal{I}(C, B/D)$ are in the same orbit of the natural action of A on $H^1(C, B/D)$.*

We now need to calculate the derivations, the inner derivations and the quotients. Let ϕ be the endomorphism of B/D defined by $bD \mapsto b^f D$ where $f = (q^{|A|} - 1)/(q^{|A:C|} - 1)$. An element of B/D is the image of a generator of C under some derivation $C \to B/D$ if and only if that element lies in $\ker\phi$; once we know how a derivation acts on a given generator of C, there is no doubt how it must act on the other elements of C; hence $\mathcal{D}(C, B/D)$ is A-isomorphic to $\ker\phi$. This isomorphism maps $\mathcal{I}(C, B/D)$ onto the group $[C, B/D] = \{ [c_1, b_1]D : c_1 \in C,\ b_1 \in B \}$. Since B/D is cyclic, the subgroups $\ker\phi$ and $[C, B/D]$ are also cyclic. It now follows that $\mathcal{D}(C, B/D)$, $\mathcal{I}(C, B/D)$ and the quotient $H^1(C, B/D)$ are all cyclic. It is now sufficient to know the orders of the groups only.

We list the orders here without proof in the case when A acts faithfully on B.

LEMMA 3.2.
(i) $|\mathcal{D}(C,B/D)| = |\ker\phi| = \gcd\left(|B/D|,\ \frac{q^{|A|}-1}{q^{|A:C|}-1}\right)$
$= \min\{|C|,|B/D|\}$;
(ii) $|\mathcal{I}(C,B/D)| = \frac{|B/D|}{\gcd\left(|B/D|,\ q^{|A:C|}-1\right)} = \max\{1,|C|/|D|\}$;
(iii) $h(C,D) = \min\{|C|,|D|,|B|/|C|,|B|/|D|\}$.

As before, let a and b be fixed generators of A and B, and let q be a positive integer such that $b^a = b^q$.

Proof of Theorem 1.1. We first note that each subgroup U of P has a unique realization $U = [C,D,\delta]$ with $C \in A$, $D \in B$ and $\delta \in \mathcal{D}(C,B/D)$. Then $U \cap B = D$ and $U/D \cong C$. Since D is a normal subgroup of the whole group P, we see that D is determined by the conjugacy class of U in P. Moreover C is the unique subgroup of A with the order $|U/D|$. So C and D is completely determined by the conjugacy class of U. This amounts to say that each conjugate V of U in P has the realization $V = [C,D,\delta']$ for some δ' in $\mathcal{D}(C,B/D)$.

Let d be the order of the subgroup generated by $\delta + \mathcal{I}(C,B/D)$. Consider the natural action of A on the set of all generators of the group generated $\delta + \mathcal{I}(C,B/D)$. We see that the set of generators consists of exactly $\phi(d)$ elements. It is easy to see that a^m acts trivially on $\delta + \mathcal{I}(C,B/D)$ if and only if $|q \bmod d|$ divides m. So by Orbit-Stabilizer Theorem, $|q \bmod d|$ is the length of the A-orbit containing $\delta + \mathcal{I}(C,B/D)$ of order d in $H^1(C,B/D)$. Thus the set of generators is divided into $\phi(d)/|q \bmod d|$ orbits. Since $h(C,D) = |H^1(C,B/D)|$ and $H^1(C,B/D)$ is a cyclic p-group, the claim now follows from Lemma 3.1. □

We are now ready to prove Theorem 1.2.

Proof of Theorem 1.2. Suppose that $|A||p(q-1)$. The assumption is equivalent to $\alpha - 1 \leq \beta$. Note that P' is the subgroup of B such that $|P'| = |A|$ and $|B/P'| = p^\beta$. Let d be a positive divisor of $h(C,D)$. If $d < |A|$, then it is obvious that $|q \bmod d| = 1$. Suppose that $d = |A|$.

Then from Lemma 3.2 (iii), $h(C,D) = \min\{|C|, |D|, |B|/|C|, |B/D|\}$; so we have $|B/D| \geq |A|$ and $|D| \geq |A|$. It follows that $D \geq P'$, and so $|B/D|$ divides p^β. Since $d \leq |B/D|$, we have $|q \bmod d| = 1$. Consequently, for every divisor d of $H^1(C, B/D)$, we have $|q \bmod d| = 1$. As we observed in the proof of Theorem 1.1, $|q \bmod d|$ is the length of the A-orbit containing $\delta + \mathcal{I}(C, B/D)$ of order d in $H^1(C, B/D)$. So the first part of the Theorem is proved by Lemma 3.1.

Since

$$\sum_{C\in A, D\in B} \sum_{d|h(C,D)} \phi(d) = \sum_{C\in A, D\in B} h(C,D) = |H^1(P)|,$$

it follows from Theorem 1.1 that there exist precisely $|H^1(P)|$ conjugacy classes of subgroups of P, which completes the proof of the theorem. □

We now prove Theorem 1.3.

