COMMUTATOR EXTENSIONS OF FINITE GROUPS

Hironori Onishi

Let K and H be groups. Let us call an extension G of K by H a *commutator extension* if K is the commutator subgroup G' of G. In order that there may exist a commutator extension of K by H, H must be abelian. Henceforth, we assume that H is abelian and finite. On the other hand, if K' is the commutator subgroup of K, then K/K' is abelian. We assume that K/K' is also finite. Our problem is to find necessary and sufficient conditions for the existence of a commutator extension of K by H.

We shall first reduce the problem to the case in which K is an elementary abelian p-group. Theorem 4 then gives necessary and sufficient conditions for the existence of a split commutator extension. Following that come other results on nonsplit commutator extensions.

To begin, let us note that the commutator subgroup K' of K is normal not only in K, but also in every extension of K, because K' is a characteristic subgroup of K.

THEOREM 1. G *is a commutator extension of* K *by* H *if and only if* G/K' *is a commutator extension of* K/K' *by* H.

Proof. From the isomorphism $G/K \cong (G/K')/(K/K')$, it follows that G is an extension of K by H if and only if G/K' is an extension of K/K' by H. Now, if $K = G'$, then $(G/K')' = G'K'/K' = K/K'$. Conversely, if $(G/K')' = K/K'$, then $K/K' = G'K'/K' = G'/K'$, and hence, $K = G'$. q.e.d.

This theorem reduces the problem to the case in which K is finite abelian. If K is trivial, then every extension of K by H is a commutator extension (because H is abelian). Therefore, we assume that K is a nontrivial finite abelian group.

Before proceeding further, we propose to summarize the theory of extensions of K by H, where K and H are finite abelian groups [3, Chapter III, Sections 6 to 8].

Let G be an extension of K by H, so that $G/K \cong H$. Let $\phi: G \to H$ be the epimorphism whose kernel is K. An element $\bar{u}$ of G is called a *representative* of $u \in H$ if $\phi(\bar{u}) = u$. Let $(z_1, \cdots, z_s)$ be a basis of H, and let m_i be the order of z_i. An s-tuple $S = (\bar{z}_1, \cdots, \bar{z}_s)$ is called a *representative set* of the basis if each $\bar{z}_i$ is a representative of z_i. Given a pair (G, S), we define a triple (X, B, M), where

$$X = (x_1, \cdots, x_s), \quad B = (b_1, \cdots, b_s), \quad M = (b_{ij}) \quad (1 \leq i \leq s,\ 1 \leq j \leq s),$$

by the conditions

(1) $a^{x_i} = \bar{z}_i^{-1} a \bar{z}_i$ for all $a \in K$,

(2) $\bar{z}_i^{m_i} = b_i \in K$,

(3) $\bar{z}_i^{-1} \bar{z}_j^{-1} \bar{z}_i \bar{z}_j = b_{ij} \in K$.

Received May 11, 1965.

Here $x_1, \cdots, x_s$ are automorphisms of K. We shall indicate the definition of the triple by $(G, S) \to (X, B, M)$.

The triple satisfies the following conditions:

(4) $a^{x_i^{m_i}} = a$ for all $a \in K$; that is, $x_i^{m_i} = 1$;

(5) $a^{x_i x_j} = a^{x_j x_i}$ for all $a \in K$; that is, $x_i x_j = x_j x_i$;

(6) $b_{ii} = 1,\ b_{ij} b_{ji} = 1$;

(7) $b_i^{x_k} = b_i b_{ik}^{1+x_i+\cdots+x_i^{m_i-1}}$;

(8) $b_{ij}^{x_k} = b_{ij} b_{ik}^{-1+x_j} b_{jk}^{1-x_i}$.

Note that X generates a homomorph $\overline{H}$ of H in the automorphism group A(K) of K. For this reason, we sometimes write $\overline{H}$ for X, as in the triple $(\overline{H}, B, M)$.

