N. Nakagoshi
Nagoya Math. J.
Vol. 73 (1979), 41-60

THE STRUCTURE OF THE MULTIPLICATIVE GROUP OF RESIDUE CLASSES MODULO $\mathfrak{p}^{N+1}$

NORIKATA NAKAGOSHI

§1. Introduction

Let k be an algebraic number field of finite degree and $\mathfrak{p}$ be a prime ideal of k, lying above a rational prime p. We denote by $G(\mathfrak{p}^{N+1})$ the multiplicative group of residue classes modulo $\mathfrak{p}^{N+1}$ ($N \geqq 0$) which are relatively prime to $\mathfrak{p}$. The structure of $G(\mathfrak{p}^{N+1})$ is well-known, when $N = 0$, or k is the rational number field $\boldsymbol{Q}$. If k is a quadratic number field, then the direct decomposition of $G(\mathfrak{p}^{N+1})$ is determined by A. Ranum [6] and F.H-Koch [4] who gives a basis of a group of principal units in the local quadratic number field according to H. Hasse [2]. In [5, Theorem 6.2], W. Narkiewicz obtains necessary and sufficient conditions so that $G(\mathfrak{p}^{N+1})$ is cyclic, in connection with a group of units in the $\mathfrak{p}$-adic completion of k.

The structure of $G(\mathfrak{p}^{N+1})$ is confirmed by that of the p-Sylow subgroup and the p-rank of $G(\mathfrak{p}^{N+1})$ is given by T. Takenouchi [8]. If an algebraic number field k contains a primitive p-th root of unity, the p-rank is also given by H. Hasse [3, Teil I_a, § 15].

In the present paper we shall establish the direct decomposition of $G(\mathfrak{p}^{N+1})$ for each N which gives another proof of T. Takenouchi's results [8].

§ 2. Notation and an outline of the investigation

Let e and f be the ramification index and the degree of $\mathfrak{p}$ over $\boldsymbol{Q}$, respectively. Put $e_1 = \left[\dfrac{e}{p-1}\right]$, where $[x]$ is the maximal integer $\leqq x$. We denote by $Z(m)$ a cyclic group of order m.

Let H_{N+1} be the $(N+1)$-th unit group of the $\mathfrak{p}$-adic completion $k_{\mathfrak{p}}$ of k, that is,

Received October 3, 1977.

$$H_{N+1} = \{\eta \in k_{\mathfrak{p}} \mid \eta \equiv 1 \bmod \mathfrak{p}^{N+1}\} \qquad (N = 0, 1, \cdots) .$$

H_1 is called a group of principal units of $k_{\mathfrak{p}}$. Then one verifies easily that

$$G(\mathfrak{p}^{N+1}) \cong Z(p^f - 1) \times H_1/H_{N+1} \qquad \text{(direct)} ,$$

whence H_1/H_{N+1} is isomorphic to the p-Sylow subgroup of $G(\mathfrak{p}^{N+1})$.

Let $b_N(\nu)$ be a number of elements of a basis of H_1/H_{N+1} whose orders are exactly $p^\nu (\nu \geqq 1)$. Then H_1/H_{N+1} is expressed as direct product:

$$H_1/H_{N+1} \cong \prod_{\nu=1}^{\infty} (\underbrace{Z(p^\nu) \times \cdots \times Z(p^\nu)}_{b_N(\nu)\text{-times}}) .$$

For our purpose it will suffice to establish a basis of H_1/H_{N+1} for each $N \geqq 0$.

For any multiplicative group G we denote by G^{p^ν} a subgroup of G generated by σ^{p^ν} where $\sigma \in G$ and $\nu \geqq 1$. We define the p-rank R_N of $G(p^{N+1})$ by

$$p^{R_N} = (G(\mathfrak{p}^{N+1}) : G(\mathfrak{p}^{N+1})^p) .$$

R_N will be given by Theorem 1 in § 3.

We let π be a prime element of $k_{\mathfrak{p}}$, fixed once for all. Put

$$(1) \qquad -p = \varepsilon \pi^e ,$$

where ε is a unit of $k_{\mathfrak{p}}$. Moreover, we let $\{\omega_i\}_{1 \leqq i \leqq f}$ be a system of representatives in $k_{\mathfrak{p}}$ for a basis of the residue class field modulo $\mathfrak{p}$ over the prime field.

Let $\boldsymbol{Z}_p$ be the ring of p-adic integers. Then H_1 is a multiplicative $\boldsymbol{Z}_p$-group and its system of generators over $\boldsymbol{Z}_p$ is given by H. Hasse [2].

THEOREM A (H. Hasse [2]). *Suppose that $k_{\mathfrak{p}}$ does not contain a primitive p-th root of unity. Put*

$$\eta_{is} = 1 + \omega_i \pi^s \qquad \begin{pmatrix} i = 1, \cdots, f \\ 1 \leqq s \leqq pe/(p-1),\ s \not\equiv 0 \bmod p \end{pmatrix} .$$

Then $\{\eta_{is}\}$ is a $\boldsymbol{Z}_p$-basis of H_1.

Let ζ_μ be a primitive p^μ-th root of unity for each $\mu \geqq 0$. Then we have

THEOREM B (H. Hasse [2]). *Suppose that $k_\mathfrak{p}$ contains ζ_μ ($\mu \geqq 1$), but does not contain $\zeta_{\mu+1}$. Let λ and e_0 be integers such that*

$$e = \varphi(p^\lambda)e_0 ,$$

where φ is Euler's function and e_0 is prime to p. Put

$$\eta_{is} = 1 + \omega_i\pi^s \qquad \begin{pmatrix} i = 1, \cdots, f \\ 1 \leqq s \leqq e + e_1 = pe/(p-1), s \not\equiv 0 \bmod p \end{pmatrix},$$
$$\eta_* = 1 + \omega_0\pi^{e+e_1}$$

where $\omega_1, \cdots, \omega_f$ satisfy the following conditions:

$$\omega_1^{p^\lambda} - \varepsilon\omega_1^{p^{\lambda-1}} \equiv 0 \bmod \mathfrak{p} , \qquad \omega_i^{p^\lambda} - \varepsilon\omega_i^{p^{\lambda-1}} \not\equiv 0 \bmod \mathfrak{p} \ (2 \leqq i \leqq f)$$

and ω_0 is a unit of $k_\mathfrak{p}$ for which a congruence

$$X^p - \varepsilon X \equiv \omega_0 \bmod \mathfrak{p}$$

has no solution X in $k_\mathfrak{p}$.

Then $\{\eta_{is}, \eta_*\}$ is a system of generators of H_1 over Z_p.

We note that $\lambda \geqq \mu$.

Now we sketch a plan to determine a basis of H_1/H_{N+1}. Let $\mu e + e_1 \leqq N < (\mu+1)e + e_1$ and $t \geqq 1$. Then we see by Lemma 7 in §5 that if $\mu = 0$, $b_{te+N}(\nu + t) = b_N(\nu)$; if $\mu \geqq 1$, $b_{te+N}(\mu) = 1 + b_N(\mu - t)$, $b_{te+N}(\mu + t) = b_N(\mu) - 1$ and $b_{te+N}(\nu + t) = b_N(\nu)$, where $\nu \not\equiv \mu$ and $\nu + t \not\equiv \mu$. Hence it is enough to compute $b_N(\nu)$ for $0 \leqq N < (\mu+1)e + e_1$.

We assume that $k_\mathfrak{p}$ contains ζ_μ ($\mu \geqq 0$) but does not contain $\zeta_{\mu+1}$.

First suppose that $\mu = 0$. Let $\eta_{is}H_{N+1}$ be cosets of H_{N+1} in H_1, where η_{is} are principal units defined by Theorem A. From Theorem A a system of canonical generators for H_1/H_{N+1} is given by

$$\{\eta_{is}H_{N+1}\} , \tag{2}$$

where $1 \leqq i \leqq f, 1 \leqq s \leqq \min(N, pe/(p-1))$ and $s \not\equiv 0 \bmod p$. Let $g_N(\nu)$ be a number of generators of (2) such that $\eta_{is}^{p^\nu} \equiv 1 \bmod \mathfrak{p}^{N+1}$. In §5 we shall prove

$$g_N(1) + \sum_{\nu=2}^{\infty} \nu(g_N(\nu) - g_N(\nu - 1)) = Nf \tag{3}$$

(see (17) in §5), hence (2) is a basis of H_1/H_{N+1}. Then $b_N(\nu)$ are given as follows:

$$(4) \qquad \begin{cases} b_N(1) = g_N(1) , \\ b_N(\nu) = g_N(\nu) - g_N(\nu - 1) \qquad (\nu \geqq 2) . \end{cases}$$

Furthermore, we shall compute orders $p^{\nu(N:i,s)}$ of η_{is} modulo $\mathfrak{p}^{N+1}$, using Corollary 8 in § 5. Then we can determine a basis of H_{N+1} for each N (see Proposition 11 in § 5). Since a basis of H_1 is given by Theorem A, the direct decomposition of H_1/H_{N+1} is easily obtained.

