

**SOME p -GROUPS WITH TWO GENERATORS
WHICH SATISFY CERTAIN CONDITIONS ARISING
FROM ARITHMETIC IN IMAGINARY
QUADRATIC FIELDS**

KATSUYA MIYAKE

(Received September 30, 1991, revised March 30, 1992)

Abstract. Let p be an odd prime. We give a list of certain types of p -groups G with two generators which satisfy the following two conditions (A) and (B): (A) $[\text{Ker } V_{G \rightarrow H}: [G, G]] = [G: H]$ for the transfer homomorphism $V_{G \rightarrow H}: G \rightarrow H/[H, H]$ of G to every normal subgroup H with cyclic quotient G/H , and (B) there exists an automorphism φ of G of order 2 such that $g^{\varphi+1} \in [G, G]$ for every $g \in G$. These conditions are necessary for G to be the Galois group of the second p -class field of an imaginary quadratic field. The list contains such a group that it may be useful for us to find an imaginary quadratic field with an interesting property on the capitulation problem.

1. Introduction. We fix an odd prime number p , and consider a finite metabelian p -group G with two generators which satisfies the following two conditions (A) and (B):

- (A) For every normal subgroup H of G with cyclic quotient G/H , the index $[\text{Ker } V_{G \rightarrow H}: [G, G]]$ for the transfer homomorphism $V_{G \rightarrow H}: G \rightarrow H/[H, H]$ coincides with the index $[G: H]$;
- (B) There exists an automorphism φ of G of order 2 such that $g^{\varphi+1}$ belongs to $[G, G]$ for every $g \in G$.

It is known as Hilbert's Theorem 94 that the former index in (A) is a multiple of the latter (cf. Suzuki [Su] for the general case); therefore, the condition (A) claims the extreme for the normal subgroups H of the kind. If G is abelian, then it satisfies (A) if and only if it is a cyclic group. It is also easy to see that G is not a metacyclic group if it satisfies the condition (B). On his list in [Ja], roughly and boldly speaking, James gave about 500 types of p -groups of order up to p^6 ; however, we find only 8 of them with two generators satisfy both of (A) and (B).

In this paper we determine all of such groups of the following form with either one of the three conditions, (1) $m = n = 2$, (2) $\mu = 1 \leq v$, and (3) $\mu = v = 2$ (Theorems 1–3 in Section 7, respectively):

$$\begin{aligned}
 G &= \langle a, b, c_{i,1}, c_{1,j} \mid 1 \leq i \leq m, 1 \leq j \leq n \rangle, \\
 [a, b] &= c_{1,1}, \quad [c_{i,1}, a] = c_{i+1,1}, \quad [c_{1,j}, b] = c_{1,j+1}, \\
 [c_{i+1,1}, b] &= [c_{1,j+1}, a] = [c_{i,1}, c_{1,j}] = 1, \\
 c_{m+1,1} &= c_{1,n+1} = 1, \\
 a^{p^\mu} &= \prod_{i,j} c_{i,j}^{q_{i,j}}, \quad b^{p^\nu} = \prod_{i,j} c_{i,j}^{r_{i,j}}, \\
 q_{i,j}, r_{i,j} &\in \mathbf{Z}, \quad (i-1)(j-1) = 0, \\
 c_{i,1}^{p^{\mu-t(i)}} &= c_{1,j}^{p^{\min(\mu, \nu-t(j))}} = 1, \\
 \mu \leq \nu, \quad &1 \leq i \leq m, 1 \leq j \leq n,
 \end{aligned}$$

where $t(i)$ is the maximal integer which satisfies the inequality, $p^{t(i)} \leq i < p^{t(i)+1}$

They consist of 13 families; 3 of them are classified with the condition (1), 7 with (2), and 3 with (3). As for the groups on the list of James, all of them belong to the first class of ours. It may be remarkable that we have either $m=2$ or $n=2$ under the conditions (A) and (B) (Proposition 10 in Section 6).

In Section 2, we explain the arithmetic background.

In Section 3, we give some basic lemmas.

In Section 4, we see some fundamental structures of metabelian p -groups with two generators.

Section 5 is devoted to calculations of transfers of our groups to three types of subgroups. From the results, we extract some necessary conditions for (A) to be satisfied, and show it in Section 6. Our three main theorems are given in the big Section 7.

In the final Section 8, we show a proposition on the capitulation problem in imaginary quadratic number fields.

2. Arithmetic background. Let F be an imaginary quadratic number field, \tilde{F} the Hilbert p -class field of F , and $\tilde{\tilde{F}}$ the second p -class field of F ; hence \tilde{F} is the maximal unramified abelian p -extension of F , and $\tilde{\tilde{F}}$ is that of \tilde{F} . We denote the Galois groups, $\text{Gal}(\tilde{\tilde{F}}/F)$ and $\text{Gal}(\tilde{F}/F)$, simply by G and by A , respectively; A is isomorphic to $G/[G, G]$. By class field theory, the Artin maps give isomorphisms of A and of $[G, G]$, respectively, onto the p -primary parts, $\text{Cl}^{(p)}(F)$ and $\text{Cl}^{(p)}(\tilde{F})$, of the ideal class group $\text{Cl}(F)$ of F and that of \tilde{F} . Let K be an unramified abelian p -extension of F and H the corresponding subgroup of G ; then $H/[H, H]$ is isomorphic to the p -primary part $\text{Cl}^{(p)}(K)$ of the ideal class group $\text{Cl}(K)$ of K by the Artin map for K . We have a natural homomorphism

$$j_{K/F}: \text{Cl}(F) \rightarrow \text{Cl}(K)$$

defined by regarding ideals of F naturally as those of K . By the Artin maps of F and of K this is transformed to the homomorphism

$$\bar{V}_{G \rightarrow H}: G/[G, G] \rightarrow H/[H, H]$$

which is naturally induced from the transfer $V_{G \rightarrow H}$ of G to H (cf., e.g., Miyake [Mi2]); therefore the order of the kernel of $j_{K/F}$ coincides with the index $[\text{Ker } V_{G \rightarrow H}: [G, G]]$. Hence we see that $G = \text{Gal}(\tilde{F}/F)$ satisfies the condition (A) given in the preceding section, by the following proposition.

PROPOSITION 1. *Let K be an unramified cyclic extension of odd degree of an imaginary quadratic field F . Then the order of the capitulation kernel, $|\text{Ker } j_{K/F}|$, is equal to the degree $[K:F]$.*

PROOF. Since K/F is unramified and cyclic, we have

$$|\text{Ker } j_{K/F}| = [K:F] \cdot [E_F : N_{K/F}(E_K)]$$

where E_F and E_K are, respectively, the unit groups of F and of K , and $N_{K/F}$ is the norm map (cf., e.g., Schmithals [Sch]). We have $E_F = \{\pm 1\}$ because F is an imaginary quadratic field; (note that the field of the third or the fourth roots of 1 has the class number 1). Therefore we have $[E_F : N_{K/F}(E_K)] = 1$ because $[K:F]$ is odd by the assumption. q.e.d.

Next let us see that our group $G = \text{Gal}(\tilde{F}/F)$ satisfies the condition (B) given in the preceding section. Take an element ρ of order 2 in $\text{Gal}(\tilde{F}/\mathbb{Q})$; this induces the non-trivial automorphism of F . The inner automorphism of $\text{Gal}(\tilde{F}/\mathbb{Q})$ defined by ρ induces an automorphism φ of $G = \text{Gal}(\tilde{F}/F)$ and an action of ρ on $A = \text{Gal}(\tilde{F}/F)$. We also have a natural action of ρ on $\text{Cl}^{(p)}(F)$. The Artin isomorphism of $\text{Cl}^{(p)}(F)$ onto A is then compatible with these actions of ρ . Hence we have the desired result by the following proposition due to Suzuki.

PROPOSITION 2. *Let F be a quadratic extension of an algebraic number field F_0 of finite degree, and denote the non-trivial automorphism of F/F_0 by ρ . Let c be an element of the ideal class group $\text{Cl}(F)$ of F , and suppose that its order is relatively prime to the class number h_{F_0} of F_0 . Then we have $c^\rho = c^{-1}$.*

PROOF. It is clear that $c^{1+\rho}$ belongs to $j_{F/F_0}(\text{Cl}(F_0))$ and has the order relatively prime to $h_{F_0} = |\text{Cl}(F_0)|$; therefore, it must be equal to 1. Hence we have $c^\rho = c^{-1}$.
q.e.d.

If the p -class group $\text{Cl}^{(p)}(F)$ of an imaginary quadratic field F is cyclic, then we have $\tilde{F} = \tilde{F}$ because a cyclic group does not possess any non-abelian central extensions. If $\text{Cl}^{(p)}(F)$ is of type (p^μ, p^ν) , $1 \leq \mu \leq \nu$, however, \tilde{F} is actually bigger than \tilde{F} .

PROPOSITION 3. *Let F be an imaginary quadratic field and suppose that $\text{Cl}^{(p)}(F)$ is of type (p^μ, p^ν) , $1 \leq \mu \leq \nu$. Then F has an unramified Galois extension whose group is isomorphic to $D = \langle a, b, c_{1,1} \rangle$,*

$$[a, b] = c_{1,1}, \quad [a, c_{1,1}] = [b, c_{1,1}] = a^{p^\mu} = b^{p^\nu} = c_{1,1}^{p^\mu} = 1.$$

The proposition is an easy consequence of Nomura [No, Th.1]. In fact, apply the theorem to our case step by step starting from $E = D / \langle c_{1,1}^p \rangle$, and then $E = D / \langle c_{1,1}^{p^2} \rangle$, and so on. Here we omit the detail. Also cf. [Mi3, Theorem 1 and its proof in Section 3].

The group D of the proposition, however, does not satisfy the condition (A). Therefore $\text{Gal}(\tilde{F}/F)$ must be a non-trivial extension of it. This paper grew out of the author's search for some candidates for $\text{Gal}(\tilde{F}/F)$.

3. Basic lemmas. To examine whether the condition (A) is satisfied or not, it is not necessary to study all of the subgroups of the kind.