Conversely, given K and $H = (z_1) \times \cdots \times (z_s)$, let us suppose that we have a triple (X, B, M), where $x_1, \cdots, x_s$ are automorphisms of K and satisfy conditions (4) to (8). We shall call such a triple *admissible* with respect to (K, H). We can construct a pair (G, S), where G is an extension of K by H and $S = (\bar{z}_1, \cdots, \bar{z}_s)$ is a representative set of the basis $(z_1, \cdots, z_s)$, such that $(G, S) \to (X, B, M)$ (that is, the triple satisfies conditions (1), (2), and (3)). We shall denote this construction by $(X, B, M) \to (G, S)$.

If two pairs (G, S) and (G', S') give the same triple (X, B, M), where $S = (\bar{z}_1, \cdots, \bar{z}_s)$ and $S' = (\bar{z}_1', \cdots, \bar{z}_s')$, then

$$\bar{z}_1'^{n_1} \cdots \bar{z}_s'^{n_s} a \longleftrightarrow \bar{z}_1^{n_1} \cdots \bar{z}_s^{n_s} a \qquad (a \in K)$$

is an isomorphism $G' \cong G$ that reduces to the identity on K, and $\bar{z}_i' \longleftrightarrow \bar{z}_i$ for each i. Thus, up to such an isomorphism, (G', S') and (G, S) are the same, and in this sense we may write $(G, S) \longleftrightarrow (X, B, M)$.

We shall call two extensions G and G' of K by H *equivalent* (and write $G \sim G'$) if there exists an isomorphism α: $G \cong G'$ such that α is the identity on K and $\phi = \phi' \alpha$, where ϕ: $G \to H$ and ϕ': $G' \to H$ are the epimorphisms whose kernels are K. On the other hand, we shall call two admissible triples (X, B, M) and (X', B', M') *equivalent* (and write $(X, B, M) \sim (X', B', M')$) if $X = X'$ and there exist $c_1, \cdots, c_s$ in K such that

(9) $b_i = b_i' c_i^{1+x_i+\cdots+x_i^{m_i-1}}$,

(10) $b_{ij} = b_{ij}' c_i^{-1+x_j} c_j^{1-x_i}$.

Under these conditions, $G \sim G'$ if and only if $(X, B, M) \sim (X', B', M')$, where $(G, S) \longleftrightarrow (X, B, M)$ and $(G', S') \longleftrightarrow (X', B', M')$. The isomorphism α and the s-tuple $(c_1, \cdots, c_s)$ are related by

(11) $\alpha(\bar{z}_i) = \bar{z}_i' c_i \quad (i = 1, \cdots, s)$.

In particular, any two triples corresponding to the same extension are equivalent. If G is an extension of K by H, then we agree, without explicitly mentioning it, that

:, B, M correspond to it by some choice of S. Conversely, if we have an admissible riple (X, B, M), then G will be the corresponding extension, which is unique up to he equivalence.

Finally, we mention that an extension G of K by H splits over K if and only if, or some choice of S, all b_i are 1 and all b_{ij} are 1. Also, $G = K \times H$ if and only if, or some choice of S, all x_i are 1, all b_i are 1, and all b_{ij} are 1.

Let G be an extension of K by H. A subgroup N of K is normal in G if and only if N is invariant under the corresponding automorphisms X of K. Note that in this case the x_i are automorphisms of N, and G/N is an extension of K/N by H. Let $(G, S) \to (X, B, M)$, $S = (\bar{z}_1, \cdots, \bar{z}_s)$. Then $S/N = (\bar{z}_1 N, \cdots, \bar{z}_s N)$ is a representative set in G/N of the basis $(z_1, \cdots, z_s)$ of H. If $(G/N, S/N) \to (X^*, B^*, M^*)$, then

$$(12) \qquad (aN)^{\sigma^*} = a^{\sigma} N, \qquad b_i^* = b_i N, \qquad b_{ij}^* = b_{ij} N,$$

where $a \in K$, $\sigma \in \overline{H}$, and σ^* is the corresponding automorphism of K/N. The following lemma is trivial; in fact, we have used it in the proof of Theorem 1.

LEMMA 1. *If* G *is a commutator extension of* K *by* H, *then, for each subgroup* N *of* K *invariant under* X, G/N *is a commutator extension of* K/N *by* H.

LEMMA 2. *Suppose that* $K = K_1 \times K_2$ *(direct product), and the orders* n_1 *and* n_2 *of* K_1 *and* K_2 *are relatively prime. If there exist commutator extensions of* K_1 *and* K_2 *by* H, *then there exists a commutator extension of* K *by* H.

