ACTA ARITHMETICA
LXXXV.3 (1998)

Index for subgroups of the group of units in number fields

by

Tsutomu Shimada (Yamato)

We define a sequence of rational integers $u_i(E)$ for each finite index subgroup E of the group of units in some finite Galois number fields K in which prime p ramifies. For two subgroups $E' \subset E$ of finite index in the group of units of K we prove the formula $v_p([E : E']) = \sum_{i=1}^{r}\{u_i(E') - u_i(E)\}$. This is a generalization of results of P. Dénes [3], [4] and F. Kurihara [5].

Introduction. Let p be an odd prime number, $\mathbb{Q}$ and $\mathbb{Z}$ the field of rational numbers and the ring of rational integers, respectively. For each unit ε of $\mathbb{Q}(\zeta_p)$ which is not in $\mathbb{Z}$, there exist rational integers a, b and c satisfying $\varepsilon \equiv a + b(1-\zeta_p)^c \bmod (1-\zeta_p)^{c+1}$, $ab \not\equiv 0 \bmod p$ and $c \not\equiv 0 \bmod (p-1)$, where c is uniquely determined by ε. P. Dénes [2] defined the *p-character* of the Bernoulli numbers to be the rational integers $u_2, u_4, \ldots, u_{p-3}$ such that $B_{ip^j} \equiv 0 \bmod p^{2j+1}$ for $0 \le j < u_i$ and $B_{ip^{u_i}} \not\equiv 0 \bmod p^{2u_i+1}$, where $i = 2, 4, \ldots, p-3$, and proved the following results under the assumption that the p-character of the Bernoulli numbers exists:

Theorem A. *There exists a basis* $\{\theta_2, \theta_4, \ldots, \theta_{p-3}\}$ *for the group of units of* $\mathbb{Q}(\zeta_p)^+$ *modulo* $\{\pm 1\}$ *such that*

$$\theta_i \equiv a_i + b_i\,(1-\zeta_p)^{c_i} \bmod (1-\zeta_p)^{c_i+1}$$

with $c_i = i + (p-1)u_i'$ *for some integer* $0 \le u_i' \le u_i$.

Theorem B. *We have*

$$v_p(h(\mathbb{Q}(\zeta_p)^+)) = \sum_{i=2,\,even}^{p-3} (u_i - u_i').$$

Here $h(*)$ denotes the class number of a field $*$ and v_p the p-adic valuation normalized by $v_p(p) = 1$.

1991 *Mathematics Subject Classification*: 11R21, 11R29.

L. C. Washington [6] showed that $u_i = v_p(L_p(1, \omega^i))$, $i = 2, 4, \ldots, p-3$, and then proved Dénes' assumption stated above, where ω is the Teichmüller character. Furthermore, Washington gave simple proofs of the theorems above. In [5], F. Kurihara generalized the results above to a subfield K_{n+1} of $\mathbb{Q}(\zeta_{p^{n+1}})^+$, $0 \le n \in \mathbb{Z}$, and showed the following two theorems.

THEOREM C. *Let E be a subgroup of $E_{K_{n+1}}$, the group of units of K_{n+1}, such that $[E_{K_{n+1}} : E]$ is finite. Then there exists a basis $\{\theta_1, \ldots, \theta_r\}$ for E modulo $\{\pm 1\}$ such that*

$$\theta_i^{p^n} \equiv a_i + b_i \pi^{c_i} \bmod \pi^{c_i+1}, \qquad i = 1, \ldots, r,$$

with $c_i = i + \frac{1}{2d}\varphi(p^{n+1})u_i$ for some rational integer $u_i \ge 0$.

Here $d = [\mathbb{Q}(\zeta_{p^{n+1}})^+ : K_{n+1}]$, $r = \operatorname{rank} E_{K_{n+1}} = \frac{1}{2d}\varphi(p^{n+1}) - 1$ and π is the image of $(1-\zeta_{p^{n+1}})(1-\zeta_{p^{n+1}}^{-1})$ by the norm from $\mathbb{Q}(\zeta_{p^{n+1}})^+$ to K_{n+1}. Now since c_i and hence u_i depends only on E, it is denoted by $c_i(E)$ and $u_i(E)$, respectively.

THEOREM D. *Let E be a subgroup of $E_{K_{n+1}}$ and E' a subgroup of E. Suppose that the index $[E_{K_{n+1}} : E']$ is finite. Then*

$$v_p([E : E']) = \sum_{i=1}^{r} \{u_i(E') - u_i(E)\}.$$

Considering the case where $K_{n+1} = \mathbb{Q}(\zeta_{p^{n+1}})^+$, $E = E_{K_{n+1}}$ and E' is the group of cyclotomic units in the sense of Sinnott, we see that Theorem D is a generalization of Theorem B.

Our aim is to prove similar results in some other number fields: the composite of two Galois extensions of finite degree over $\mathbb{Q}$, one unramified at p and the other totally ramified.

Now we introduce some notations. Let K_T be a finite Galois extension over $\mathbb{Q}$ which is unramified at p and K_V a finite Galois extension which is totally ramified at p. Let $K = K_T K_V$, $[K_T : \mathbb{Q}] = d_K$ and $[K_V : \mathbb{Q}] = e_K$. We fix an embedding of K into $\mathbb{C}$, the field of complex numbers. Let J denote the restriction of the complex conjugation to K. Let K^+ and K_T^+ be the fixed field of $\langle J \rangle$ in K and K_T, respectively. Let $\wp_1, \ldots, \wp_g$ be the primes of K_T over p, $\wp_i'$ $(i = 1, \ldots, g)$ the primes of K over $\wp_i$, and $\wp$ the unique prime of K_V over p. Then $\wp_i = \wp_i'^{e_K}$ and $(p) = \wp_1 \ldots \wp_g = (\wp_1' \ldots \wp_g')^{e_K} = \wp^{e_K}$ in the ring O_K of integers of K. Let E_* be the group of units of a field $*$. Let δ be the least natural number a that satisfies $e_K/(p-1) < p^{a-1}$.

Throughout this paper, we assume the following three conditions:

(A_1) $\wp$ is a principal ideal.

(A_2) The exponent of the torsion part of $E_{K^+}/E_{K_T^+}$ is prime to p.

(A_3) The Leopoldt conjecture is valid for K and p.

Then we may write $\wp = (\pi_K)$ with some $\pi_K \in O_{K_V}$. Let m be the exponent in (A_2).

