J. Math. Soc. Japan
Vol. 20, Nos. 1-2, 1968

On the number of fundamental relations with respect to minimal generators of a p-group

Dedicated to Professor Shôkichi Iyanaga on his 60th birthday

By Yasumasa AKAGAWA

(Received Aug. 25, 1967)
(Revised Nov. 8, 1967)

Let p be a prime number and G a finite p-group. We denote by $d(G)$ the number of minimal generators of G and by $r(G)$ the number of fundamental relations with respect to these generators. I. R. Safarevic and E. S. Golod proved in [2] the inequality

(1) $$r(G)\geqq(d(G)-1)^2/4.$$

The purpose of this paper is to prove a better inequality

(2) $$r(G)\geqq\frac{\sqrt{p}}{\sqrt{p}+1}\,\frac{d(G)(d(G)-1)}{2}$$

by an elementary method which is different from that used in [2]. If we apply the inequality (2) to the problem of existence of infinite class field towers after [6] we can improve the results of [2].

In § 1 we shall give several known lemmas as a preparation for § 2. We shall find in § 2 sufficient conditions for a function f to satisfy $r(G)\geqq f(d(G))$ and prove the inequality (2) in § 3. In § 4 we shall apply (2) to the existence of infinite class field towers.

The author is greatful to Professor Y. Kawada for his many valuable advices.

NOTATIONS:

$A_N=\{\alpha\in A\mid\alpha^\nu=\alpha$ for any $\nu\in N\}$, where N is a group of operators acting on A

$\iota_{A\to B}=$ the injection from a subset $A\subset B$ into B

$\eta_{G\to G/N}$ (or η if there is no possibility of confusion) $=$ the canonical homomorphism from a group G into its factor group G/N

$\pi_{A\times B\to A}=$ the projection from a direct product $A\times B$ to A.

§ 1. Preliminaries.

Let A be an abelian group and let a group $\mathfrak{G}$ be an operator domain of A. If a group G and an exact sequence

$$(3) \qquad 1 \longrightarrow A \xrightarrow{f} G \xrightarrow{g} \mathfrak{G} \longrightarrow 1$$

are given such that for any $\sigma \in \mathfrak{G}$ there is an $s \in g^{-1}(\sigma)$ satisfying

$$(4) \qquad f(\alpha^{\sigma}) = s^{-1}f(\alpha)s \qquad \text{for any } \alpha \in A,$$

then the triple $\{G, f, g\}$ is called *a group extension of A by $\mathfrak{G}$*. We denote by $\mathrm{Ext}\{\mathfrak{G}, A\}$ the set of all group extensions of A by $\mathfrak{G}$. If, for $\{G, f, g\}$ and $\{G', f', g'\} \in \mathrm{Ext}\{\mathfrak{G}, A\}$, there is an isomorphism $\varphi : G \cong G'$ satisfying

$$(5) \qquad \varphi \circ f = f', \qquad g = g' \circ \varphi,$$

we write $\{G, f, g\} \sim \{G', f', g'\}$. This relation $\sim$ is an equivalence relation. Define $\mathrm{Ext}(\mathfrak{G}, A) = \mathrm{Ext}\{\mathfrak{G}, A\}/\sim$ and denote the equivalence class of $\{G, f, g\}$ by (G, f, g). Identifying the factor system of $\{G, f, g\}$ with the 2-cocycle f^* of G with coefficients in A, we set

$$(6) \qquad \mathrm{Ext}(\mathfrak{G}, A) = H^2(\mathfrak{G}, A) \quad \text{(2-cohomology group of } \mathfrak{G} \text{ with coefficients in } A).$$

Especially we have $(G, f, g) = 1$ if and only if there is an injective isomorphism $h : \mathfrak{G} \to G$ such that $g \circ h = \text{identity}$.

Let A and B be abelian $\mathfrak{G}$-groups and let $\mu : A \to B$ be a $\mathfrak{G}$-homomorphism. If f^* is the factor system of $\{G, f, g\} (\in (G, f, g) \in \mathrm{Ext}(\mathfrak{G}, A))$, the 2-cocycle μf^* determines uniquely an element of $H^2(\mathfrak{G}, B)$. We denote this element by $\mu^{\#}(G, f, g)$. Then $\mu^{\#} : \mathrm{Ext}(G, A) \to \mathrm{Ext}(\mathfrak{G}, B)$ is a homomorphism. Let $\mathfrak{N}$ be a normal subgroup of $\mathfrak{G}$. Then $A_{\mathfrak{N}}$ is a $\mathfrak{G}/\mathfrak{N}$-group canonically. We define the inflation homomorphism: $\mathrm{Inf}_{\mathfrak{G}/\mathfrak{N} \to \mathfrak{G}} : H^2(\mathfrak{G}/\mathfrak{N}, A_{\mathfrak{N}}) \to H^2(\mathfrak{G}, A)$ as usual. If $\mu : A \to B$ is surjective, then we can represent $\mu^{\#}$ on $\mathrm{Ext}(\mathfrak{G}, A)$, using the identification (6), by

$$(7) \qquad \mu^{\#}(G, f, g) = (G/f(\ker \mu), f \circ \mu^{-1}, g)$$

for $(G, f, g) \in \mathrm{Ext}(\mathfrak{G}, A)$. Similarly we can represent $\mathrm{Inf}_{\mathfrak{G}/\mathfrak{N} \to \mathfrak{G}}$ on $\mathrm{Ext}(\mathfrak{G}/\mathfrak{N}, A_{\mathfrak{N}})$ in the case $A_{\mathfrak{N}} = A$. Denote, in general

$$(8) \qquad G_g \otimes_{g'} G' \text{ (or } G \otimes G' \text{ if there is no possibility of confusion)} = \{(s, s') \in G \times G' \mid g(s) = g'(s')\}$$

for $\{G, f, g\} \in \mathrm{Ext}\{\mathfrak{G}, A\}$ and $\{G', f', g'\} \in \mathrm{Ext}\{\mathfrak{G}, B\}$. Then

$$(9) \qquad \mathrm{Inf}_{\mathfrak{G}/\mathfrak{N} \to \mathfrak{G}}(\bar{G}, \bar{f}, \bar{g}) = (\bar{G}_{\bar{g}} \otimes_{\eta} \mathfrak{G}, \iota_{\bar{f}(A) \to \bar{G} \otimes \mathfrak{G}} \circ \bar{f}, \pi_{\bar{G} \otimes \mathfrak{G} \to \mathfrak{G}})$$

for $(\bar{G}, f, \bar{g}) \in \mathrm{Ext}(\mathfrak{G}/\mathfrak{N}, A_{\mathfrak{N}})$, where $\pi_{\bar{G}\otimes\mathfrak{G}\to\mathfrak{G}} = \pi_{\bar{G}\times\mathfrak{G}\to\mathfrak{G}}|_{\bar{G}\otimes\mathfrak{G}}$.