LEMMA 1. *Let G be a finite group and H a normal subgroup of it. Suppose that G/H is cyclic and that we have*

$$[\text{Ker } V_{G \rightarrow H} : [G, G]] = [G : H].$$

Then for every subgroup N which contains H , we also have

$$[\text{Ker } V_{G \rightarrow N} : [G, G]] = [G : N].$$

PROOF (by Suzuki). It is well known that we have an equality,

$$[\text{Ker } V_{G \rightarrow H} : [G, G]] = [G : H] \cdot [(H/[H, H])^G : \text{Im } V_{G \rightarrow H}],$$

if G/H is cyclic in general. (E.g. check the formula for q in the case $H = A$ in Miyake [Mi1, p. 88], and apply [Mi1, Lemma 5, p. 89].) Hence we also have

$$[\text{Ker } V_{G \rightarrow N} : [G, G]] = [G : N] \cdot [(N/[N, N])^G : \text{Im } V_{G \rightarrow N}].$$

We are given

$$(H/[H, H])^G = \text{Im } V_{G \rightarrow H}$$

by the assumption on H of the lemma, and must show

$$(N/[N, N])^G = \text{Im } V_{G \rightarrow N}.$$

For simplicity, we may assume $[H, H] = 1$ by replacing G with $G/[H, H]$ if necessary. Take an element g of G such that $G = \langle g \rangle \cdot H$, and put $d = [G : N]$. Then we see

$$N = \langle g^d \rangle \cdot H$$

and

$$[N, N] = H^{g^{d-1}}.$$

Since $\langle g^d \rangle \cdot [N, N]/[N, N]$ is contained in $(N/[N, N])^G$, we have

$$(N/[N, N])^G = (\langle g^d \rangle \cdot [N, N]/[N, N]) \cdot (H/[N, N])^G.$$

Hence it is sufficient to show

$$(H/[N, N])^G \subset \text{Im } V_{G \rightarrow N}$$

because the coset $g^d \cdot [N, N]$ is equal to $V_{G \rightarrow N}(g)$ and belongs to $\text{Im } V_{G \rightarrow N}$. Let x be an element of H such that the coset $x \cdot [N, N]$ belongs to $(H/[N, N])^G$. Since

$$x^{g^{-1}} \in [N, N] = H^{g^{d-1}},$$

there exists an element y of H such that

$$x^{g^{-1}} = y^{g^{d-1}} = y^{(g^{d-1} + g^{d-2} + \dots + 1)(g-1)}.$$

Then $x \cdot y^{-(g^{d-1} + g^{d-2} + \dots + 1)}$ belongs to H^G . Hence there is an element z of G such that

$$x \cdot y^{-(g^{d-1} + g^{d-2} + \dots + 1)} = V_{G \rightarrow H}(z)$$

because of the assumption, $H^G = \text{Im } V_{G \rightarrow H}$. Since y belongs to N , we have

$$V_{G \rightarrow N}(y) = y^{g^{d-1} + g^{d-2} + \dots + 1} \cdot [N, N]$$

by the definition of the transfer homomorphism. For simplicity, put $u = g^d$ and $e = [N : H]$. Then we have

$$V_{G \rightarrow H}(z) = (V_{G \rightarrow N}(z) \cdot [N, N])^{u^{e-1} + u^{e-2} + \dots + 1},$$

and hence, in $H/[N, N]$,

$$V_{G \rightarrow H}(z) \cdot [N, N] = V_{G \rightarrow N}(z^{u^{e-1} + u^{e-2} + \dots + 1})$$

(cf. [Mil, Proposition 3] with the inner automorphism φ of G defined by u^j , $1 \leq j \leq e-1$). Thus we have obtained

$$x \cdot [N, N] = V_{G \rightarrow N}(y \cdot z^{u^{e-1} + u^{e-2} + \dots + 1}) \in \text{Im } V_{G \rightarrow N}.$$

The proof is completed.

In this paper we frequently use the following well-known lemma. A proof of it is found in Blackburn [Bl].

LEMMA 2. *Let x, y and z be elements of a metabelian group. We have $[[z, x], y] = [[z, y], x]$ and $[yz, x] = [y, x] \cdot [z, x]$ if z commutes with $[x, y]$. Put*

$$\gamma_1 = [z, x], \quad \gamma_i = [\gamma_{i-1}, x], \quad i = 2, 3, \dots,$$

and suppose that z commutes with each of γ_i , $i = 1, 2, \dots$. Then we have

$$(xz)^j = x^j \cdot z^{x^{j-1} + x^{j-2} + \dots + 1} = x^j \cdot z^j \cdot \gamma_1 \binom{j}{1} \dots \gamma_{j-1} \binom{j}{j}$$

and

$$z^{x^j - 1} = \gamma_1 \binom{j}{1} \cdot \gamma_2 \binom{j}{2} \dots \gamma_j \binom{j}{j}.$$

For the condition (B) of Section 1 to be satisfied, we have a useful necessary condition. Let $G = \langle a, b \rangle$ be a finite metabelian p -group with two generators, and put

$$[a, b] = c_{1,1},$$

$$[c_{i,j}, a] = c_{i+1,j}, \quad [c_{i,j}, b] = c_{i,j+1},$$

for $i, j = 1, 2, 3, \dots$. The first statement of the preceding lemma assures that these $c_{i,j}$ are well defined. Put

$$C_{i,j} = \langle c_{u,v} \mid u = i, i+1, i+2, \dots, v = j, j+1, j+2, \dots \rangle$$

and

$$C'_{i,j} = \langle c_{u,v} \mid u = i, i+1, i+2, \dots, v = j, j+1, j+2, \dots, \text{ and } (u, v) \neq (i, j) \rangle$$

for $i, j = 1, 2, 3, \dots$. These are abelian normal subgroups of G .

LEMMA 3. *Let the notation and the assumptions be as above and suppose that G satisfies the condition (B). Then for $i, j = 1, 2, 3, \dots$, we have*

$$c_{i,j}^\varphi \equiv c_{i,j}^{(-1)^{i+j}} \pmod{C'_{i,j}}.$$

PROOF. We proceed by mathematical induction on $i+j$. First of all, note that $c_{i,j} = 1$ if $i+j$ is larger than the class of G . Let x and y be the elements of $[G, G] = C_{1,1}$ such that $a^\varphi = a^{-1}x$ and $b^\varphi = b^{-1}y$. Then we easily see

$$\begin{aligned} c_{1,1}^\varphi &= [a^\varphi, b^\varphi] = [a^{-1}x, b^{-1}y] \\ &= [a^{-1}, b^{-1}] \cdot [x, b^{-1}] \cdot [y^{-1}, a^{-1}] \\ &\equiv [a^{-1}, b^{-1}] \pmod{C'_{1,1}}. \end{aligned}$$

Since $[a^{-1}, b^{-1}] = bac_{1,1}a^{-1}b^{-1} = c_{1,1} \cdot [c_{1,1}, a^{-1}b^{-1}]$, we have the congruence relation of the lemma for $c_{1,1}$. By definition, we have

$$c_{i+1,j}^\varphi = [c_{i,j}^\varphi, a^\varphi] = [c_{i,j}^\varphi, a^{-1}x] = [c_{i,j}^\varphi, a^{-1}],$$

and

$$c_{i,j+1}^\varphi = [c_{i,j}^\varphi, b^\varphi] = [c_{i,j}^\varphi, b^{-1}y] = [c_{i,j}^\varphi, b^{-1}].$$

The desired relations for $c_{i+1,j}^\varphi$ and $c_{i,j+1}^\varphi$ now easily follow from the induction hypotheses and the next lemma.

LEMMA 4. *The notation and the assumptions being as above, we have*

$$ac_{i,j}a^{-1} = \prod_{u=0}^{\infty} c_{i+u,j}^{(-1)^u}, \quad \text{and} \quad bc_{i,j}b^{-1} = \prod_{u=0}^{\infty} c_{i,j+u}^{(-1)^u};$$

hence, in particular, we have

$$[C'_{i,j}, a^{-1}] \subset C'_{i+1,j} \quad \text{and} \quad [C'_{i,j}, b^{-1}] \subset C'_{i,j+1}.$$

PROOF. The first equality is easily obtained if we study the conjugate of the right hand side by *a*. The second will be also clear in a similar way. The rest follows from these two equalities at once.

4. Metabelian *p*-groups with two generators. Let $G = \langle a, b \rangle$ be a finite metabelian *p*-group with two generators, and let the notation be as in the preceding section. We consider the case of

$$(4.1) \quad C_{2,2} = 1, \quad \text{i.e. } c_{i,j} = 1 \quad \text{if } i \geq 2 \quad \text{and} \quad j \geq 2,$$

and take such *m* and *n* that $c_{m,1} \neq 1$, $c_{1,n} \neq 1$ and $c_{m+1,1} = c_{1,n+1} = 1$. We suppose, furthermore, that $G/[G, G]$ is of type (p^μ, p^ν) , $1 \leq \mu \leq \nu$, i.e.

$$(4.2) \quad a^{p^\mu} = \prod_{i,j} c_{i,j}^{q_{i,j}}, \quad b^{p^\nu} = \prod_{i,j} c_{i,j}^{r_{i,j}},$$

$$q_{i,j}, r_{i,j} \in \mathbf{Z}, \quad 1 \leq i \leq m, \quad 1 \leq j \leq n.$$

Throughout this paper, we assume

$$(4.3) \quad q_{1,1} = r_{1,1} = 0, \quad \text{i.e. } a^{p^\mu}, b^{p^\nu} \in C'_{1,1} = G_3 = [[G, G], G],$$

because of Lemma 3 for *G* to satisfy (B). Since a^{p^μ} (resp. b^{p^ν}) commutes with *a* (resp. *b*), we must have

$$(4.4) \quad \prod_{i=2}^m c_{i+1,1}^{q_{i,1}} = 1 \quad \text{and} \quad \prod_{j=2}^n c_{1,j+1}^{r_{1,j}} = 1.$$

For an element $c_{i,j}$ of $C_{1,1} = G_2 = [G, G]$ and for a positive integer *k*, we denote

$$c_{i,j}^{[k]} := c_{i,j}^{\binom{k}{1}} \cdot c_{i+1,j}^{\binom{k}{2}} \cdots c_{i+k-1,j}^{\binom{k}{k}}$$

and

$$c_{i,j}^{(k)} := c_{i,j}^{\binom{k}{1}} \cdot c_{i,j+1}^{\binom{k}{2}} \cdots c_{i,j+k-1}^{\binom{k}{k}}.$$

It is clear that we have

$$(4.5) \quad [c_{i,j}^{[k]}, a] = c_{i+1,j}^{[k]};$$

$$[c_{i,j}^{[k]}, b] = c_{i,j+1}^{[k]} \quad (= c_{i,j+1}^k);$$

$$(4.6) \quad [c_{i,j}^{(k)}, a] = c_{i+1,j}^{(k)} \quad (= c_{i+1,j}^k);$$

$$[c_{i,j}^{(k)}, b] = c_{i,j+1}^{(k)}.$$

Since $b^{-1}ab = ac_{1,1}$, we have by Lemma 2

$$b^{-1}a^{p^\mu}b = a^{p^\mu}c_{1,1}^{[p^\mu]},$$

and hence by (4.2) and (4.3)

$$(4.7) \quad c_{1,1}^{[p^\mu]} = \prod_{j=2}^n c_{1,j+1}^{q_{1,j}}.$$

Similarly with $a^{-1}ba = bc_{1,1}^{-1}$, we also have

$$(4.8) \quad c_{1,1}^{[p^\nu]} = \prod_{i=2}^m c_{i+1,1}^{-r_{i,1}}.$$

PROPOSITION 4. Under the conditions (4.1) and (4.2), we have

$$c_{2,1}^{[p^\mu]} = c_{3,1}^{[p^\mu]} = \cdots = c_{m,1}^{[p^\mu]} = 1,$$

and

$$c_{1,2}^{[p^\nu]} = c_{1,3}^{[p^\nu]} = \cdots = c_{1,n}^{[p^\nu]} = 1.$$

In particular, we have

$$c_{m,1}^{p^\mu} = c_{1,n}^{p^\mu} = 1.$$

PROOF. By (4.7), we see $[c_{1,1}^{[p^\mu]}, a] = 1$. Hence we have the first assertion by using (4.5) successively. It is apparent that we have the second in a similar way. By definition, we see $c_{m,1}^{[p^\mu]} = c_{m,1}^{p^\mu} = 1$. To obtain $c_{1,n}^{p^\mu} = 1$, transform $c_{1,1}^{[p^\mu]}$ by forming the commutator with b successively $n - 1$ times; then by (4.5) and (4.7), we have $c_{1,n}^{[p^\mu]} = c_{1,n}^{p^\mu} = 1$. The proof is completed.