Proof. Let (X', B', M') and (X", B", M") be admissible triples given by the commutator extensions of K_1 and K_2 by H. Extend the automorphisms X' to K by letting them act trivially on K_2. Similarly, extend X" to K trivially on K_1. Define a triple (X, B, M) with respect to (K, H) by

$$x_i = x_i' x_i'', \qquad b_i = b_i' b_i'', \qquad b_{ij} = b_{ij}' b_{ij}''.$$

It is easily verified that (X, B, M) is admissible with respect to (K, H), and we have an extension G of K by H.

Now, K_2 is invariant under X, and to the extension G/K_2 of K/K_2 by H there corresponds the triple (X^*, B^*, M^*);

$$(aK_2)^{x_i^*} = a_1^{x_i'} K_2, \qquad b_i^* = b_i' K_2, \qquad b_{ij}^* = b_{ij}' K_2,$$

where $a = a_1 a_2$ $(a_i \in K_i)$. Since (X', B', M') corresponds to a commutator extension of K_1 by H, it follows that G/K_2 is a commutator extension of K/K_2 by H. Indicating the commutator subgroups by ', we have the relations

$$K/K_2 = (G/K_2)' = G' K_2/K_2,$$

and hence, $K = G' K_2$. Similarly, $K = G' K_1$. Since $(n_1, n_2) = 1$, this implies that $K = G'$. In fact, for each $a_1 \in K_1$ there exists an $a_2 \in K_2$ such that $a_1 = (a_1 a_2) a_2^{-1}$ and $a_1 a_2 \in G'$. Then

$$a_1^{n_2} = (a_1 a_2)^{n_2} \in G'.$$

Since n_2 is relatively prime to the order of a_1, we see that $a_1 \in G'$. Thus we have shown that $K_1 \subset G'$. Similarly, $K_2 \subset G'$. Therefore $K = G'$. q.e.d.

The following theorem is a simple consequence of these two lemmas.

THEOREM 2. *Let* K *and* H *be finite abelian groups. There exists a commutator extension of* K *by* H *if and only if, for each Sylow subgroup* K_p *of* K, *there exists a commutator extension of* K_p *by* H.

This theorem reduces the problem to the case in which K is a finite abelian p-group.

THEOREM 3. *Let* K *be a finite abelian* p*-group, and let* H *be a finite abelian group.* G *is a commutator extension of* K *by* H *if and only if* G/K^p *is a commutator extension of* K/K^p *by* H.

Proof. K^p is a characteristic subgroup of K, and the necessity follows from Lemma 1. Conversely, suppose that G/K^p is a commutator extension of K/K^p by H. Then G is an extension of K by H. Moreover, $K/K^p = (G/K^p)' = G'K^p/K^p$, and hence, $K = G'K^p$. But then $K = G'$ because K^p is the Frattini subgroup of K. q.e.d.

Note that K/K^p is an elementary abelian p-group of the same rank as K. Thus we have reduced the problem to the case in which K is an elementary abelian p-group.

Let K be an elementary abelian p-group of rank r. We shall write K additively, so that K is an r-dimensional vector space over the prime Galois field $F = GF(p)$. The linear transformations of K into K are the endomorphisms of K, and they form a ring, while the nonsingular linear transformations of K onto K are the automorphisms of K and form the multiplicative group A(K).

Let $\overline{H}$ be a homomorph of H in A(K). For each $\sigma \in \overline{H}$, let K_σ denote the image $K(\sigma - 1)$ of K under the endomorphism $\sigma - 1$. Let K^* denote the subspace $\langle K_\sigma \mid \sigma \in \overline{H} \rangle$ generated by all K_σ. If G is an extension of K by H, then M will denote the set $\{b_{ij} \mid 1 \leq i \leq s,\ 1 \leq j \leq s\}$ as well as the matrix (b_{ij}). Since $\overline{H}$ is abelian, each K_σ is invariant under $\overline{H}$, and so is K^*.

LEMMA 3. G *is a commutator extension of* K *by* H *if and only if* K *is generated by* M *and* K^*; $K = \langle M, K^* \rangle$.