Secondly we assume $\mu \geqq 1$. Put

$$(5) \qquad \begin{aligned} S = \{(i, s) \mid 1 \leqq i \leqq f, 1 \leqq s \leqq e + e_1 = pe_1 , \\ s \not\equiv 0 \bmod p, (i, s) \neq (1, e_0)\} . \end{aligned}$$

The number of elements of S is equal to $(ef - 1)$. If $\lambda = \mu$, then $\eta_{1e_0} = \zeta_\mu$ and $\{\eta_*, \eta_{is}\}_{(i,s)\in S}$ is a Z_p-basis of H_1([2, p. 232]). If $\lambda > \mu$, then we observe by [2, p. 231] that

$$(6) \qquad \eta_{1e_0}^{p^{\lambda-\mu}} = \zeta_\mu \cdot \eta_*^{\beta_*} \prod_{(i,s)\in S} \eta_{is}^{\beta_{is}} ,$$

where β_* and β_{is} are p-adic integers. Let H_{01} be a multiplicative Z_p-group generated by $\{\eta_*, \eta_{is}\}_{(i,s)\in S}$. Then by [2, p. 230] we have a direct decomposition of H_{01}:

$$(7) \qquad H_{01} = \langle \eta_* \rangle \times \prod_{(i,s)\in S} \langle \eta_{is} \rangle \qquad \text{(direct)} ,$$

where $\langle \eta \rangle$ stands for a cyclic group generated by η.

Let $\eta_* H_{N+1}, \eta_{is} H_{N+1}$ be cosets of H_{N+1} in H_1 and $p^{\nu(N:*)}, p^{\nu(N:i,s)}$ be their orders in H_1/H_{N+1}, respectively. From Theorem B we have a system of canonical generators for H_1/H_{N+1} as follows:

$$(8_1) \qquad \{\eta_{is} H_{N+1}\} , \qquad \text{if } 1 \leqq N < e + e_1 ,$$

$$(8_2) \qquad \{\eta_* H_{N+1}, \eta_{is} H_{N+1}\} , \qquad \text{if } e + e_1 \leqq N ,$$

where $1 \leqq i \leqq f, 1 \leqq s \leqq \min(N, e + e_1)$ and $s \not\equiv 0 \bmod p$. Let $g_N(\nu)$ be a number of generators defined by (8_1) or (8_2) such that $\eta_{is}^{p^\nu} \equiv 1 \bmod \mathfrak{p}^{N+1}$, $\eta_*^{p^\nu} \equiv 1 \bmod \mathfrak{p}^{N+1}$. Then (8_1) or (8_2) is a basis of H_1/H_{N+1} if and only if the equality (3) holds. It will be proved by (17) in § 5 that (i) (8_1) is a basis of H_1/H_{N+1}, (ii) (8_2) is a basis of H_1/H_{N+1} if and only if $\nu(N: 1, e_0) = \lambda$. If the equality (3) holds, then $b_N(\nu)$ are given by (4).

If $N \geqq e + e_1$ and $\nu(N: 1, e_0) \neq \lambda$, then it will be possible to determine a basis of H_{N+1} (see Proposition 11 in § 5) and we observe that

H_{N+1} is a subgroup of H_{01}. Hence we can find a relation between η_*, η_{1e_0} and η_{is} modulo $\mathfrak{p}^{N+1}$ (see (18) in § 6) which is induced by (6). Let $\boldsymbol{Z}$ be the ring of rational integers. Let M be a free $\boldsymbol{Z}$-module generated by $\tilde{\eta}_*, \tilde{\eta}_{1e_0}$ and $\tilde{\eta}_{is}$ $((i,s)\in S)$. Let $\psi: M \to H_1/H_{N+1}$ be a homomorphism defined by $\psi(\tilde{\eta}_*) \equiv \eta_* \bmod \mathfrak{p}^{N+1}$, $\psi(\tilde{\eta}_{1e_0}) \equiv \eta_{1e_0} \bmod \mathfrak{p}^{N+1}$ and $\psi(\tilde{\eta}_{is}) \equiv \eta_{is} \bmod \mathfrak{p}^{N+1}$. Then we shall have a system of canonical generators for $\operatorname{Ker}\psi$. Hence the direct decomposition of $H_1/H_{N+1} \cong M/\operatorname{Ker}\psi$ will be obtained using elementary divisors of a certain matrix (see (9) of Theorem 3) whose entries are $p^{\nu(N:i,s)}$, $p^{\nu(N:*)}$ and p-components of exponents appearing in the relation (18) in § 6.

§ 3. Theorems

We shall prove the following assertions:

THEOREM 1 (cf. [3] and [8]). *The p-rank R_N of $G(\mathfrak{p}^{N+1})$ is given by*

$$R_N = \begin{cases} \left(N - \left[\dfrac{N}{p}\right]\right)f\,, & \text{if } 0 \leqq N < e + e_1\,, \\ ef\,, & \text{if } N \geqq e + e_1 \text{ and } k_{\mathfrak{p}} \not\ni \zeta_1\,, \\ ef + 1\,, & \text{if } N \geqq e + e_1 \text{ and } k_{\mathfrak{p}} \ni \zeta_1\,. \end{cases}$$

THEOREM 2. *Suppose that $k_{\mathfrak{p}}$ does not contain ζ_1. Let $0 \leqq N \leqq e + e_1$. Then it follows that for each $t \geqq 0$*

$$G(\mathfrak{p}^{te+N+1}) \cong Z(p^f - 1) \times \prod_{\nu=1}^{\infty} (\underbrace{Z(p^{\nu+t}) \times \cdots \times Z(p^{\nu+t})}_{b_N(\nu)\text{-times}})$$
$$\times (\underbrace{Z(p^t) \times \cdots \times Z(p^t)}_{(R_{te+N}-R_N)\text{-times}})$$

where R_{te+N}, R_N are p-ranks of $G(\mathfrak{p}^{te+N+1})$, $G(\mathfrak{p}^{N+1})$, respectively, and

$$b_N(\nu) = \left(\left[\frac{N}{p^{\nu-1}}\right] - 2\left[\frac{N}{p^{\nu}}\right] + \left[\frac{N}{p^{\nu+1}}\right]\right)f\,.$$

THEOREM 3. *Suppose that $k_{\mathfrak{p}}$ contains ζ_μ $(\mu \geqq 1)$ but does not contain $\zeta_{\mu+1}$. Let λ and e_0 be as in Theorem* B. *Then the direct decomposition of $G(\mathfrak{p}^{N+1})$ is expressed as follows*:

(I) *In the case where $1 \leqq N < e + e_1$,*

$$G(\mathfrak{p}^{N+1}) \cong Z(p^f - 1) \times \prod_{\nu=1}^{\infty} (\underbrace{Z(p^{\nu}) \times \cdots \times Z(p^{\nu})}_{b_N(\nu)\text{-times}})\,,$$

where $b_N(\nu)$ are equal to those of Theorem 2.

(II) *In the case where* $e + e_1 \leqq N < (\mu + 1)e + e_1$ *and* $\nu(N:1, e_0) = \lambda$,

$$G(\mathfrak{p}^{N+1}) \cong Z(p^f - 1) \times \prod_{\nu=1}^{\infty} (\underbrace{Z(p^\nu) \times \cdots \times Z(p^\nu)}_{b_N(\nu)\text{-times}});$$

$b_N(\nu)$ *are given as follows*:

Let a *be a rational integer* $(1 \leqq a \leqq \mu)$ *such that* $ae + e_1 \leqq N < (a + 1)e + e_1$.

For $\nu \leqq a - 1$, $b_N(\nu) = 0$.

For $\nu = a$, $b_N(a) = \left((a + 1)e - N + \left[\frac{N - ae}{p}\right]\right)f + \beta_N(a)$.

For $\nu \geqq a + 1$,

$$b_N(\nu) = \left(\left[\frac{N - (a + \delta - 1)e}{p^{\nu-a-\delta}}\right] - 2\left[\frac{N - (a + \delta - 1)e}{p^{\nu-a-\delta+1}}\right] + \left[\frac{N - (a + \delta - 1)e}{p^{\nu-a-\delta+2}}\right]\right)f + \beta_N(\nu),$$

where

$$\beta_N(a) = \begin{cases} 2, & \text{if } a = \lambda = \mu, \\ 1, & \text{if } a \neq \lambda, \end{cases} \qquad \beta_N(\nu) = \begin{cases} 1, & \text{if } \nu = \lambda \geqq a + 1, \\ -1, & \text{if } \nu = \lambda + a, \\ 0, & \text{otherwise } (\nu \geqq a + 1) \end{cases}$$

and

$$\delta = \begin{cases} 0, & \text{if } N = ae + e_1, \\ 1, & \text{if } ae + e_1 < N < (a + 1)e + e_1. \end{cases}$$