PROPOSITION 5. Let $p^{e_{i,j}}$ be the exponent of $c_{i,j}$.

(1) If $\mu = \nu$, we have

$$e_{1,1} \leq \mu + \min \left\{ \max \left\{ \left\lfloor \frac{m-1}{p-1} \right\rfloor, \mu + \left\lfloor \frac{n-3}{p-1} \right\rfloor \right\}, \max \left\{ \mu + \left\lfloor \frac{m-3}{p-1} \right\rfloor, \left\lfloor \frac{n-1}{p-1} \right\rfloor \right\} \right\},$$

$$e_{i,1} \leq \mu + \left\lfloor \frac{m-i}{p-1} \right\rfloor, \quad 2 \leq i \leq m,$$

$$e_{1,j} \leq \mu + \left\lfloor \frac{n-j}{p-1} \right\rfloor, \quad 2 \leq j \leq n.$$

(2) If $\mu < \nu$, we have

$$e_{1,1} \leq \min \left\{ \mu + \max \left\{ \left\lfloor \frac{m-1}{p-1} \right\rfloor, \nu + \left\lfloor \frac{n-5}{p-1} \right\rfloor \right\}, \nu + \max \left\{ \mu + \left\lfloor \frac{m-3}{p-1} \right\rfloor, \left\lfloor \frac{n-3}{p-1} \right\rfloor \right\} \right\},$$

$$e_{i,1} \leq \mu + \left\lfloor \frac{m-i}{p-1} \right\rfloor, \quad 2 \leq i \leq m,$$

$$e_{1,j} \leq v + \left\lceil \frac{n-2-j}{p-1} \right\rceil, \quad 2 \leq j \leq n-2,$$

$$e_{1,j} \leq \mu, \quad n-1 \leq j \leq n.$$

Here $[r]$ for $r \in \mathbf{Q}$ is the largest integer which does not exceed r .

PROOF. First we show $e_{i,1} \leq \mu + [(m-i)/(p-1)]$, $2 \leq i \leq m$, by mathematical induction on $m-i$. The case of $m-i=0$ has been shown by the preceding proposition. Suppose $2 \leq i < m$ and that the statement is true for all $m-k$, $i < k \leq m$. By the preceding proposition, we also have

$$c_{i,1}^{[p^\mu]} = c_{i,1}^{p^\mu} \cdot c_{i+1,1}^{\binom{p^\mu}{2}} \cdots c_{i+k-1,1}^{\binom{p^\mu}{k}} \cdots = 1.$$

To complete the induction process, it is enough to show that

$$\binom{p^\mu}{k} \cdot p^{\lceil \frac{m-i}{p-1} \rceil} \text{ is divisible by } p^{\mu + \lceil \frac{m-(i+k-1)}{p-1} \rceil}$$

for every k , $i < k \leq m$. This will be seen by the next lemma.

LEMMA 5. (1) If $p^e | k$, then $p^{\mu-e} | \binom{p^\mu}{k}$.

(2) If $p^e \nmid k$, then

$$\left\lceil \frac{m-i}{p-1} \right\rceil \geq \left\lceil \frac{m-(i+k-1)}{p-1} \right\rceil + kp^{-e} \cdot \frac{p^e-1}{p-1} \geq \left\lceil \frac{m-(i+k-1)}{p-1} \right\rceil + e.$$

PROOF. For k , $2 \leq k \leq p^\mu$, we have

$$\binom{p^\mu}{k} = \binom{p^\mu}{k-1} \cdot \frac{p^\mu - (k-1)}{k}.$$

Hence (1) is easily shown by induction on k . As for (2), we have an equality,

$$m-i = m-(i+k-1) + (kp^{-e}-1) + kp^{-e} \cdot (p^e-1);$$

since $kp^{-e} \cdot (p^e-1)/(p-1)$ is a positive integer, (2) follows from this at once. q.e.d.

Now let us go back to the proof of Proposition 5. If $\mu = v$, the third statement of (1) is shown in the same way as the second was done above. Then the first immediately follows from these, (4.7) and (4.8). If $\mu < v$, we have $c_{m,1}^{p^\mu} = c_{1,n}^{p^\mu} = 1$ by Proposition 4. Furthermore we also have $c_{1,n-1}^{p^\mu} = 1$ in the same way as we did for $c_{1,n}^{p^\mu} = 1$. With these and the second statement of Proposition 4, we easily obtain all of (2) by a careful modification of the proof above to (1). Here we omit the detail.

From now on, we impose much stronger conditions on the orders of $c_{i,j}$ given in

Section 1 than what we saw in Proposition 5; namely, we suppose the following additional relations

$$(4.9) \quad c_{i,1}^{p^\mu - t(i)} = c_{1,j}^{p^{\min(\mu, \nu - t(j))}} = 1, \quad 1 \leq i \leq m, \quad 1 \leq j \leq n,$$

where $t(i)$ is the maximal integer which satisfies the condition, $p^{t(i)} \leq i < p^{t(i)+1}$. These are so chosen, beside the condition $C_{2,2} = 1$, that we have

$$(4.10) \quad c_{1,1}^{[p^\mu]} = c_{1,1}^{[p^\nu]} = 1$$

and hence, automatically, all of the relations in Propositions 4 and 5, and that we have small groups which seem easy to be handled. In particular, it follows from (4.7) and (4.8) together with (4.4) that

$$(4.11) \quad \prod_{i=2}^m c_{i+1,1}^{q_{i,1}} = \prod_{i=2}^m c_{i+1,1}^{r_{i,1}} = 1$$

and

$$(4.12) \quad \prod_{j=2}^n c_{1,j+1}^{q_{1,j}} = \prod_{j=2}^n c_{1,j+1}^{r_{1,j}} = 1.$$

PROPOSITION 6. *If either $q_{2,1}$ or $r_{2,1}$ is not congruent to 0 modulo p , then we have $m \leq 2$, i.e. $c_{3,1} = c_{4,1} = \dots = 1$. Similarly, if either $q_{1,2}$ or $r_{1,2}$ is not congruent to 0 modulo p , we have $n \leq 2$, i.e. $c_{1,3} = c_{1,4} = \dots = 1$.*

PROOF. Assume, on the contrary, that either $q_{2,1}$ or $r_{2,1}$ is not congruent to 0 modulo p and $m > 2$. Then we have

$$c_{m,1}^{q_{2,1}} = c_{m,1}^{r_{2,1}} = 1$$

by forming commutators of the first or the second term of (4.11) successively $m - 3$ times with a . Hence we should have $c_{m,1} = 1$ in contradiction to the choice of m . The latter half of the proposition is shown in a similar way.

5. Calculation of transfers. There are three types of minimal ones among those normal subgroups H of G whose quotient groups G/H are cyclic:

Type 1: $H = \langle a^s b \rangle \cdot [G, G], \quad (s, p) = 1;$

Type 2: $H = \langle a^s b \rangle \cdot [G, G], \quad s = s' p^e, \quad (s', p) = 1, \quad 1 \leq e \leq \mu;$

Type 3: $H = \langle a b^s \rangle \cdot [G, G], \quad s = s' p^e, \quad (s', p) = 1, \quad 1 \leq e \leq \nu.$

PROPOSITION 7. *The images of the transfer homomorphism*

$$V_{G \rightarrow H}: G \rightarrow H/[H, H]$$

are given in the following list:

Type 1: $V_{G \rightarrow H}(a) = a^{p^\mu} \cdot [H, H]$, $V_{G \rightarrow H}(b) = b^{p^\mu} \cdot [H, H]$;

Type 2: $V_{G \rightarrow H}(a) = a^{p^\mu} \cdot [H, H]$,

$$V_{G \rightarrow H}(b) = b^{p^\mu} \cdot \prod_{k=2}^{p^\mu} c_{k-1,1}^{-\binom{p^\mu}{k}} \cdot [H, H].$$

Type 3: $V_{G \rightarrow H}(a) = a^{p^\lambda} \cdot \prod_{k=2}^{p^\lambda} c_{1,k-1}^{\binom{p^\lambda}{k}} \cdot [H, H]$,

$$V_{G \rightarrow H}(b) = b^{p^\lambda} \cdot [H, H]$$

where $p^\lambda = [G : H]$, $\lambda = \min\{\mu + e, v\}$.

PROOF. Type 1: We have

$$G = \langle a \rangle \cdot H = \langle b \rangle \cdot H, \text{ and } [G : H] = p^\mu.$$

Hence by the definition of transfers, we obtain the desired results at once.

Type 2: We have $G = \langle a \rangle \cdot H$ and $[G : H] = p^\mu$. Hence we see $V_{G \rightarrow H}(a) = a^{p^\mu} \cdot [H, H]$. Since $a^s b \in H$, we have

$$V_{G \rightarrow H}(a^s b) = (a^s b)^{a^{p^\mu-1} + a^{p^\mu-2} + \dots + 1} \cdot [H, H].$$

In $G/[H, H]$, the coset of $a^s b$ commutes with each member of $[G, G]/[H, H]$. Therefore we may apply Lemma 2 to the right hand side of this equality with $x = a$ and $z = a^s b$, and obtain

$$V_{G \rightarrow H}(a^s b) = (a^s b)^{p^\mu} \cdot \prod_{k=2}^{p^\mu} (c_{k-1,1})^{-\binom{p^\mu}{k}} \cdot [H, H]$$

because $[a^s b, a] = [b, a] = c_{1,1}^{-1}$.