Our main result is the following:

THEOREM E. *Let E be a subgroup of E_{K^+} such that $E \supset E_{K_T^+}$ and $[E_{K^+} : E] < \infty$. Then there exists a basis $\{\eta_1, \ldots, \eta_r\}$ of $E^{mp^\delta e_K} E_{K_T^+}$ modulo $E_{K_T^+}$ such that*

$$\eta_i \equiv a_i + b_i \pi_K^{c_i} \bmod \pi_K^{c_i+1}, \quad i = 1, \ldots, r = \operatorname{rank} E_{K^+}/E_{K_T^+},$$

where a_i and b_i belong to the ring O_{K_T} of integers of K_T, $a_i \not\equiv 0$ modulo any prime over p, $b_i \not\equiv 0 \bmod p$ and c_i is a natural number such that $c_i \not\equiv 0 \bmod e_K$.

Further, let $u_i(E) = \left[\frac{c_i}{e_K}\right]$ (Gauss symbol) and E' be a subgroup of E such that $E' \supset E_{K_T^+}$ and $[E_{K^+} : E'] < \infty$. Then

$$v_p([E : E']) = \sum_{i=1}^{r} \{u_i(E') - u_i(E)\}.$$

REMARK 1. Let η be any element of $E_{K^+} \setminus K_T$ such that $\eta^a \in E_{K_T^+}$ for some natural number a. Then, for any $\sigma \in \mathrm{Gal}(K/K_T)$, $(\eta^\sigma/\eta)^a = (\eta^a)^\sigma/\eta^a = \eta^a/\eta^a = 1$. So, $\eta^{\sigma-1}$ is an ath root of unity. Moreover, when K is a real or *CM*-field, $\eta^{\sigma-1}$ is real, hence ± 1 and $(\eta^2)^{\sigma-1} = 1$. Thus, $\eta^2 \in E_{K_T^+}$ and m equals 1 or 2, hence in this case it is prime to p, i.e. (A_2) is valid.

REMARK 2. When $K = \mathbb{Q}(\zeta_{ap^n})$ with a prime to p, then $K_T = \mathbb{Q}(\zeta_a)$. Note that the condition (A_3) is valid by the theorem of A. Brumer [1]. Let $E = E_{K^+}$ and $E' = C_K^+ E_{K_T^+}$, where C_K is the group of cyclotomic units and $C_K^+ = C_K \cap K^+$. Then, since $v_p([E : E']) = v_p(h(K^+)/h(K_T^+))$, we get a generalization of Theorem B:

$$v_p(h(\mathbb{Q}(\zeta_{ap^n})^+)/h(\mathbb{Q}(\zeta_a)^+)) = \sum_{i=1}^{r} \{u_i(E') - u_i(E)\}.$$

1. The Fermat quotient and the level of unit. Let the notations be as in the introduction. Note that $K_V = \mathbb{Q}(\pi_K)$. Let $f(X) = X^{e_K} + c'_{e_K-1} X^{e_K-1} + \ldots + c'_1 X + c'_0 \in \mathbb{Z}[X]$ be the minimal polynomial of π_K which is of Eisenstein type. That is, $c'_{e_K-1} \equiv \ldots \equiv c'_0 \equiv 0 \bmod p$ and $c'_0 \not\equiv 0 \bmod p^2$. We write $c'_i = -pc_i$ $(i = 0, 1, \ldots, e_K - 1)$. Then

$$\pi_K^{e_K} \equiv pc_0 \bmod \pi_K^{e_K+1} \quad \text{and} \quad p \equiv b_0 \pi_K^{e_K} \bmod \pi_K^{e_K+1}, \tag{1}$$

where b_0 is the natural number such that $c_0 b_0 \equiv 1 \bmod p$ and $1 \le b_0 \le p-1$.

For any $z \in O_K \setminus K_T$ which is prime to p, we define

$$c(z) = \max\{0 \le c \in \mathbb{Z} : z \equiv x + y\pi_K^c \bmod \pi_K^{c+1} \text{ with some } x, y \in O_{K_T}\}.$$

It can be easily seen that $1 \le c(z) < \infty$. Furthermore, we define $c(z) = \infty$ for $z \in O_{K_T}$.

When x_0 and y_0 give $c(z)$ $(z \in O_K \setminus K_T)$, it is clear that

$$x_0 \not\equiv 0 \bmod \wp_i \quad (i = 1, \ldots, g) \quad \text{and} \quad y_0 \not\equiv 0 \bmod p.$$

If $c(z)$ is a multiple of e_K, then writing $c(z) = ce_K$ with a natural number c, we have

$$z \equiv x_0 + y_0\pi_K^{ce_K} \equiv x_0 + y_0 p^c c_0^c \bmod \pi_K^{ce_K+1},$$

which contradicts the maximality of $c(z)$. Thus, we get $c(z) \not\equiv 0 \bmod e_K$.

To sum up, we have the following:

LEMMA 1.1. *For any $z \in O_K \setminus K_T$ which is prime to p,*

$$c(z) = \max\{0 \le c \in \mathbb{Z} : z \equiv x + y\pi_K^c \bmod \pi_K^{c+1} \text{ for some } x, y \in O_{K_T}\}$$

is a natural number which depends only on z (it does not depend on the choice of π_K) and $c(z) \not\equiv 0 \bmod e_K$. Let x_0 and y_0 be elements in O_{K_T} giving $c(z)$. Then $x_0 \not\equiv 0 \bmod \wp_i$ $(i = 1, \ldots, g)$ and $y_0 \not\equiv 0 \bmod p$, and further, x_0 and y_0 are uniquely determined by z modulo $\pi_K^{c(z)+1}$ and p, respectively.

Let $\eta \in E_K \setminus K_T$. Let $\eta \equiv x + y\pi_K^{c(\eta)} \bmod \pi_K^{c(\eta)+1}$ be a congruence giving $c(\eta)$ according to Lemma 1.1. Then, in the following, we call $c(\eta)$ the *level* of η and $(y/x) \bmod p \in O_{K_T}/(p)$ the (generalized) *Fermat quotient* of η and we denote the latter by $f(\eta)$. Of course they are uniquely determined by η.

In the rest of this section, we present several elementary properties of the level and the Fermat quotient.

The next lemma immediately follows from the definitions of the Fermat quotient and the level.