(III) *In the case where* $e + e_1 < N < (\mu + 1)e + e_1$ *and* $\nu(N:1, e_0) > \lambda$, *there exists a rational integer* $a\,(1 \leqq a \leqq \mu)$ *such that* $ae + e_1 \leqq N < (a + 1)e + e_1$. *Let* $p^{a'_{is}}$ *be p-components of* $\beta_{is}p^\mu$ *where* β_{is} *are p-adic integers defined by* (6). *Put*

$$a_{is} = \min\{\nu(N:i, s), a'_{is}\} \qquad \text{for } (i, s) \in S,$$

where S *is given by* (5). *If* $N = ae + e_1$ *and* $(e + e_1)/p^{\nu-a+1} < s \leqq (e + e_1)/p^{\nu-a}$, *then* $\nu(N:i, s) = \nu \geqq a$; *if* $ae + e_1 < N < (a + 1)e + e_1$ *and* $(N - ae)/p^{\nu-a} < s \leqq (N - ae)/p^{\nu-a-1}$, *then* $\nu(N:i, s) = \nu \geqq a$. *Let* $p^{c_0}, p^{c_1}, \cdots, p^{c_{ef}}$ *be elementary divisors of the following* $(ef + 2) \times (ef + 1)$-*matrix*

$$
(9) \qquad \begin{bmatrix}
p^{a} & & & & & & & & \\
 & p^{\nu(N:1,e+e_1-1)} & & & & & & & \\
 & & \ddots & & & & & 0 & \\
 & & & p^{\nu(N:i,s)} & & & & & \\
 & & & & \ddots & & & & \\
 & 0 & & & & p^{\nu(N:1,e_0)} & & & \\
 & & & & & & \ddots & & \\
 & & & & & & & p^{\nu(N:f,e_0)} & \\
 & & & & & & & & \ddots \\
 & & & & & & & & p^{\nu(N:f,1)} \\
p^{a} & p^{a_{1,e+e_1-1}} \cdots & p^{a_{is}} \cdots & p^{\lambda} \cdots & p^{a_{fe_0}} \cdots & p^{a_{f1}} & & &
\end{bmatrix} (i,s) \in S
$$

It then follows that

$$G(\mathfrak{p}^{N+1}) \cong Z(p^f - 1) \times Z(p^{c_0}) \times Z(p^{c_1}) \times \cdots \times Z(p^{c_{ef}}) .$$

(IV) *In the case where* $\mu e + e_1 \leqq N < (\mu + 1)e + e_1$, *we let* $G(\mathfrak{p}^{N+1})$ *be of type* $(p^f - 1, p^{\mu}, p^{d_1}, \cdots, p^{d_{ef}})$ *which is determined by* (II) *and* (III). *Then* $G(\mathfrak{p}^{te+N+1})$ *is of type* $(p^f - 1, p^{\mu}, p^{d_1+t}, \cdots, p^{d_{ef}+t})$ *for each* $t \geqq 0$.

Remarks. Under the hypothesis of Theorem 3 (i) if $\lambda = \mu$ and $N \geqq e + e_1$, then $\nu(N:1, e_0) = \lambda$ (cf. [2, p. 216]); (ii) if $N = ae + e_1$, then $\lambda \leqq \nu(N:1, e_0) \leqq \lambda + a - 1$; (iii) if $ae + e_1 < N < (a + 1)e + e_1$, then $\lambda \leqq \nu(N:1, e_0) \leqq \lambda + a$ (cf. proof of Corollary 10 of § 5); (iv) if $N \geqq \mu e + e_1$, then H_{N+1} is a subgroup of a free part of H_1.

COROLLARY 4. *If* $\mathfrak{p}$ *is an unramified prime ideal of* k, *lying above a rational prime* p, *then we have*

$$G(\mathfrak{p}^{N+1}) \cong \begin{cases} Z(p^f - 1) \times \underbrace{Z(p^N) \times \cdots \times Z(p^N)}_{f\text{-times}} , & \text{if } p \geqq 3 , \\ Z(2^f - 1) \times Z(2) \times Z(2^{N-1}) \times \underbrace{Z(2^N) \times \cdots \times Z(2^N)}_{(f-1)\text{-times}} , & \\ & \text{if } p = 2 . \end{cases}$$

§ 4. Proof of Theorem 1

It follows from (1) that

LEMMA 5 (cf. [2, p. 220] and [3, Teil I_a, § 15]). *Let* γ *be an integer of* $k_{\mathfrak{p}}$. *Then*

$$(1+\gamma\pi^s)^p \equiv \begin{cases} 1+\gamma^p\pi^{ps} \bmod \mathfrak{p}^{ps+1}\,, & if\ 1 \leqq s < e/(p-1)\,, \\ 1+(\gamma^p-\varepsilon\gamma)\pi^{ps} \bmod \mathfrak{p}^{ps+1}\,, & if\ s = e/(p-1)\,, \\ 1-\varepsilon\gamma\pi^{s+e} \bmod \mathfrak{p}^{s+e+1}\,, & if\ if\ s > e/(p-1)\,. \end{cases}$$

Now we shall prove Theorem 1. First we note that $k_{\mathfrak{p}}$ contains a primitive p-th root of unity if and only if $e \equiv 0 \bmod (p-1)$ and a congruence

$$(*)\qquad X^p - \varepsilon X \equiv 0 \bmod \mathfrak{p}$$

has a solution $X \not\equiv 0 \bmod \mathfrak{p}$ in $k_{\mathfrak{p}}$ (cf. [2, p. 215]).

According to H. Hasse [3], we shall use the following notation:

α: a number of $k_{\mathfrak{p}}$, prime to $\mathfrak{p}$.
γ: an integer of $k_{\mathfrak{p}}$.
γ_0: an integer of $k_{\mathfrak{p}}$ such that $\gamma_0 \equiv 0 \bmod \mathfrak{p}$.
η: a principal unit of $k_{\mathfrak{p}}$.
μ_s: an integer of $k_{\mathfrak{p}}$ such that $\mu_s \equiv \alpha^p \bmod \mathfrak{p}^s$ $(s \geqq 1)$.
α_s: an integer of $k_{\mathfrak{p}}$ such that $\alpha_s^p \equiv 1 \bmod \mathfrak{p}^s$.
γ_s: an integer of $k_{\mathfrak{p}}$ such that

$$(10)\qquad \alpha_s^p \equiv 1+\gamma_s\pi^s \bmod \mathfrak{p}^{s+1}\,.$$

Each of these notations stands for a general element of a group, but will sometimes be used to stand for the group itself. The p-rank R_N of $G(p^{N+1})$ is then given by

$$(11)\qquad \begin{aligned} p^{R_N} &= (G(\mathfrak{p}^{N+1}) : G(\mathfrak{p}^{N+1})^p) = (\alpha : \mu_{N+1}) \\ &= (\alpha:\mu_1)(\mu_1:\mu_2)\cdots(\mu_N:\mu_{N+1}) \end{aligned}$$

and we have

$$(12)\qquad (\mu_s:\mu_{s+1}) = (\gamma:\gamma_s) \qquad (1 \leqq s \leqq N)\,.$$

It will be verified that

$$(a)\qquad (\alpha:\mu_1) = 1\,,$$

$$(b)\qquad (\mu_s:\mu_{s+1}) = \begin{cases} 1\,, & \text{if } 1 \leqq s < e+e_1 \text{ and } s \equiv 0 \bmod p\,, \\ p^f\,, & \text{if } 1 \leqq s < e+e_1 \text{ and } s \not\equiv 0 \bmod p\,, \end{cases}$$

$$(c)\qquad (\mu_{e+e_1}:\mu_{e+e_1+1}) = \begin{cases} 1\,, & \text{if } e \equiv 0 \bmod (p-1) \text{ and } k_{\mathfrak{p}} \not\ni \zeta_1\,, \\ p\,, & \text{if } k_{\mathfrak{p}} \ni \zeta_1\,, \\ p^f\,, & \text{if } e \not\equiv 0 \bmod (p-1)\,, \end{cases}$$

$$(d)\qquad (\mu_s:\mu_{s+1}) = 1\,, \qquad \text{if } s > e+e_1\,.$$

Proof of (*a*). Since $(\alpha:\mu_1)=(\alpha:\alpha^p\eta)$ is a power of p and α/η is a cyclic group of order $(p^f-1), (\alpha:\mu_1)=1$.

Proof of (*b*), (*c*) *and* (*d*). Since $\alpha_s^p\equiv 1 \bmod \mathfrak{p}$ and the order of $G(\mathfrak{p})$ is equal to p^f-1 which is prime to p, $\alpha_s\equiv 1 \bmod \mathfrak{p}$. If $\alpha_s=1$, then by (10) we see that $\gamma_s\equiv 0 \bmod \mathfrak{p}$. Let $\alpha_s\neq 1$. We can put

$$\alpha_s=1+\varepsilon_s\pi^{\bar{s}}\ ,$$

where $\bar{s}\geqq 1$ and ε_s is a unit of $k_{\mathfrak{p}}$. Then it follows from Lemma 5

$$\alpha_s^p\equiv\begin{cases}1+\varepsilon_s^p\pi^{p\bar{s}} \bmod \mathfrak{p}^{p\bar{s}+1}\ , & \text{if } 1\leqq\bar{s}<e/(p-1)\ ,\\ 1+(\varepsilon_s^p-\varepsilon\varepsilon_s)\pi^{p\bar{s}} \bmod \mathfrak{p}^{p\bar{s}+1}\ , & \text{if } \bar{s}=e/(p-1)\ ,\\ 1-\varepsilon\varepsilon_s\pi^{\bar{s}+e} \bmod \mathfrak{p}^{\bar{s}+e+1}\ , & \text{if } \bar{s}>e/(p-1)\ .\end{cases}$$

If $1\leqq s<e+e_1$ and $s\equiv 0 \bmod p$, then by (10) γ_s modulo $\mathfrak{p}$ contains $(\varepsilon_s^p+\gamma_0)$ modulo $\mathfrak{p}$. Hence $(\gamma:\gamma_s)=1$, because of $(\gamma:\gamma_s)\leqq(\gamma:\varepsilon_s^p+\gamma_0)=1$.