LEMMA 6. If H is of Type 2, we have

$$[H, H] = \langle c_{2,1}^{[s]} \cdot c_{1,2}, c_{i,1}^{[s]}, c_{1,j} \mid 3 \leq i \leq m, 3 \leq j \leq n \rangle;$$

moreover, for $k \geq 1$,

$$(1) \quad ba^{sk}b^{-1} \equiv a^{sk} \cdot (c_{1,1}^{[s]})^{-k} \cdot (c_{2,1}^{[s]})^{-s \binom{k+1}{2}} \pmod{[H, H]};$$

$$(2) \quad (a^s b)^k \equiv a^{sk} \cdot (c_{1,1}^{[s]})^{-\binom{k}{2}} \cdot (c_{2,1}^{[s]})^{-s \{ \binom{k}{3} + \binom{k+1}{3} \}} \cdot b^k \pmod{[H, H]}.$$

Here we read $\binom{k}{i} = 0$ if $k < i$.

PROOF. It is clear that $[H, H]$ is generated by $[c_{i,1}, a^s b]$ and $[c_{1,j}, a^s b]$, $1 \leq i \leq m$, $1 \leq j \leq n$. Since $C_{2,2} = 1$, we easily see $[c_{1,1}, a^s b] = c_{2,1}^{[s]} \cdot c_{1,2}$, and $[c_{i,1}, a^s b] = c_{i+1,1}^{[s]}$, $2 \leq i \leq m$, by Lemma 2, and also $[c_{1,j}, a^s b] = c_{1,j+1}$, $2 \leq j \leq n$. Next we show (1). Since $c_{1,j}$, $3 \leq j \leq n$, belongs to $[H, H]$, we have

$$bab^{-1} = ac_{1,1}^{-1}c_{1,2} \equiv ac_{1,1}^{-1}(c_{2,1}^{[s]})^{-1} \pmod{[H, H]}.$$

Therefore

$$ba^s b^{-1} \equiv a^s (c_{1,1}^{[s]})^{-1} (c_{2,1}^{[s]})^{-s} \pmod{[H, H]},$$

because $[c_{2,1}^{[s]}, a] = c_{3,1}^{[s]} \in [H, H]$. Then

$$\begin{aligned} ba^{sk} b^{-1} &\equiv a^{sk} (c_{1,1}^{[s]})^{-k} (c_{2,1}^{[s]})^{-s \binom{k}{2}} (c_{2,1}^{[s]})^{-sk} \\ &\equiv a^{sk} (c_{1,1}^{[s]})^{-k} (c_{2,1}^{[s]})^{-s \binom{k+1}{2}} \pmod{[H, H]}, \end{aligned}$$

because $[c_{1,1}^{[s]}, a^s] \equiv (c_{2,1}^{[s]})^s \pmod{[H, H]}$ by the last statement of Lemma 2. Finally (2) will easily be shown by induction on k to utilize (1) because we have

$$\begin{aligned} (a^s b)^{k+1} &= a^s \cdot b (a^s b)^k b^{-1} \cdot b, \\ [c_{1,1}^{[s]}, b^{-1}] &\equiv c_{1,2}^{-s} \equiv (c_{2,1}^{[s]})^s \pmod{[H, H]} \end{aligned}$$

and

$$\binom{k}{i} + \binom{k}{i+1} = \binom{k+1}{i+1}.$$

The detail is omitted.

Now we resume the calculation of the transfer for H of Type 2. By (2) of this lemma, we see

$$(a^s b)^{p^\mu} \equiv a^{sp^\mu} \cdot b^{p^\mu} \pmod{[H, H]},$$

because p^μ divides all of

$$\binom{p^\mu}{2}, \quad s \binom{p^\mu}{3} \quad \text{and} \quad s \binom{p^\mu + 1}{3} = s \left\{ \binom{p^\mu}{2} + \binom{p^\mu}{3} \right\}$$

in our case of $s = s'p^e, e \geq 1$. Therefore we have

$$V_{G \rightarrow H}(a^s b) = a^{sp^\mu} \cdot b^{p^\mu} \cdot \prod_{k=2}^{p^\mu} (c_{k-1,1})^{-\binom{p^\mu}{k}} \cdot [H, H].$$

Since $V_{G \rightarrow H}(a) = a^{p^\mu} \cdot [H, H]$ as we have already seen, we obtain what the proposition claims for H of Type 2.

Type 3: We have $G = \langle b \rangle \cdot H$ and $\langle b \rangle \cap H = \langle b^{p^\lambda} \rangle$ in this case.

LEMMA 7. If H is of Type 3, we have

$$[H, H] = \langle c_{2,1} \cdot c_{1,2}^{[s]}, c_{i,1}, c_{1,j}^{[s]} \mid 3 \leq i \leq m, 3 \leq j \leq n \rangle;$$

moreover, for $k \geq 1$,

- (1) $a^{-1}b^{sk}a \equiv b^{sk} \cdot (c_{1,1}^{(s)})^{-k} \cdot (c_{1,2}^{(s)})^{-s\binom{k}{2}} \pmod{[H, H]}$;
- (2) $(ab^s)^k \equiv a^k \cdot b^{sk} \cdot (c_{1,1}^{(s)})^{-\binom{k}{2}} \cdot (c_{1,2}^{(s)})^{-s\binom{k+1}{3}} \pmod{[H, H]}$.

PROOF. The proof may be carried out in a way similar to that of Lemma 6. It is almost trivial to determine the commutator. As for (1), we have $a^{-1}ba = bc_{1,1}^{-1}$ by definition, and hence $a^{-1}b^sa = b^s \cdot (c_{1,1}^{(s)})^{-1}$. Since $[c_{1,1}^{(s)}, b] = c_{1,2}^{(s)}$ and $[c_{1,2}^{(s)}, b] = c_{1,3}^{(s)} \in [H, H]$, we have $[c_{1,1}^{(s)}, b^s] \equiv (c_{1,2}^{(s)})^s \pmod{[H, H]}$ by the last statement of Lemma 2. Then we obtain (1) immediately again by Lemma 2. The second and the third factors at the right hand side of the congruence relation of (2) belong to H , and so does ab^s . Hence they commute with each other in $H/[H, H]$. The induction argument, therefore, easily proves (2) by making use of (1).

Now in the same way as we did first for Type 2, we obtain

$$V_{G \rightarrow H}(b) = b^{p^\lambda} \cdot [H, H]$$

and

$$\begin{aligned} V_{G \rightarrow H}(ab^s) &= (ab^s)^{b^{p^\lambda-1} + b^{p^\lambda-2} + \dots + 1} \cdot [H, H] \\ &= (ab^s)^{p^\lambda} \cdot \prod_{k=2}^{p^\lambda} (c_{1,k-1})^{\binom{p^\lambda}{k}} \cdot (c_{1,2}^{(s)})^{\binom{p^\lambda}{2}} \cdot [H, H] \\ &= (ab^s)^{p^\lambda} \cdot \prod_{k=2}^{p^\lambda} (c_{1,k-1})^{\binom{p^\lambda}{k}} \cdot [H, H], \end{aligned}$$

because

$$\begin{aligned} [ab^s, b] &= b^{-s}[a, b]b^s = c_{1,1} \cdot c_{1,2}^{(s)}, \\ [c_{1,1} \cdot c_{1,2}^{(s)}, b] &\equiv c_{1,2} \pmod{[H, H]}, \end{aligned}$$

and

$$p^\mu \mid \binom{p^\lambda}{2}.$$

Since p^μ divides

$$s \binom{p^\lambda + 1}{3} = s \left\{ \binom{p^\lambda}{2} + \binom{p^\lambda}{3} \right\},$$

we now have the desired results for H of Type 3 by (2) of Lemma 7. The proof is completed.

PROPOSITION 8. (1) *If H is of Type 2, then*

$$\prod_{k=2}^{p^\mu} (c_{k-1,1})^{-\binom{p^\mu}{k}} = \prod_{d=1}^{\mu} (c_{p^d-1,1})^{-\binom{p^\mu}{p^d}};$$

moreover, the p -th powers of these products are equal to 1.

(2) If H is of Type 3, then

$$\prod_{k=2}^{p^\lambda} (c_{1,k-1})^{\binom{p^\mu}{k}} = \prod_{k=p^{\lambda-\mu+1}}^{p^\lambda} (c_{1,k-1})^{\binom{p^\lambda}{k}}.$$

Furthermore if $\mu = \nu$, we have $\lambda = \mu$, and

$$\prod_{k=2}^{p^\mu} (c_{1,k-1})^{\binom{p^\mu}{k}} = \prod_{d=1}^{\mu} (c_{1,p^d-1})^{\binom{p^\mu}{p^d}};$$

the p -th powers of these products are equal to 1.

PROOF. (1): If k is not a power of p , then we have $t(k-1) = t(k)$ by definition; for $k = p^d$, $t(k-1) = t(k) - 1$. Therefore (1) follows from (1) of Lemma 5. As for (2), we see p^μ divide $\binom{p^\lambda}{k}$ if $k < p^{\lambda-\mu+1}$, again by (1) of Lemma 5; furthermore if $\mu = \nu$, we have the conclusion for the same reason as that for (1) above.

6. Necessary conditions for (A). First we consider subgroups of Type 1.

PROPOSITION 9. If H is of Type 1, then

$$[H, H] = \langle c_{2,1}^s \cdot c_{1,2}, c_{i,1}, c_{1,j} \mid 3 \leq i \leq m, 3 \leq j \leq n \rangle.$$

Hence we have

$$[\text{Ker } V_{G \rightarrow H} : [G, G]] = [G : H]$$

for every H of Type 1 if and only if we are in one of the following three cases:

- (6-i) $q_{2,1} \cdot r_{1,2} - q_{1,2} \cdot r_{2,1} \not\equiv 0 \pmod p$; hence $1 \leq m, n \leq 2$;
- (6-ii) $(q_{2,1}, r_{2,1}) \equiv 0$ and $(q_{1,2}, r_{1,2}) \not\equiv 0 \pmod p$; hence $1 \leq n \leq 2$;
- (6-iii) $(q_{2,1}, r_{2,1}) \not\equiv 0$ and $(q_{1,2}, r_{1,2}) \equiv 0 \pmod p$; hence $1 \leq m \leq 2$.