LEMMA 1.2. (1) *For any $\eta \in E_K \setminus K_T$ and any natural number a prime to p, we have $c(\eta^J) = c(\eta)$, $c(\eta^a) = c(\eta)$, $f(\eta^a) = af(\eta)$ and $c(\eta^{-1}) = c(\eta)$, $f(\eta^{-1}) = -f(\eta)$.*

(2) *Let η_1 and η_2 be elements in $E_K \setminus K_T$ such that $c(\eta_1) < c(\eta_2)$. Then*

$$c(\eta_1\eta_2) = c(\eta_1) \quad \text{and} \quad f(\eta_1\eta_2) = f(\eta_1).$$

(3) *Let $\eta_1, \ldots, \eta_s$ be elements in $E_K \setminus K_T$ such that $c(\eta_1) = \ldots = c(\eta_s)$ and $f(\eta_1) + \ldots + f(\eta_s) \not\equiv 0 \bmod p$. Then*

$$c(\eta_1 \ldots \eta_s) = c(\eta_1) \quad \text{and} \quad f(\eta_1 \ldots \eta_s) = f(\eta_1) + \ldots + f(\eta_s).$$

LEMMA 1.3. *If K_V is imaginary, then $\pi_K^J \equiv -\pi_K \bmod \pi_K^2$.*

Proof. By the definition of π_K, we have $(\pi_K^J) = (\pi_K)$. So, there exists $u \in E_{K_V}$ such that $\pi_K^J = \pi_K u$. We have $\pi_K = (\pi_K^J)^J = (\pi_K u)^J = \pi_K u u^J$. Thus, $uu^J = 1$.

First, we assume $u \notin K_T$. Let $u \equiv a + b\pi_K^{c(u)} \bmod \pi_K^{c(u)+1}$ according to Lemma 1.1. For any $\sigma \in \mathrm{Gal}(K/K_V)$, $u^\sigma = u$, $\pi_K^\sigma = \pi_K$ and $u \equiv a^\sigma + b^\sigma \pi_K^{c(u)} \bmod \pi_K^{c(u)+1}$. Because $O_{K_V}/(\pi_K) = \mathbb{Z}/(p)$, we can always write $u \equiv a + b\pi_K^c \bmod \pi_K^{c+1}$ where $a, b \in \mathbb{Z}$ are prime to p. Then $1 = uu^J \equiv a^2 \bmod \pi_K$, so $a \equiv \pm 1 \bmod p$. Since $\pi_K^J \equiv a\pi_K \bmod \pi_K^2$, we have $u^J \equiv a + ba^{c(u)}\pi_K^{c(u)} \bmod \pi_K^{c(u)+1}$. By Lemma 1.2, $f(u^{-1}) = f(u^J) \equiv ba^{c(u)-1} \bmod p$ and $f(u^{-1}) = -f(u) \equiv -ba^{-1} \bmod p$. This means $a^{c(u)} \equiv -1 \bmod p$, so that $a \equiv -1 \bmod p$ and the lemma is proved in this case.

Secondly, we assume $u \in K_T$. Then $u \in K_T \cap K_V = \mathbb{Q}$ and $u = \pm 1$. Now, $\pi_K^J \neq \pi_K$ by our assumption, so that $u = -1$. The proof is complete.

LEMMA 1.4. *For any $\eta \in E_K \setminus K_T$ we have $c(\eta^{p^\delta}) > e_K/(p-1)$. If $c(\eta) > e_K/(p-1)$, then $c(\eta^{p^a}) = c(\eta) + ae_K$ and $f(\eta^{p^a}) = b_0^a f(\eta)$ for all natural numbers a. Here δ and b_0 are as in the introduction.*

Proof. Let $\eta \equiv x + y\pi_K^{c(\eta)} \bmod \pi_K^{c(\eta)+1}$ according to Lemma 1.1. Then there exists $y_1 \in O_K$ such that $\eta = x + y_1\pi_K^{c(\eta)}$ and $y_1 \equiv y \bmod \pi_K$. So,

$$\eta^p = x^p + px^{p-1}y_1\pi_K^{c(\eta)} + \binom{p}{2}x^{p-2}y_1^2\pi_K^{2c(\eta)} + \ldots + \binom{p}{p-1}xy_1^{p-1}\pi_K^{(p-1)c(\eta)} + y_1^p\pi_K^{pc(\eta)}. \tag{2}$$

Since the π_K-orders of terms on the right hand side are

$$0, e_K + c(\eta), e_K + 2c(\eta), \ldots, e_K + (p-1)c(\eta) \text{ and } pc(\eta),$$

it follows that

$$c(\eta^p) \geq \min\{e_K + c(\eta), pc(\eta)\} \geq \min\left\{\frac{e_K}{p-1}, pc(\eta)\right\}.$$

Further,

$$c(\eta^{p^2}) \geq \min\left\{\frac{e_K}{p-1}, pc(\eta^p)\right\} \geq \min\left\{\frac{e_K}{p-1}, p\min\left\{\frac{e_K}{p-1}, pc(\eta)\right\}\right\} = \min\left\{\frac{e_K}{p-1}, p^2c(\eta)\right\}.$$

For all natural numbers a, we get by induction

$$c(\eta^{p^a}) \geq \min\left\{\frac{e_K}{p-1}, p^a c(\eta)\right\}.$$

Since $c(\eta^{p^{\delta-1}}) \geq e_K/(p-1)$, (2) means that

$$c(\eta^{p^{\delta}}) \geq \min\{e_K + c(\eta^{p^{\delta-1}}), pc(\eta^{p^{\delta-1}})\} > \frac{e_K}{p-1}.$$

When $e_K/(p-1) < c(\eta)$, we have

$$e_K + c(\eta) < pc(\eta) \quad \text{and} \quad \eta^p \equiv x^p + px^{p-1}y_1\pi_K^{c(\eta)} \bmod \pi_K^{e_K+c(\eta)+1}.$$

Now from (1), we have

$$\eta^p \equiv x^p + b_0x^{p-1}y\pi_K^{e_K+c(\eta)} \bmod \pi_K^{e_K+c(\eta)+1}. \tag{3}$$

So, we conclude that $c(\eta^p) \geq c(\eta) + e_K$.

Suppose $c(\eta^p) > c(\eta)+e_K$. Let $\eta^p \equiv x_2+y_2\pi_K^{c(\eta^p)} \bmod \pi_K^{c(\eta^p)+1}$ according to Lemma 1.1. Then

$$x_2 \equiv \eta^p \equiv x^p + b_0x^{p-1}y\pi_K^{e_K+c(\eta)} \bmod \pi_K^{e_K+c(\eta)+1}$$

and

$$x_2 - x^p \equiv b_0x^{p-1}y\pi_K^{e_K+c(\eta)} \bmod \pi_K^{e_K+c(\eta)+1}.$$

Take a prime $\wp_i'$ dividing π_K of K such that $y \not\equiv 0 \bmod \wp_i'$. Then, from the above, $e_K+c(\eta) = v_{\wp_i'}(b_0x^{p-1}y\pi_K^{e_K+c(\eta)}) = v_{\wp_i'}(x_2-x^p)$. This is a multiple of e_K, so that $c(\eta)$ is also a multiple of e_K. That is a contradiction. Therefore, $c(\eta^p) = c(\eta)+e_K$. Inductively, we obtain $c(\eta^{p^a}) = c(\eta)+ae_K$ for all natural numbers a.

