K. Miyake
Nagoya Math. J.
Vol. 99 (1985), 73-88

THE APPLICATION OF THE PRINCIPAL IDEAL THEOREM TO p-GROUPS

KATSUYA MIYAKE

Introduction

Let p be a fixed prime integer, and G a finite p-group. For a subgroup H of G, we denote the centralizer of H in G by $C_G(H)$. The commutator subgroup of G is denoted by $[G, G]$. One of the main results of this paper is

THEOREM 1. *Let A be a normal abelian subgroup of G. Suppose that* (1) *$G/C_G(A)$ is regular, and that* (2) *$\langle g \rangle \cdot A$ is regular for each $g \in G$. Then the exponent of G divides the index $[G: A \cap [G, G]]$.*

Because a p-group of class less than p is regular, we have the following theorem as a corollary: Let

$$K_1(G) = G \supset K_2(G) \supset \cdots \supset K_n(G) \supset \cdots$$

and

$$Z_0(G) = 1 \subset Z_1(G) \subset \cdots \subset Z_{n-1}(G) \subset \cdots$$

be the lower and the upper central series of G, respectively.

THEOREM 2. *Let A be a maximal one among normal abelian subgroups of G which are contained in $Z_{p-1}(G) \cap C_G(K_p(G))$. Then the exponent of G divides $[G: A \cap [G, G]]$.*

If A is as in the theorem, then the center $Z(G) = Z_1(G)$ of G is a subgroup of A. Therefore, the index of the theorem certainly divides $[G: Z(G) \cap [G, G]]$. Hence Theorem 2 is a generalization of the result of Alperin and Tzee-Nan Kuo [1]. Furthermore, it is best possible since the exponent of G coincides with the index $[G: A \cap [G, G]]$ if G is the irregular p-group of Blackburn exhibited by Huppert [3, Ch. III, 10.15] with $A = [G, G]$. In this case, $[G: A] = p^2$ and $[G: Z(G)] = p^p$. (See Ch. II, § 3 for the detail.)

Received April 17, 1984.

To prove Theorem 1, we first calculate the transfer $V_{G\to A}: G \to A$ of G to A in Chapter I to see

$$V_{G\to A}(x) = x^{[G:A]} \qquad \text{for } {}^{\forall}x \in G$$

under the conditions (1) and (2) (Theorem 4). We need a uniqueness basis of cosets of $G/\langle x\rangle \cdot C_G(A)$ for each $x \in G$. But the proof of the existence of such a basis will be shown later in Chapter III, just following the way of P. Hall [2], mainly because it has its own meaning independent of the rest of this paper.

Once we have the above formula, then we get, on one hand,

$$V_{G\to A\cap[G,G]}(x) = x^{[G:A\cap[G,G]]} \qquad \text{for } {}^{\forall}x \in G$$

because

$$V_{G\to A\cap[G,G]} = V_{A\to A\cap[G,G]} \circ V_{G\to A}$$

as is well known, and because A is abelian. On the other hand, we have

$$V_{G\to A\cap[G,G]} = V_{[G,G]\to A\cap[G,G]} \circ V_{G\to[G,G]} .$$

The Principal Ideal Theorem, therefore, implies Theorem 1 now at once because it states that the transfer $V_{G\to[G,G]}$ of G to its commutator subgroup $[G, G]$ is trivial. (See Zassenhaus [7, Ch. V, § 4] for a simple proof. Also see Huppert [3, Ch. IV, 2.12 Bemerkung], the last sentence of which is 'In der Gruppentheorie hat der Satz bisher keine Verwendung gefunden'.)

In Chapter II, we give the applications of Terada's Principal Ideal Theorem and of the results of the author in [5]. If G is regular, then the method of [5] can directly be applicable to obtain the following: Let G be a regular p-group, and A a normal abelian subgroup. Let $\mu_1 \geq \mu_2 \geq \cdots$ be the type-invariants of G/A. If G/A is cyclic, then put $\mu_2 = 0$. Put $\mu = \mu_1$ and let ν be an integer such that $\nu \geq \mu_2$.

THEOREM 3. *The notation and the assumptions being as above, the following* (i) ~ (iii) *hold*:

(i) $\Omega_{\mu+\nu}(G) \supset [G, A]\cdot\Omega_\nu(A)$;

(ii) $\mho_{\mu+\nu}(G) \subset \mho_\nu(A) \cap Z(G)$;

(iii) $[\Omega_{\mu+\nu}(G): [G, A]\cdot\Omega_\nu(A)] = [G: A]\cdot[\mho_\nu(A) \cap Z(G): \mho_{\mu+\nu}(G)]$.

If G/A is cyclic, then $[G, A] = [G, G]$. Under the conditions of the theorem, we have $\Omega_{\mu+\nu}(G) \supset [G, G]$ in general. We close Chapter II posing

problems, one of which is whether the index $[G: A]$ divides $[\Omega_{\mu+\nu}(G): [G, G]]$ in general or not.