PROOF. If $(s, p) = 1$, then $\langle c^s \rangle = \langle c \rangle$ for each $c \in C_{1,1} = [G, G]$. Therefore it is easy to see by induction on $m-i, i = 1, 2, \dots, m$, that

$$\langle c_{k,1}^{[s]} \mid k = i, i+1, \dots, m \rangle = \langle c_{k,1} \mid k = i, i+1, \dots, m \rangle$$

for $1 \leq i \leq m$. Hence the first assertion of the proposition is clear because

$$c_{2,1}^{[s]} \equiv c_{2,1}^s \pmod{\langle c_{k,1} \mid k = 3, 4, \dots, m \rangle}.$$

Then by Proposition 7, we have

$$V_{G \rightarrow H}(a) = a^{p^\mu} \cdot [H, H] = c_{2,1}^{q_{2,1}} \cdot c_{1,2}^{q_{1,2}} \cdot [H, H] = c_{2,1}^{q_{2,1} - s \cdot q_{1,2}} \cdot [H, H],$$

and

$$V_{G \rightarrow H}(b^{p^\nu}) = b^{p^\nu} \cdot [H, H] = c_{2,1}^{r_{2,1}} \cdot c_{1,2}^{r_{1,2}} \cdot [H, H] = c_{2,1}^{r_{2,1} - s \cdot r_{1,2}} \cdot [H, H].$$

Since $\langle c_{2,1} \rangle \cap [H, H] = 1$ and $|\langle c_{2,1} \rangle| = p^\mu$, we see

$$[\text{Ker } V_{G \rightarrow H} : [G, G]] = [G : H]$$

for every H of Type 1 if and only if

$$(q_{2,1} - s \cdot q_{1,2}, r_{2,1} - s \cdot r_{1,2}) \not\equiv (0, 0) \pmod p$$

for every s , $(s, p) = 1$; evidently, this happens if and only if either the two vectors $(q_{2,1}, r_{2,1})$ and $(q_{1,2}, r_{1,2})$ are linearly independent over $\mathbf{Z}/p\mathbf{Z}$ or one of them is equal to $(0, 0)$ and the other is not. In the former case, neither one of the vectors is equal to $(0, 0)$; by Proposition 6, therefore, we have $1 \leq m, n \leq 2$. This shows (6-i) of the proposition. The rest is now also obvious.

PROPOSITION 10. *If the condition (A) is satisfied, then we have either $m = 2$ or $n = 2$.*

PROOF. Suppose that n is equal to 1, and take an H of Type 3. Then by Lemma 7, we have

$$[H, H] = \langle c_{i,1} \mid 2 \leq i \leq m \rangle;$$

therefore by Propositions 7 and 8 together with (4.3), we see that $V_{G \rightarrow H} : G \rightarrow H/[H, H]$ is trivial, i.e. $\text{Ker } V_{G \rightarrow H} = G$. Hence (A) is not satisfied. If $m = 1$, we similarly see that $V_{G \rightarrow H}$ is trivial for every H of Type 2. The proposition now immediately follows from the preceding one.

Now suppose that $n = 2$ and that H is of Type 3. In this case we have

$$[H, H] = \langle c_{2,1} \cdot c_{1,2}^s, c_{i,1} \mid 3 \leq i \leq m \rangle$$

by Lemma 7 because $c_{1,2}^{(s)} = c_{1,2}^s$. Since $p^d - 1 = 2$ if and only if $p = 3$ and $d = 1$, and since p^μ divides $\binom{p^\mu}{3}$ if $p \neq 3$, we obtain

$$V_{G \rightarrow H}(a) = c_{1,2}^{p^\lambda - \mu \cdot (q_{1,2} - s \cdot q_{2,1}) + \delta_{\lambda, \mu} \binom{p^\mu}{3}} \cdot [H, H]$$

and

$$V_{G \rightarrow H}(b^{p^v - \lambda}) = c_{1,2}^{r_{1,2} - s \cdot r_{2,1}} \cdot [H, H]$$

by Propositions 7 and 8; here $\delta_{\lambda, \mu}$ is Kronecker's δ . Note also that $\mu < \lambda$ if $\mu < v$. Since p divides s in this case, simple observations show us the following proposition.

PROPOSITION 11. *Suppose that $n = 2$. Then we have*

$$[\text{Ker } V_{G \rightarrow H} : [G, G]] = [G : H] = p^\lambda$$

for every H of Type 3 if and only if we are in one of the following three cases:

(6-iv) $\mu < v$ and $r_{1,2} \not\equiv 0 \pmod p$;

(6-v) either $\mu = v$ and $p > 3$, or, $\mu = v > 1$ and $p = 3$, and $(q_{1,2}, r_{1,2}) \not\equiv (0, 0) \pmod p$;

(6-vi) $\mu = v = 1, p = 3,$ and $(q_{1,2}, r_{1,2}) \not\equiv (-1, 0) \pmod p.$

By a parallel argument, we obtain

PROPOSITION 12. *Suppose that $m = 2.$ Then we have*

$$[\text{Ker } V_{G \rightarrow H} : [G, G]] = [G : H] = p^\mu$$

for every H of Type 2 if and only if we are in one of the following three cases:

(6-vii) $\mu < v$ and $(q_{2,1}, r_{2,1}) \not\equiv (0, 0) \pmod p;$

(6-viii) either $\mu = v$ and $p > 3,$ or, $\mu = v > 1$ and $p = 3,$ and $(q_{2,1}, r_{2,1}) \not\equiv (0, 0) \pmod p;$

(6-ix) $\mu = v = 1, p = 3,$ and $(q_{2,1}, r_{2,1}) \not\equiv (0, 1) \pmod p.$

The proof is omitted.

7. Groups with the conditions (A) and (B).

7.1. Simply summing up the results in the preceding section, we have a necessary and sufficient condition for (A) when $m = n = 2.$

THEOREM 1. *Suppose $m = n = 2.$ Then the condition (A) is satisfied if and only if we are in one of the following five cases:*

(I) $\mu < v$ and $r_{1,2} \cdot (q_{2,1} \cdot r_{1,2} - q_{1,2} \cdot r_{2,1}) \not\equiv 0 \pmod p;$

(II) either $\mu = v$ and $p > 3,$ or, $\mu = v > 1$ and $p = 3,$ and $q_{2,1} \cdot r_{1,2} - q_{1,2} \cdot r_{2,1} \not\equiv 0 \pmod p;$

(III) $\mu = v = 1, p = 3,$ and either one of (III-1)–(III-3):

(III-1) $q_{2,1} \cdot r_{1,2} - q_{1,2} \cdot r_{2,1} \not\equiv 0, (q_{2,1}, r_{2,1}) \not\equiv (0, 1)$ and $(q_{1,2}, r_{1,2}) \not\equiv (-1, 0) \pmod p;$

(III-2) $(q_{2,1}, r_{2,1}) \equiv (0, 0) \pmod p$ and $(q_{1,2}, r_{1,2}) \not\equiv (0, 0)$ nor $(-1, 0) \pmod p;$

(III-3) $(q_{1,2}, r_{1,2}) \equiv (0, 0) \pmod p$ and $(q_{2,1}, r_{2,1}) \not\equiv (0, 0)$ nor $(0, 1) \pmod p.$

Furthermore, the condition (B) is also satisfied in every one of these cases.

PROOF. All except the last assertion of the theorem easily follow from Propositions 9–12; we omit the detail. To see the last assertion, put

$$a^\varphi = a^{-1}, \quad b^\varphi = b^{-1}, \quad c_{1,1}^\varphi = c_{1,1} \cdot c_{2,1}^{-1} \cdot c_{1,2}^{-1}, \quad c_{2,1}^\varphi = c_{2,1}^{-1}, \quad c_{1,2}^\varphi = c_{1,2}^{-1};$$

it is easy to see that these new generators of the group under consideration satisfy all and the same relations as the original ones $a, b, c_{1,1}, c_{2,1}$ and $c_{1,2}$ do. Hence we have a desired automorphism φ by assigning x^φ to each member x of the last system of generators. The proof is completed.

REMARK. In (III) of the theorem, we see anti-symmetry which is caused by the relation, $[b, a] = [a, b]^{-1}.$

PROPOSITION 13. *Let the assumptions be as in Theorem 1, and suppose that one of the conditions (I)–(III) is satisfied. Then for any subgroup N which contains $[G, G],$ the transfer homomorphism $V_{G \rightarrow N} : G \rightarrow N/[N, N]$ is not trivial unless N coincides with $[G, G].$*

PROOF. First let us consider the case (I). For a subgroup of the form

$$N = \langle (ab^s)^{p^{\mu-1}} \rangle \cdot [G, G], \quad s = s'p^{v-\mu}, \quad (s', p) = 1,$$

it is easy to see $[N, N] = \langle c_{2,1}^{p^{\mu-1}} \rangle$ because $p^\mu \leq p^{v-1}$. Let us take $H = \langle ab^s \rangle \cdot [G, G]$; then we have $\lambda = v$ for this H , and hence

$$V_{G \rightarrow H}(b) = c_{1,2}^{r_{1,2} - s'r_{2,1}} \cdot [H, H]$$

as we saw just above Proposition 11. Since $c_{1,2}$ belongs to the center of G , we have

$$V_{G \rightarrow N}(b) = \bar{V}_{H \rightarrow N}(V_{G \rightarrow H}(b)) = (V_{G \rightarrow H}(b))^{p^{\mu-1}} \cdot [N, N] = c_{1,2}^{p^{\mu-1} \cdot r_{1,2}} \cdot [N, N].$$

Therefore $V_{G \rightarrow H}$ is not trivial because $r_{1,2} \not\equiv 0 \pmod p$ by assumption. For $N = \langle a^{p^{\mu-1}} \rangle \cdot [G, G]$, we can similarly see $V_{G \rightarrow N}(b) \neq 1$ by using

$$H = \langle ab^s \rangle \cdot [G, G], \quad s = s'p^{v-\mu+1}, \quad (s', p) = 1.$$

For $N = \langle b^{p^{v-1}} \rangle \cdot [G, G]$, we have $[N, N] = \langle c_{1,2}^{p^{v-1}} \rangle = 1$. Take $H = \langle b \rangle \cdot [G, G]$; then we see

$$V_{G \rightarrow H}(b) = b^{p^\mu} \cdot (c_{2,1})^{-\binom{p^\mu}{3}} \cdot [H, H]$$

by Proposition 7. Hence by the same reason as above, we have

$$V_{G \rightarrow N}(b) = c_{2,1}^{p^{\mu-1} \cdot r_{2,1}} \cdot c_{1,2}^{p^{\mu-1} \cdot r_{1,2}} \cdot [N, N].$$

Since $r_{1,2} \not\equiv 0 \pmod p$, we see $V_{G \rightarrow N}(b) \neq 1$.