Furthermore, from (3),

$$f(\eta^p) \equiv b_0\frac{x^{p-1}y}{x^p} \equiv b_0\frac{y}{x} \equiv b_0f(\eta) \bmod p.$$

This means that $f(\eta^{p^a}) = b_0^af(\eta)$ for all natural numbers a. The proof is complete.

LEMMA 1.5. *Let $\eta_1,\ldots,\eta_s$ be elements in $E_K \setminus K_T$ such that $c(\eta_1) = \ldots = c(\eta_s) > e_K/(p-1)$ and $\{f(\eta_1),\ldots,f(\eta_s)\}$ is an $\mathbb{F}_p$-independent system. Then $\eta_1,\ldots,\eta_s$ are $\mathbb{Z}$-independent.*

Proof. Suppose that $\eta_1,\ldots,\eta_s$ are $\mathbb{Z}$-dependent, that is, $\eta_1^{e_1}\ldots\eta_s^{e_s} = 1$ with some $e_1,\ldots,e_s \in \mathbb{Z}$. We may assume $e_i \neq 0$ for all i.

Let $e_i = a_ip^{b_i}$ ($\mathbb{Z} \ni a_i \not\equiv 0 \bmod p$, $0 \leq b_i \in \mathbb{Z}$, $i = 1,\ldots,s$). Then from Lemmas 1.2 and 1.4 we have

$$c(\eta_i^{e_i}) = c(\eta_i^{p^{b_i}}) = c(\eta_i) + b_ie_K \quad \text{and} \quad f(\eta_i^{e_i}) = a_if(\eta_i^{p^{b_i}}) = b_0^{b_i}a_if(\eta_i).$$

We denote by β the minimum of $\{b_1,\ldots,b_s\}$ and assume, without loss of generality, $\beta = b_1 = \ldots = b_t < b_{t+1},\ldots,b_s$ with some t ($1 \leq t \leq s$).

From our assumption,

$$\sum_{i=1}^{t} f(\eta_i^{e_i}) = \sum_{i=1}^{t} b_0^{b_i}a_if(\eta_i) \not\equiv 0 \bmod p.$$

Now, $c(\eta_i^{e_i}) = c(\eta_i) + b_i e_K = c(\eta_i) + \beta e_K$ for all $i = 1, \ldots, t$. So, from Lemma 1.2, $c(\prod_{i=1}^t \eta_i^{e_i}) = c(\eta_1) + \beta e_K < c(\eta_j^{e_j})$ for all $t+1 \le j \le s$. Therefore, $c(\prod_{i=1}^s \eta_i^{e_i}) = c(\prod_{i=1}^t \eta_i^{e_i}) = c(\eta_1)+\beta e_K$. This contradicts $\prod_{i=1}^s \eta_i^{e_i} = 1$ (whose level is ∞) and the lemma is proved.

In the end we investigate the action of J on the Fermat quotient of a real unit.

LEMMA 1.6. *For any* $\eta \in E_{K^+} \setminus K_T$, $f(\eta)^J = (-1)^{c(\eta)} f(\eta)$ *if* K_V *is imaginary*, *and* $f(\eta)^J = f(\eta)$ *if* K_V *is real.*

Proof. First, we assume that K_V is imaginary. Let $\eta \equiv x + y\pi_K^{c(\eta)} \bmod \pi_K^{c(\eta)+1}$ according to Lemma 1.1. From Lemmas 1.2 and 1.3,

$$\eta = \eta^J \equiv x^J + y^J(-1)^{c(\eta)}\pi_K^{c(\eta)} \bmod \pi_K^{c(\eta)+1}.$$

Therefore,

$$f(\eta) = f(\eta^J) \equiv \frac{y^J(-1)^{c(\eta)}}{x^J} \equiv (-1)^{c(\eta)}\left(\frac{y}{x}\right)^J \equiv (-1)^{c(\eta)} f(\eta)^J \bmod p.$$

When K_V is real, $\eta = \eta^J \equiv x^J + y^J\pi_K^{c(\eta)} \bmod \pi_K^{c(\eta)+1}$. Thus, $f(\eta) = f(\eta^J) \equiv (y/x)^J \equiv f(\eta)^J$ as desired.

2. A basis of units modulo units of K_T^+. Let the notation be as before. In this section, we shall prove the existence of a set of representatives of a basis of $E^{mp^\delta e_K} E_{K_T^+}/E_{K_T^+}$ which satisfies some conditions on the Fermat quotient and the level.

When K_T is imaginary, let

$$O_{K_T}/(p) = (O_{K_T}/(p))^+ \oplus (O_{K_T}/(p))^-$$

be the decomposition associated with $(1 + J)/2$ and $(1 - J)/2$. Then it is easy to see that

(i) $\dim_{\mathbb{F}_p}(O_{K_T}/(p))^+ = \dim_{\mathbb{F}_p}(O_{K_T}/(p))^- = d_K/2$.

(ii) $E_K^{e_K} \subset \mathrm{Ker}(N) \cdot E_{K_T}$ and $E_{K^+}^{[K^+:K_T^+]} \subset \mathrm{Ker}(N^+) \cdot E_{K_T^+}$, where N and N^+ is the norm map from K to K_T and from K^+ to K_T^+, respectively.

The next lemma is due to Washington [6].

LEMMA 2.1. *Let* E *be a subgroup of* E_K *of finite index and let* η *be a non-torsion element of* E. *If* $v_{\wp_i'}(\log_p\eta)$ *is sufficiently large for all primes* $\wp_i'$ $(i = 1, \ldots, g)$ *then* η *is a pth power in* E. *Here*, *we consider* $v_{\wp_i'}(\log_p\eta)$ *and* $\log_p \eta$ *in the localization of* K *with respect to* $\wp_i'$.