I. The transfers of p-groups under the regularity conditions

1. Let p be a fixed prime integer, and G a finite p-group. Let A be a normal abelian subgroup of G and $V_{G\to A}$ be the transfer homomorphism of G to A. The centralizer of A in G is denoted by $C_G(A)$, i.e.

$$C_G(A) = \{g \in G \mid ga = ag \quad \text{for } {}^\forall a \in A\} .$$

Then this contains A because A is abelian. Since A is a normal subgroup of G, so is $C_G(A)$. We show

THEOREM 4. *Suppose that* (1) $G/C_G(A)$ *is regular, and that* (2) $\langle g\rangle \cdot A$ *is regular for each* $g \in G$. *Then we have*

$$V_{G\to A}(x) = x^{[G:A]} \qquad \textit{for } {}^\forall x \in G .$$

2. We need a few lemmas.

LEMMA 1. *Let* x *be an element of* G. *Put* $H = \langle x\rangle \cdot C_G(A)$, $f = [H: A]$ *and* $t = [G: H]$. *Let* $\{g_1, \cdots, g_t\}$ *be a set of representatives of* G/H. *Then we have*

$$V_{G\to A}(x) = \prod_{i=1}^{t} g_i \cdot x^f \cdot g_i^{-1} .$$

Proof. For g, h and h' in G, we have

$$Agh = Agh' \Longleftrightarrow h \equiv h' \bmod A$$

because A is a normal subgroup of G. Therefore each orbit of H in $A\backslash G$ has exactly f cosets. Furthermore, for g and g' in G, we have $Ag' = Agh$ with $h \in H$ if and only if $g' = gh'$ with $h' \in H$ because H contains A. Hence the $t \cdot f$ elements $g_i \cdot h_j$, $i = 1, \cdots, t$, $j = 1, \cdots, f$, form a set of representatives of $A\backslash G$ $(= G/A)$ whenever $\{h_1, \cdots, h_f\}$ represents the cosets of H/A. Put $d = [\langle x\rangle \cdot A: A]$ and $e = [H: \langle x\rangle \cdot A]$. Then $f = d \cdot e$. Note that d is the minimal positive integer such that x^d belongs to A. Then we can choose $\{h_1, \cdots, h_f\}$ of form

$$\{h'_j \cdot x^k \mid j = 1, \cdots, e;\ k = 0, 1, \cdots, d-1\}$$

with $h'_j \in H$ because A is a normal subgroup of G. Using the set of representatives $\{g_i \cdot h'_j \cdot x^k \mid 1 \le i \le t,\ 1 \le j \le e,\ 0 \le k \le d-1\}$ of $A\backslash G$, we have

$$V_{G\to A}(x) = \prod_{i=1}^{t}\prod_{j=1}^{e} g_i\cdot h'_j\cdot x^d\cdot h'^{-1}_j\cdot g_i^{-1}\ .$$

(See Zassenhaus [7, Ch. p. 168], or Huppert [3, Ch. IV, 1.7].) But it is obvious that $H = \langle x\rangle\cdot C_G(A)$ lies in $C_G(\langle x\rangle \cap A)$. Since $x^d \in \langle x\rangle \cap A$, we have $h'_j\cdot x^d\cdot h'^{-1}_j = x^d$ for $j = 1, \cdots, e$. Hence we get $V_{G\to A}(x) = \prod_{i=1}^{t} g_i\cdot x^f\cdot g_i^{-1}$ because $d\cdot e = f$. Q.E.D.

LEMMA 2. *For g and a in G, we have*

$$(g\cdot a)^n = g^n\cdot(g^{-(n-1)}ag^{n-1}\cdot g^{-(n-2)}ag^{n-2}\cdots g^{-1}ag\cdot a)\ .$$

One can easily see this by induction on n.

LEMMA 3. *Let g be an element of G, and a of A. Suppose that $\langle g, a\rangle$ is regular, and that g^m commutes with a for a power m of p. Then we have*

$$\prod_{i=0}^{m-1} g^i\cdot a\cdot g^{-i} = a^m\ .$$

Proof. By the assumption, $\langle g, a\rangle$ is regular. Therefore $[g, a]^m = 1$ by P. Hall [2, Th. 4.22] or by Huppert [3, Ch. III, 10.6 b)] since g^m commutes with a. As is well known, the commutator subgroup of $\langle g, a\rangle$ is generated by $[g, a] = g^{-1}a^{-1}ga$ and its conjugates in $\langle g, a\rangle$. Therefore the exponent of the commutator group divides m. Then we have $(g^{-1}\cdot a)^m = g^{-m}\cdot a^m$ since $\langle g, a\rangle$ is regular. The lemma now follows from the preceding one at once.

3. *Proof of Theorem* 4. Now suppose that G and A satisfy the conditions (1) and (2) of Theorem 4. Let x be an element of G, and put $H = \langle x\rangle\cdot C_G(A)$ as above. We need the results of Chapter III, which will be shown independently from Chapters I and II. Since $G/C_G(A)$ is regular, we can find, by Theorem 8 of Chapter III, a sequence of elements, $g_1, \cdots, g_\tau$, of G which satisfy the following condition: For each $i(1 \le i \le \tau)$, let μ_i be the minimal positive integer such that $g_i^{\mu_i}$ belongs to H. Then $t = \mu_1\cdot\mu_2\cdots\mu_\tau = [G: H]$, and the set of t elements,

$$g_1^{m_1}\cdot g_2^{m_2}\cdots g_\tau^{m_\tau};\quad 0 \le m_1 < \mu_1,\quad 0 \le m_2 < \mu_2, \cdots, 0 \le m_\tau < \mu_\tau\ ,$$

is a complete set of representatives of G/H.

Put $f = [H: A]$. Then by Lemma 1, we have

$$V_{G\to A}(x) = \prod_{m_\tau=0}^{\mu_\tau-1}\cdots\prod_{m_2=0}^{\mu_2-1}\prod_{m_1=0}^{\mu_1-1} g_\tau^{m_\tau}\cdots g_2^{m_2}g_1^{m_1}\cdot x^f\cdot g_1^{-m_1}g_2^{-m_2}\cdots g_\tau^{-m_\tau}\ .$$

Each $g_i^{\mu_i}$ belongs to $H = \langle x \rangle \cdot C_G(A)$, and commutes with every element of $\langle x \rangle \cap A$. Since x^f belongs to $\langle x \rangle \cap A$, each $\langle g_i, x^f \rangle$ is regular by the condition (2) of Theorem 4. Therefore, we can apply Lemma 3 successively, and finally obtain

$$V_{G \to A}(x) = x^{f \cdot \mu_1 \cdot \mu_2 \cdots \mu_\tau} = x^{f \cdot t} .$$

Since $f \cdot t = [H: A] \cdot [G: H] = [G: A]$, we have

$$V_{G \to A}(x) = x^{[G:A]}$$

for an arbitrary element x of G. Q.E.D.