Proof. It is sufficient to show that, given an extension G of K by H, $\langle M, K^* \rangle$ is the commutator subgroup of G. But this is clear because b_{ij} and $a(\sigma - 1)$ are commutators, while any two elements of G commute modulo $\langle M, K^* \rangle$. q.e.d.

The following, our main theorem, concerns the existence of a split commutator extension of K by H.

THEOREM 4. *Let* K *be an elementary abelian* p*-group of rank* r, *and let* H *be a finite abelian group of order* m. *Let* $q_1, \cdots, q_h$ *be the distinct prime divisors of* m *different from* p, *and let* $\gamma_1, \cdots, \gamma_h$ *be the orders of* p mod $q_1, \cdots, q_h$, *respectively. Then a necessary and sufficient condition for the existence of a split commutator extension of* K *by* H *is that*

$$(13) \qquad r = n_1\gamma_1 + \cdots + n_h\gamma_h \qquad (n_i \text{ nonnegative integers})$$

is solvable for n_i. *In particular,* $h \geq 1$.

Remarks. If $(m, p) = 1$, then, by Schur's Theorem, every extension of K by H splits over K, and hence the solvability of (13) is necessary and sufficient for the existence of a commutator extension of K by H. Further, the theorem says, in articular, that there is no split commutator extension of K by H if H is also a -group.

Proof. For a split extension, for some choice of representative set S, $b_{ij} = 0$ or all i and j, and hence, G is a split commutator extension if and only if $K = K^* = \langle K_\sigma \mid \sigma \in \overline{H} \rangle$.

Suppose that G is a split commutator extension of K by H. Since $K = K^* \neq 0$, $\overline{H} \neq 1$. First suppose that the rank r is 1. Then A(K) is the multiplicative group of $F = GF(p)$, and $\sigma^{p-1} = 1$ for all $\sigma \in A(K)$. Therefore, every $\sigma \in \overline{H}$ has an order dividing $p - 1$. But then there exists a $\sigma \in \overline{H}$ of order equal to some q_i. This means that $h \geq 1$ and q_i divides $p - 1$, and the corresponding order γ_i of p mod q_i is 1. Thus (13) is trivially solvable.

Suppose now that $r \geq 2$ and that the necessity is proved for all elementary abelian p-groups of rank less than r. Moreover, as a part of the induction hypothesis, assume that some corresponding automorphism has an order q_i for some i. Now consider the homomorph $\overline{H}$ corresponding to K. If no $\sigma \in \overline{H}$ is of order q_i for any i, then every $\sigma \in \overline{H}$ is of order p^f for some f. Choose a $\sigma \in \overline{H}$ of order p. Since $(\sigma - 1)^p = \sigma^p - 1 = 0$, $\sigma - 1$ is singular. Therefore K_σ is a nontrivial proper invariant subgroup of K under $\overline{H}$. From (12) we see that G/K_σ is a split commutator extension of K/K_σ by H, and the rank of K/K_σ is less than r. But the corresponding homomorph $\overline{H}^*$ of H contains no automorphisms of order q_i for any i, which is contrary to the induction hypothesis. Thus some $\sigma \in \overline{H}$ has an order q_i for some i.

Let $\sigma \in \overline{H}$ be of order $q = q_i$, and let $\gamma = \gamma_i$ be the order of p mod q. Consider the characteristic polynomial $|x - \sigma|$, and factor it into irreducible factors over F;

$$|x - 1| = P_1(x)^{e_1} \cdots P_t(x)^{e_t}.$$

Since $\sigma^q - 1 = 0$, each irreducible factor $P_i(x)$ is a divisor of $x^q - 1$. Since $\sigma \neq 1$, some $P(x) = P_i(x) \neq x - 1$. Then the degree of P(x) is precisely γ [1, Chapter V, Section 7, Theorem 14]. Let

$$N = \{a \in K \mid aP(\sigma)^n = 0 \text{ for some } n \geq 1\}.$$

Then N is a nontrivial subgroup of K invariant under $\overline{H}$, and its rank is $e\gamma$ ($e = e_i$). If $K = N$, then $r = e\gamma$, and we have a solution of (13). If $K \neq N$, then G/N is a split commutator extension of K/N by H, and the rank of K/N is equal to $r - e\gamma < r$. Thus, by the induction hypothesis, the equation $r - e\gamma = n_1\gamma_1 + \cdots + n_h\gamma_h$ is solvable for integers $n_i \geq 0$, and so is (13). This completes the proof of the necessity.