Proof. If η is not a pth power in E, then we can take $u_2, \ldots, u_r \in E$ $(r = \mathrm{rank}_{\mathbb{Z}} E_K)$ such that $\{\eta, u_2, \ldots, u_r\}$ generates a subgroup E' of E of finite index prime to p. Let $\mathrm{R}_p(*)$ be the p-adic regulator of $*$ (see Washington [7]). From our assumption, $\mathrm{R}_p(E') \equiv 0 \bmod \wp_i'^{c}$ for all $\wp_i' \mid p$, where c is sufficiently large. Now,

$$\mathrm{R}_p(E') = [E_K : E][E : E']\mathrm{R}_p(E_K) \neq 0$$

by our assumption (A_3). So, $v_p(\mathrm{R}_p(E')) = v_p([E_K : E]) + v_p(\mathrm{R}_p(E_K))$. The right hand side depends only on K and E. But the left hand side is sufficiently large. That is a contradiction and the proof is complete.

Next we prove a relation between $v_{\wp_i'}(\log_p \eta)$ and the level of η.

LEMMA 2.2. *Let η be any element of $E_K \setminus K_T$ and $\wp_i'$ $(i = 1, \ldots, g)$ the prime of K over p. Suppose $N(\eta) = 1$ and $c(\eta) > e_K/(p-1)$. Then*

$$v_{\wp_i'}(\log_p \eta) \geq \min\{c(\eta) + 1 - v_p(e_K)e_K, c(\eta)\} \quad \textit{for all } \wp_i'.$$

Proof. Let $\eta \equiv x + y\pi_K^{c(\eta)} \bmod \pi_K^{c(\eta)+1}$ according to Lemma 1.1. Let $c = c(\eta)$. Fix any prime $\wp_i' \mid p$. From the assumption, $1 = N(\eta) \equiv x^{e_K} \bmod \pi_K^c$. Observe that the π_K-order of $x^{e_K} - 1$ is a multiple of e_K and c is not a multiple of e_K by Lemma 1.1. Thus $x^{e_K} \equiv 1 \bmod \pi_K^{c+1}$. As $c > e_K/(p-1)$, we have $v_{\wp_i'}(\log_p x^{e_K}) \geq c + 1$ (see Lemma 5.5 of Washington [7]). Thus, $v_{\wp_i'}(e_K) + v_{\wp_i'}(\log_p x) \geq c + 1$. From $v_{\wp_i'}(e_K) = v_p(e_K)e_K$, we obtain $v_{\wp_i'}(\log_p x) \geq c + 1 - v_p(e_K)e_K$. There exists $y_1 \in O_K$ such that $\eta = x + y_1\pi_K^c$ and $y_1 \equiv y \bmod \pi_K$. Then, since $\log_p \eta = \log_p x + \log_p(1 + y_1\pi_K^c/x)$, we have

$$\begin{aligned} v_{\wp_i'}(\log_p \eta) &\geq \min\left\{v_{\wp_i'}(\log_p x), v_{\wp_i'}\left(\log_p\left(1 + \frac{y_1}{x}\pi_K^c\right)\right)\right\} \\ &\geq \min\{c + 1 - v_p(e_K)e_K, c\}. \end{aligned}$$

The lemma is proved.

For any natural number c, we define

$$F_K^c = \{f(\eta) : \eta \in E_{K^+} \setminus K_T \text{ such that } c(\eta) = c\} \subset O_{K_T}/(p).$$

LEMMA 2.3. (I) *If K_T and K_V are imaginary, then $F_K^c \subset (O_{K_T}/(p))^+$ if c is even, and $F_K^c \subset (O_{K_T}/(p))^-$ if c is odd. Moreover, $\dim_{\mathbb{F}_p} F_K^c \leq \frac{1}{2}d_K$.*

(II) *If K_T is imaginary and K_V is real, then $F_K^c \subset (O_{K_T}/(p))^+$ for all c, and $\dim_{\mathbb{F}_p} F_K^c \leq \frac{1}{2}d_K$.*

(III) *If K_T is real and K_V is imaginary, then e_K is even and $c(\eta)$ is even for all $\eta \in E_{K^+} \setminus K_T$. Obviously, $F_K^c \subset (O_{K_T}/(p)) = (O_{K_T}/(p))^+$ and $\dim_{\mathbb{F}_p} F_K^c \leq d_K$.*

(IV) *If K_T and K_V are real, then $F_K^c \subset (O_{K_T}/(p)) = (O_{K_T}/(p))^+$ and $\dim_{\mathbb{F}_p} F_K^c \leq d_K$.*

Proof. (I) Clearly, K is imaginary. Let $\eta \in E_{K^+} \setminus K_T$ and $\eta \equiv x + y\pi_K^{c(\eta)} \bmod \pi_K^{c(\eta)+1}$ according to Lemma 1.1. Let $c = c(\eta)$. Since K_V is imaginary, the statement follows from Lemma 1.6 and (i).

(II) In this case, our statement follows easily from Lemma 1.6 and (i).

(III) Let $\eta \in E_{K^+} \setminus K_T$ and $\eta \equiv x + y\pi_K^{c(\eta)} \bmod \pi_K^{c(\eta)+1}$ according to Lemma 1.1. Let $c = c(\eta)$. Because the order of J is 2, e_K is clearly even. From Lemma 1.3,

$$\eta = \eta^J \equiv x^J + y^J(-1)^c\pi_K^c \bmod \pi_K^{c+1}.$$

Here, $x^J = x$ and $y^J = y$ because K_T is real. So, $x + y\pi_K^c \equiv x + y(-1)^c\pi_K^c \bmod \pi_K^{c+1}$. This means that c is even.

(IV) It is clear.

REMARK 3. We have $r = \operatorname{rank}_{\mathbb{Z}}(E_{K^+}/E_{K_T^+}) = \operatorname{rank}_{\mathbb{Z}} E_{K^+} - \operatorname{rank}_{\mathbb{Z}} E_{K_T^+}$. Hence we easily observe that:

$r = \frac{1}{2}d_K(e_K - 1)$ and $\dim_{\mathbb{F}_p} F_K^c \le \frac{1}{2}d_K$ in the case (I) or (II).
$r = d_K(\frac{1}{2}e_K - 1)$ and $\dim_{\mathbb{F}_p} F_K^c \le d_K$ in the case (III).
$r = d_K(e_K - 1)$ and $\dim_{\mathbb{F}_p} F_K^c \le d_K$ in the case (IV).