We have actually shown, under the condition (1), that $V_{G \to A}(x)$ is equal to $x^{[G:A]}$ as far as $\langle g, x^f \rangle$ is regular for each $g \in G$, where $f = [\langle x \rangle \cdot C_G(A): A]$. Therefore we have the following three corollaries because a p-group of class less than p is regular:

COROLLARY 1. *Suppose that the condition* (1) *of the theorem is satisfied by G and A. If x^f belongs to $Z_{p-1}(G)$, then we have*

$$V_{G \to A}(x) = x^{[G:A]}$$

where $f = [\langle x \rangle \cdot C_G(A): A]$ and $Z_{p-1}(G)$ is the member of the upper central series $Z_0(G) = 1 \subset Z_1(G) \subset Z_2(G) \subset \cdots$ of G.

COROLLARY 2. *Let G be a finite p-group, and A a normal abelian subgroup of G. Suppose that $G/C_G(A)$ is regular and that A lies in $Z_{p-1}(G)$. Then, for every $x \in G$, we have*

$$V_{G \to A}(x) = x^{[G:A]} .$$

COROLLARY 3. *Let G be a finite p-group, and A a normal abelian subgroup of G. If A is contained in $Z_{p-1}(G) \cap C_G(K_p(G))$, then, for every $x \in G$, we have*

$$V_{G \to A}(x) = x^{[G:A]} .$$

Here $K_p(G)$ is the member of the lower central series $K_1(G) = G \supset K_2(G) \supset K_3(G) \supset \cdots$ of G.

COROLLARY 4. *Let G be a finite p-group, and H a proper normal subgroup of G. If the exponent of $G/[H, H]$ is equal to p, then the transfer $V_{G \to H}$ is trivial, that is, $V_{G \to H}(G) = [H, H]$.*

Proof. Replacing G and H by $G/[H, H]$ and $H/[H, H]$, we may assume that H is abelian, and that the exponent of G is equal to p. Then G is regular. Therefore, we have

$$V_{G\to H}(x) = x^{[G:H]} = 1$$

for each $x \in G$ because H is a proper subgroup of G. Q.E.D.

COROLLARY 5. *Let G and A be as in Theorem 4, satisfying the conditions (1) and (2). Then the exponent of the commutator subgroup $[G, G]$ of G divides the index $[G: A]$.*

Proof. For every $x \in [G, G]$, we have

$$x^{[G:A]} = V_{G\to A}(x) = 1$$

because $V_{G\to A}$ is a homomorphism of G to the abelian group A. The corollary is, therefore, clear.

EXAMPLE. Let G be the group defined by

$$G = \langle x, a\rangle$$
$$x^p = a^{p^2} = 1\,, \qquad [a, x] = a^p\,.$$

We have $[G, G] = Z(G) = \langle a^p\rangle$. The exponent of $[G, G]$ is p. If $p \geq 3$, then G is regular. Therefore, we can apply Corollary 5 to G and $A = \langle a\rangle$, and see that the exponent of $[G, G]$ actually coincides with $[G:A]$ in this case. If $p = 2$, we cannot apply the corollary to G and A as it is. But, since $[G, G] = Z(G)$, we can also conclude that the exponent of $[G, G]$ divides $[G: A]$ if we use Corollary 1.

II. The exponents of finite p-groups

1. The Principal Ideal Theorem. Let us state the most general form of the Principal Ideal Theorem (of group theoretic version).

Let G be a finite group, and ρ be an endomorphism of G. We define two subgroups of G by ρ as follows:

$$G[\rho] = \langle \rho(g)\cdot g^{-1} \mid g \in G\rangle \cdot [G, G];$$
$$G^*[\rho] = \{g \in G \mid \rho(g)\cdot g^{-1} \in [G, G]\}\,.$$

THEOREM. $\mathrm{Ker}\,(V_{G\to G[\rho]}) \supset G^*[\rho]$.

For the proof, see Terada [6, § 3] and Miyake [4, § 4]. If ρ is the identity of G (or any inner automorphism), then we have $G[\rho] = [G, G]$

and $G^*[\rho] = G$. Therefore, the theorem is just the original Principal Ideal Theorem in this case.

2. We prove the following theorem, from which Theorem 1 of Introduction is induced as a special case:

THEOREM 5. *Let G be a finite p-group, ρ be an endomorphism of G, and, $G[\rho]$ and $G^*[\rho]$ be as above. Let A be a normal abelian subgroup of G which satisfies that* (1) *$G/C_G(A)$ is regular and that* (2) *$\langle g\rangle \cdot A$ is regular for each $g \in G$. (For example, a subgroup A of $Z_{p-1}(G) \cap C_G(K_p(G))$ satisfies* (1) *and* (2).) *Then the exponent of $G^*[\rho]$ divides the index $[G: A \cap G[\rho]]$.*

Proof. Put $d = [G: A]$ and $e = [A: A \cap G[\rho]]$. It is sufficient to show that $x^{de} = 1$ for $\forall x \in G^*[\rho]$. By Theorem 4, we have $x^d = V_{G\to A}(x)$. Since A is abelian, we also have $V_{A\to A\cap G[\rho]}(x^d) = (x^d)^{[A: A\cap G[\rho]]} = x^{de}$. Therefore, $x^{de} = V_{A\to A\cap G[\rho]}(V_{G\to A}(x)) = V_{G\to A\cap G[\rho]}(x)$, by Zassenhaus [7, Ch. V, Th. 3] or by Huppert [3, Ch. IV, 1.6]. But $V_{G\to A\cap G[\rho]}(x) = V_{G[\rho]\to A\cap G[\rho]}(V_{G\to G[\rho]}(x))$. Therefore, we have $x^{de} = 1$ if $x \in G^*[\rho]$ by the theorem of Section 1 above. Q.E.D.