Conversely, suppose that (after reindexing the primes q_i) we have a solution of (13) with $n_1, \cdots, n_t > 0$ and $n_i = 0$ for $i > t$. For each $i \leq t$, let λ ($= \lambda_i$) be a primitive qth ($= q_i$th) root of unity over F. Then γ ($= \gamma_i$) is the degree of the field extension $F(\lambda)$ over F (*ibid.*, Theorem 14). Let $\beta_1, \cdots, \beta_\gamma$ be a basis of $F(\lambda)$ over F, and define a matrix $A = (a_{ij})$ by

$$\lambda\beta_j = \sum_{i=1}^{\gamma} a_{ij}\beta_i \qquad (a_{ij} \in F).$$

Applying this argument to each q_i ($i = 1, \cdots, t$), we obtain matrices A_i of degree γ_i. For each $i \leq t$, let

$$A_i' = \text{diag}(1, \cdots, 1, A_i, \cdots, A_i, 1, \cdots, 1),$$

where A_i appears n_i times stretching from the $(n_1\gamma_1 + \cdots + n_{i-1}\gamma_{i-1} + 1)$st position to the $(n_1\gamma_1 + \cdots + n_i\gamma_i)$th position along the diagonal. Choose a basis $(g_1, \cdots, g_r)$ of K. Then A_i' represents an automorphism σ_i of K relative to the basis $(g_1, \cdots, g_r)$. Since σ_i represents multiplication by λ_i and $\lambda_i^{q_i} = 1$, $\sigma_i^{q_i} = 1$. Let $\overline{H}$ be the group of automorphisms generated by the σ_i, which is clearly a homomorph of H in A(K). Divide the basis $(g_1, \cdots, g_r)$ into t blocks of lengths $n_1\gamma_1, \cdots, n_t\gamma_t$, and let $K_1, \cdots, K_t$ be the subgroups generated by the corresponding blocks of the basis elements. Then σ_i is an automorphism of K_i. Moreover, since $\lambda_i \neq 1$, $\sigma_i - 1$ is nonsingular on K_i, and hence, $K_i(\sigma_i - 1) = K_i$. Since σ_i is the indentity on K_j for $j \neq i$,

$$K_{\sigma_i} = K(\sigma_i - 1) = K_i \quad \text{and} \quad K^* = \langle K_{\sigma_i} \mid i = 1, \cdots, t \rangle = K_1 \oplus \cdots \oplus K_t = K.$$

Taking $b_i = 0$ and $b_{ij} = 0$ for all i and j, we obtain a split commutator extension of K by H. This completes the proof of Theorem 4.

By tracing back the preceding theorems, we see that Theorem 4 gives necessary and sufficient conditions for the existence of a split commutator extension of K by H in terms of invariants of K and H, where K is a group whose commutator factor group is finite and H is a finite abelian group. Turning our attention to nonsplit commutator extensions of K by H, we assume that K is an elementary abelian p-group of rank r and that p divides the order m of H. Let $p, q_1, \cdots, q_h$ be the prime divisors of m.

LEMMA 4. *Let* $\sigma \in A(K)$. *If* $\sigma^\mu = 1$ *and* $(\mu, p) = 1$, *then*

$$\text{Im}(\sigma - 1) = \text{Ker}(1 + \sigma + \cdots + \sigma^{\mu-1}).$$

Proof. Since $(\sigma - 1)(1 + \sigma + \cdots + \sigma^{\mu-1}) = \sigma^\mu - 1 = 0$, we have the inclusions

$$\text{Im}(\sigma - 1) \subset \text{Ker}(1 + \sigma + \cdots + \sigma^{\mu-1}), \qquad \text{Im}(1 + \sigma + \cdots + \sigma^{\mu-1}) \subset \text{Ker}(\sigma - 1).$$