THEOREM 2.4. *Let $E \supset E_{K_T^+}$ be a subgroup of E_{K^+} of finite index. Let $r = \operatorname{rank}_{\mathbb{Z}}(E_{K^+}/E_{K_T^+})$. Then there exists a set of representatives $\{\eta_1, \ldots, \eta_r\}$ of a basis of $E^{mp^\delta e_K}E_{K_T^+}/E_{K_T^+}$ such that*

(1) *$c(\eta_i) > e_K/(p-1)$ $(i = 1, \ldots, r)$.*
(2) *$N^+(\eta_i) = 1$ $(i = 1, \ldots, r)$.*
(3) *$c_1 \le c_2 \le \ldots \le c_r$ where $c_i = c(\eta_i)$.*
(4) *Let $S_j = \{\eta_i : c(\eta_i) \equiv j \bmod e_K\}$ $(1 \le j < e_K$ and j is even only if K_T is real and K_V is imaginary). Then $\sharp S_j = \frac{1}{2}d_K$ (d_K resp.) when K_T is imaginary (resp. real) and $\{f(\eta_i) : \eta_i \in S_j\}$ is an $\mathbb{F}_p$-independent system for each j which defines S_j.*

Proof. Let $\{\xi_1, \ldots, \xi_r\}$, $\xi_i \in E$, be a set of representatives of a basis of $E^mE_{K_T^+}/E_{K_T^+}$. Observe that $E^mE_{K_T^+}/E_{K_T^+}$ is torsion-free. From Lemma 1.4, $c(\xi_i^{p^\delta}) > e_K/(p-1)$. From (ii), as $[K^+ : K_T^+] = e_K$ or $e_K/2$, we have $\xi_i^{p^\delta e_K} \in \operatorname{Ker}(N^+) \cdot E_{K_T^+}$. Therefore,

$$\xi_i^{p^\delta e_K} = \eta_i u_i \quad \text{with some } \eta_i \in \operatorname{Ker}(N^+) \cap E \text{ and } u_i \in E_{K_T^+},\ 1 \le i \le r.$$

Here, $\{\eta_1, \ldots, \eta_r\}$ is also a set of representatives of a basis of the quotient $E^{mp^\delta e_K}E_{K_T^+}/E_{K_T^+}$ that satisfies (1) and (2). And (3) is satisfied by an appropriate change of indices.

Now we define the condition (C_s) for $1 \le s < r$: $\{f(\eta_i) : c(\eta_i) \equiv j \bmod e_K,\ 1 \le i \le s\}$ is an $\mathbb{F}_p$-independent system for all j $(1 \le j < e_K$, j is even if K_T is real and K_V is imaginary). Clearly, (C_1) is true. Suppose that (C_s) is valid. Let $c(\eta_{s+1}) = l$. If $\{f(\eta_i) : c(\eta_i) \equiv l \bmod e_K,\ 1 \le i \le s\}$

$\cup \{f(\eta_{s+1})\}$ is an $\mathbb{F}_p$-independent system, then (C_{s+1}) is valid. If it is not $\mathbb{F}_p$-independent, then

$$f(\eta_{s+1}) = \sum_{1\le i\le s,\, c_i\equiv l \bmod e_K} a_i b_0^{\alpha_i} f(\eta_i) \quad \text{with some } a_i \in \mathbb{Z},$$

where $\alpha_i = \frac{1}{e_K}(c(\eta_{s+1})-c(\eta_i))$. We have $c(\eta_i^{a_i p^{\alpha_i}}) = c(\eta_{s+1})$ and $f(\eta_i^{a_i p^{\alpha_i}}) = a_i b_0^{\alpha_i} f(\eta_i)$. Then

$$f\Big(\prod_{1\le i\le s,\, c_i\equiv l \bmod e_K} \eta_i^{a_i p^{\alpha_i}}\Big) = \sum_{1\le i\le s,\, c_i\equiv l \bmod e_K} a_i b_0^{\alpha_i} f(\eta_i) = f(\eta_{s+1}).$$

So, letting

$$\eta'_{s+1} = \eta_{s+1}\Big(\prod_{1\le i\le s,\, c_i\equiv l \bmod e_K} \eta_i^{a_i p^{\alpha_i}}\Big)^{-1},$$

we get $c(\eta'_{s+1}) > c(\eta_{s+1})$. Now $\{\eta_1,\ldots,\eta_s,\eta'_{s+1},\eta_{s+2},\ldots,\eta_r\}$ is also a set of representatives that satisfies (1) and (2). By means of some permutation of $\{\eta'_{s+1},\eta_{s+2},\ldots,\eta_r\}$, we may write it $\{\eta_{s+1},\eta_{s+2},\ldots,\eta_r\}$ again with $c(\eta_{s+1}) \le \ldots \le c(\eta_r)$. Then, further, we repeat the above procedure for η_{s+1}. Lemmas 2.1 and 2.2 imply that the procedure must stop after a finite number of steps. Hence (C_{s+1}) becomes true. So, inductively, we get $\{\eta_1,\ldots,\eta_r\}$ as desired.

Note that, in this theorem, the sum of $\sharp S_j$ for $1 \le j < e_K$ (j is even when K_T is real and K_V is imaginary) is equal to r by Remark 3.

3. A formula for index of subgroups. Let E and E' be subgroups of E_{K^+} such that $E \supset E' \supset E_{K_T^+}$ and $[E_{K^+} : E'] < \infty$. Let $\{\eta_i\}$ and $\{\theta_i\}$ be as in Theorem 2.4 for E and E', respectively.

For $\eta \in E_K$, let $\overline{\eta}$ denote $\eta \bmod E_{K_T^+}$, and $c(\overline{\eta}) = c(\eta)$ and $f(\overline{\eta}) = f(\eta)$. They are well defined because $c(\eta u) = c(\eta)$ and $f(\eta u) = f(\eta)$ for any $u \in E_{K_T^+}$.

We define d_0 to be $\frac{1}{2}d_K$ if K_T is imaginary (in the case (I) or (II) in Lemma 2.3) and d_K if K_T is real (in the case (III) or (IV) in Lemma 2.3). We let $R = \{1,\ldots,r\}$ and $B_l = \{(l-1)d_0+1,\ldots,ld_0\}$ ($1 \le l < e_K$), in the case (I), (II) or (IV) in Lemma 2.3. Moreover we define B_l in the case (III) as follows:

$$B_l = \big\{\big(\tfrac{l}{2}-1\big)d_0+1,\ldots,\tfrac{l}{2}d_0\big\} \quad \text{for } 1 < l < e_K \text{ and } l \text{ even}.$$

Then R is the union of all B_l.