COROLLARY 1. *Let G, ρ, $G[\rho]$ and $G^*[\rho]$ be as in the theorem. Then the exponent of $G^*[\rho]$ divides $[G: Z(G) \cap G[\rho]]$.*

For the proof, apply the theorem to $A = Z(G)$.

If ρ is the identity of G, then $G^*[\rho] = G$. Therefore, we have the corollary to Theorem 1 of Alperin and Tzee-Nan Kuo [1] in this case.

COROLLARY 2. *Let G, ρ, $G[\rho]$ and $G^*[\rho]$ be as in the theorem. Suppose that $G[\rho]$ is abelian (hence G is metabelian), and that $\langle g\rangle \cdot G[\rho]$ is regular for every $g \in G$. Put $p^{\alpha(\rho)} = [G: G[\rho]]$ and*

$$\Omega_{\alpha(\rho)}(G) = \langle g \in G \mid g^{p^{\alpha(\rho)}} = 1\rangle .$$

Then $\Omega_{\alpha(\rho)}(G)$ contains $G^*[\rho]$, and the index $[\Omega_{\alpha(\rho)}(G): [G, G]]$ is a multiple of $[G: G[\rho]]$.

Proof. Put $A = G[\rho]$. Since G/A is abelian, and so, regular, we can apply Theorem 5. Then we have $G^*[\rho] \subset \Omega_{\alpha(\rho)}(G)$ by the definitions. It is, therefore, sufficient to show $[G^*[\rho]: [G, G]] = [G: G[\rho]]$. Put $M = G/[G, G]$. Then ρ induces an endomorphism of M, which we also denote by ρ for simplicity. Define $\psi: M \to M$ by $\psi(x) = \rho(x)\cdot x^{-1}$ for $x \in M$. Then this is a homomorphism because M is abelian. Therefore, we have

$$|M| = [G: [G, G]] = |\mathrm{Ker}\,(\psi)| \cdot |\mathrm{Im}\,(\psi)| .$$

But $|\mathrm{Ker}\,(\psi)| = [G^*[\rho]: [G, G]]$ and $|\mathrm{Im}\,(\psi)| = [G[\rho]: [G, G]]$. Hence we have

$$\begin{aligned}[G^*[\rho]: [G, G]] &= [G: [G, G]] \cdot [G[\rho]: [G, G]]^{-1} \\ &= [G: G[\rho]] . \end{aligned}$$

Q.E.D.

3. EXAMPLE. Blackburn's irregular p-group (cf. Huppert [3, Ch. III, 10.15]).

Let G be the p-group defined by

$$\begin{aligned} G = \langle x, a_1, a_2, \cdots, a_{p-1} \rangle & \\ x^p = a_1^p , \qquad & a_1^{p^2} = a_2^p = \cdots = a_{p-1}^p = 1 , \\ a_i \cdot a_j = a_j \cdot a_i \qquad & (i, j = 1, \cdots, p-1) , \\ [a_i, x] = a_{i+1} \qquad & (i = 1, \cdots, p-2) , \\ [a_{p-1}, x] = a_1^{-p} . & \end{aligned}$$

This is an irregular p-group of class p. We have $|G| = p^{p+1}$,

$$[G, G] = Z_{p-1}(G) = \langle a_1^p, a_2, \cdots, a_{p-1} \rangle$$

and

$$Z(G) = K_p(G) = \langle a_1^p \rangle .$$

Therefore $Z_{p-1}(G) \cap C_G(K_p(G)) = Z_{p-1}(G) = [G, G]$.

Take $A = [G, G]$. Then the exponent of G is equal to

$$p^2 = [G: A] = [G: A \cap [G, G]] .$$

Therefore, this example shows that Theorems 1, 2 and 5 are best possible. Note that

$$[G: Z(G) \cap [G, G]] = p^p > p^2$$

if $p \geq 3$.

Let ρ be the automorphism of G determined by

$$\rho(x) = x \cdot a_1 , \quad \text{and} \quad \rho(a_i) = a_i \quad (i = 1, \cdots, p-1) .$$

Then

$$G[\rho] = G^*[\rho] = \langle a_1, a_2, \cdots, a_{p-1} \rangle .$$

In this case, therefore, the exponent of $G^*[\rho]$ coincides with the index $[G: A \cap G[\rho]] = p^2$ if we take $A = [G, G]$.

4. The application of Hilbert's Theorem 94 and its generalization

The group theoretic proof of Hilbert's Theorem 94 and its generalization shown in [5] are also applicable by means of Theorem 4 of Chapter I.

LEMMA 4. *Let G be a finite group, A be a normal abelian subgroup of G and $\Phi: G \to A$ be a homomorphism. Let φ and ψ be endomorphisms of A such that $\varphi \circ \psi = \psi \circ \varphi$. Suppose that the following* (i) *and* (ii) *are satisfied*:

(i) $\Phi^{-1}(1) \supset \varphi^{-1}(1) \cdot \psi(A)$,

(ii) $\Phi(G) \subset \varphi(A) \cap \psi^{-1}(1)$.

Then $[\Phi^{-1}(1): \varphi^{-1}(1) \cdot \psi(A)] = [G: A] \cdot [\varphi(A) \cap \psi^{-1}(1): \Phi(G)]$.