Suppose that $1\leqq s<e+e_1$ and $s\not\equiv 0 \bmod p$. Then from the above congruences and (10) we can conclude that

$$\begin{cases}\gamma_s\equiv 0 \bmod \mathfrak{p}\ , & \text{if } 1\leqq\bar{s}<e/(p-1) \text{ and } s<p\bar{s}\ ,\\ \varepsilon_s^p\pi^{p\bar{s}}\equiv 0 \bmod \mathfrak{p}^{p\bar{s}+1}, \text{ a contradiction}\ , & \text{if } s>p\bar{s}\\ \gamma_s\equiv 0 \bmod \mathfrak{p}\ , & \text{if } \bar{s}\geqq e/(p-1)\ .\end{cases}$$

Hence we have $(\gamma:\gamma_s)=(\gamma:\gamma_0)=p^f$ which shows (b) by (12).

Let $s=e+e_1$. Using the above congruences and (10) we see that

$$\begin{cases}\varepsilon_s^p\pi^{p\bar{s}}\equiv 0 \bmod \mathfrak{p}^{p\bar{s}+1}, \text{ a contradiction}\ , & \text{if } 1\leqq\bar{s}<e/(p-1)\ ,\\ \gamma_s\equiv\varepsilon_s^p-\varepsilon\varepsilon_s \bmod \mathfrak{p}\ , & \text{if } \bar{s}=e/(p-1)\ ,\\ \gamma_s\equiv 0 \bmod \mathfrak{p}\ , & \text{if } \bar{s}>e/(p-1)\ .\end{cases}$$

If $k_{\mathfrak{p}}\ni\zeta_1$, then $\gamma/\gamma_0'\cong((\gamma^p-\varepsilon\gamma)+\gamma_0)/\gamma_0$, where γ_0' are solutions of $X^p-\varepsilon X\equiv 0 \bmod \mathfrak{p}$, and $(\gamma:\gamma_0)/(\gamma:\gamma_0')=p$. Hence $(\gamma:\gamma_s)=(\gamma:(\gamma^p-\varepsilon\gamma)+\gamma_0)=p$. If $e\equiv 0 \bmod (p-1)$ and $k_{\mathfrak{p}}\not\ni\zeta_1$, then $\gamma_s\equiv\varepsilon_s^p-\varepsilon\varepsilon_s\not\equiv 0 \bmod \mathfrak{p}$ and $(\gamma:\gamma_s)=1$. If $e\not\equiv 0 \bmod (p-1)$, then $(\gamma:\gamma_s)=(\gamma:\gamma_0)=p^f$. Therefore (c) is obtained by (12).

Assume that $s>e+e_1$. Then we have by Lemma 5

$$(1+\gamma\pi^{s-e})^p\equiv 1-\varepsilon\gamma\pi^s \bmod \mathfrak{p}^{s+1}\ .$$

Hence by (10) γ_s modulo $\mathfrak{p}$ contains $(-\varepsilon\gamma+\gamma_0)$ modulo $\mathfrak{p}$ and $(\gamma:\gamma_s)=(\gamma:(-\varepsilon\gamma+\gamma_0))=1$, thereby proving (d). By (11) and (12) we have Theorem 1.

For instance, we compute R_N when $N \geqq e + e_1$ and $e \not\equiv 0 \bmod (p-1)$. Put $e = (p-1)e_1 + r, 1 \leqq r \leqq p-2$. Then by (11), (a), (b), (c) and (d) we have

$$R_N = \left(e + e_1 - 1 - \left[\frac{e + e_1 - 1}{p}\right]\right)f + f$$
$$= \left(e + e_1 - 1 - \left[e_1 + \frac{r-1}{p}\right]\right)f + f = ef\,.$$

§ 5. Preliminaries to the proof of Theorem 2 and Theorem 3

In order to prove Theorem 2 and Theorem 3 we need some results which we obtain in this section. Throughout this section we assume that $k_\mathfrak{p}$ contains ζ_μ ($\mu \geqq 0$) but does not contain $\zeta_{\mu+1}$.

The following proposition is well-known:

PROPOSITION 6 (cf. [2, § 15] and [5, Chap. V]). *If $N \geqq e_1$, then H_{N+1} is a free Z_p-group and $H_{N+1} \cong H_{e+N+1}$ by $\eta \to \eta^p$ ($\eta \in H_{N+1}$).*

LEMMA 7. *Suppose that $N \geqq e_1$ and H_{N+1} is a subgroup of a Z_p-free part $\overline{H_{01}}$ of H_1. Let H_1/H_{N+1} be of type $(p^{s_0}, p^{s_1}, \cdots, p^{s_{ef}})$. Then we can take $s_0 = \mu$ and H_1/H_{te+N+1} is of type $(p^{s_0}, p^{s_1+t}, \cdots, p^{s_{ef}+t})$ for each $t \geqq 0$.*

Remark. In Lemma 7 we allow that $s_j = 0$ ($0 \leqq j \leqq ef$).

Proof. We have an expression of H_1 as direct product (cf. [2, p. 222]):

$$H_1 = \langle\zeta_\mu\rangle \times \overline{H_{01}}\,,$$

where $\langle\zeta_\mu\rangle$ is a cyclic group generated by ζ_μ and $\overline{H_{01}}$ is of rank ef. By the hypothesis of the Lemma 7 we have

$$H_1/H_{N+1} \cong \langle\zeta_\mu\rangle \times \overline{H_{01}}/H_{N+1} \qquad \text{(direct)}\,.$$

Hence there exists a Z_p-basis $\{\eta_1, \cdots, \eta_{ef}\}$ of $\overline{H_{01}}$ such that $\{\eta_1^{p^{s_1}}, \cdots, \eta_{ef}^{p^{s_{ef}}}\}$ is a Z_p-basis of H_{N+1}. It then follows from Proposition 6 that $\{\eta_1^{p^{s_1+1}}, \cdots, \eta_{ef}^{p^{s_{ef}+1}}\}$ is a Z_p-basis of H_{e+N+1}. Thus the Lemma 7 is proved by induction. q.e.d.

If $\mu = 0$ and $N \geqq e_1$, then we observe by Lemma 7 that $b_{te+N}(\nu + t) = b_N(\nu)$ for each $t \geqq 0$. Hence all $G(\mathfrak{p}^{N+1})$ are determined by factor groups $H_1/H_1, \cdots, H_1/H_{e+e_1}$. If $\mu \geqq 1$ and $N \geqq \mu e + e_1$, then H_{N+1} is a subgroup of $H_1^{p^\mu} = \{\eta^{p^\mu} \mid \eta \in H_1\}$. Hence H_{N+1} is a subgroup of a free part of H_1. In this case for each $t \geqq 1$ it follows that $b_{te+N}(\mu) = 1 + b_N(\mu - t)$,

$b_{te+N}(\mu+t)=b_N(\mu)-1$ and $b_{te+N}(\nu+t)=b_N(\nu)$, where $\nu\neq\mu$ and $\nu+t\neq\mu$. Hence all $G(\mathfrak{p}^{N+1})$ are determined by factor groups $H_1/H_2,\cdots,H_1/H_{\mu e+e_1}$.

In order to compute $g_N(\nu),\nu(N:i,s)$ and $\nu(N:*)$ defined in §2 we need the following corollary to Lemma 5 (cf. [7] and [9, Corollary 1.2]):

COROLLARY 8. *Let η be an element of $k_{\mathfrak{p}}$ such that $\eta\equiv 1 \bmod \mathfrak{p}^s$ and $\eta\not\equiv 1 \bmod \mathfrak{p}^{s+1}\,(s\geqq 1)$. Let τ be the least non-negative integer such that $p^\tau s\geqq e/(p-1)$. Then*

$$\eta^{p^\nu}\equiv 1 \bmod \mathfrak{p}^{sp^\nu}\,,\quad \eta^{p^\nu}\not\equiv 1 \bmod \mathfrak{p}^{sp^\nu+1}\qquad \textit{for } \nu=0,1,\cdots,\tau$$

and

$$\eta^{p^\nu}\equiv 1 \bmod \mathfrak{p}^{sp^\tau+(\nu-\tau)e}\qquad \textit{for } \nu\geqq\tau\,.$$

More precisely we have the following congruences by (1):

$$(1+\gamma\pi^s)^{p^\nu}$$
$$\equiv\begin{cases}1+\gamma^{p^\nu}\pi^{sp^\nu} \bmod \mathfrak{p}^{sp^\nu+1}\,, & \textit{if } e/(p-1)<p^\tau s \textit{ and } 1\leqq\nu\leqq\tau\,,\\ 1+\gamma^{p^\tau}p^{\nu-\tau}\pi^{sp^\tau} \bmod \mathfrak{p}^{sp^\tau+(\nu-\tau)e+1}\,, & \textit{if } e/(p-1)<p^\tau s \textit{ and } 1\leqq\tau<\nu\,,\\ 1+\gamma^{p^\nu}\pi^{sp^\nu} \bmod \mathfrak{p}^{sp^\nu+1}\,, & \textit{if } e/(p-1)=p^\tau s \textit{ and } 1\leqq\nu\leqq\tau\,,\\ 1+(\gamma^{p^{\tau+1}}-\varepsilon\gamma^{p^\tau})p^{\nu-\tau-1}\pi^{e+e_1} \bmod \mathfrak{p}^{(\nu-\tau)e+e_1+1}\,, & \\ & \textit{if } e/(p-1)=p^\tau s \textit{ and } 0\leqq\tau<\nu\,,\\ 1+\gamma p^\nu\pi^s \bmod \mathfrak{p}^{\nu e+s+1}\,, & \textit{if } e/(p-1)<s\,,\end{cases}$$

where γ is an integer of $k_{\mathfrak{p}}$.