Let $\mathfrak{N}$ be a normal subgroup of $\mathfrak{G}$. We shall investigate $\ker(\mathrm{Inf}_{\mathfrak{G}/\mathfrak{N}\to\mathfrak{G}}: H^2(\mathfrak{G}/\mathfrak{N}, A_{\mathfrak{N}}) \to H^2(\mathfrak{G}, A))$ in the case $A_{\mathfrak{N}} = A$. Choose $(\bar{G}, \bar{f}, \bar{g}) \in \ker(\mathrm{Inf}_{\mathfrak{G}/\mathfrak{N}\to\mathfrak{G}}: H^2(\mathfrak{G}/\mathfrak{N}, A) \to H^2(\mathfrak{G}, A))$. From (8) and (9) we know that

$$(\bar{G}_{\bar{g}}\otimes_{\eta}\mathfrak{G},\ \iota_{\bar{f}(A)\to\bar{G}\otimes\mathfrak{G}} \circ \bar{f},\ \pi_{\bar{G}\otimes\mathfrak{G}\to\mathfrak{G}}) = \mathrm{Inf}_{\mathfrak{G}/\mathfrak{N}\to\mathfrak{G}}(\bar{G}, \bar{f}, \bar{g}) = 1\,,$$

therefore there is an injective isomorphism $h: \mathfrak{G} \to \bar{G}_{\bar{g}}\otimes_{\eta}\mathfrak{G}$ such that $\pi_{\bar{G}\otimes\mathfrak{G}\to\mathfrak{G}} \circ h = \text{identity}$. Define a homomorphism $\mu: \mathfrak{N} \to A$ and an isomorphism $\varphi: \mathfrak{G}/\ker\mu \cong \bar{G}$ by

$$\mu = \bar{f}^{-1} \circ \pi_{\bar{G}\otimes\mathfrak{G}\to\bar{G}} \circ h|_{\mathfrak{N}}, \qquad \varphi = \pi_{\bar{G}\otimes\mathfrak{G}\to\bar{G}} \circ h\,,$$

where $\ker\mu$ is equal to $\ker(\pi_{\bar{G}\otimes\mathfrak{G}\to\bar{G}} \circ h: \mathfrak{G} \to \bar{G})$. Since

$$\varphi \circ \eta_{\mathfrak{N}\to\mathfrak{N}/\ker\mu} = f \circ \mu\,, \qquad \eta_{\mathfrak{G}/\ker\mu\to\mathfrak{G}/\mathfrak{N}} = \bar{g} \circ \varphi\,,$$

we have, for $\{\mathfrak{G}, \iota_{\mathfrak{N}\to\mathfrak{G}}, \eta_{\mathfrak{G}\to\mathfrak{G}/\mathfrak{N}}\} \in \mathrm{Ext}\{\mathfrak{G}/\mathfrak{N}, \mathfrak{N}\}$, an equality

$$\mu^{\#}(\mathfrak{G}, \iota_{\mathfrak{N}\to\mathfrak{G}}, \eta_{\mathfrak{G}\to\mathfrak{G}/\mathfrak{N}}) = (\bar{G}, \bar{f}, \bar{g})\,.$$

Conversely, let $\mu: \mathfrak{N} \to A$ be a $\mathfrak{G}$-homomorphism. Put

$$\mu^{\#}(\mathfrak{G}, \iota_{\mathfrak{N}\to\mathfrak{G}}, \eta_{\mathfrak{G}\to\mathfrak{G}/\mathfrak{N}}) = (\bar{G}, \bar{f}, \bar{g}) \in \mathrm{Ext}(\mathfrak{G}/\mathfrak{N}, A)\,.$$

The formulae (5) and (7) show that there is a $\mathfrak{G}$-isomorphism φ: $\mathfrak{G}/\ker\mu \cong \bar{G}$ satisfying

$$\varphi \circ \mu^{-1} = \bar{f}\,, \qquad \eta_{\mathfrak{G}\to\mathfrak{G}/\mathfrak{N}} = \bar{g} \circ \varphi\,.$$

The formulae (8) and (9) prove that

$$\mathrm{Inf}_{\mathfrak{G}/\mathfrak{N}\to\mathfrak{G}}(\bar{G}, \bar{f}, \bar{g}) = (\bar{G}_{\bar{g}}\otimes_{\eta}\mathfrak{G},\ \iota_{\bar{f}(A)\to\bar{G}\otimes\mathfrak{G}} \circ \bar{f},\ \pi_{\bar{G}\otimes\mathfrak{G}\to\mathfrak{G}})\,.$$

Define $h: \mathfrak{G} \to \bar{G}_{\bar{g}}\otimes_{\eta}\mathfrak{G}$ by $h(\sigma) = (\varphi(\sigma), \sigma)$ for $\sigma \in \mathfrak{G}$. Since $\pi_{\bar{G}\otimes\mathfrak{G}\to\mathfrak{G}} \circ h = \text{identity}$, we have $\mathrm{Inf}_{\mathfrak{G}/\mathfrak{N}\to\mathfrak{G}}(\bar{G}, \bar{f}, \bar{g}) = 1$. Thus we obtain the following proposition.

PROPOSITION 1. *Let $\mathfrak{G}$ be a finite group and $\mathfrak{N}$ a normal subgroup of $\mathfrak{G}$. Let A be a finite abelian $\mathfrak{G}$-group which is elementwise invariant under the action of each element of $\mathfrak{N}$. Regard A as a $\mathfrak{G}/\mathfrak{N}$-group canonically and* $(\mathfrak{G}, \iota_{\mathfrak{N}\to\mathfrak{G}}, \eta_{\mathfrak{G}\to\mathfrak{G}/\mathfrak{N}}) \in \mathrm{Ext}(\mathfrak{G}/\mathfrak{N}, \mathfrak{N})$. *Then*

$$\ker(\mathrm{Inf}_{\mathfrak{G}/\mathfrak{N}\to\mathfrak{G}}: \mathrm{Ext}(\mathfrak{G}/\mathfrak{N}, A) \to \mathrm{Ext}(\mathfrak{G}, A))$$
$$= \bigcup_{\mu} \mu^{\#}(\mathfrak{G}, \iota_{\mathfrak{N}\to\mathfrak{G}}, \eta_{\mathfrak{G}\to\mathfrak{G}/\mathfrak{N}})\,,$$

where μ runs over all the $\mathfrak{G}$-homomorphisms $\mathfrak{N} \to A$.