Next we consider the cases (II) and (III). If $\mu = v = 1$, then our proposition is obvious because G/N is cyclic unless $N = [G, G]$. Suppose $\mu = v > 1$; we are in the case of (II). For

$$N = \langle (ab^s)^{p^{\mu-1}} \rangle \cdot [G, G], \quad (s, p) = 1,$$

we have $[N, N] = \langle c_{2,1}^{p^{\mu-1}} \cdot c_{1,2}^{s \cdot p^{\mu-1}} \rangle$,

$$\begin{aligned} V_{G \rightarrow N}(a) &= V_{H \rightarrow N}(V_{G \rightarrow H}(a)) = (a^{p^\mu})^{p^{\mu-1}} \cdot [N, N] \\ &= c_{2,1}^{p^{\mu-1} \cdot q_{2,1}} \cdot c_{1,2}^{p^{\mu-1} \cdot q_{1,2}} \cdot [N, N] = c_{1,2}^{p^{\mu-1} \cdot (-s \cdot q_{2,1} + q_{1,2})} \cdot [N, N] \end{aligned}$$

and

$$\begin{aligned} V_{G \rightarrow N}(b) &= V_{H \rightarrow N}(V_{G \rightarrow H}(b)) = (b^{p^\mu})^{p^{\mu-1}} \cdot [N, N] \\ &= c_{2,1}^{p^{\mu-1} \cdot r_{2,1}} \cdot c_{1,2}^{p^{\mu-1} \cdot r_{1,2}} \cdot [N, N] = c_{1,2}^{p^{\mu-1} \cdot (-s \cdot r_{2,1} + r_{1,2})} \cdot [N, N] \end{aligned}$$

by using $H = \langle ab^s \rangle \cdot [G, G]$ of Type 1. Since we have

$$q_{2,1} \cdot r_{1,2} - q_{1,2} \cdot r_{2,1} \not\equiv 0 \pmod p,$$

we see that

$$(-s \cdot q_{2,1} + q_{1,2}, -s \cdot r_{2,1} + r_{1,2}) \not\equiv (0, 0) \pmod{p}.$$

This shows that $V_{G \rightarrow N}$ is not trivial. When N is equal to either $\langle a^{p^{\mu-1}} \rangle \cdot [G, G]$ or $\langle b^{p^{\mu-1}} \rangle \cdot [G, G]$, we easily check it in a similar way, and complete the proof.

7.2. The case of $\mu = 1$: In this paragraph, we assume $\mu = 1$.

LEMMA 8. For $p^e, e \geq 1$, we have

$$\langle c_{k,1}^{[p^e]} \mid k = 3, 4, \dots \rangle = \langle c_{k,1} \mid k = p^e + 2, p^e + 3, \dots \rangle$$

and

$$\langle c_{1,k}^{[p^e]} \mid k = 3, 4, \dots \rangle = \langle c_{1,k} \mid k = p^e + 2, p^e + 3, \dots \rangle.$$

PROOF. Since p divides $\binom{p^e}{k}$ for each $k, 1 \leq k < p^e$, we have $c_{k,1}^{[p^e]} = c_{k+p^e-1,1}$ by definition. Hence we see the first equality. The second is also clear by definition.

First suppose $m > 2$ and $n = 2$. Since we have Propositions 9 and 11, it is enough to study $V_{G \rightarrow H}$ for H of Type 2. There exists only one such subgroup because $\mu = 1$, namely, $H = \langle b \rangle \cdot [G, G]$; we have $[H, H] = \langle c_{1,2} \rangle$,

$$V_{G \rightarrow H}(a) = a^p \cdot [H, H] = \prod_{i=2}^m c_{i,1}^{q_{i,1}} \cdot [H, H],$$

and

$$V_{G \rightarrow H}(b^{p^{v-1}}) = b^{p^v} \cdot \left(\prod_{k=2}^p (c_{k-1,1})^{-\binom{p}{k}} \right)^{p^{v-1}} \cdot [H, H] = \prod_{i=2}^m c_{i,1}^{r_{i,1}} \cdot c_{p-1,1}^{-p^{v-1}} \cdot [H, H]$$

by Lemma 6 and Proposition 7. Here we should assume

$$(7.1) \quad (q_{2,1}, r_{2,1}) \equiv (0, 0) \pmod{p},$$

because of Proposition 9, (6-ii). Actually we must have

$$(7.2) \quad q_{i,1} = r_{i,1} = 0, \quad 1 \leq i \leq m-1,$$

and (7.1) is included in this because of our assumption, $m > 2$. We see (7.2) from the relations

$$\prod_{i=2}^m c_{i+1,1}^{q_{i,1}} = \prod_{i=2}^m c_{i+1,1}^{r_{i,1}} = 1$$

of (4.11) by the same argument as in the proof of Proposition 6. Note also that we must have $m \leq p-1$ automatically from the assumption (4.9) on the order of $c_{i,j}$. Therefore we obtain

$$V_{G \rightarrow H}(a) = c_{m,1}^{q_{m,1}} \cdot [H, H],$$

and

$$V_{G \rightarrow H}(b^{p^v-1}) = c_{m,1}^{r_{m,1}} \cdot c_{p-1,1}^{-p^{v-1}} \cdot [H, H];$$

here $c_{p-1,1} = 1$ if $m < p-1$; note that $3 \leq m \leq p-1$ only if $p > 3$. It is now clear that we have (IV) and (VI) of the following theorem.

THEOREM 2. *Suppose $\mu = 1$ and either $m > 2$ or $n > 2$. Then the condition (A) is satisfied if and only if we are in one of the following seven cases:*

(IV) $\mu = v = 1, p \geq 5, 3 \leq m \leq p-1, n = 2$ and

$$q_{i,1} = r_{i,1} = 0, \quad 1 \leq i \leq m-1,$$

$$(q_{m,1}, r_{m,1}) \not\equiv (0, \delta_{m,p-1}) \pmod{p}, \quad (q_{1,2}, r_{1,2}) \not\equiv (0, 0) \pmod{p};$$

(V) $\mu = v = 1, p \geq 5, m = 2, 3 \leq n \leq p-1$ and

$$q_{1,j} = r_{1,j} = 0, \quad 1 \leq j \leq n-1,$$

$$(q_{2,1}, r_{2,1}) \not\equiv (0, 0) \pmod{p}, \quad (q_{1,n}, r_{1,n}) \not\equiv (-\delta_{n,p-1}, 0) \pmod{p};$$

(VI) $\mu = 1 < v, p \geq 5, 3 \leq m \leq p-1, n = 2$ and

$$q_{i,1} = r_{i,1} = 0, \quad 1 \leq i \leq m-1,$$

$$(q_{m,1}, r_{m,1}) \not\equiv (0, 0) \pmod{p}, \quad r_{1,2} \not\equiv 0 \pmod{p};$$

(VII) $\mu = 1 < v, p \geq 3, m = 2, 3 \leq n \leq p$ and

$$q_{1,j} = r_{1,j} = 0, \quad 1 \leq j \leq n-1,$$

$$(q_{2,1}, r_{2,1}) \not\equiv (0, 0) \pmod{p}, \quad r_{1,n} \not\equiv 0 \pmod{p};$$

(VIII) $\mu = 1 < v, p \geq 3, m = 2, n = p+1$ and

$$q_{1,j} = r_{1,j} = 0, \quad 1 \leq j \leq n-1,$$

$$r_{2,1} \equiv 0 \pmod{p}, \quad q_{2,1} \cdot r_{1,n} \not\equiv 0 \pmod{p};$$

(IX) $\mu = 1 < v, p \geq 3, m = 2, p+1 < n < p^v-1, n \neq p^e+1$ for $1 < e < v$ if $v \geq 3$, and

$$q_{1,j} = r_{1,j} = 0, \quad 1 \leq j \leq n-1,$$

$$r_{2,1} \cdot r_{1,n} \not\equiv 0 \pmod{p};$$

(X) $\mu = 1 < v, p \geq 3, m = 2, n = p^v-1$ and

$$q_{1,j} = r_{1,j} = 0, \quad 1 \leq j \leq n-1,$$

$$r_{2,1} \not\equiv 0 \pmod{p}.$$

Furthermore, in every one of these cases, the condition (B) is also satisfied if and only if both of m and n are even integers.

PROOF. The two cases (IV) and (VI) have been shown. Suppose now $m=2$ and $n>2$. Then for the reason which is parallel to that for (7.2), we have

$$(7.3) \quad q_{1,j} = r_{1,j} = 0, \quad 1 \leq j \leq n-1.$$

Since we have Propositions 9 and 12, it is sufficient to study $V_{G \rightarrow H}$ for H of Type 3, i.e.

$$H = \langle ab^s \rangle \cdot [G, G], \quad s = s'p^e, \quad (s', p) = 1, \quad 1 \leq e \leq v.$$

Take an integer t such that $t \cdot s' \equiv 1 \pmod p$. Then we have

$$H = \langle a^t b^{p^e} \rangle \cdot [G, G]$$

and

$$[H, H] = \langle c_{2,1}^t \cdot c_{1,2}^{\{p^e\}}, c_{1,j}^{\{p^e\}} \mid 3 \leq j \leq n \rangle.$$

Then by Lemma 8 and its proof, we easily see

$$[H, H] = \langle c_{2,1}^t \cdot c_{1,p^e+1}, c_{1,j} \mid j = p^e + 2, p^e + 3, \dots \rangle.$$

Hence by Proposition 7 and (7.3), we obtain

$$\begin{aligned} V_{G \rightarrow H}(a) &= a^{p^\lambda} \cdot \prod_{k=2}^{p^\lambda} (c_{1,k-1})^{\binom{p^\lambda}{k}} \cdot [H, H] = c_{2,1}^{q_{2,1} \cdot p^{\lambda-1}} \cdot c_{1,n}^{q_{1,n} \cdot p^{\lambda-1}} \cdot c_{1,p^\lambda-1} \cdot [H, H] \\ &= c_{1,p^e+1}^{-s' \cdot q_{2,1} \cdot p^{\lambda-1}} \cdot c_{1,n}^{q_{1,n} \cdot p^{\lambda-1}} \cdot c_{1,p^\lambda-1} \cdot [H, H], \end{aligned}$$

$$V_{G \rightarrow H}(b^{p^{v-\lambda}}) = b^{p^v} \cdot [H, H] = c_{2,1}^{r_{2,1}} \cdot c_{1,n}^{r_{1,n}} \cdot [H, H] = c_{1,p^e+1}^{-s' \cdot r_{2,1}} \cdot c_{1,n}^{r_{1,n}} \cdot [H, H],$$

where $p^\lambda = [G : H]$, $\lambda = \min\{1 + e, v\}$; note that (4.9) gives $n \leq p^v - 1$. Since $\lambda = 1$ if and only if $v = \mu = 1$, we always have $c_{1,p^e+1}^{-s' \cdot q_{2,1} \cdot p^{\lambda-1}} = 1$. Therefore

$$V_{G \rightarrow H}(a) = c_{1,n}^{q_{1,n} \cdot p^{\lambda-1}} \cdot c_{1,p^\lambda-1} \cdot [H, H],$$

$$V_{G \rightarrow H}(b^{p^{v-\lambda}}) = c_{1,p^e+1}^{-s' \cdot r_{2,1}} \cdot c_{1,n}^{r_{1,n}} \cdot [H, H].$$

Suppose $v = \mu = 1$. Then $c_{1,p^e+1} = 1$. Hence we easily obtain (V) by Propositions 9 and 12. Next suppose $v > \mu = 1$. Then we always have $\lambda \geq 2$ and hence $c_{1,n}^{q_{1,n} \cdot p^{\lambda-1}} = 1$. For $e = v$ we have $\lambda = v$ and $c_{1,p^e+1} = 1$; therefore $V_{G \rightarrow H}$ is not trivial if and only if either $n = p^v - 1$ or $r_{1,n} \not\equiv 0 \pmod p$. For $e \leq v - 1$, we have $\lambda = e + 1$ and $p^e + 1 < p^\lambda - 1$; hence $c_{1,p^\lambda-1}$ belongs to $[H, H]$ by Lemma 8, and $V_{G \rightarrow H}(a) = 1$ in this case. If $n = p^v - 1$, therefore, $c_{1,n}$ also belongs to $[H, H]$; hence $V_{G \rightarrow H}$ is not trivial if and only if $r_{2,1} \not\equiv 0 \pmod p$; this gives (X). Suppose $n < p^v - 1$ and $r_{1,n} \not\equiv 0 \pmod p$. Then it is easy to see that we have $V_{G \rightarrow H}(b^{p^{v-\lambda}}) \neq 1$ for every s' and for every λ with $e \leq v - 1$ if and only if either one of the following three conditions holds: (1) $3 \leq n < p + 1$; (2) $n = p + 1$ and $r_{2,1} \equiv 0 \pmod p$; (3) $n > p + 1$, $n \neq p^e + 1$, $2 \leq e \leq v - 1$, and $r_{2,1} \not\equiv 0 \pmod p$. These correspond to (VII), (VIII) and (IX), respectively.