Proof of Theorem 1.3. The condition $\alpha - 1 \leq \beta$ implies that $|A| \leq p|B|/|P'|$. Note that $|P'| = |A|$ provided β is positive. Let

$$\mathcal{X} = \{(C,D) : C \leq A,\ P' \leq D \leq B,\ |P'| \leq |B/D|\}.$$

If $D \geq P'$ and $|B/D| < |P'|$, then there exits a proper subgroup D^* of P' such that $|B/D| = |D^*|$; so $h(C,D) = h(C,D^*)$ from Lemma 3.2 (iii). Thus

$$|H^1(P)| = \sum_{(C,D)\in\mathcal{X}} h(C,D) + 2 \sum_{C\leq A,\ D<P'} h(C,D).$$

We proceed with some convention:

$$\begin{aligned}
\mathcal{Y} &= \{(C,D) : C \leq A,\ |D| < |C|,\ D < P'\} \\
\mathcal{Z} &= \{(C,D) : C \leq A,\ |C| \leq |D|,\ D < P'\} \\
\mathcal{Y}(D) &= \{C : (C,D) \in \mathcal{Y}\} \\
\mathcal{Z}(C) &= \{D : (C,D) \in \mathcal{Z}\}
\end{aligned}$$

Then $|\mathcal{Y}(D)| = |\mathcal{Z}(C)| = \alpha - i$ provided that $|C| = |D| = p^i$, and the sets of all proper subgroups of A and P' have the same cardinality. Hence there exists a one-to-one correspondence between $\mathcal{Y}$ and $\mathcal{Z}$.

If $D < P'$ and $C \leq A$ then $|D| \leq |B|/|C|$ from condition $\alpha - 1 \leq \beta$. We easily observe that if $(C, D) \in \mathcal{Y}$ then $h(C, D) = |D|$; otherwise the order is $|C|$. So

$$\sum_{(C,D)\in\mathcal{Y}} h(C,D) = \sum_{(C,D)\in\mathcal{Z}} h(C,D).$$

Moreover, it is also obvious from Lemma 3.2 that $h(C, D) = |C|$ if $(C, D) \in \mathcal{X}$. On the other hand, the set $\{D : (C, D) \in \mathcal{X}\}$ has $(\beta-\alpha+1)$ elements. Consequently, we have

$$\begin{aligned}
|H^1(P)| &= \sum_{(C,D)\in\mathcal{X}} h(C,D) + 4 \sum_{(C,D)\in\mathcal{Y}} h(C,D) \\
&= \sum_{C\leq A} |C|(\beta - \alpha + 1) + 4 \sum_{D<P'} |D||\mathcal{Y}(D)| \\
&= \sum_{i=0}^{\alpha} p^i(\beta - \alpha + 1) + 4 \sum_{i=0}^{\alpha-1} p^i(\alpha - i) \\
&= \frac{p^{\alpha+1} - 1}{p - 1}(\beta - \alpha + 1) + 4 \sum_{i=0}^{\alpha-1} p^i(\alpha - i).
\end{aligned}$$

So the theorem is proved. □

4. An application

We here apply our result to determine the number of conjugacy classes of metacyclic primitive subgroups of the general linear group $G = GL(p, q)$ for odd prime p.

Let $Y = \langle y \rangle$ be irreducible cyclic subgroup of order $q^p - 1$ and let H be the normalizer of Y in G. Then H is a split extension of Y by a cyclic group $X = \langle x \rangle$ of order p, where $x^{-1}yx = y^q$. Thus we have $H = PQ$, where P is a Hall p-subgroup of H and Q the Hall p'-subgroup of Y.

With this notation, we first mention a special case of Theorem 1.1 of [3]:

LEMMA 4.1. *Every primitive metacyclic subgroup of G has a conjugate of the form MN, where M is a subgroup of P and N is an irreducible subgroup of Q; conversely, each such product is metacyclic and primitive. Two such products, M_1N_1 and M_2N_2 are conjugate in G if, and only if, M_1 is P-conjugate to M_2 and $N_1 = N_2$.*

The following lemma is easy to derive from well-known results:

LEMMA 4.2. *A subgroup U of Y is irreducible if and only if $|U|$ does not divide $q-1$.*

Let $A := X$ and $B := P \cap Y$. Then $P = A \ltimes B$. Utilizing Theorem 1.3, we now have the following immediate consequence of the above observations.

COROLLARY 4.3. *Let p be an odd prime. Let $\delta(m)$ be the number of divisors of an integer m and let β be the largest positive integer such that p^β divides $q-1$.*

(1) If p does not divide $q-1$, then there exist precisely $2[\delta(q^p - 1) - \delta(q-1)]$ different conjugacy classes of the primitive metacyclic subgroups in $GL(p,q)$.

(2) If p divide $q-1$, there exist precisely $[(p+1)\beta + 4] \cdot [\delta((q^p - 1)/p^{\beta+1}) - \delta((q-1)/p^\beta)]$ different conjugacy classes of the primitive metacyclic subgroups in $GL(p,q)$.

References

[1] F. R. Beyl and J. T. Tappen, *Group Extensions, Representations, and the Schur Multiplicator*, vol. 958, Lecture Notes in Math., Springer-Verlag, Berlin New York, 1982.

[2] Derek J. Robinson, *A Course in the Theory of Groups*, Springer-Verlag, Berlin New York, 1982.

[3] Hyo-Seob Sim, *Metacyclic primitive linear groups*, Communications in Algebra **22** (1994), 269–278.

DIVISION OF MATHEMATICAL SCIENCES, PUKYONG NATIONAL UNIVERSITY, PUSAN 608-737, KOREA

E-mail: hsim@dolphin.pknu.ac.kr