LEMMA 9. *Let η_{is} be principal units defined by Theorem* A *or Theorem* B $(1\leqq i\leqq f, 1\leqq s\leqq pe/(p-1), s\not\equiv 0 \bmod p)$. *Let $1\leqq N<2e+e_1$. Then we have for $\nu\geqq 1$*

$$\eta_{is}^{p^\nu}\not\equiv 1 \bmod \mathfrak{p}^{N+1}$$

if and only if indices i and s satisfy the following conditions:

(i) $1\leqq s\leqq N/p^\nu$, *when* $1\leqq N<e+e_1$;

(ii) $1\leqq s\leqq (e+e_1)/p^\nu$, *but if $\mu\geqq 1$ and $\nu=\lambda$, then $(i,s)\neq(1,e_0)$, when $N=e+e_1$*;

(iii) $1\leqq s\leqq (N-e)/p^{\nu-1}$, *but if $\nu=\lambda$ and $\lambda\geqq\nu(N:1,e_0)$, then $(i,s)\neq(1,e_0)$, when $e+e_1<N<2e+e_1$ and $\mu\geqq 1$.*

Proof. Let τ be the least non-negative integer such that

$$p^{\tau-1}s < e/(p-1) \leqq p^{\tau}s .$$

Let $1 \leqq N < e + e_1$. If $1 \leqq s \leqq N/p^{\nu}$, then $\nu \leqq \tau$, otherwise it follows that $p^{\nu}s = p^{\tau}s \cdot p^{\nu-\tau} \geqq pe/(p-1) \geqq e + e_1 > N$. Hence we see by Corollary 8 that $\eta_{is}^{p^{\nu}} \not\equiv 1 \bmod \mathfrak{p}^{N+1}$. If $N/p^{\nu} < s$, then by Corollary 8 we have $\eta_{is}^{p^{\nu}} \equiv 1 \bmod \mathfrak{p}^{N+1}$.

Let $N = e + e_1$. If $1 \leqq s \leqq N/p^{\nu}$ and $p^{\tau-1}s < e/(p-1) < p^{\tau}s$, then $\nu \leqq \tau$. Hence by Corollary 8 we have $\eta_{is}^{p^{\nu}} \not\equiv 1 \bmod \mathfrak{p}^{N+1}$. If $e \equiv 0 \bmod (p-1)$, we put $e = \varphi(p^{\lambda})e_0, (e_0, p) = 1$. If $1 \leqq s \leqq N/p^{\nu}$ and $p^{\tau}s = e/(p-1)$, then $\nu \leqq \tau + 1$. In this case $s = e_0$ and $\tau = \lambda - 1$, because of $s \not\equiv 0 \bmod \mathrm{p}$. If $\nu \leqq \tau = \lambda - 1$, then by Corollary 8 we have $\eta_{is}^{p^{\nu}} = \eta_{ie_0}^{p^{\nu}} \not\equiv 1 \bmod \mathfrak{p}^{N+1}$. If $\nu = \tau + 1 = \lambda$, then we observe by Corollary 8 that

$$\eta_{is}^{p^{\nu}} = \eta_{ie_0}^{p^{\lambda}} \equiv 1 + (\omega_i^{p^{\lambda}} - \varepsilon\omega_i^{p^{\lambda-1}})\pi^{e+e_1} \bmod \mathfrak{p}^{e+e_1+1} .$$

If $\mu = 0$, then $\eta_{ie_0}^{p^{\lambda}} \not\equiv 1 \bmod \mathfrak{p}^{e+e_1+1}$, because of $\omega_i^{p^{\lambda}} - \varepsilon\omega_i^{p^{\lambda-1}} \not\equiv 0 \bmod \mathfrak{p}$ (cf. (*) of § 4). If $\mu \geqq 1$, then by Theorem B we have

$$\eta_{1e_0}^{p^{\lambda}} \equiv 1 \bmod \mathfrak{p}^{e+e_1+1} , \quad \eta_{ie_0}^{p^{\lambda}} \not\equiv 1 \bmod \mathfrak{p}^{e+e_1+1} \qquad \text{for } i \neq 1 .$$

Suppose that $(e + e_1)/p^{\nu} < s \leqq e + e_1 = N$. If $0 < \nu \leqq \tau$, then by Corollary 8 we get $\eta_{is}^{p^{\nu}} \equiv 1 \bmod \mathfrak{p}^{N+1}$. If $p^{\tau}s > e/(p-1)$ and $0 \leqq \tau < \nu$, then $\eta_{is}^{p^{\nu}} \equiv 1 \bmod \mathfrak{p}^{N+1}$. If $p^{\tau}s = e/(p-1)$, then $s = e_0$ and $\tau = \lambda - 1$. By the inequality $(e + e_1)/p^{\nu} < s = e_0 = e_1/p^{\lambda-1}$, it follows $\nu > \lambda$. Hence $\eta_{ie_0}^{p^{\nu}} \equiv 1 \bmod \mathfrak{p}^{N+1}$.

Let $e + e_1 < N < 2e + e_1$ and assume $\mu \geqq 1$. If $1 \leqq s \leqq (N-e)/p^{\nu-1}$, then $\nu \leqq \tau + 1$, otherwise $p^{\nu-1}s = p^{\tau}s \cdot p^{\nu-\tau-1} \geqq pe/(p-1) = e + e_1 > N - e$. If $e/(p-1) < p^{\tau}s$ and $s \leqq (N-e)/p^{\nu-1}$, then by Corollary 8 we have $\eta_{is}^{p^{\nu}} \not\equiv 1 \bmod \mathfrak{p}^{N+1}$. If $e/(p-1) = p^{\tau}s$ and $\nu \leqq \tau$, then $\eta_{is}^{p^{\nu}} \not\equiv 1 \bmod \mathfrak{p}^{N+1}$. If $e/(p-1) = p^{\tau}s$ and $\nu = \tau + 1$, then $s = e_0$ and $\tau = \lambda - 1$. In this case we see by Theorem B that $\eta_{ie_0}^{p^{\nu}} \not\equiv 1 \bmod \mathfrak{p}^{N+1}$ for $i \neq 1$. On the other hand we have for $i = 1$

$$\eta_{1e_0}^{p^{\nu}} \equiv \begin{cases} 1 + \omega_1^{p^{\nu}}\pi^{e_0p^{\nu}} \bmod \mathfrak{p}^{e_0p^{\nu}+1} & \text{if } \nu \leqq \lambda - 1 , \\ 1 + (\omega_1^{p^{\lambda}} - \varepsilon\omega_1^{p^{\lambda-1}})p^{\nu-\lambda}\pi^{e+e_1} \bmod \mathfrak{p}^{(\nu-\lambda+1)e+e_1+1} , & \text{if } \nu \geqq \lambda , \end{cases}$$

where $\omega_1^{p^{\lambda}} - \varepsilon\omega_1^{p^{\lambda-1}} \equiv 0 \bmod \mathfrak{p}$. If $\nu \leqq \lambda - 1$, then $\eta_{1e_0}^{p^{\nu}} \not\equiv 1 \bmod \mathfrak{p}^{N+1}$, and $e_0 \leqq (N-e)/p^{\nu-1}$. If $\nu > \lambda$, then $\eta_{1e_0}^{p^{\nu}} \equiv 1 \bmod \mathfrak{p}^{N+1}$ and $e_0 > (N-e)/p^{\nu-1}$. If $\nu = \lambda$, it may happen that $\eta_{1e_0}^{p^{\lambda}} \equiv 1 \bmod \mathfrak{p}^{N+1}$, namely $\lambda \geqq \nu(N : 1, e_0)$. Hence $\eta_{is}^{p^{\nu}} \not\equiv 1 \bmod \mathfrak{p}^{N+1}$, where $1 \leqq i \leqq f, 1 \leqq s \leqq (N-e)/p^{\nu-1}, s \not\equiv 0 \bmod p$, but if $\nu = \lambda$ and $\lambda \geqq \nu(N:1, e_0)$, then $(i, s) \neq (1, e_0)$. Finally, suppose $(N-e)/p^{\nu-1} < s \leqq e + e_1$, where $e + e_1 < N < 2e + e_1$. It then follows that $\nu \geqq \tau + 1$. If $e/(p-1) < p^\tau s$, then $\eta_{is}^{p^\nu} \equiv 1 \bmod \mathfrak{p}^{N+1}$, because $sp^\tau + (\nu - \tau)e > e_1 + 2e > N$, if $\tau \leqq \nu - 2$; $sp^\tau + (\nu-\tau)e = sp^{\nu-1} + e > N$, if $\tau = \nu - 1$. If $e/(p-1) = p^\tau s$, then $s = e_0$ and $\tau = \lambda - 1$. By the inequality $(N-e)/p^{\nu-1} < s = e_0 = e_1/p^{\lambda-1}$ we have $\nu > \lambda$ and then $\eta_{ie_0}^{p^\nu} \equiv 1 \bmod \mathfrak{p}^{N+1}$. If $s > e/(p-1)$ and $(N-e)/p^{\nu-1} < s$, then $\eta_{is}^{p^\nu} \equiv 1 \bmod \mathfrak{p}^{N+1}$.