Finally let us study the existence of a claimed automorphism. We have two relations

$$a^{p^\mu} = c_{m,1}^{q_{m,1}} \cdot c_{1,n}^{q_{1,n}} \quad \text{and} \quad b^{p^v} = c_{m,1}^{r_{m,1}} \cdot c_{1,n}^{r_{1,n}}.$$

By Lemma 3, therefore, it is easy to see that the condition for the existence stated in the theorem is necessary; note that p is odd and that the condition may be automatically satisfied like in the cases (VIII) and (X). It may be seen by a straightforward way that a good automorphism φ is well defined by

$$\begin{aligned} a^\varphi &= a^{-1}, & b^\varphi &= b^{-1}, \\ c_{1,1}^\varphi &= c_{1,1} \cdot \prod_{k=2}^m c_{k,1}^{(-1)^{k+1}} \cdot \prod_{k=2}^n c_{1,k}^{(-1)^{k+1}}, \\ c_{i,1}^\varphi &= \prod_{k=i}^m c_{k,1}^{(-1)^{k+1}}, & 2 \leq i < m, \\ c_{1,j}^\varphi &= \prod_{k=j}^n c_{1,k}^{(-1)^{k+1}}, & 2 \leq j < n, \end{aligned}$$

if the condition is satisfied. The detail is omitted.

REMARK. The cases (IV) and (V) obviously give pairs of isomorphic groups.

7.3. The case of $\mu = \nu = 2$: In this paragraph, we assume $\mu = \nu = 2$. Because of the anti-symmetry, we only consider the case, $m \geq 3$ and $n = 2$. First of all, we have $m \leq p^2 - 1$ by our assumption (4.9) on the orders of $c_{i,j}$.

THEOREM 3. Suppose $\mu = \nu = 2, m > 2$ and $n = 2$. Then the condition (A) is satisfied if and only if we are in one of the following three cases:

(XI) $\mu = \nu = 2, p \geq 5, 3 \leq m \leq p - 1, n = 2$ and

$$\begin{aligned} q_{i,1} &= r_{i,1} = 0, & 1 \leq i \leq m - 1, \\ q_{m,1} \cdot r_{1,2} - q_{1,2} \cdot r_{m,1} &\not\equiv 0 \pmod{p}; \end{aligned}$$

(XII) $\mu = \nu = 2, p \leq m \leq 2(p - 1), n = 2$ and

$$\begin{aligned} q_{i,1} &= r_{i,1} = 0, & 1 \leq i \leq m - 1, \\ q_{m,1} \cdot (r_{1,2} \pm \delta_{p,3}) - q_{1,2} \cdot (r_{m,1} + \delta_{m,2(p-1)}) &\not\equiv 0 \pmod{p}, \\ q_{m,1} &\not\equiv 0 \pmod{p}, & (q_{1,2}, r_{1,2}) &\not\equiv (0, 0) \pmod{p}; \end{aligned}$$

(XIII) $\mu = \nu = 2, 2p - 1 \leq m \leq p^2 - 1, n = 2$ and

$$\begin{aligned} q_{i,1} &= r_{i,1} = 0, & 1 \leq i \leq m - 1, \\ q_{m,1} \cdot q_{1,2} &\not\equiv 0 \pmod{p}. \end{aligned}$$

Furthermore, in every one of these cases, the condition (B) is also satisfied if and only if m is an even integer.

PROOF. Because of Propositions 9 and 11, we need only to study the subgroups

$$H = \langle a^s b \rangle \cdot [G, G], \quad s = s'p, \quad (s', p) = 1,$$

and

$$H = \langle b \rangle \cdot [G, G]$$

of Type 2. For the former H , take an integer t such that $t \cdot s' \equiv 1 \pmod{p}$. Then we have

$$H = \langle a^p b^t \rangle \cdot [G, G]$$

and

$$[H, H] = \langle c_{2,1}^{[p]} \cdot c_{1,2}^t, c_{i,1}^{[p]} \mid 3 \leq i \leq m \rangle.$$

For the latter, $[H, H] = \langle c_{1,2} \rangle$.

LEMMA 9. (1) *We also have*

$$(7.4) \quad q_{i,1} = r_{i,1} = 0, \quad 1 \leq i \leq m-1,$$

in the present case;

(2) *If $3 \leq m \leq p-1$, then we have*

$$\langle c_{i,1}^{[p]} \mid 3 \leq i \leq m \rangle = \langle c_{i,1}^p \mid 3 \leq i \leq m \rangle;$$

(3) *If $p \leq m \leq p^2-1$, then $c_{i,1}, i \geq 2p-1$, belongs to*

$$\langle c_{i,1}^{[p]} \mid 3 \leq i \leq m \rangle;$$

for $p > 3$, moreover, we have

$$c_{p-1,1}^p \equiv c_{2(p-1),1}^{-1} \pmod{\langle c_{i,1}^{[p]} \mid 3 \leq i \leq m \rangle}.$$

PROOF. If $3 \leq m \leq p-1$, the orders of $c_{i,1}, 1 \leq i \leq m$, are same, and equal to p^2 . Therefore the argument for (7.2) given in the preceding paragraph shows our (7.4). If $m > p-1$, it is clear that we have at least

$$q_{i,1} = r_{i,1} \equiv 0 \pmod{p}, \quad 1 \leq i \leq m-1,$$

in place of (7.4); hence by (4.11) we also have

$$\prod_{i=2}^{p-2} c_{i+1,1}^{q_{i,1}} = \prod_{i=2}^{p-2} c_{i+1,1}^{r_{i,1}} = 1;$$

then by forming commutators of these products with a successively, we obtain $c_{p-1,1}^{q_{2,1}} = 1$; since the order of $c_{p-1,1}$ is p^2 by assumption, we must have $q_{2,1} \equiv 0 \pmod{p^2}$ and, equivalently in this case, $q_{2,1} = 0$; repeating the process, we finally attain (7.4). The proof of the assertion (2) will be easy enough to be omitted. If $p \leq i \leq m$, we have $c_{i,1}^p = 1$ and hence

$$c_{p-1,1}^{[p]} = c_{p-1,1}^p \cdot c_{2(p-1),1}$$

and

$$c_{p,1}^{[p]} = c_{2p-1,1}, \quad c_{p+1,1}^{[p]} = c_{2p,1}, \dots$$

This shows (3).

q.e.d.

Let us resume the proof of Theorem 3. By Proposition 7, we have

$$V_{G \rightarrow H}(a) \equiv a^{p^2} \equiv c_{m,1}^{q_{m,1}} \cdot c_{1,2}^{q_{1,2}} \pmod{[H, H]},$$

and

$$\begin{aligned} V_{G \rightarrow H}(b) &\equiv b^{p^2} \cdot \prod_{k=2}^{p^2} (c_{k-1,1})^{-\binom{p^2}{k}} \\ &\equiv c_{m,1}^{r_{m,1}} \cdot c_{1,2}^{r_{1,2}} \cdot (c_{p-1,1})^{-\binom{p^2}{p}} \cdot c_{p^2-1,1}^{-1} \pmod{[H, H]}. \end{aligned}$$

First we consider the simpler case, $H = \langle b \rangle \cdot [G, G]$; $[H, H] = \langle c_{1,2} \rangle$. If $m \leq p-1$, then $\text{Im } V_{G \rightarrow H}$ is a subgroup of a cyclic group $\langle c_{m,1} \rangle \cdot [H, H]/[H, H]$ of order p^2 ; hence we have

$$[\text{Ker } V_{G \rightarrow H} : [G, G]] = [G : H],$$

if and only if

$$(q_{m,1}, r_{m,1}) \not\equiv (0, 0) \pmod{p},$$

because $p \mid \binom{p^2}{p}$ by Lemma 5, (1). If $p-1 < m \leq p^2-1$, then $\text{Im } V_{G \rightarrow H}$ is contained in a direct product of two cyclic groups of order p ; since $V_{G \rightarrow H}(b)$ is a non-trivial element which does not lie in $\langle c_{m,1} \rangle \cdot [H, H]$, we see that

$$[\text{Ker } V_{G \rightarrow H} : [G, G]] = [G : H]$$

if and only if $q_{m,1} \not\equiv 0 \pmod{p}$.