Let G be a pro-p-group, namely, the projective limit of a set of finite p-groups and let N be a closed normal subgroup $\neq \{1\}$ of G. We denote by $d(G)$ the number of minimal generators of G in the sense of pro-finite groups. Let Σ be a subset of N such that Σ and their conjugates in G generate a dense subgroup of N. Then Σ is called a normal generator system of the normal subgroup N of G. Define

$$d_G(N)=\inf_{\Sigma}\ \#(\Sigma)\,.$$

We shall define

$$\delta_G(N)=[G,N]N^p$$

to be the normal subgroup of G generated by the commutator of G and N and the p-th powers of the elements of N. Now we obtain from Burnside's basis theorem about finite p-groups the following lemma concerning pro-p-groups.

LEMMA 1. *Σ is a normal generator system of the normal subgroup N of G, if and only if $\Sigma \bmod \delta_G(N)$ is a normal generator system of the normal subgroup $N/\delta_G(N)$ of $G/\delta_G(N)$.*

Let G_n^* be a free group with free generators $\sigma_1, \cdots, \sigma_n$. The pro-$p$-group

$$\mathfrak{G}_n^*=\varprojlim G_n^*/N^*$$

is called a free pro-p-group, where N^* runs over those normal subgroups of G_n^* of which the indices are p-powers. It is generated also by $\sigma_1, \cdots, \sigma_n$. The following proposition can be obtained by a straightforward translation from the analogous theorem on free groups [4, p. 33].

PROPOSITION 2. *Any open and cloesd subgroup $\mathfrak{H}$ of a free pro-p-group $\mathfrak{G}$ is a free pro-p-group. Let Σ be a minimal generator system of $\mathfrak{G}$ and $\mathfrak{N}$ a normal subgroup of $\mathfrak{G}$ generated by a subset T of Σ. Then $\mathfrak{G}/\mathfrak{N}$ is a free pro-p-group with the minimal generator system $\Sigma-T \bmod \mathfrak{N}$.*

Let $\overline{\mathfrak{G}}$ be a pro-p-group with a minimal generator system $\bar{\sigma}_1, \cdots . \bar{\sigma}_n$. There is a homomorphism $\phi:\mathfrak{G}_n^*\to\overline{\mathfrak{G}}$ such that $\phi(\sigma_i)=\bar{\sigma}_i$; $i=1, \cdots, n$. Define

$$d_{\mathfrak{G}_n^*}(\ker\phi)=r(\overline{\mathfrak{G}}) \quad (=0 \text{ if } \ker\phi=\{1\})$$

and call it *the number of relations of* $\overline{\mathfrak{G}}$. Regard the discrete abelian group $(\ker\phi/\delta_{\mathfrak{G}_n^*}(\ker\phi))^\wedge$ as a $GF(p)$-vector space, which is the dual of the compact group $\ker\phi/\delta_{\mathfrak{G}_n^*}(\ker\phi)$. Then, from Lemma 1, we get

PROPOSITION 3.

$$r(\overline{\mathfrak{G}})=\dim(\ker\phi/\delta_{\mathfrak{G}_n^*}(\ker\phi))^\wedge \quad (n=d(\overline{\mathfrak{G}}))\,.$$

This proposition implies that the number $r(\overline{\mathfrak{G}})$ is independent of the choice of the minimal generator system $\bar{\sigma}_1, \cdots, \bar{\sigma}_n$.

PROPOSITION 4. *Let $n=d(\overline{\mathfrak{G}})$. Take $\chi\in(\ker\phi/\delta_{\mathfrak{G}_n^*}(\ker\phi))^\wedge$. The mapping*

$$\chi\to\begin{cases}(\mathfrak{G}_n^*/\ker\chi,\ \chi^{-1},\ \phi) & \textit{if}\ \ \chi\neq 0\\ 0 & \textit{if}\ \ \chi=0\end{cases}$$

defines an isomorphism

$$(\ker \psi/\delta_{\mathfrak{G}_n^*}(\ker \psi))^\wedge \cong \mathrm{Ext}\,(\bar{\mathfrak{G}}, GF(p)) .$$

PROOF. It is easy to see that this mapping is an injective isomorphism. We shall show the surjectivity. Take any (G, f, g) $(\in \mathrm{Ext}\,(\bar{\mathfrak{G}}, GF(p))) \neq 0$. Choose an $s_i \in g^{-1}(\bar{\sigma}_i)$ for each $\bar{\sigma}_i$. $\{s_i\}$ is again a minimal generator system of G and there is a unique homomorphism $\tilde{\psi}: \mathfrak{G}_n^* \to G$ such that $\tilde{\psi}(\sigma_i) = s_i$. Define $f^{-1}\tilde{\psi}|_{\ker\psi} = \chi \in (\ker \psi/\delta_{\mathfrak{G}_n^*}(\ker \psi))^\wedge$. Then $(\mathfrak{G}_n^*/\ker \chi, \chi^{-1}, \psi) = (G, f, g)$.

q. e. d.

REMARK. Let G be a pro-p-group and let N be its normal subgroup. Then we have an exact sequence [7]

$$0 \longrightarrow H^1(G/N, GF(p)) \xrightarrow{\mathrm{Inf}} H^1(G, GF(p)) \xrightarrow{\mathrm{Res}} H^1(N, GF(p))_G$$
$$\xrightarrow{\delta} H^2(G/N, GF(p)) \xrightarrow{\mathrm{Inf}} H^2(G, GF(p)) .$$

All propositions of this § can be obtained from this sequence if we notice that $H^2(\mathfrak{G}_n^*, GF(p)) = 0$.

§ 2. Main theorem.

We shall use the following Lemma which is an easy consequence of linear algebra.

LEMMA 2. *Let V be a vector space over $GF(p)$ and σ_1 a linear transformation on V such that $\sigma_1^p =$ identity. Then V has a basis of the form*

$$\{(1-\sigma_1)^j v_\lambda \,|\, 0 \leqq j \leqq \nu_\lambda,\ \lambda \in \Lambda\}$$

where ν_λ are rational integers satisfying $0 \leqq \nu_\lambda \leqq p-1$ and $(1-\sigma_1)^{\nu_\lambda+1} v_\lambda = 0$.

Our purpose is to prove the following

THEOREM. *Let $f(x)$ be a real valued function defined on the non-negative rational integers satisfying two conditions:*

I. $$f(0) \leqq 0 \quad and \quad f(1) \leqq 1 ,$$

II. $$\max\left\{\frac{1}{p} f(p(x-1)+d-x),\ f(d-1)\right\} + d - x \geqq f(d) ;$$

where d is any natural number and $x = 1, \cdots, d$. Let $\bar{\mathfrak{G}}$ be a finite p-group with $d(\bar{\mathfrak{G}})$ generators. Let $r(\bar{\mathfrak{G}})$ be the number of relations of $\bar{\mathfrak{G}}$. Then we have

$$r(\bar{\mathfrak{G}}) \geqq f(d(\bar{\mathfrak{G}})) .$$

(Here we put $d(\mathfrak{E}) = r(\mathfrak{E}) = 0$ for the identity group $\mathfrak{E} = \{1\}$.)