Thus Lemma 9 is proved. q.e.d.

COROLLARY 10. *Suppose $\mu \geqq 1$. Let η_{is} and η_* be principal units of Theorem B. Let $ae + e_1 \leqq N < (a+1)e + e_1$ and $1 \leqq a \leqq \mu$. Then we have*

$$\eta_{is}^{p^\nu} \neq 1 \bmod \mathfrak{p}^{N+1}, \quad \eta_*^{p^\nu} \neq 1 \bmod \mathfrak{p}^{N+1} \qquad \text{for } \nu \leqq a-1,$$
$$\eta_{is}^{p^\nu} \neq 1 \bmod \mathfrak{p}^{N+1}, \quad \eta_*^{p^\nu} \equiv 1 \bmod \mathfrak{p}^{N+1} \qquad \text{for } \nu \geqq a,$$

if and only if indices i and s satisfy the following conditions:

For $\nu \leqq a-1$, $\quad 1 \leqq s \leqq e + e_1$.

For $\nu \geqq a$, $\quad 1 \leqq s \leqq (N - (a + \delta - 1)e)/p^{\nu-a-\delta+1}$,

but if $\nu(N:1, e_0) \leqq \nu \leqq \lambda + a - 1$, then $(i, s) \neq (1, e_0)$, where

$$\delta = \begin{cases} 0, & \text{if } N = ae + e_1, \\ 1, & \text{if } ae + e_1 < N < (a+1)e + e_1. \end{cases}$$

Proof. Let $N = ae + e_1$. It is obvious by Proposition 6 that $H_{e+e_1+1}^{p^{a-1}} \cong H_{N+1}$. Since we have $\eta_{is} \neq 1 \bmod \mathfrak{p}^{e+e_1+1}$ $(1 \leqq s \leqq e + e_1)$ and $\eta_* \neq 1 \bmod \mathfrak{p}^{e+e_1+1}$, $\eta_{is}^{p^\nu} \neq 1 \bmod \mathfrak{p}^{N+1}$ and $\eta_*^{p^\nu} \neq 1 \bmod \mathfrak{p}^{N+1}$ for $\nu \leqq a - 1$. Let $(i, s) \neq (1, e_0)$ and $\nu \geqq a$. By Lemma 9 we find that $\eta_{is}^{p^\nu} \neq 1 \bmod \mathfrak{p}^{e+e_1+1}$ for $1 \leqq s \leqq (e+e_1)/p^\nu$. Hence it follows that $\eta_{is}^{p^{\nu+a-1}} \neq 1 \bmod \mathfrak{p}^{N+1}$ for $1 \leqq s \leqq (e+e_1)/p^\nu$. Moreover, since $H_{e+e_1+1}^{p^{a-1}} \cong H_{N+1}$, we see that $\eta_{is}^{p^\nu} \neq 1 \bmod \mathfrak{p}^{N+1}$ for $1 \leqq s \leqq (e+e_1)/p^{\nu-a+1}$. Let $(i, s) = (1, e_0)$. Then $e_0 = e_1/p^{\lambda-1} \leqq (e+e_1)/p^{\nu-a+1} = e_1/p^{\nu-a}$ if and only if $\nu \leqq \lambda + a - 1$. By Corollary 8 we have $\eta_{1e_0}^{p^\lambda} \equiv 1 \bmod \mathfrak{p}^{e+e_1+1}$ and hence $\eta_{1e_0}^{p^{\lambda+a-1}} \equiv 1 \bmod \mathfrak{p}^{N+1}$, that is, $\lambda \leqq \nu(N:1, e_0) \leqq \lambda + a - 1$.

Since $\eta_* \equiv 1 \bmod \mathfrak{p}^{e+e_1}$, $\eta_* \neq 1 \bmod \mathfrak{p}^{e+e_1+1}$, we have $\eta_*^{p^\nu} \equiv 1 \bmod \mathfrak{p}^{(\nu+1)e+e_1}$, $\eta_*^{p^\nu} \neq 1 \bmod \mathfrak{p}^{(\nu+1)e+e_1+1}$ for $\nu = 0, 1, \cdots$.

Let $ae + e_1 < N < (a+1)e + e_1$. It then follows from Proposition 6 that $H_{N-(a-1)e+1}^{p^{a-1}} \cong H_{N+1}$. Hence by the same arguments as above we have the latter half of Corollary 10. We note that $\lambda \leqq \nu(N:1, e_0) \leqq \lambda + a$.

q.e.d.

From Lemma 9 and Corollary 10, the numbers $g_N(\nu)$, exponents $\nu(N:i, s)$ and $\nu(N:*)$ defined in §2 are given as follows:

If $1 \leqq N < e + e_1$, or if $\mu = 0$ and $N = e + e_1$, then

$$g_N(\nu) = \left(N - \left[\frac{N}{p}\right] - \left[\frac{N}{p^\nu}\right] + \left[\frac{N}{p^{\nu+1}}\right]\right)f, \qquad (\nu \geqq 1), \tag{13}$$

and

$$\nu(N:i, s) = \nu \qquad \text{for } N/p^\nu < s \leqq N/p^{\nu-1}, \tag{14}$$

where $1 \leqq i \leqq f, 1 \leqq s \leqq N$ and $s \not\equiv 0 \bmod p$.

If $\mu \geqq 1$ and $ae + e_1 \leqq N < (a+1)e + e_1$ $(1 \leqq a \leqq \mu)$, then

$$\begin{cases} g_N(\nu) = 0, & \text{for } \nu \leqq a - 1, \\ g_N(\nu) = \left(e + e_1 - \left[\dfrac{e+e_1}{p}\right] - \left[\dfrac{N-(a+\delta-1)e}{p^{\nu-a-\delta+1}}\right] \right. & \\ \qquad \left. + \left[\dfrac{N-(a+\delta-1)e}{p^{\nu-a-\delta+2}}\right]\right)f + \bar{g}_N(\nu), & \text{for } \nu \geqq a, \end{cases} \tag{15}$$

where

$$\bar{g}_N(\nu) = \begin{cases} 2, & \text{if } \nu(N:1, e_0) \leqq \nu \leqq \lambda + a - 1, \\ 1, & \text{otherwise}, \end{cases}$$

and

$$\begin{cases} \nu(N:*) = a, & \lambda \leqq \nu(N:1, e_0) \leqq \lambda + a - 1 + \delta, \\ \nu(N:i, s) = \nu & \text{for } (N-(a+\delta-1)e)/p^{\nu-a-\delta+1} \\ & \qquad < s \leqq (N-(a+\delta-1)e)/p^{\nu-a-\delta}, \end{cases} \tag{16}$$

where $1 \leqq i \leqq f, 1 \leqq s \leqq e + e_1, s \not\equiv 0 \bmod p, (i, s) \neq (1, e_0)$ and δ is given by Corollary 10. We note that if $\lambda = \mu$, or $N = e + e_1$, then $\nu(N:1, e_0) = \lambda$.

It then follows from (13) and (15) that

$$\begin{aligned} & g_N(1) + \sum_{\nu=2}^{\infty} \nu(g_N(\nu) - g_N(\nu-1)) \\ & = \begin{cases} Nf, & \text{if } 1 \leqq N \leqq e + e_1, \\ Nf + \nu(N:1, e_0) - \lambda, & \text{if } ae + e_1 \leqq N < (a+1)e + e_1 \\ & \text{and } 1 \leqq a \leqq \mu. \end{cases} \end{aligned} \tag{17}$$

Thus (2) or (8_1) is a basis of H_1/H_{N+1} and (8_2) is a basis of H_1/H_{N+1} if and only if $\nu(N:1, e_0) = \lambda$.

Now we establish a basis of H_{N+1}.

PROPOSITION 11. (A). *Suppose that* $\mu = 0$. *It then follows that for each* $t \geqq 0$ *and* $1 \leqq N \leqq e + e_1$

$$H_{te+N+1} = \prod_{1\leqq i\leqq f} \prod_{\substack{1\leqq s\leqq N \\ s\not\equiv 0 \bmod p}} \langle \eta_{is}^{p^{\nu(N:i,s)+t}} \rangle \times \prod_{1\leqq i\leqq f} \prod_{\substack{N<s\leqq pe/(p-1) \\ s\not\equiv 0 \bmod p}} \langle \eta_{is}^{p^t} \rangle \qquad (direct)\ ,$$

where η_{is} *are principal units of Theorem* A *and* $\nu(N:i,s)$ *are given by* (14).

(B). *Suppose* $\mu \geqq 1$. *Let* $ae + e_1 \leqq N < (a+1)e + e_1$ *and* $1 \leqq a \leqq \mu$. *Then it follows that for each* $t \geqq 0$

$$H_{te+N+1} = \langle \eta_*^{p^{a+t}} \rangle \times \prod_{(i,s)\in S} \langle \eta_{is}^{p^{\nu(N:i,s)+t}} \rangle \qquad (direct)\ ,$$

where η_*, η_{is} *are principal units of Theorem* B, $\nu(N:i,s)$ *are given by* (16) *and* S *is the set defined by* (5).