Proof. Put $q = [\Phi^{-1}(1): \varphi^{-1}(1) \cdot \psi(A)]/[G: A] \cdot [\varphi(A) \cap \psi^{-1}(1): \Phi(G)]$. We show $q = 1$. Multiplying both of the numerator and the denominator of q by $|\Phi(G)| = [G: \Phi^{-1}(1)]$, we have

$$
\begin{aligned}
q &= \frac{[G: \varphi^{-1}(1) \cdot \psi(A)]}{[G: A] \cdot |\varphi(A) \cap \psi^{-1}(1)|} = \frac{[A: \varphi^{-1}(1) \cdot \psi(A)]}{|\varphi(A) \cap \psi^{-1}(1)|} \\
&= \frac{[A: \psi(A)]}{|\varphi(A) \cap \psi^{-1}(1)| \cdot [\varphi^{-1}(1) \cdot \psi(A): \psi(A)]} \\
&= \frac{|\psi^{-1}(1)|}{|\varphi(A) \cap \psi^{-1}(1)| \cdot [\varphi^{-1}(1) \cdot \psi(A): \psi(A)]} \\
&= \frac{[\psi^{-1}(1): \varphi(A) \cap \psi^{-1}(1)]}{[\varphi^{-1}(1) \cdot \psi(A): \psi(A)]} \\
&= \frac{[\psi^{-1}(1) \cdot \varphi(A): \varphi(A)]}{[\varphi^{-1}(1) \cdot \psi(A): \psi(A)]} .
\end{aligned}
$$

Since we have $\varphi \circ \psi = \psi \circ \varphi$, the last quotient is equal to 1 by Herbrand's lemma. For the detail, see the latter half of the proof of Lemma 5 of [5, § 3].

THEOREM 6. *Let G be a finite p-group, and A a normal abelian subgroup of G, which satisfy the conditions* (1) *and* (2) *of Theorem* 4. *Let α and β be the integers such that p^α is the exponent of G/A and $p^{\alpha+\beta} = [G: A]$. Then the following* (i) $\sim$ (iii) *hold*:

(i) $\Omega_{\alpha+\beta}(G) \supset [G, A] \cdot \Omega_\beta(A)$;

(ii) $\mho_{\alpha+\beta}(G) \subset \mho_\beta(A) \cap Z(G)$;

(iii) $[\Omega_{\alpha+\beta}(G): [G, A] \cdot \Omega_\beta(A)] = [G: A] \cdot [\mho_\beta(A) \cap Z(G): \mho_{\alpha+\beta}(G)]$.

Here $\Omega_\gamma(G) = \langle g \in G \mid g^{p^\gamma} = 1 \rangle$, $\mho_\gamma(G) = \langle g^{p^\gamma} \mid g \in G \rangle$ *etc.*

Proof. Let $\pi: G \to G$ be the mapping defined by $\pi(g) = g^p$ for $g \in G$. Put $\Phi = \pi^{\alpha+\beta}$ and $\varphi = \pi^{\beta}|_A$. By the assumption, we have $\Phi = V_{G \to A}$, which is a homomorphism of G to the abelian group A. Therefore $\Omega_{\alpha+\beta}(G) = \mathrm{Ker}(\Phi) = \Phi^{-1}(1)$, and

$$\Omega_{\alpha+\beta}(G) = \{g \in G \mid g^{p^{\alpha+\beta}} = 1\} .$$

It is obvious that $\Omega_{\alpha+\beta}(G)$ contains the commutators in $[G, A]$, and $\Omega_{\beta}(A)$. Hence we have (i). Since $\pi^{\alpha}(G)$ lies in A, by the choice of α, we have $\mho_{\alpha+\beta}(G) \subset \mho_{\beta}(A)$. We also have

$$\mho_{\alpha+\beta}(G) = V_{G \to A}(G) \subset Z(G)$$

because A is a normal abelian subgroup of G (cf. [5, § 3, Corollary to Proposition 3]). Thus we get (ii), too. Let $\mu_1, \mu_2, \cdots, \mu_\omega$ be the type-invariants of the regular p-group $G/C_G(A)$, which are arranged in the order, $\mu_1 \geq \mu_2 \geq \cdots \geq \mu_\omega$ (cf. P. Hall [2]). Put $p^\gamma = \exp(C_G(A)/A)$, the exponent of $C_G(A)/A$. Then we have

$$\mu_1 \leq \alpha \leq \mu_1 + \gamma$$

since $p^{\mu_1} = \exp(G/C_G(A))$. Therefore

$$\alpha + \mu_2 + \cdots + \mu_\omega \leq \gamma + \mu_1 + \mu_2 + \cdots + \mu_\omega \leq \alpha + \beta$$

because we have

$$p^{\gamma+\mu_1+\cdots+\mu_\omega} \leq [G: A] = p^{\alpha+\beta} .$$

Thus we get

$$\mu_2 + \cdots + \mu_\omega \leq \beta .$$

Take a canonical basis $g_1, \cdots, g_\omega$ of the regular group $G/C_G(A)$ so that

$$p^{\mu_i} = [\langle g_i \rangle \cdot C_G(A): C_G(A)]$$

for $i = 1, 2, \cdots, \omega$. If $i \geq 2$, then $g_i^{p^\beta}$ belongs to $C_G(A)$, and $\langle g_i \rangle \cdot A$ is regular by the condition (2). Therefore we have

$$\pi^{\beta}([g_2, A]) = \cdots = \pi^{\beta}([g_\omega, A]) = \{1\}$$

by P. Hall [2, Theorem 4.22] or by Huppert [3, Ch. III, 10.6 b)]. For g and h in G, and for $a \in A$,

$$\begin{aligned} [g \cdot h, a] &= [g, a] \cdot [[g, a], h] \cdot [h, a] \\ &= [g, a] \cdot [h, [g, a]]^{-1} \cdot [h, a] \\ &= [g, a] \cdot [h, [g, a]^{-1} \cdot a] \end{aligned}$$

because A is abelian and normal in G. Therefore

$$[G, A] = [g_1, A]\cdot[g_2, A]\cdots[g_\omega, A] .$$

Since $[g_i, A]$ lies in $\Omega_\beta(A)$ if $i \geq 2$, we have

$$(*) \qquad [G, A]\cdot\Omega_\beta(A) = [g_1, A]\cdot\Omega_\beta(A) .$$

Furthermore

$$[g_i, a^{p^\beta}] = [g_i, a]^{p^\beta} = 1$$

for each $a \in A$ if $i \geq 2$. Hence we get

$$\mathfrak{V}_\beta(A) \subset Z(\langle g_2, \cdots, g_\omega\rangle\cdot C_G(A)) .$$