PROOF. When $d(\bar{\mathfrak{G}}) = 0$ or 1, $r(\bar{\mathfrak{G}}) = 0$ or 1, respectively, and our theorem is trivial. Suppose $2 \leqq d(\bar{\mathfrak{G}}) < \infty$. Let $\mathfrak{G}$ be a free pro-p-group such that $d(\mathfrak{G}) = d(\bar{\mathfrak{G}})$ and $\mathfrak{N}$ a normal subgroup of $\mathfrak{G}$ of finite index. Regarding $(\mathfrak{N}/\delta_{\mathfrak{G}}(\mathfrak{N}))^\wedge$

as $GF(p)$-vector space, we shall prove

$$\dim(\mathfrak{N}/\delta_{\mathfrak{G}}(\mathfrak{N}))^{\wedge} \geqq f(d(\mathfrak{G}/\mathfrak{N}))+d(\mathfrak{G})-d(\mathfrak{G}/\mathfrak{N}). \tag{10}$$

Prop. 3 shows then our theorem if we apply $\mathfrak{N}=\ker(\psi:\mathfrak{G}\to\bar{\mathfrak{G}})$ under the notation there.

When $\mathfrak{N}=\mathfrak{G}$, (10) follows from the three facts that $\dim(\mathfrak{N}/\delta_{\mathfrak{G}}(\mathfrak{N}))^{\wedge} =\dim(\mathfrak{G}/\delta_{\mathfrak{G}}(\mathfrak{G}))^{\wedge}=d(\mathfrak{G})$, $d(\mathfrak{G}/\mathfrak{N})=d(\mathfrak{E})=0$, and that $f(d(\mathfrak{G}/\mathfrak{N}))=f(0)\leqq 0$. So, we prove (10) by the induction about $[\mathfrak{G}:\mathfrak{N}]$. We may assume $[\mathfrak{G}:\mathfrak{N}]\geqq p$ and that (10) holds good for a free pro-p-group with an arbitrary finite number of generators and for its arbitrary normal subgroup of index less than $[\mathfrak{G}:\mathfrak{N}]$.

(I) Let $\mathfrak{H}$ be a maximal proper normal subgroup of $\mathfrak{G}$ containing $\mathfrak{N}$. Then $[\mathfrak{G}:\mathfrak{H}]=p$. Select at first a minimal generator system $\Sigma=\{\sigma_i\,|\,i=1,2,\cdots\}$ of $\mathfrak{G}$ so that

$$\begin{cases} \sigma_1 \notin \mathfrak{H} \\ \sigma_i \in \mathfrak{H} \text{ but not in } \mathfrak{N} \text{ for } 1<i\leqq d(\mathfrak{G}/\mathfrak{N}) \\ \sigma_j \in \mathfrak{N} \qquad\qquad \text{for } d(\mathfrak{G}/\mathfrak{N})<j\leqq d(\mathfrak{G}). \end{cases} \tag{11}$$

Notice that $1\leqq d(\mathfrak{G}/\mathfrak{N})\leqq d(\mathfrak{G})$ and that the minimal one among all the generator systems of $\mathfrak{G}$ satisfying (11) becomes a minimal generator system of G. Therefore $\sharp(\Sigma)=d(\mathfrak{G})$ (cf. Lemma 1). $\mathfrak{H}$ is a free pro-p-group by Prop. 2. By a straightforward calculation or by an application of a general method finding a minimal generator system of a subgroup of a free group [4] to our case of free pro-p-group, we find that

$$\{\sigma_1^p,\ \sigma_i^{\sigma_1^{\mu}}\,|\,1<i\leqq d(\mathfrak{G}),\ 0\leqq\mu<p\} \tag{12}$$

forms a minimal generator system of $\mathfrak{H}$. Now, take a $GF(p)$-vector space V on which the cyclic group $\mathfrak{G}/\mathfrak{H}=\langle\sigma_1\mathfrak{H}\rangle$ acts as an operator group. Let the action of $\sigma_1\mathfrak{H}$ on V be as follows: there are $v_1,\cdots,v_{d(\mathfrak{G})}$ in V such that $\sigma_1 v=v_1$ and $v_1, v_2, \sigma_1 v_2,\cdots,\sigma_1^{p-1}v_2, v_3,\cdots,v_{d(\mathfrak{G})},\sigma_1 v_{d(\mathfrak{G})},\cdots,\sigma_1^{p-1}v_{d(\mathfrak{G})}$ form a basis of V. Since there is a unique $\mathfrak{G}$-isomorphism $\mathfrak{H}/\delta_{\mathfrak{H}}(\mathfrak{H})\cong V$ which maps σ_1^p to v_1 and σ_i to v_i; $i=2,\cdots,d(\mathfrak{G})$, we shall identify $\mathfrak{H}/\delta_{\mathfrak{H}}(\mathfrak{H})=V$.

(II) Define two subspace U, W of V by $U=\langle\sigma_1^p\rangle\cup\delta_{\mathfrak{H}}(\mathfrak{H})/\delta_{\mathfrak{H}}(\mathfrak{H})$ and $W=\langle\sigma_1^p\rangle\cup\mathfrak{N}\cup\delta_{\mathfrak{H}}(\mathfrak{H})/\delta_{\mathfrak{H}}(\mathfrak{H})$ which are $\mathfrak{G}/\mathfrak{H}$-subspaces of V. Since the action of σ_1 on V satisfies that σ_1^p is the identity operator, we can apply Lemma 2 to the quotient space V/W. Hence we can suppose in addition that

$$\begin{cases} \{v_2,(\sigma_1-1)v_2,\cdots,(\sigma_1-1)^{\nu_2}v_2,\cdots,v_{d(\mathfrak{G}/\mathfrak{N})},(\sigma_1-1)v_{d(\mathfrak{G}/\mathfrak{N})}, \\ \qquad \cdots,(\sigma_1-1)^{\nu_{d(\mathfrak{G}/\mathfrak{N})}}v_{d(\mathfrak{G}/\mathfrak{H})}\} \\ \text{is a basis of } V/W=\mathfrak{H}/\langle\sigma_1^p\rangle\cup\mathfrak{N}\cup\delta_{\mathfrak{H}}(\mathfrak{H}) \text{ and} \\ (\sigma_1-1)^{\nu_2+1}v_2\equiv\cdots\equiv(\sigma_1-1)^{\nu_{d(\mathfrak{G}/\mathfrak{N})}+1}v_{d(\mathfrak{G}/\mathfrak{N})}=0 \bmod W. \end{cases} \tag{13}$$

Then, since V/U is $\mathfrak{G}/\mathfrak{H}$-split,

$$(14) \qquad \begin{cases} \{(\sigma_1-1)^{\mu_i}v_i,\ (\sigma_1-1)^{\mu_j}v_j \mid 1 < i \leqq d(\mathfrak{G}/\mathfrak{N}),\ \nu_i < \mu_i < p, \\ d(\mathfrak{G}/\mathfrak{N}) < j \leqq d(\mathfrak{G}),\ 0 \leqq \mu_j < p\} \text{ is a basis of } W/U. \end{cases}$$

Moreover, we can suppose that

$$(15) \qquad \begin{cases} \nu_i = p-1 & \text{if } 1 < i \leqq c \\ \nu_i < p-1 & \text{if } c < i \leqq d(\mathfrak{G}/\mathfrak{N}) \end{cases}$$

where $1 < c \leqq d(\mathfrak{G}/\mathfrak{N})$.