Proof. We first notice that by Theorem A or (7) multiplicative expressions described as above are surely direct products.

(A). Suppose that $\mu = 0$ and $1 \leqq N \leqq e + e_1$. Put

$$H'_{N+1} = \prod_{1\leqq i\leqq f} \prod_{\substack{1\leqq s\leqq N \\ s\not\equiv 0 \bmod p}} \langle \eta_{is}^{p^{\nu(N:i,s)}} \rangle \times \prod_{1\leqq i\leqq f} \prod_{\substack{N<s\leqq pe/(p-1) \\ s\not\equiv 0 \bmod p}} \langle \eta_{is} \rangle \qquad \text{(direct)}\ .$$

Then H'_{N+1} is a subgroup of H_{N+1}. It is proved that $H'_{N+1} = H_{N+1}$. Indeed,

$$(H_1 : H'_{N+1}) = \prod_{1\leqq i\leqq f} \prod_{\substack{1\leqq s\leqq N \\ s\not\equiv 0 \bmod p}} p^{\nu(N:i,s)}\ ;$$

from (13) and (17) we have

$$\sum_{1\leqq i\leqq f} \sum_{\substack{0\leqq s\leqq N \\ s\not\equiv 0 \bmod p}} \nu(N:i,s) = g_N(1) + \sum_{\nu=2}^{\infty} \nu(g_N(\nu) - g_N(\nu-1)) = Nf\ .$$

Hence we have $(H_1 : H'_{N+1}) = p^{Nf} = (H_1 : H_{N+1})$, as was to be shown.

If $e_1 \leqq N \leqq e + e_1$, then we observe by Proposition 6 that $H_{N+1}^{p^t} \cong H_{te+N+1}$ for each $t \geqq 0$. Therefore, we have the direct decomposition of H_{te+N+1}.

(B). Suppose $\mu \geqq 1$. Let $ae + e_1 \leqq N < (a+1)e + e_1$ and $1 \leqq a \leqq \mu$.

Put

$$H'_{N+1} = \langle \eta_*^{p^a} \rangle \times \prod_{(i,s)\in S} \langle \eta_{is}^{p^{\nu(N:i,s)}} \rangle \qquad \text{(direct)} .$$

Then H'_{N+1} is a subgroup of H_{N+1} and H_{01}. We contend $H'_{N+1} = H_{N+1}$. Indeed, since we have $(H_1 : H_{01}) = p^\lambda$ by [2, p. 231],

$$(H_1 : H'_{N+1}) = (H_1 : H_{01})(H_{01} : H'_{N+1}) = p^\lambda p^a \prod_{(i,s)\in S} p^{\nu(N:i,s)} ;$$

it follows from (15), (16) and (17) that

$$\begin{aligned}
\sum_{(i,s)\in S} & \nu(N : i, s) \\
&= a(g_N(a) - 1) + \sum_{\nu=a+1}^{\nu(N:1,e_0)-1} \nu\{(g_N(\nu) - 1) - (g_N(\nu - 1) - 1)\} \\
&\quad + \nu\,(N : 1, e_0)\{(g_N(\nu(N : 1, e_0)) - 2) - (g_N(\nu(N : 1, e_0) - 1) - 1)\} \\
&\quad + \sum_{\nu=\nu(N:1,e_0)+1}^{\infty} \nu\{(g_N(\nu) - 2) - (g_N(\nu - 1) - 2)\} \\
&= a g_N(a) + \sum_{\nu=a+1}^{\infty} \nu(g_N(\nu) - g_N(\nu - 1)) - a - \nu(N : 1, e_0) \\
&= Nf - (\lambda + a) .
\end{aligned}$$

Hence we get $(H_1 : H'_{N+1}) = p^{Nf} = (H_1 : H_{N+1})$, as desired.

Finally it is clear that $H_{te+N+1} \cong H_{N+1}^{p^t}$ for each $t \geqq 0$ by Proposition 6. Thus we have the direct decomposition of H_{te+N+1}. q.e.d.

§ 6. Proof of Theorem 2 and Theorem 3

From Theorem A, Proposition 11, (4) and (13) we have Theorem 2.

Now we shall prove Theorem 3. Suppose that $k_\mathfrak{p}$ contains ζ_μ ($\mu \geqq 1$), but does not contain $\zeta_{\mu+1}$.

(I). In the case where $1 \leqq N < e + e_1$, it is verified by (17) that (8_1) is a basis of H_1/H_{N+1}. Hence the direct decomposition of $G(\mathfrak{p}^{N+1})$ is obtained by (4), (13) and (14).

(II). In the case where $e + e_1 \leqq N < (\mu + 1)e + e_1$ and $\nu(N : 1, e_0) = \lambda$, we know by (17) that (8_2) is a basis of H_1/H_{N+1}. Hence the direct decomposition of $G(\mathfrak{p}^{N+1})$ is obtained by (4), (15) and (16).

(III). In the case where $e + e_1 < N < (\mu + 1)e + e_1$ and $\nu(N : 1, e_0) > \lambda$, we see by Proposition 11 and (7) that $\eta_*, \eta_{is}((i, s) \in S)$ are independent modulo $\mathfrak{p}^{N+1}$, that is, $\eta_*^{x_*} \cdot \prod_{(i,s)\in S} \eta_{is}^{x_{is}} \equiv 1 \bmod \mathfrak{p}^{N+1}$ if and only if $x_* \equiv 0 \bmod p^a$ and $x_{is} \equiv 0 \bmod p^{\nu(N:i,s)}$ for all $(i, s) \in S$.

From the relation (6) we have a congruence

$$(18) \qquad \eta_{1e_0}^{p^\lambda(p^{\nu(N:1,e_0)-\lambda}-1)} \prod_{\substack{(i,s)\in S\\ \nu(N:i,s)\geqq\mu+1}} \eta_{is}^{\beta_{is}p^\mu} \equiv 1 \bmod \mathfrak{p}^{N+1}\ .$$

Since $(H_1: H_{01}) = p^\lambda$ and H_{N+1} is a subgroup of H_{01}, p^λ is the least positive integer such that $\eta_{1e_0}^{p^\lambda} \equiv \eta_0 \bmod \mathfrak{p}^{N+1}$ for some $\eta_0 \in H_{01}$. Hence the structure of H_1/H_{N+1} having a system of canonical generators (8_2) is determined by (18) only. We put

$$\beta_* p^\mu = \beta'_* p^{a'_*}\ , \quad (\beta'_*, p) = 1\ ,$$
$$\beta_{is} p^\mu = \beta'_{is} p^{a'_{is}}\ , \quad (\beta'_{is}, p) = 1 \qquad \text{for } (i, s) \in S\ .$$

It is then clear that instead of (8_2)

$$\{\eta_{1e_0}^{p^{\nu(N:1,e_0)-\lambda}-1} H_{N+1}, \eta_*^{\beta'_*} H_{N+1}, \eta_{is}^{\beta'_{is}} H_{N+1}\}_{(i,s)\in S}$$

is also a system of canonical generators for H_1/H_{N+1}.

Let M, a free Z-module, and $\psi: M \to H_1/H_{N+1}$ be as defined in §2. Put

$$a_{is} = \min\{\nu(N: i, s), a'_{is}\} \qquad \text{for } (i, s) \in S\ .$$

Then from Proposition 11 and by (18) a system of canonical generators for $\operatorname{Ker}\psi$ is given by

$$\left\{p^{a}\tilde{\eta}_*, p^{\nu(N.1,e_0)}\tilde{\eta}_{1e_0}, p^{\nu(N:i,s)}\tilde{\eta}_{is}, p^\lambda\tilde{\eta}_{1e_0} + \sum_{(i,s)\in S} p^{a_{is}}\tilde{\eta}_{is}\right\}\ ,$$

where $(i, s) \in S$. Then the rank of $\operatorname{Ker}\psi$ is equal to $(ef + 1)$ because the rank of H_1/H_{N+1} is equal to $(ef + 1)$ from Theorem 1. The direct decomposition of $H_1/H_{N+1} \cong M/\operatorname{Ker}\psi$ is determined by elementary divisors of the matrix (9) of Theorem 3. Thus (III) of Theorem 3 is proved.

Finally, (IV) of Theorem 3 is trivially obtained from Lemma 7. Thus Theorem 3 is completely proved.

§7. Proof of Corollary 4

Let $\mathfrak{p}$ be an unramified prime ideal of k, lying above a rational prime p. Assume that p is odd. Then by Theorem 2 we observe that $b_1(1) = f$ and $b_1(\nu) = 0$ for $\nu \geqq 2$. Let $p = 2$. Then $e = e_1 = 1$ and $\lambda = \mu = 1$. Therefore, we have by (I) and (II) of Theorem 3

$$b_1(1) = f\ , \quad b_1(\nu) = 0 \qquad \text{for } \nu \geqq 2\ ,$$
$$b_2(1) = 2\ , \quad b_2(2) = f - 1\ , \quad b_2(\nu) = 0 \qquad \text{for } \nu \geqq 3\ .$$

Thus Corollary 4 is obtained from Theorem 2 and Theorem 3.