Let

$$i = \text{rank}(\text{Im}(\sigma - 1)), \qquad i' = \text{rank}(\text{Im}(1 + \sigma + \cdots + \sigma^{\mu-1})),$$

$$k = \text{rank}(\text{Ker}(\sigma - 1)), \qquad k' = \text{rank}(\text{Ker}(1 + \sigma + \cdots + \sigma^{\mu-1})).$$

Then $i + k = i' + k'$. It is sufficient to show that $\text{Ker}(\sigma - 1) \subset \text{Im}(1 + \sigma + \cdots + \sigma^{\mu-1})$, for then $k = i'$, and hence, $i = k'$. Let $a \in \text{Ker}(\sigma - 1)$, so that $a\sigma = a$. Since μ is relatively prime to the order of a, there exists an integer η such that $\mu\eta \equiv 1$ modulo the order of a. Let $a' = \eta a \in \text{Ker}(\sigma - 1)$. Since $a'\sigma = a'$,

$$a = \mu a' = a'(1 + \sigma + \cdots + \sigma^{\mu-1}). \qquad \text{q.e.d.}$$

LEMMA 5. *Let* H_p *be the* p-Sylow *subgroup of* H, *so that* $H = H_p \times H'$. *Let* $s = \text{rank}(H_p)$, *and let* $(z_{s+1}, \cdots)$ *be a basis of* H'. *If* G *is an extension of* K *by* H, *then*

$$b_{ij} \in K^* = \langle K_\sigma \mid \sigma \in \overline{H} \rangle \text{ if } i > s \text{ or } j > s.$$

Proof. Let (X, B, M) be a triple corresponding to the extension G of K by H. Let (X', B', M') be the restriction of (X, B, M) to H', that is, let

$$X' = (x_{s+1}, \cdots), \quad B' = (b_{s+1}, \cdots), \quad M = (b_{ij}) \quad (i > s,\ j > s).$$

Then (X', B', M') is clearly admissible with respect to (K, H'). Since the order of H' is relatively prime to p, the corresponding extension of K by H' splits over K, and hence, $(X', B', M') \sim (X', 0, 0)$. Thus the original triple (X, B, M) is equivalent to a triple in which $b_i = 0$ and $b_{ij} = 0$ for all $i > s$ and $j > s$. According to (10), equivalent b_{ij} are congruent modulo K^*, so that we may assume that $b_i = 0$ and $b_{ij} = 0$ for all $i > s$ and $j > s$ in (X, B, M). If $i > s$, then, by (7),

$$b_{ij}(1 + x_i + \cdots + x_i^{m_i - 1}) = b_i(x_j - 1) = 0.$$

Then, by Lemma 4, $b_{ij} \in K_{x_i}$ and $b_{ji} = -b_{ij} \in K_{x_i}$ if $i > s$. q.e.d.

PROPOSITION 1. *Let* G *be a commutator extension of* K *by* H, *and let* $r^* = \operatorname{rank}(K^*)$, $K^* = \langle K_\sigma \mid \sigma \in \overline{H} \rangle$. *Then* $\binom{s}{2} \geq r - r^*$, *where* $s = \operatorname{rank}(H_p)$ *and* H_p *is the* p-*Sylow subgroup of* H.

Proof. Consider the commutator extension G/K^* of K/K^* by H. If (X, B, M) is a triple corresponding to G, then a triple (X^*, B^*, M^*) corresponding to G/K^* is given by (12);

$$(a + K)\sigma^* = a\sigma + K, \qquad b_i^* = b_i + K^*, \qquad b_{ij}^* = b_{ij} + K^*.$$

Since $a\sigma \equiv a \pmod{K^*}$ and $b_{ij} \in K^*$ if $i > s$ or $j > s$, we see that $\overline{H}^* = 1$, and we must have the relation $K/K^* = \langle b_{ij}^* \mid i \leq s,\ j \leq s \rangle$. But this is possible only if $\binom{s}{2} \geq \operatorname{rank}(K/K^*) = r - r^*$. q.e.d.

COROLLARY 1. *If* H *is a cyclic* p-*group, then there exists no commutator extension of* K *by* H.

Proof. Since H is a p-group, there exists no homomorph $\overline{H}$ of H in A(K) such that $K^* = K$, for otherwise, we would have a split commutator extension of K by H. Thus $r - r^* \geq 1$ for every choice of $\overline{H}$. Hence $s \geq 2$ if there is a commutator extension of K by H. q.e.d.