(III) Define two groups

$$(16) \qquad \begin{cases} \mathfrak{N}_1 = \text{the normal subgroup of } \mathfrak{H} \text{ generated by } \{\sigma_1^p,\ \sigma_i^{1-\sigma_1^{\mu_i}}, \\ \quad \sigma_j^{\sigma_1^{\mu_j}} \mid c<i\leqq d(\mathfrak{G}/\mathfrak{N}),\ 1\leqq \mu_i<p,\ d(\mathfrak{G}/\mathfrak{N})<j\leqq d(\mathfrak{G}),\ 0\leqq \mu_j<p\}, \end{cases}$$

$$(17) \qquad \begin{cases} \mathfrak{N}_2 = \text{the normal subgroup of } \mathfrak{G} \text{ generated by} \\ \quad \{\sigma_1,\ \sigma_j \mid d(\mathfrak{G}/\mathfrak{N}) < j \leqq d(\mathfrak{G})\}. \end{cases}$$

By the calculation

$$(\sigma_i^{1-\sigma_1^{\mu}})^{1-\sigma_1} = (\sigma_i^{1-\sigma_1^{\mu}})\{(\sigma_i^{1-\sigma_1^{\mu}})^{\sigma_1}\}^{-1} = \sigma_i(\sigma_i^{\sigma_1^{\mu}})^{-1}\sigma_i^{\sigma_1^{\mu+1}}(\sigma_i^{\sigma_1})^{-1}$$

$$\equiv \begin{cases} \sigma_i\sigma_i^{-1}\sigma_i\sigma_i^{-1} \equiv 1 \bmod \mathfrak{N}_1 & \text{if } \mu < p-1 \\ \sigma_i\sigma_i^{-1}\sigma_i^{\sigma_1^p}\sigma_i \equiv 1 \bmod \mathfrak{N}_1 & \text{if } \mu = p-1 \end{cases}$$

$c < i \leqq d(\mathfrak{G}/\mathfrak{N})$, we know that $\mathfrak{N}_1$ is a normal subgroup of $\mathfrak{G}$. So, from (16), (17), and Prop. 2, follows that

$$(18) \qquad \begin{cases} \mathfrak{H}/\mathfrak{N}_1 \text{ is a free pro-}p\text{-group on which } \sigma_1 \text{ acts in the canonical} \\ \text{way and } d(\mathfrak{H}/\mathfrak{N}_1) = p(c-1) + d(\mathfrak{G}/\mathfrak{N}) - c; \end{cases}$$

$$(19) \qquad \mathfrak{G}/\mathfrak{N}_2 \text{ is a free pro-}p\text{-group and } d(\mathfrak{G}/\mathfrak{N}_2) = d(\mathfrak{G}/\mathfrak{N}) - 1.$$

(IV) Since $(\mathfrak{N}/(\mathfrak{N} \cap \mathfrak{N}_1)\delta_{\mathfrak{G}}(\mathfrak{N}))^\wedge$ is a subspace of $(\mathfrak{N}/(\mathfrak{N} \cap \mathfrak{N}_1)\delta_{\mathfrak{H}}(\mathfrak{N}))^\wedge$ and in fact the former is composed of all the σ_1-invariant elements of the latter, we know by Lemma 2

$$(20) \qquad \dim (\mathfrak{N}/(\mathfrak{N} \cap \mathfrak{N}_1)\delta_{\mathfrak{G}}(\mathfrak{N}))^\wedge \geqq p^{-1} \dim (\mathfrak{N}/(\mathfrak{N} \cap \mathfrak{N}_1)\delta_{\mathfrak{H}}(\mathfrak{N}))^\wedge.$$

Set a canonically defined isomorphism

$$\theta:\ \mathfrak{N}/\mathfrak{N} \cap (\mathfrak{N}_1\delta_{\mathfrak{H}}(\mathfrak{N})) \cong \mathfrak{N}\mathfrak{N}_1/\mathfrak{N}_1/\delta_{\mathfrak{H}/\mathfrak{N}_1}(\mathfrak{N}\mathfrak{N}_1/\mathfrak{N}_1).$$

From $(\mathfrak{N} \cap \mathfrak{N}_1)\delta_{\mathfrak{H}}(\mathfrak{N}) = \mathfrak{N} \cap (\mathfrak{N}_1\delta_{\mathfrak{H}}(\mathfrak{N}))$ and the existence of this θ, follows

$$(21) \qquad \dim (\mathfrak{N}/(\mathfrak{N} \cap \mathfrak{N}_1)\delta_{\mathfrak{H}}(\mathfrak{N}))^\wedge = \dim (\mathfrak{N}\mathfrak{N}_1/\mathfrak{N}_1/\delta_{\mathfrak{H}/\mathfrak{N}_1}(\mathfrak{N}\mathfrak{N}_1/\mathfrak{N}_1))^\wedge.$$

By Lemma 1 we know that a representative system in $\mathfrak{H}$ of a generator system of $\mathfrak{H}/\mathfrak{N}\mathfrak{N}_1$ is a representative system of a generator system of $\mathfrak{H}/\mathfrak{N}\mathfrak{N}_1\delta_{\mathfrak{H}}(\mathfrak{H})$. Hence from (13) follows that

$$\{\sigma_2, \sigma_2^{\sigma_1}, \cdots, \sigma_2^{\sigma_1^{p-1}}, \cdots, \sigma_c, \sigma_c^{\sigma_1}, \cdots, \sigma_c^{\sigma_1^{p-1}}, \sigma_{c+1}, \cdots, \sigma_{d(\mathfrak{G}/\mathfrak{N})}\}$$

is a minimal generator system of $\mathfrak{H}/\mathfrak{N}\mathfrak{N}_1$, consequently, we have

$$d(\mathfrak{H}/\mathfrak{N}\mathfrak{N}_1)=p(c-1)+d(\mathfrak{G}/\mathfrak{N})-c\,. \tag{22}$$