We permute $\overline{\eta}_1,\ldots,\overline{\eta}_r$ and $\bar{\theta}_1,\ldots,\bar{\theta}_r$ such that $c(\eta_i) \equiv l \bmod e_K$ for all $i \in B_l$ and $c(\theta_j) \equiv l \bmod e_K$ for all $j \in B_l$.

We let, for all $j = 1, \ldots, r$,

$$(5) \quad \bar{\theta}_j = \prod_{i=1}^{r} \bar{\eta}_i{}^{a_{ji}p^{e_{ji}}} \quad \text{where } a_{ji} \in \mathbb{Z} \text{ is 0 or prime to } p, \text{ and } 0 \le e_{ji} \in \mathbb{Z}.$$

Then

$$\begin{aligned} \det(a_{ji}p^{e_{ji}}) &= [E^{mp^{\delta}e_K} E_{K_T^+}/E_{K_T^+} : (E')^{mp^{\delta}e_K} E_{K_T^+}/E_{K_T^+}] \\ &= [E^m E_{K_T^+}/E_{K_T^+} : (E')^m E_{K_T^+}/E_{K_T^+}] \\ &= [E : E'] \times (\text{a natural number prime to } p) \end{aligned}$$

since $E^m E_{K_T^+}/E_{K_T^+}$ and $(E')^m E_{K_T^+}/E_{K_T^+}$ are torsion-free and m is prime to p by our assumption (A_2). Consequently, we have:

LEMMA 3.1. *Let E and E' be subgroups of E_{K^+} such that $E \supset E' \supset E_{K_T^+}$ and $[E_{K^+} : E'] < \infty$. Then $v_p(\det(a_{ji}p^{e_{ji}})) = v_p([E : E'])$.*

Next we prove a formula for index $[E : E']$.

THEOREM 3.2. *Let E and E' be subgroups of E_{K^+} such that $E \supset E' \supset E_{K_T^+}$ and $[E_{K^+} : E'] < \infty$. Let $\{\eta_j\}$ and $\{\theta_j\}$ be as in Theorem 2.4 for E and E', respectively. Then*

$$v_p([E : E']) = \frac{1}{e_K}\Big\{\sum_{j=1}^{r} c(\bar{\theta}_j) - \sum_{j=1}^{r} c(\bar{\eta}_j)\Big\}.$$

Proof. By the properties of level given in Section 1,

$$c(\bar{\theta}_j) = \min\{c(\bar{\eta}_i{}^{a_{ji}p^{e_{ji}}}) : 1 \le i \le r\}.$$

Define $A_j = \{i \in R : c(\bar{\theta}_j) = c(\bar{\eta}_i{}^{a_{ji}p^{e_{ji}}})\}$, $1 \le j \le r$. Clearly, A_j is non-empty and $A_j \subset B_l$ if $j \in B_l$. Further,

$$f(\bar{\theta}_j) = \sum_{i \in A_j} f(\bar{\eta}_i{}^{a_{ji}p^{e_{ji}}}) = \sum_{i \in A_j} a_{ji} b_0^{e_{ji}} f(\bar{\eta}_i) \quad \text{for all } j \in R.$$

Since $\{f(\bar{\eta}_i)\}_{i \in B_l}$ and $\{f(\bar{\theta}_j)\}_{j \in B_l}$ are $\mathbb{F}_p$-independent systems, it follovs that

$$(6) \qquad \det(a'_{ji} b_0^{e_{ji}})_{j,i \in B_l} \not\equiv 0 \bmod p \quad \text{for all } l,$$

where $a'_{ji} = a_{ji}$ if $i \in A_j$ and $a'_{ji} = 0$ if $i \notin A_j$.

Now we define P_l ($1 \le l < e_K$, l is even in the case (III) in Lemma 2.3) to be the set of all permutations on B_l and $P'_l = \{\tau_l \in P_l : \tau_l(j) \in A_j$ for all $j \in B_l\}$.

Then, for each l,

$$(7) \qquad \det(a'_{ji} b_0^{e_{ji}})_{j,i \in B_l} = \sum_{\tau_l \in P'_l} \Big(\mathrm{sgn}(\tau_l) \cdot \prod_{j \in B_l} a_{j\tau_l(j)} b_0^{e_{j\tau_l(j)}}\Big).$$

From (6) and (7), we see that P'_l is non-empty for every l. Let P be the set of all permutations on R and $P' = \{\varrho \in P : \varrho(j) \in A_j \text{ for all } j \in R\}$. It is clear that any element of P' is a product of $\tau_l \in P'_l$ ($1 \le l < e_K$, l is even in the case (III) of Lemma 2.3) and the restriction of each $\varrho \in P'$ to B_l is an element of P'_l. So, we see that P' is non-empty. In general, for any $\varrho \in P$, $c(\bar\theta_j) \le c(\bar\eta_{\varrho(j)}^{a_{j\varrho(j)}p^{e_{j\varrho(j)}}})$ for all $j \in R$, while for each $\varrho \in P \setminus P'$, $c(\bar\theta_j) < c(\bar\eta_{\varrho(j)}^{a_{j\varrho(j)}p^{e_{j\varrho(j)}}})$ with some $j \in R$. Therefore, for each $\varrho \in P \setminus P'$,

$$\sum_{j=1}^{r} c(\bar\theta_j) < \sum_{j=1}^{r} c(\bar\eta_{\varrho(j)}^{a_{j\varrho(j)}p^{e_{j\varrho(j)}}}). \tag{8}$$

For $\varrho \in P'$, by the definition,

$$\sum_{j=1}^{r} c(\bar\theta_j) = \sum_{j=1}^{r} c(\bar\eta_{\varrho(j)}^{a_{j\varrho(j)}p^{e_{j\varrho(j)}}}).$$

Since

$$\sum_{j=1}^{r} c(\bar\eta_{\varrho(j)}^{a_{j\varrho(j)}p^{e_{j\varrho(j)}}}) = \sum_{j=1}^{r}\{c(\bar\eta_{\varrho(j)}) + e_K e_{j\varrho(j)}\} = \sum_{j=1}^{r} c(\bar\eta_{\varrho(j)}) + e_K \sum_{j=1}^{r} e_{j\varrho(j)},$$

we have

$$\sum_{j=1}^{r} e_{j\varrho(j)} = \frac{1}{e_K}\Big\{\sum_{j=1}^{r} c(\bar\theta_j) - \sum_{j=1}^{r} c(\bar\eta_j)\Big\} \quad \text{for all } \varrho \in P'. \tag{9}$$