Now, let ψ be the endomorphism of A defined by

$$\psi(a) = [g_1, a] \qquad \text{for } a \in A .$$

Then $\psi(A) = [g_1, A]$ and $\psi^{-1}(1) = C_A(g_1)$. Therefore, especially,

$$(**) \qquad \mathfrak{V}_\beta(A) \cap \psi^{-1}(1) = \mathfrak{V}_\beta(A) \cap Z(G) .$$

It is obvious that $\varphi\circ\psi = \psi\circ\varphi$ where $\varphi = \pi^\beta|_A$. By (*) and (**) with (i) and (ii), which have been proved, we can apply Lemma 4 to $\Phi = \pi^{\alpha+\beta}$, φ and ψ, and obtain (iii) at once. The proof is completed.

5. The proof of Theorem 3. When G is regular, we can use Lemma 4 directly (without using transfers) to get a better result, Theorem 3. Let $g_1, g_2, \cdots$ be the canonical basis of G/A such that $p^{\mu_i} = [\langle g_i\rangle\cdot A : A]$. The commutator subgroup $[G, G]$ of G is generated by $[g_i, a]$ with $a \in A$, $[g_i, g_j]$ $(i < j)$, and their conjugates. Since $g_i^{p^\mu}$ and $g_j^{p^\nu}$ $(j \geq 2)$ belong to the abelian group A, they commute with each other and with each $a \in A$. Therefore, the orders of $[g_i, a]$ and $[g_i, g_j]$ divide $p^{\mu+\nu}$. Hence the exponent of $[G, G]$ is less than or equal to $p^{\mu+\nu}$. Then, by the definition of regularity, we have

$$\pi^{\mu+\nu}(g\cdot h) = \pi^{\mu+\nu}(g)\cdot\pi^{\mu+\nu}(h)$$

for g and h in G. This shows that $\pi^{\mu+\nu}$ is a homomorphism. Since $p^\mu = p^{\mu_1}$ is the exponent of G/A, the image of $\pi^{\mu+\nu}$ lies in A. Put $\Phi = \pi^{\mu+\nu}: G \to A$, $\varphi = \pi^\nu|_A$ and $\psi(a) = [g_1, a]$ for $a \in A$. Then a similar argument to the one in the proof of the preceding section will complete the proof of Theorem 3. The rest of the proof is, therefore, omitted.

6. The comments and the problems. As one of the simplest cases of Theorem 6, we have

THEOREM 7. *Let G be a finite metabelian regular p-group, and A be a normal abelian subgroup of G such that G/A is cyclic. Put $p^{\mu} = [G: A]$. Then we have*

$$[\Omega_{\mu}(G): [G, G]] = [G: A] \cdot [A \cap Z(G): \mho_{\mu}(G)] .$$

Proof. In this case, we have $[G, A] = [G, G]$. If $\nu = 0$, then $\Omega_{\nu}(A) = \{1\}$, and $\mho_{\nu}(A) = A$. Therefore, (iii) of Theorem 3 is just this formula of the theorem. Q.E.D.

We can not dispense with the condition that G is regular. In fact: Let G be the group of Example of Section 3, and take $A = \langle a_1, a_2, \cdots, a_{p-1} \rangle$. Then $[G: A] = p$ and $\mu = 1$. Since $\Omega_1(G)$ coincides with $[G, G] = \langle a_1^p, a_2, \cdots, a_{p-1} \rangle$, the index $p = [G: A]$ cannot divide $[\Omega_1(G): [G, G]]$.

As far as G is regular, the group $\Omega_{\mu+\nu}(G)$ of Theorem 3 is the kernel of the homomorphism $\Phi(= \pi^{\mu+\nu})$ of G to the abelian group A. Therefore, it contains $[G, G]$. Then we may ask

PROBLEM 1. Let the notation and the assumptions be as in Theorem 3. Determine the minimal ν $(\geq \mu_2)$ such that the index $[G: A]$ divides $[\Omega_{\mu+\nu}(G): [G, G]]$ in the case where A contains $[G, G]$. (Therefore G is metabelian.)

If $A = G[\rho]$ for some $\rho \in \mathrm{End}(G)$, then we see that the minimal ν is at most $\alpha(\rho) - \mu$ by Corollary 2 of Theorem 5.

PROBLEM 2. Let G be a metabelian p-group, and A be an abelian subgroup of G which contains $[G, G]$. Does the index $[G: A]$ divides $[\mathrm{Ker}(V_{G \to A}): [G, G]]$?

When G is regular, this problem is a part of the preceding one by Theorem 4.

Let G be the irregular p-group of Example of Section 3, and $A = \langle a_1, a_2, \cdots, a_{p-1} \rangle$. We have $\mathrm{Ker}(V_{G \to A}) = A$ in this case. (Cf. Huppert [3, Ch. III, 10.15].) Therefore the answer is 'Yes'.

If $A = G[\rho]$ for some $\rho \in \mathrm{End}(G)$, then the answer is also 'Yes' by Terada's Principal Ideal Theorem. In the case of $A = [G, G]$, the answer 'Yes' is equivalent to the original Principal Ideal Theorem.