Next we consider the case of $H = \langle a^p b^t \rangle \cdot [G, G]$ with

$$[H, H] = \langle c_{2,1}^{[p]}, c_{1,2}^t, c_{i,1}^{[p]} \mid 3 \leq i \leq m \rangle.$$

Since the orders of $c_{i,1}$, $i \geq p$, are at most p , $c_{2,1}^{[p]}$ is also of order p ; in particular, we have

$$\langle c_{2,1}^{[p]} \rangle \cap \langle c_{i,1}^{[p]} \mid 3 \leq i \leq m \rangle = 1;$$

hence the order of $c_{1,2} \cdot [H, H]$ in $H/[H, H]$ is equal to p . If $3 \leq m \leq p-1$, then we see by (2) of Lemma 9 that the order of $c_{m,1} \cdot [H, H]$ in $H/[H, H]$ is equal to p ; since $p \mid \binom{p^2}{p}$ and $p > 3$, we have

$$V_{G \rightarrow H}(a) = c_{m,1}^{q_{m,1}} \cdot c_{1,2}^{q_{1,2}} \cdot [H, H],$$

$$V_{G \rightarrow H}(b) = c_{m,1}^{r_{m,1}} \cdot c_{1,2}^{r_{1,2}} \cdot [H, H]$$

in this case; hence

$$[\text{Ker } V_{G \rightarrow H} : [G, G]] = [G : H],$$

if and only if

$$q_{m,1} \cdot r_{1,2} - q_{1,2} \cdot r_{m,1} \not\equiv 0 \pmod{p}.$$

If $p - 1 < m \leq p^2 - 1$, we see by (3) of Lemma 9 that $c_{p^2-1,1}$ is contained in $[H, H]$. Suppose $p > 3$. Then also by (3) of Lemma 9, we see

$$\begin{aligned} V_{G \rightarrow H}(a) &= c_{m,1}^{q_{m,1}} \cdot c_{1,2}^{q_{1,2}} \cdot [H, H], \\ V_{G \rightarrow H}(b) &= c_{m,1}^{r_{m,1} + \delta_{m,2(p-1)}} \cdot c_{1,2}^{r_{1,2}} \cdot [H, H], \end{aligned}$$

if $m \leq 2(p - 1)$ because $\binom{p^2}{p} \cdot p^{-1} \equiv 1 \pmod{p}$, and

$$\begin{aligned} V_{G \rightarrow H}(a) &= c_{1,2}^{q_{1,2}} \cdot [H, H], \\ V_{G \rightarrow H}(b) &= c_{1,2}^{r_{1,2}} \cdot c_{2(p-1),1} \cdot [H, H], \end{aligned}$$

if $m > 2(p - 1)$; therefore

$$[\text{Ker } V_{G \rightarrow H} : [G, G]] = [G : H],$$

if and only if either

- (i) $p - 1 < m \leq 2(p - 1)$ and $q_{m,1} \cdot r_{1,2} - q_{1,2} \cdot (r_{m,1} + \delta_{m,2(p-1)}) \not\equiv 0 \pmod{p}$, or
- (ii) $2(p - 1) < m \leq p^2 - 1$ and $q_{1,2} \not\equiv 0 \pmod{p}$.

Finally suppose $p - 1 < m \leq p^2 - 1$ and $p = 3$. If $m \leq 2(p - 1) = 4$, we have

$$\begin{aligned} V_{G \rightarrow H}(a) &= c_{m,1}^{q_{m,1}} \cdot c_{1,2}^{q_{1,2}} \cdot [H, H], \\ V_{G \rightarrow H}(b) &= c_{m,1}^{r_{m,1}} \cdot c_{1,2}^{r_{1,2}} \cdot c_{2,1}^{-p} \cdot [H, H] = c_{m,1}^{r_{m,1}} \cdot c_{1,2}^{r_{1,2} + t} \cdot c_{4,1} \cdot [H, H], \end{aligned}$$

because $c_{2,1}^{[p]} = c_{2,1}^p \cdot c_{4,1}$. If $4 < m \leq p^2 - 1 = 8$, we have

$$\begin{aligned} V_{G \rightarrow H}(a) &= c_{1,2}^{q_{1,2}} \cdot [H, H], \\ V_{G \rightarrow H}(b) &= c_{1,2}^{r_{1,2}} \cdot c_{2,1}^{-p} \cdot [H, H]. \end{aligned}$$

Therefore

$$[\text{Ker } V_{G \rightarrow H} : [G, G]] = [G : H] \quad \text{for every } H,$$

if and only if $V_{G \rightarrow H}$ is surjective for every H ; this is the case if and only if either

- (i) $3 \leq m \leq 4$ and $q_{m,1} \cdot (r_{1,2} \pm 1) - q_{1,2} \cdot (r_{m,1} + \delta_{m,4}) \not\equiv 0 \pmod{p}$, or
- (ii) $4 < m \leq p^2 - 1 = 8$ and $q_{1,2} \not\equiv 0 \pmod{p}$.

One may now easily obtain the three cases (XI)–(XIII) of the theorem by summing up our results here together with Propositions 9 and 11.

As for the last assertion of the theorem on the condition (B), one can demonstrate

it in the same way as we did in the final portion of the proof of Theorem 2. The proof is completed.

REMARK. It is an easy exercise left to the reader to show the existence of all of the groups on the lists of Theorems 1–3.

8. An application to the capitulation problem. Let F be an algebraic number field of finite degree. As is well known, every ideal of F becomes a principal ideal in the Hilbert class field of F ; in other words, every ideal of F is represented by an actual number of the class field. In his short notes [Iw] of lively interest, Iwasawa gave infinitely many examples of totally real F such that there exists a proper subfield of the Hilbert class field of F in which all ideals of F already become principal. It has not yet been shown, however, that such an imaginary quadratic number field exists. It is natural to consider the “ p -version” of the problem for each prime p . In the case of $p=2$, Iwasawa’s method in [Iw] for real quadratic fields may also allow us to obtain the desired examples of imaginary quadratic fields. As for odd p , however, it seems necessary to find a new approach not only for imaginary ones but also even for real ones as far as quadratic number fields are concerned.

Now let F be an imaginary quadratic number field, \tilde{F} the Hilbert p -class field of F , and $\tilde{\tilde{F}}$ the second p -class field of F , as in Section 2; put $G = \text{Gal}(\tilde{\tilde{F}}/F)$. Then F is an example of this sort if

- (C) there exists a subgroup N of G which properly contains the commutator group $[G, G]$ of G and for which the transfer homomorphism $V_{G \rightarrow N}: G \rightarrow N/[N, N]$ is trivial;

(cf., e.g., [Mi2]). Hence we can group-theoretically examine whether F is a desired example or not once we are given $G = \text{Gal}(\tilde{\tilde{F}}/F)$. Here let us single out from our candidates for $\text{Gal}(\tilde{\tilde{F}}/F)$ given in Theorems 1 and 2 a small group which satisfies this condition (C).

We have already seen by Proposition 13 that the condition holds for none of the groups of Type (I)–(III) of Theorem 1. When $\mu = \nu = 1$, G/N is always cyclic if N properly contains $[G, G]$; hence (C) does not hold because of the condition (A). Therefore groups of Type (IV) or (V) of Theorem 2 are not what we want. Let us restrict ourselves to the case $\mu = 1$. Then $N = \langle b^{p^{\nu-1}} \rangle \cdot [G, G]$ is the only minimal subgroup for which G/N is not cyclic.

PROPOSITION 14. *Let G be one of p -groups on the lists of Theorems 1 and 2. Then G satisfies the condition (C) if and only if G is of Type (VIII) with $\nu = 2$. If this is the case, G satisfies both of the conditions (A) and (B); G is of order p^{p+5} , and $G/[G, G]$ is of type (p, p^2) .*

PROOF. Take $H = \langle b \rangle \cdot [G, G]$. Since H is of Type 2 in the sense of Section 5, we easily see

$$V_{G \rightarrow H}(a) = a^p \cdot [H, H],$$

$$V_{G \rightarrow H}(b) = b^p \cdot c_{p-1,1}^{-1} \cdot [H, H], \quad \text{or} \quad = b^p \cdot (c_{2,1})^{-\binom{p}{3}} \cdot [H, H],$$

respectively, in the cases of (VI) and (VII)–(X), by Proposition 7. (Note that $c_{p-1,1} = 1$ if $m < p-1$.) Since a^p and either $c_{p-1,1}$ or $c_{2,1}$ lie in the center of the corresponding group, we have

$$V_{G \rightarrow N}(a) = \bar{V}_{H \rightarrow N}(V_{G \rightarrow H}(a)) = V_{G \rightarrow H}(a)^{p^v-1} \cdot [N, N] = 1$$

and similarly

$$V_{G \rightarrow N}(b) = b^{p^v} \cdot [N, N] = c_{m,1}^{r_{m,1}} \cdot c_{1,2}^{r_{1,2}} \cdot [N, N], \quad \text{or} \quad = c_{2,1}^{r_{2,1}} \cdot c_{1,n}^{r_{1,n}} \cdot [N, N].$$

In the case of (VI), we always have $[N, N] = 1$; hence $V_{G \rightarrow N}(b) \neq 1$ because $r_{1,2} \not\equiv 0 \pmod{p}$. In the case (VII), we also have the same because $[N, N] = 1$ and $r_{1,n} \not\equiv 0 \pmod{p}$. In the case (VIII), $V_{G \rightarrow N}$ is neither trivial for the same reason if $v > 2$; if $v = 2$, however, we have $[N, N] = \langle c_{1,n} \rangle$ and $r_{2,1} \equiv 0 \pmod{p}$; therefore $V_{G \rightarrow N}$ is certainly trivial. In the cases (IX) and (X), we have $r_{2,1} \not\equiv 0 \pmod{p}$; therefore $V_{G \rightarrow N}(b) \neq 1$. The proof is completed.

COROLLARY. *Let F be an imaginary quadratic number field, \tilde{F} the Hilbert p -class field of F , and $\tilde{\tilde{F}}$ the second p -class field of F . If $\text{Gal}(\tilde{\tilde{F}}/F)$ is isomorphic to G of Type (VIII) with $v = 2$, then the p -class group of F capitulates in a proper intermediate field of $\tilde{\tilde{F}}/F$.*

Finally we raise two naïve problems to close this paper.

PROBLEM 1. Give various types of p -groups of small orders which satisfy the conditions (A) and (B).

PROBLEM 2. Do there exist imaginary quadratic number fields F with $G \cong \text{Gal}(\tilde{\tilde{F}}/F)$ for every small p -group G satisfying (A) and (B) ?

REFERENCES

- [B1] N. BLACKBURN, On prime-power groups with two generators, *Math. Proc. Cambridge Philos. Soc.* 54 (1958), 327–337.
- [Iw] K. IWASAWA, A note on capitulation problem for number fields I, II; *Proc. Japan Acad. Ser. A Math. Sci.* 65 (1989), 59–61; 183–186.
- [Ja] R. JAMES, The groups of order p^6 (p an odd prime), *Math. of Comp.* 34, no. 150, (1980), 613–637.
- [Mi1] K. MIYAKE, A generalization of Hilbert's Theorem 94, *Nagoya Math. J.* 96 (1984), 83–94.
- [Mi2] K. MIYAKE, Algebraic investigations of Hilbert's Theorem 94, the principal ideal theorem and the capitulation problem, *Exposition. Math.* 7 (1989), 289–346.
- [Mi3] K. MIYAKE, On the ideal class groups of the p -class fields of quadratic number fields, *Proc. Japan Acad. Ser. A Math. Sci.* 68 (1992), 62–67.
- [No] A. NOMURA, On the existence of unramified p -extensions, *Osaka J. Math.* 28 (1991), 55–62.
- [Sch] B. SCHMITHALS, Kapitulation der Idealklassen und Einheitenstruktur in Zahlkörpern, *J. Reine Angew. Math.* 358 (1985), 43–60.
- [Su] H. SUZUKI, A generalization of Hilbert's Theorem 94, *Nagoya Math. J.* 121 (1991), 161–169.

DEPARTMENT OF MATHEMATICS
COLLEGE OF GENERAL EDUCATION
NAGOYA UNIVERSITY
NAGOYA 464-01
JAPAN