COROLLARY 2. *The commutator factor group* G/G' *of a nonabelian finite* p-*group is noncyclic.*

PROPOSITION 2. *A necessary and sufficient condition for the existence of a commutator extension of* K *by* H *such that* $\overline{H} = 1$ *is that* $\binom{s}{2} \geq r$, *where* $s = \operatorname{rank}(H_p)$.

Proof. Since $\overline{H} = 1$, $K^* = 0$. Therefore, by Proposition 1, the condition $\binom{s}{2} \geq r$ is necessary. Conversely, suppose that $\binom{s}{2} \geq r$. Let $(g_1, \cdots, g_r)$ be a basis of K, and let b_{ij} be equal to $g_1, \cdots, g_r$ in some order $(i < j \leq s)$, and let the remaining b_{ij} $(i < j)$ be 0. Of course, we let $b_{ji} = -b_{ij}$ and $b_{ii} = 0$. Since $\overline{H} = 1$ and $pa = 0$ for all $a \in K$ and $b_{ij} = 0$ if $i > s$ or $j > s$, we may take $b_i = 0$ to obtain an admissible triple $(\overline{H}, B, M)$. Since $K = \langle M \rangle$, the corresponding extension is a commutator extension. q.e.d.

LEMMA 6. *For each* $\sigma \in A(K)$, $1 + \sigma + \cdots + \sigma^{p^f - 1} = (\sigma - 1)^{p^f - 1}$.

Proof. Let $\beta = \sigma - 1$, so that $\sigma = 1 + \beta$. Then

$$\sum_{k=0}^{p^f-1} \sigma^k = \sum_{k=0}^{p^f-1} (1+\beta)^k = \sum_{k=0}^{p^f-1} \sum_{j=0}^{k} \binom{k}{j} \beta^j = \sum_{j=0}^{p^f-1} \beta^j \sum_{k=j}^{p^f-1} \binom{k}{j}.$$

But

$$\sum_{k=j}^{p^f-1} \binom{k}{j} = \binom{p^f}{j+1} \equiv \begin{cases} 0 \pmod p & \text{if } j < p^f - 1, \\ 1 & \text{if } j = p^f - 1. \end{cases}$$

Hence

$$\sum_{k=0}^{p^f-1} \sigma^k = \beta^{p^f-1} = (\sigma - 1)^{p^f-1}. \qquad \text{q.e.d.}$$

PROPOSITION 3. *If* $p^f > r$ *for the order* p^f *of some basis element* z_i $(i \leq s)$ *of* H_p, *then the condition* $s \geq 2$ *is sufficient for the existence of a nonsplit commutator extension of* K *by* H.

Proof. Let z_1 be of order $p^f > r$. Choose a nilpotent endomorphism β of rank $r - 1$ on K, and let $x_1 = 1 + \beta$. Then $\beta^{p^f-1} = \beta^r = 0$, and hence, $x_1^{p^f} = (1+\beta)^{p^f} = 1$. Let all other x_i be 1. Let all $b_i = 0$. Choose $b_{12} = -b_{21}$ to be an element not in $K_{x_1} = K(x_1 - 1)$, and all other b_{ij} to be 0. Since

$$1 + x_1 + \cdots + x_1^{p^f-1} = (x_1 - 1)^{p^f-1} = \beta^{p^f-1} = 0,$$

the triple (X, B, M) is clearly admissible. Since

$$\operatorname{rank}(K_{x_1}) = \operatorname{rank}(\beta) = r - 1 \quad \text{and} \quad b_{12} \notin K_{x_1},$$

$K = \langle b_{12}, K_{x_1} \rangle$. Thus the corresponding extension is a nonsplit commutator extension of K by H. q.e.d.

REFERENCES

1. A. A. Albert, *Fundamental concepts of higher algebra,* The University of Chicago Press, Chicago, Illinois, 1956.

2. R. Baer, *Erweiterung von Gruppen und ihren Isomorphismen,* Math. Z. 38 (1934), 375-416.

3. H. J. Zassenhaus, *The theory of groups*, Second Edition, Chelsea Publishing Company, New York, 1958.

The City College of New York