III. The relative uniqueness bases of regular p-groups

1. The relative uniqueness basis. Let G be a finite regular p-group for a fixed prime integer p. Let H be a given subgroup of G. We call

an ordered set of elements of G,

$$g_1, g_2, \cdots, g_\tau ,$$

a uniqueness basis of (the left cosets) G/H if every coset of G/H can be represented by one and only one element of G of the form

$$g_1^{m_1} \cdot g_2^{m_2} \cdots g_\tau^{m_\tau}$$

with

$$0 \leq m_i < \mu_i \qquad (i = 1, \cdots, \tau)$$

where μ_i is the minimal positive integer such that $g_i^{\mu_i}$ belongs to H. P. Hall [2] showed the existence of a uniqueness basis for $H = \{1\}$, or, we may say, for a normal subgroup H because a quotient group of a regular p-group is also regular.

But if H is not normal in G, it is far from obviousness, at least at a first glance, that there exists a uniqueness basis of G/H. This part of the paper is devoted to show it, essencially by following the way of P. Hall [2]. Hence we show that such a basis is obtained if we construct a canonical basis of G/H, which will be defined in Section 3 below.

2. The L-series. Let $\omega = \omega(G)$ be the invariant of G determined by the relation $p^\omega = [G: \mathfrak{O}_1(G)]$. An L-series Λ of G is a decending series of normal subgroups L_i of G,

$$\Lambda: L_0 = G \supset L_1 \supset \cdots \supset L_\omega = \mathfrak{O}_1(G)$$

such that $[L_{i-1}: L_i] = p$ for $i = 1, 2, \cdots, \omega$.

We denote the exponent of G by $\varepsilon = p^\mu$, and let $\lambda = \lambda(\Lambda)$ be the maximal index such that the exponent of $L_{\lambda-1}$ is equal to ε. Put

$$K = \mathfrak{O}_{\mu-1}(L_{\lambda-1}) = \{g^{\varepsilon/p} \mid g \in L_{\lambda-1}\} .$$

LEMMA 5 (P. Hall [2]). *K is a cyclic group of order p, and lies in the center of G.*

For the proof, see P. Hall [2, the proof of (e), pp 92–93].

LEMMA 6. *Let i be an index of the L-series Λ other than λ, and e be a positive integer. If there is an element g of $L_{i-1} - L_i$ such that g^e belongs to $K \cdot H$, then there exists an element x in $L_{i-1} - L_i$ such that x^e belongs to H.*

Proof. Take an element $z \in L_{\lambda-1} - L_\lambda$. Then $K = \langle z^{\varepsilon/p} \rangle$ because the exponent of L_λ is less than or equal to ε/p by the choice of λ. Suppose that $g^e \in K \cdot H$ for some $g \in L_{i-1} - L_i$. We may assume that $e = p^\nu$ for some non-negative integer ν and $\nu < \mu$. Take an integer m and an element h of H so that $g^e = z^{m\varepsilon/p} \cdot h$. Put $n = p^{\mu-\nu-1} = \varepsilon/p^{\nu+1}$ and $x = g \cdot z^{-mn}$. Since $(z^{-mn})^e$ belongs to the center of G, the commutators of $\langle g, z^{-mn} \rangle$ have the orders at most e by P. Hall [2, Th. 4.22]. Therefore, we have

$$x^e = g^e \cdot z^{-mne}$$

since G is regular. Then by the choice of n, we have $x^e = h \in H$. If $\nu = \mu - 1$, then we may assume that g is of order $\varepsilon = p^\mu$ because $g^e = 1 \in H$ otherwise. In this case, then, we have $i < \lambda$, and $L_i \supset L_{\lambda-1}$. Therefore, $x = g \cdot z^{-mn}$ certainly belongs to $L_{i-1} - L_i$. If $\nu < \mu - 1$, then z^{-mn} belongs to $\mathfrak{O}_1(G)$. Since $\mathfrak{O}_1(G)$ lies in L_i, we have $x \in L_{i-1} - L_i$ in this case, too. The proof is completed.

3. The relative canonical basis. For each i $(1 \leq i \leq \omega)$, define a positive integer $e_i = e_i(\Lambda, H)$ by

$$e_i = \min \{e \mid e \geq 1, \ {}^\exists g \in L_{i-1} - L_i \ (g^e \in H)\}$$

and put

$$C_i = C_i(\Lambda, H) = \{g \in L_{i-1} - L_i \mid g^{e_i} \in H\} .$$

Determine the positive integer $\tau = \tau(G, H)$ by the relation,

$$p^\tau = [G : \mathfrak{O}_1(G) \cdot H] .$$

Then there exists exactly τ indices $i_1, i_2, \cdots, i_\tau$ such that

$$1 \leq i_1 < i_2 < \cdots < i_\tau \leq \omega$$

and

$$L_{i_\nu - 1} \cdot H \supsetneq L_{i_\nu} \cdot H \qquad (\nu = 1, \cdots, \tau) .$$

The sequence of τ elements of G,

$$g_1, g_2, \cdots, g_\tau$$

will be called a canonical basis of G/H belonging to the L-series Λ if each of the τ sets C_{i_ν} $(\nu = 1, \cdots, \tau)$ contains just one of the τ elements g_j.