§ 8. Supplement to Theorem 3

We assume that $k_{\mathfrak{p}}$ contains ζ_μ $(\mu \geqq 1)$ but does not contain $\zeta_{\mu+1}$. Suppose that $\lambda > \mu \geqq 1$ and $ae + e_1 \leqq N < (a+1)e + e_1$ $(1 \leqq a \leqq \mu)$. In this section we shall prove that if one of exponents ν $(N: i, s)$ satisfies a certain condition, then the direct decomposition of H_1/H_{N+1} is induced by that of H_1/H_{N-e+1}.

If $\lambda > \mu \geqq 1$, then a Z_p-basis of H_1 is given as follows (cf. [2, p. 232–233]). Let H_{01} be the free Z_p-group of H_1 defined by (7). By (6) we observe that $\eta_{1e_0}^{p^{\lambda-\mu}}\zeta_\mu^{-1}$ does not belong to $H_{01}^p = \{\eta_0^p \mid \eta_0 \in H_{01}\}$. There exists $\beta_{i_0 s_0}$ such that $\beta_{i_0 s_0}$ is prime to p. If β_* is prime to p, we may take $\beta_{i_0 s_0} = \beta_*$. Hence $\eta_{i_0 s_0}$ can be written in the form

$$\eta_{i_0 s_0} = \zeta_\mu^{\alpha_\mu} \prod_{\substack{(i,s)\in S' \\ (i,s)\neq(i_0,s_0)}} \eta_{is}^{\alpha_{is}} \cdot \eta_{1e_0}^{p^{\lambda-\mu}\alpha_{1e_0}}, \tag{19}$$

where $S' = S \cup \{*\}$, α_μ is a rational integer, prime to p $(1 \leqq \alpha_\mu < p^\mu)$, α_{is} are p-adic integers and α_{1e_0} is a p-adic integer, prime to p (cf. [2, II in p. 209]). We then have a Z_p-free part $\tilde{H}_{01}$ of H_1, expressed as direct product:

$$\tilde{H}_{01} = \prod_{\substack{(i,s)\in S' \\ (i,s)\neq(i_0,s_0)}} \langle \eta_{is} \rangle \times \langle \eta_{1e_0} \rangle \qquad \text{(direct)} .$$

From Proposition 6 we find that $H_{N-e+1}^p \cong H_{N+1}$, where $ae + e_1 \leqq N < (a+1)e + e_1$ and $1 \leqq a \leqq \mu$. Therefore by Proposition 11 we have

$$H_{N-e+1} = \langle \eta_*^{p^{a-1}} \rangle \times \prod_{(i,s)\in S} \langle \eta_{is}^{p^{\nu(N:i,s)-1}} \rangle \qquad \text{(direct)} .$$

It then follows from (19) that H_{N-e+1} is a subgroup of $\tilde{H}_{01}$ if and only if $\nu(N: i_0, s_0) - 1 \geqq \mu$. We note that $\nu(N: *) = a \langle \mu + 1$ (see (16)). If $\nu(N: i_0, s_0) \geqq \mu + 1$, one see also that

$$H_1/H_{N-e+1} \cong \langle \zeta_\mu \rangle \times \tilde{H}_{01}/H_{N-e+1} \qquad \text{(direct)} .$$

The direct decomposition of $G(\mathfrak{p}^{N-e+1})$ is obtained from (I) $\sim$ (III) of Theorem 3 and by Lemma 7, say of type $(p^f - 1, p^\mu, p^{c_1'}, \cdots, p^{c_{ef}'})$. Then $G(\mathfrak{p}^{N+1})$ is of type $(p^f - 1, p^\mu, p^{c_1'+1}, \cdots, p^{c_{ef}'+1})$ by Lemma 7.

§ 9. Examples

(i). Let p be an odd prime and ζ_1 be a primitive p-th root of unity. Put $k = \boldsymbol{Q}(\zeta_1)$ and $\mathfrak{p} = (1-\zeta_1)$. Then we have an expression of $G(\mathfrak{p}^{N+1})$ as direct product for each $t \geqq 0$:

$$G(\mathfrak{p}^{N+1}) \cong \begin{cases} Z(p-1) \times \underbrace{Z(p) \times \cdots \times Z(p)}_{N\text{-times}} , & \text{if } 1 \leqq N < p , \\ Z(p-1) \times \underbrace{Z(p) \times Z(p^{1+t}) \times \cdots \times Z(p^{1+t})}_{p\text{-times}} , & \\ & \text{if } N = (p-1)t + p , \\ Z(p-1) \times \underbrace{Z(p) \times Z(p^{1+t}) \times \cdots \times Z(p^{1+t})}_{(p-1)\text{-times}} \times Z(p^{2+t}) , & \\ & \text{if } N = (p-1)t + p + 1 , \\ Z(p-1) \times \underbrace{Z(p) \times Z(p^{1+t}) \times \cdots \times Z(p^{1+t})}_{(p-2)\text{-times}} \times Z(p^{2+t}) \times Z(p^{2+t}) , & \\ & \text{if } N = (p-1)t + p + 2 , \\ \cdots\cdots\cdots\cdots & \\ Z(p-1) \times Z(p) \times Z(p^{1+t}) \times \underbrace{Z(p^{2+t}) \times \cdots \times Z(p^{2+t})}_{(p-2)\text{-times}} , & \\ & \text{if } N = (p-1)t + 2p - 2 . \end{cases}$$

(ii). Let d be a square free rational integer such that $d \equiv 2 \bmod 4$. Put $k = \boldsymbol{Q}(\sqrt{d})$ and let $\mathfrak{p}$ be a prime ideal of k, lying above 2. Then $e = e_1 = 2$, $\lambda = 2$ and $\mu = 1$. By (I) of Theorem 3 we have

$$G(\mathfrak{p}^2) \cong Z(2) , \quad G(\mathfrak{p}^3) \cong Z(2^2) , \quad G(\mathfrak{p}^4) \cong Z(2) \times Z(2^2) .$$

By [4] we see that for $N = e + e_1 = 4$, $\nu(4:1,1) = 2 = \lambda > \mu$. Hence for each $t \geqq 0$ we obtain by (II) and (IV) of Theorem 3

$$G(\mathfrak{p}^{2t+5}) \cong Z(2) \times Z(2^{1+t}) \times Z(2^{2+t}) .$$

Furthermore, it is shown in [4] that $-\eta_{11}^2 \equiv \eta_{13} \bmod \mathfrak{p}^4$. It then follows that for $N = 5 (e + e_1 < N < 2e + e_1)$, $\nu(5:1,1) = 3 > \lambda$ and $\nu(5:1,3) = 2 = \lambda > \mu$. Hence from the arguments of § 8 we see that H_4 is a subgroup of the free part of H_1. From the result of § 8 and by Theorem 1 the direct decomposition of $G(\mathfrak{p}^6)$ is induced by that of $G(\mathfrak{p}^4)$, that is, expressed as follows:

$$G(\mathfrak{p}^6) \cong Z(2) \times Z(2) \times Z(2^3) .$$

Therefore, we see by (IV) of Theorem 3 that for each $t \geqq 0$

$$G(\mathfrak{p}^{2t+6}) \cong Z(2) \times Z(2^{1+t}) \times Z(2^{3+t}) .$$

For $N = 5$ the matrix (9) of Theorem 3 is equal to

$$\begin{bmatrix} 2 & 0 & 0 \\ 0 & 2^2 & 0 \\ 0 & 0 & 2^3 \\ 2 & 2 & 2^2 \end{bmatrix} .$$

It is then clear that

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ -1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 2 & 1 & 1 & -2 \end{bmatrix} \begin{bmatrix} 2 & 0 & 0 \\ 0 & 2^2 & 0 \\ 0 & 0 & 2^3 \\ 2 & 2 & 2^2 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & -2 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2^3 \\ 0 & 0 & 0 \end{bmatrix} ,$$

which shows the direct decomposition of H_1/H_6, too.

BIBLIOGRAPHY

[1] Albis Gonzalez, V. S., A remark on primitive root and ramification, Rev. Columbiana Math., **7** (1973), 93–98.
[2] Hasse, H., Zahlentheorie, Akademie-Verlag, Berlin, 2 Aufl., 1963.
[3] ——, Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper, Physica Verlag, 1965.
[4] H.-Koch, F., Einseinheitengruppen und prime Restklassengruppen in quadratischen Zahlkörper, J. Number Theory, **4** (1972), 70–77.
[5] Narkiewicz, W., Elementary and analytic theory of algebraic numbers, Monogr. Math., 57, PWN-Polish Sci. Publishers, 1974.
[6] Ranum, A., The group of classes of congruent quadratic integers with respect to composite ideal modulus, Trans. Amer. Math. Soc., **11** (1910), 172–198.
[7] Serre, J.-P., Sur les corps locaux à corps résiduel algébriquement clos, Bull. Soc. Math. France, **89** (1961), 105–154.
[8] Takenouchi, T., On the classes of congruent integers in an algebraic körper, J. College of Sci. Tokyo Imp. Univ., XXXVI, Article I (1913), 1–28.
[9] Wyman, B. F., Wildly ramified Gamma extensions, Amer. J. Math., **91** (1969), 135–152.

Department of Mathematics
College of Liberal Arts
Toyama University