Since $[\mathfrak{H}/\mathfrak{N}_1:\mathfrak{N}\mathfrak{N}_1/\mathfrak{N}_1]<[\mathfrak{H}:\mathfrak{N}]<[\mathfrak{G}:\mathfrak{N}]$, we can use the assumption of induction for the free pro-p-group $\mathfrak{H}/\mathfrak{N}_1$ and its normal subgroup $\mathfrak{N}\mathfrak{N}_1/\mathfrak{N}_1$. Then we have

$$\begin{aligned}\dim(\mathfrak{N}\mathfrak{N}_1/\mathfrak{N}_1/\delta_{\mathfrak{H}/\mathfrak{N}_1}(\mathfrak{N}\mathfrak{N}_1/\mathfrak{N}_1))^\wedge &\geqq f(d(\mathfrak{H}/\mathfrak{N}\mathfrak{N}_1))+d(\mathfrak{H}/\mathfrak{N}_1)-d(\mathfrak{H}/\mathfrak{N}\mathfrak{N}_1)\\ &=f(p(c-1)+d(\mathfrak{G}/\mathfrak{N})-c)\end{aligned} \tag{23}$$

by (22) and (18). From (20), (21), and (23) we obtain

$$\dim(\mathfrak{N}/(\mathfrak{N}\cap\mathfrak{N}_1)\delta_{\mathfrak{H}}(\mathfrak{N}))^\wedge \geqq p^{-1}f(p(c-1)+d(\mathfrak{G}/\mathfrak{N})-c)\,. \tag{24}$$

(V) Since $[\mathfrak{G}/\mathfrak{N}_2:\mathfrak{N}\mathfrak{N}_2/\mathfrak{N}_2]<[\mathfrak{G}:\mathfrak{N}]$ from $\sigma_1\notin\mathfrak{N}$ but $\sigma_1\in\mathfrak{N}_2$, we can again use the assumption of induction for the free pro-p-group $\mathfrak{G}/\mathfrak{N}_2$ and its normal subgroup $\mathfrak{N}\mathfrak{N}_2/\mathfrak{N}_2$. Using the isomorphism $\mathfrak{N}/\mathfrak{N}\cap(\mathfrak{N}_2\delta_{\mathfrak{G}}(\mathfrak{N}))\cong\mathfrak{N}\mathfrak{N}_2/\mathfrak{N}_2/\delta_{\mathfrak{G}/\mathfrak{N}_2}(\mathfrak{N}\mathfrak{N}_2/\mathfrak{N}_2)$ and (19), we have

$$\begin{aligned}\dim(\mathfrak{N}/(\mathfrak{N}\cap\mathfrak{N}_2)\delta_{\mathfrak{G}}(\mathfrak{N}))^\wedge &= \dim(\mathfrak{N}\mathfrak{N}_2/\mathfrak{N}_2/\delta_{\mathfrak{G}/\mathfrak{N}_2}(\mathfrak{N}\mathfrak{N}_2/\mathfrak{N}_2))^\wedge\\ &\geqq f(d(\mathfrak{G}/\mathfrak{N})-1)\,.\end{aligned} \tag{25}$$

(VI) Notice that $\mathfrak{N}/\mathfrak{N}\cap(\langle\sigma_1^p\rangle\delta_{\mathfrak{H}}(\mathfrak{H}))\cong W/U$. From (14),

$$\left\{\begin{array}{l}\langle\sigma_1^p\rangle\cup\mathfrak{N}\cup\delta_{\mathfrak{H}}(\mathfrak{H})/\langle\sigma_1^p\rangle\delta_{\mathfrak{G}}(\mathfrak{N})\delta_{\mathfrak{H}}(\mathfrak{H}) \text{ has a minimal generator}\\ \text{system represented by } \{\sigma_i^{(\sigma_1-1)^{\nu_i+1}}, \sigma_j\,|\,c<i\leqq d(\mathfrak{G}/\mathfrak{N}),\\ d(\mathfrak{G}/\mathfrak{N})<j\leqq d(\mathfrak{G})\}\,.\end{array}\right. \tag{26}$$

Since $\mathfrak{N}/(\mathfrak{N}\cap\langle\sigma_1^p\rangle\delta_{\mathfrak{H}}(\mathfrak{H}))\delta_{\mathfrak{G}}(\mathfrak{N})\cong\langle\sigma_1^p\rangle\mathfrak{N}\delta_{\mathfrak{H}}(\mathfrak{H})/\langle\sigma_1^p\rangle\delta_{\mathfrak{G}}(\mathfrak{N})\delta_{\mathfrak{H}}(\mathfrak{H})$ we have

$$\dim(\mathfrak{N}/(\mathfrak{N}\cap\langle\sigma_1^p\rangle\delta_{\mathfrak{H}}(\mathfrak{H}))\delta_{\mathfrak{G}}(\mathfrak{N}))^\wedge=d(\mathfrak{G})-c\,. \tag{27}$$

(VII) Regard all the vector spaces of the left hand sides of (24), (25), and (27) as subspaces of $(\mathfrak{N}/\delta_{\mathfrak{G}}(\mathfrak{N}))^\wedge$ canonically. We shall prove that

$$(\mathfrak{N}/(\mathfrak{N}\cap\mathfrak{N}_1)\delta_{\mathfrak{G}}(\mathfrak{N}))^\wedge\cap(\mathfrak{N}/(\mathfrak{N}\cap\langle\sigma_1^p\rangle\delta_{\mathfrak{H}}(\mathfrak{H}))\delta_{\mathfrak{G}}(\mathfrak{N}))^\wedge=0 \tag{28}$$

$$(\mathfrak{N}/(\mathfrak{N}\cap\mathfrak{N}_2)\delta_{\mathfrak{G}}(\mathfrak{N}))^\wedge\cap(\mathfrak{N}/(\mathfrak{N}\cap\langle\sigma_1^p\rangle\delta_{\mathfrak{H}}(\mathfrak{H}))\delta_{\mathfrak{G}}(\mathfrak{N}))^\wedge=0\,. \tag{29}$$

Take a $\chi(\neq 0)$ in $(\mathfrak{N}/(\mathfrak{N}\cap\mathfrak{N}_1)\delta_{\mathfrak{G}}(\mathfrak{N}))^\wedge$. Since there is a canonical surjective homomorphism $\eta:\mathfrak{N}\mathfrak{N}_1/\mathfrak{N}_1\delta_{\mathfrak{H}}(\mathfrak{N})\to\mathfrak{N}/(\mathfrak{N}\cap\mathfrak{N}_1)\delta_{\mathfrak{G}}(\mathfrak{N})$, we can find $\bar{\chi}\in(\mathfrak{N}\mathfrak{N}_1/\mathfrak{N}_1\delta_{\mathfrak{H}}(\mathfrak{N}))^\wedge$ such that $\bar{\chi}|_{\mathfrak{N}}=\chi$. Since $\chi\neq 0$, we have $\bar{\chi}\neq 0$. Therefore, from Prop. 4 follows

$$(\mathfrak{H}/\ker\bar{\chi}, \bar{\chi}^{-1}, \eta_{\mathfrak{H}/\ker\bar{\chi}\to\mathfrak{H}/\mathfrak{N}\mathfrak{N}_1})\neq 0 \text{ in } \operatorname{Ext}(\mathfrak{H}/\mathfrak{N}\mathfrak{N}_1, GF(p))\,. \tag{30}$$