THEOREM 8. *Every canonical basis of G/H is a uniqueness basis of G/H.*

Proof. Induction on the order $|G|$. If $|G| = p$, then the theorem is clear. Suppose that $|G| > p$. Let $g_1, \cdots, g_\tau$ be a canonical basis belonging to an L-series Λ, and we use the notation introduced above. Put $\bar{G} = G/K$ and $\bar{H} = H \cdot K/K$. If $\varepsilon = p^\mu > p$, then $K \subset \mathfrak{O}_1(G)$. If $\varepsilon = p$, then $\lambda = \omega - 1$, $L_{\omega-1} = K$ and $L_\omega = \mathfrak{O}_1(G) = \{1\}$. Put $\bar{L}_i = L_i/K$ for $i = 0, 1, \cdots, \omega - 1$. Omitting the last term if $\varepsilon = p$, we have an L-series $\bar{\Lambda}$ of $\bar{G}$,

$$\bar{\Lambda}: \bar{L}_0 \supset \bar{L}_1 \supset \cdots \supset \bar{L}_\omega = \mathfrak{O}_1(\bar{G}) .$$

Put $\bar{g}_j = g_j \cdot K \in \bar{G}$ for $j = 1, \cdots, \tau$.

Case I: Suppose that $H \supset K$. Then $\bar{g}_1, \cdots, \bar{g}_\tau$ is a canonical basis of $\bar{G}/\bar{H}$ belonging to $\bar{\Lambda}$. Since $|\bar{G}|$ is less than $|G|$, it is a uniqueness basis of $\bar{G}/\bar{H}$ by the induction hypothesis. Therefore, the natural correspondence between $\bar{G}/\bar{H}$ and G/H establishes that $g_1, \cdots, g_\tau$ is a uniqueness basis of G/H, in this case.

Case II: Suppose that $H \not\supset K$. Then $K \cap H = \{1\}$. First, we show that the index λ appears in the series, $i_1, i_2, \cdots, i_\tau$. In fact, assume, on the contrary, that $L_{\lambda-1} \cdot H = L_\lambda \cdot H$. Take $z \in L_{\lambda-1} - L_\lambda$. Then there are $x \in L_\lambda$ and $h \in H$ such that $z = x \cdot h$. Since the order of x^{-1} is less than $\varepsilon = p^\mu$, we have $x^{-\varepsilon/p} = 1$. Therefore $h^{\varepsilon/p} = (x^{-1} \cdot z)^{\varepsilon/p} = x^{-\varepsilon/p} \cdot z^{\varepsilon/p} = z^{\varepsilon/p} \neq 1$. But $h^{\varepsilon/p}$ belongs to $K \cap H$, which contradicts that $K \cap H$ is equal to $\{1\}$. Now, let k be the index such that g_k belongs to $C_\lambda = L_{\lambda-1} - L_\lambda$. Let μ_j and $\bar{\mu}_j$ be the minimal positive integers such that $g_j^{\mu_j} \in H$ and $\bar{g}_j^{\bar{\mu}_j} \in \bar{H}$, respectively, for $j = 1, \cdots, \tau$. Then $\mu_k = \varepsilon$ and $\bar{\mu}_k = \varepsilon/p$. If j is other than k, then we have $\mu_j = \bar{\mu}_j$ by Lemma 6. Suppose that $\bar{L}_{i-1} \cdot \bar{H} = \bar{L}_i \cdot \bar{H}$. Then we have $L_{i-1} \cdot K \cdot H = L_i \cdot K \cdot H$. If $\varepsilon > p$, then K lies in $\mathfrak{O}_1(G)$, and so, in L_i. Therefore, we have $L_{i-1} \cdot H = L_i \cdot H$. If $\varepsilon = p$, then $K = L_{\omega-1}$. Therefore, we also have $L_{i-1} \cdot H = L_i \cdot H$ for $i \leq \omega - 1$. Hence $\bar{L}_{i-1} \cdot \bar{H} = \bar{L}_i \cdot \bar{H}$ is equivalent to $L_{i-1} \cdot H = L_i \cdot H$ unless $\varepsilon = p$ and $i = \omega$. Thus we conclude that $\bar{g}_1, \cdots, \bar{g}_\tau$, omitting the term $\bar{g}_k$ if $\varepsilon = p$, is a canonical basis of $\bar{G}/\bar{H}$ which belongs to the L-series $\bar{\Lambda}$ of $\bar{G}$. Since $|\bar{G}| < |G|$, the sequence is a uniqueness basis of $\bar{G}/\bar{H}$ by the induction hypothesis. Then we can see that $g_1, \cdots, g_\tau$ form a uniqueness basis of G/H, in the straight forward way, knowing that $g_k^{\varepsilon/p}$ is in the center of G. And then the proof is completed.

We close this chapter pointing out

THEOREM 9. *Every canonical basis of G/H is also a uniqueness basis of $H\backslash G$.*

Proof. Let $g_1, \cdots, g_\tau$ be a canonical basis belonging to an L-series Λ. Then $g_\tau^{-1}, \cdots, g_1^{-1}$ is also a canonical basis by the definition, and so, a uniqueness basis of G/H. Assigning its inverse to each element of G, we have the natural correspondence between G/H and $H\backslash G$, which establishes the theorem at once.

References

[1] J. Alperin and Tzee-Nan Kuo, The exponent and the projective representations of a finite group, Illinois J. Math., **11** (1967), 410–414.
[2] P. Hall, A contribution to the theory of groups of prime power order, Proc. London Math. Soc., (2), **36** (1933), 29–95.
[3] B. Huppert, Endliche Gruppen I, Springer-Verlag, Berlin·Heidelberg·New York (1967).
[4] K. Miyake, On the structure of the idele groups of algebraic number fields, II, Tôhoku Math. J., **34** (1982), 101–112.
[5] ——, A generalization of Hilbert's Theorem 94, Nagoya Math. J., **96** (1984), 83–94.
[6] F. Terada, A principal ideal theorem in the genus field, Tôhoku Math. J., **23** (1971), 697–718.
[7] H. Zassenhaus, The theory of groups, 2nd edit., Chelsea Pub. Co., New York (1958).

Department of Mathematics
College of General Education
Nagoya University
Chikusa-ku, Nagoya 464, Japan