Now, from (9) we have

$$(31)\qquad \mathrm{Inf}_{\mathfrak{H}/\mathfrak{N}\mathfrak{N}_1\to\mathfrak{H}/\mathfrak{N}}(\mathfrak{H}/\ker\bar{\chi},\ \bar{\chi}^{-1},\ \eta_{\mathfrak{H}/\ker\bar{\chi}\to\mathfrak{H}/\mathfrak{N}\mathfrak{N}_1})$$
$$=(\mathfrak{H}/\ker\bar{\chi}_\eta\otimes_\eta\mathfrak{H}/\mathfrak{N},\ \iota_{\mathfrak{N}\mathfrak{N}_1/\ker\bar{\chi}\to\mathfrak{H}/\ker\bar{\chi}\otimes\mathfrak{H}/\mathfrak{N}}\bar{\chi}^{-1},\ \eta)$$
$$=(\mathfrak{H}/\ker\chi,\ \chi^{-1},\ \eta_{\mathfrak{H}/\ker\chi\to\mathfrak{H}/\mathfrak{N}}).$$

Here we can see that

$$(32)\qquad \begin{cases}\mathrm{Inf}_{\mathfrak{H}/\mathfrak{N}\mathfrak{N}_1\to\mathfrak{H}/\mathfrak{N}}:\ \mathrm{Ext}\,(\mathfrak{H}/\mathfrak{N}\mathfrak{N}_1,\ GF(p))\to\mathrm{Ext}\,(\mathfrak{H}/\mathfrak{N},\ GF(p))\\ \text{is injective.}\end{cases}$$

Because, take any $\mathfrak{H}$-homomorphism $\bar{\mu}(\neq 0):\ \mathfrak{N}\mathfrak{N}_1\to GF(p)$ such that $\ker\bar{\mu}\supset\mathfrak{N}$. If we put

$\mathfrak{H}_1=$ the (not normal!) subgroup of $\mathfrak{H}$ generated by the set (16)

$\mathfrak{C}_1=$ the normal subgroup of $\mathfrak{H}$ generated by $\{\sigma_i^{\sigma_1^{\mu_i}}\mid 2\leqq i\leqq d(\mathfrak{G}/\mathfrak{N}),\ 0\leqq\mu_i<p$ for $1<i\leqq c,\ \mu_i=0$ for $c<i\leqq d(\mathfrak{G}/\mathfrak{N})\}$,

there is a canonical isomorphism $\mathfrak{H}/\mathfrak{C}_1\cong\mathfrak{H}_1\subset\mathfrak{N}_1$ by (12) and Prop. 2. Hence $\bar{\mu}$ can be extended to $\mu:\mathfrak{H}\to GF(p)$. Since $\mu|_{\mathfrak{N}\mathfrak{N}_1}=\bar{\mu}$,

$$\ker\bar{\mu}=\ker\mu\cap\mathfrak{N}\mathfrak{N}_1.$$

This implies that $\mathfrak{H}/\ker\bar{\mu}=\mathfrak{H}/\ker\mu\times\mathfrak{H}/\mathfrak{N}\mathfrak{N}_1$, namely,

$$(\mathfrak{H}/\ker\bar{\mu},\ \bar{\mu}^{-1},\ \eta_{\mathfrak{H}/\ker\bar{\mu}\to\mathfrak{H}/\mathfrak{N}\mathfrak{N}_1})=0.$$

Thus we know (32) by Prop. 1. From (30) and (31) follows

$$(33)\qquad (\mathfrak{H}/\ker\chi,\ \chi^{-1},\ \eta_{\mathfrak{H}/\ker\chi\to\mathfrak{H}/\mathfrak{N}})\neq 0\quad\text{in }\mathrm{Ext}\,(\mathfrak{H}/\mathfrak{N},\ GF(p)).$$

On the other hand, take $\chi'(\neq 0)$ in $(\mathfrak{N}/(\mathfrak{N}\cap\langle\sigma_1^p\rangle\delta_{\mathfrak{H}}(\mathfrak{H}))\delta_{\mathfrak{G}}(\mathfrak{N}))^\wedge$. Since there is a canonical surjective homomorphism $\langle\sigma_1^p\rangle\mathfrak{N}\delta_{\mathfrak{H}}(\mathfrak{H})/\langle\sigma_1^p\rangle\delta_{\mathfrak{H}}(\mathfrak{H})\to\mathfrak{N}/\mathfrak{N}\cap\langle\sigma_1^p\rangle\delta_{\mathfrak{H}}(\mathfrak{H}))\delta_{\mathfrak{G}}(\mathfrak{N}))$ and the left hand side is contained in the elementary abelian group $\mathfrak{H}/\langle\sigma_1^p\rangle\delta_{\mathfrak{H}}(\mathfrak{H})$, χ' can be extended to $\mathfrak{H}\to GF(p)$. So,

$$(34)\qquad (\mathfrak{H}/\ker\chi',\ \chi'^{-1},\ \eta_{\mathfrak{H}/\ker\chi'\to\mathfrak{H}/\mathfrak{N}})=0\quad\text{in }\mathrm{Ext}\,(\mathfrak{H}/\mathfrak{N},\ GF(p))$$

similarly as the former case of $\bar{\mu}$. Thus from (33) and (34) we have

$$\chi\neq\chi'.$$

This proves (28).

The proof of (29) can be given similarly as that of (28). Namely, take $\chi(\neq 0)$ in $(\mathfrak{N}/(\mathfrak{N}\cap\mathfrak{N}_2)\delta_{\mathfrak{G}}(\mathfrak{N}))^\wedge$. We have only to prove

$$(35)\qquad (\mathfrak{H}/\ker\chi,\ \chi^{-1},\ \eta_{\mathfrak{H}/\ker\chi\to\mathfrak{H}/\mathfrak{N}})\neq 0.$$

Put

$\mathfrak{H}_2=$ the subgroup of $\mathfrak{H}$ generated by the set $\{\sigma_1^p,\ \sigma_i^{1-\sigma_1^\mu},\ \sigma_j^{\sigma_1^\nu}\mid 2\leqq i\leqq d(\mathfrak{G}/\mathfrak{N}),\ 1\leqq\mu<p,\ d(\mathfrak{G}/\mathfrak{N})<j\leqq d(\mathfrak{G}),\ 0\leqq\nu<p\}$

$\mathfrak{C}_2=$ the normal subgroup of $\mathfrak{H}$ generated by $\{\sigma_2,\ \cdots,\ \sigma_{d(\mathfrak{G}/\mathfrak{N})}\}$.

If we take $\mathfrak{N}_2\cap\mathfrak{H}$, $\mathfrak{H}_2$, and $\mathfrak{C}_2$ instead of $\mathfrak{N}_1$, $\mathfrak{H}_1$, and $\mathfrak{C}_1$ respectively and use the canonical isomorphism $\mathfrak{H}/\mathfrak{C}_2 \cong \mathfrak{H}_2$, (35) can be proved similarly.

(VIII) From (24), (27) and (28), we can conclude

$$\dim(\mathfrak{N}/\delta_{\mathfrak{G}}(\mathfrak{N}))^{\wedge} \geqq p^{-1}f(p(c-1)+d(\mathfrak{G}/\mathfrak{N})-c)+d(\mathfrak{G})-c \tag{36}$$

and from (25), (27) and (29), we have

$$\dim(\mathfrak{N}/\delta_{\mathfrak{G}}(\mathfrak{N}))^{\wedge} \geqq f(d(\mathfrak{G}/\mathfrak{N})-1)+d(\mathfrak{G})-c\,. \tag{37}$$

(36) and (37) imply (10) if we use the proporties of f, q. e. d.

§ 3. Example of f.

Take $x=1$ in II in the Theorem. Then as a necessary condition for f in the Theorem we have

II′ $\quad f(d-1)+d-1 \geqq f(d)$ for any natural number d.

The largest possible function satisfying I and II′ is $f(x)=\frac{x(x-1)}{2}$ and the number $\frac{d(d-1)}{2}$ is in fact equal to the number of the relations of free albian pro-p-group with d-generators. Therefore it will be meaningfull to find the largest possible function $f(x)$ defined on $[0, \infty)$ in the form

$$f(x)=k\frac{x(x-1)}{2}\,; \qquad 0<k\leqq 1\,. \tag{38}$$

The condition II becomes here

$$\max\left(p^{-1}k\frac{(p(x-1)+d-x)(p(x-1)+d-x-1)}{2},\; k\frac{(d-1)(d-2)}{2}\right)+d-x \geqq k\frac{d(d-1)}{2}\,; \quad 1\leqq x\leqq d\,. \tag{39}$$

After elementary calculations, we know

$$\min_{1\leqq x\leqq d}\left[\max\left(p^{-1}k\frac{(p(x-1)+d-x)(p(x-1)+d-x-1)}{2},\; k\frac{(d-1)(d-2)}{2}\right)+d-x\right]$$

$$=k\frac{(d-1)(d-2)}{2}+d-\frac{1+2p-2d+\sqrt{1+4p(d-1)(d-2)}}{2(p-1)}\,.$$

Hence (39) is equivalent to

$$k\leqq 1-\frac{3-2d+\sqrt{1+4p(d-1)(d-2)}}{2(p-1)(d-1)}\,.$$

Since

$$1-\frac{3-2d+\sqrt{1+4p(d-1)(d-2)}}{2(p-1)(d-1)}>1-\frac{3-2d+\sqrt{4p(d-3/2)^2}}{2(p-1)(d-1)}$$

$$=1-\frac{(2d-3)(\sqrt{p}-1)}{2(p-1)(d-1)}>1-\frac{\sqrt{p}-1}{p-1}=\frac{\sqrt{p}}{\sqrt{p}+1}$$

we can take

$$k=\frac{\sqrt{p}}{\sqrt{p}+1}$$

in (38). Thus we have

COROLLARY. *For any finite p-group G, it holds that*

$$r(G)\geqq\frac{\sqrt{p}}{\sqrt{p}+1}\frac{d(G)(d(G)-1)}{2}. \tag{40}$$

§ 4. An application to the existence of infinite class field towers.

Let k be an algebraic number field or an algebraic function field of one variable over a finite constant field. Put

$\rho=$ the number of generators of the Galois group of the unramified maximal (abalian) p-extension (not containing the constant field extension in the case of a function field)

$$\delta=\begin{cases}0 & \text{if char } k=p \text{ or char } k\neq p \text{ and } k\not\ni\sqrt[p]{1}\\ 1 & \text{if char } k\neq p \text{ and } k\ni\sqrt[p]{1}\end{cases}$$

$$r=\begin{cases}r_1+r_2-1 & \text{in the usual sense if } k \text{ is an algebraic number field}\\ 0 & \text{if } k \text{ is an algebraic function field.}\end{cases}$$

Then from our Theorem and one of [5] or [3] (in case of an algebraic number field) and from our Theorem, [3] and [1] (in case of an algebraic function field*) we have the following consequence. Namely,

" If

$$\rho+\delta+r\leqq\frac{\sqrt{p}}{\sqrt{p}+1}\frac{\rho(\rho-1)}{2}, \tag{41}$$

then the maximal unramified p-extension over k (independent of the constant field extension in the case of function field) is of infinite degree".

For example, under the condition $\delta=r=0$ and $p\geqq5$, (41) holds for $\rho\geqq4$. Hence in this case the maximal unramified p-extension has infinite degree.

---

* [6] or [3] asserts that the number of relations of the Galois group of the maximal unramified p-extension over a finite algebraic number field is atmost $\rho+\delta+r$. Since [3] uses only the Reichardt's Theorem [5], which is included in the results of [1] where only the class field theory is used, the similar assertion holds in the case of our algebraic function field.

This is an improvement of a similar result in [2] where the same conclusion holds if $\rho \geqq 6$.

Osaka University

References

[1] Y. Akagawa, The extension of groups and the imbedding of field, Osaka Math. J., **12** (1960), 195–215.

[2] E. S. Golod and I. R. Safarevic, On the class field tower, Izv. Akad. Nauk SSSR. Ser. Mat., **28** (1964), 261–272 (Russian).

[3] H. Koch, p-Erweiterungen mit vorgegebenen Verzweigungsstellen, J. reine angew. Math., **219** (1965), 30–61.

[4] A. G. Kurosh, Theory of groups, vol. II, New York, 1965.

[5] H. Reichardt, Konstruktion von Zahlkörpern mit gegebener Galoisgruppe von Primzahlpotenzordnung, J. reine angew. Math., **177** (1937), 1–5.

[6] I. R. Safarevic, Extension with given points of ramification (in Russian, with résumé in France), Publ. Math. I. H. E. S., No. 18, 1964, 71–95.

[7] J. P. Serre, Cohomologie galoisienne, Lect. Note in Math., Springer, 1964.