Similarly, from (8),

$$\sum_{j=1}^{r} e_{j\varrho(j)} > \frac{1}{e_K}\Big\{\sum_{j=1}^{r} c(\bar\theta_j) - \sum_{j=1}^{r} c(\bar\eta_j)\Big\} \quad \text{for all } \varrho \in P \setminus P'. \tag{10}$$

From (7) and (9),

$$\begin{aligned}
&\prod_l \det(a'_{ji} b_0^{e_{ji}})_{j,i\in B_l} \\
&\qquad = \sum_{\varrho\in P'} \Big(\operatorname{sgn}(\varrho) \cdot \prod_{j=1}^{r} a_{j\varrho(j)} b_0^{e_{j\varrho(j)}}\Big) \\
&\qquad = \sum_{\varrho\in P'} \Big(\operatorname{sgn}(\varrho) \cdot b_0^{\sum_{j=1}^{r} e_{j\varrho(j)}} \cdot \prod_{j=1}^{r} a_{j\varrho(j)}\Big) \\
&\qquad = b_0^{(1/e_K)(\sum_{j=1}^{r} c(\bar\theta_j) - \sum_{j=1}^{r} c(\bar\eta_j))} \cdot \sum_{\varrho\in P'} \Big(\operatorname{sgn}(\varrho) \cdot \prod_{j=1}^{r} a_{j\varrho(j)}\Big).
\end{aligned}$$

Therefore, from (6),

$$\sum_{\varrho\in P'}\Big(\operatorname{sgn}(\varrho)\cdot\prod_{j=1}^{r}a_{j\varrho(j)}\Big)\not\equiv 0 \bmod p. \tag{11}$$

Now, we have

$$\begin{aligned}(12)\quad &\det(a_{ji}p^{e_{ji}})_{1\le j,i\le r}\\ &=\sum_{\varrho\in P'}\Big(\operatorname{sgn}(\varrho)\cdot\prod_{j=1}^{r}a_{j\varrho(j)}p^{e_{j\varrho(j)}}\Big)+\sum_{\varrho\in P\setminus P'}\Big(\operatorname{sgn}(\varrho)\cdot\prod_{j=1}^{r}a_{j\varrho(j)}p^{e_{j\varrho(j)}}\Big)\\ &=\sum_{\varrho\in P'}\Big(\operatorname{sgn}(\varrho)\cdot p^{\sum_{j=1}^{r}e_{j\varrho(j)}}\cdot\prod_{j=1}^{r}a_{j\varrho(j)}\Big)\\ &\quad+\sum_{\varrho\in P\setminus P'}\Big(\operatorname{sgn}(\varrho)\cdot p^{\sum_{j=1}^{r}e_{j\varrho(j)}}\cdot\prod_{j=1}^{r}a_{j\varrho(j)}\Big)\\ &=p^{(1/e_K)(\sum_{j=1}^{r}c(\bar\theta_j)-\sum_{j=1}^{r}c(\overline\eta_j))}\cdot\sum_{\varrho\in P'}\Big(\operatorname{sgn}(\varrho)\cdot\prod_{j=1}^{r}a_{j\varrho(j)}\Big)\\ &\quad+\sum_{\varrho\in P\setminus P'}\Big(\operatorname{sgn}(\varrho)\cdot p^{\sum_{j=1}^{r}e_{j\varrho(j)}}\cdot\prod_{j=1}^{r}a_{j\varrho(j)}\Big).\end{aligned}$$

Combining (10)–(12), we get

$$v_p(\det(a_{ji}p^{e_{ji}})_{1\le j,i\le r})=\frac{1}{e_K}\Big\{\sum_{j=1}^{r}c(\bar\theta_j)-\sum_{j=1}^{r}c(\overline\eta_j)\Big\}.$$

The proof is completed by using Lemma 3.1.

LEMMA 3.3. *Let E and E' be subgroups of E_{K^+} such that $E\supset E'\supset E_{K_T^+}$ and $[E_{K^+}:E']<\infty$. Let $\{\eta_i\}$ and $\{\theta_i\}$ be as in Theorem 2.4 for E and E', respectively. Then $c(\bar\theta_i)\ge c(\overline\eta_i)$ for all $i=1,\dots,r$.*

Proof. Suppose that there exists t such that $1\le t\le r$ and $c(\bar\theta_t)<c(\overline\eta_t)$. For each l ($1\le l\le e_K-1$, l is even in the case (III)), we define

$$T_l=\{\bar\theta_h:1\le h\le t,\ c(\bar\theta_h)\equiv l \bmod e_K\}.$$

Then $\{\bar\theta_1,\dots,\bar\theta_t\}=\bigcup_l T_l$ (disjoint union) and $t=\sum_l\sharp T_l$. Fix any l. Then each $f(\bar\theta_h)$ ($\bar\theta_h\in T_l$) is a linear combination of $f(\overline\eta_1),\dots,f(\overline\eta_{t-1})$ because $c(\bar\theta_1)\le\dots\le c(\bar\theta_t)<c(\overline\eta_t)\le\dots\le c(\overline\eta_r)$. For each l ($1\le l\le e_K-1$, l is even in the case (III)), we define

$$T_l'=\{\overline\eta_i:1\le i\le t-1,\ c(\overline\eta_i)\equiv l \bmod e_K\}.$$

Then $\{\bar{\eta}_1, \ldots, \bar{\eta}_{t-1}\} = \bigcup_l T'_l$ (disjoint union) and $t - 1 = \sum_l \sharp T'_l$. Now $f(\bar{\theta}_h)$ ($\bar{\theta}_h \in T_l$) is a linear combination of $\{f(\bar{\eta}_i) : \bar{\eta}_i \in T'_l\}$. Therefore, from Theorem 2.4(4), we have $\sharp T_l \le \sharp T'_l$ for any l, and hence $\sum_l \sharp T_l \le \sum_l \sharp T'_l$. This is a contradiction.

Note that, in Theorem 3.2, it does not necessarily hold that

$$c(\bar{\theta}_i) \equiv c(\bar{\eta}_i) \bmod e_K \quad \text{for all } i = 1, \ldots, r,$$

because $c(\bar{\theta}_1)$ is not necessarily congruent to $c(\bar{\eta}_1)$ modulo e_K.

Observe that we can define integers $l(\eta_i)$ and $u(\eta_i)$ as follows:

$$c(\eta_i) = l(\eta_i) + u(\eta_i)e_K, \quad 1 \le l(\eta_i) < e_K,\ 0 \le u(\eta_i) \in \mathbb{Z},\ 1 \le i \le r.$$

Let $l(\theta_i)$ and $u(\theta_i)$ be defined in the same way for θ_i. From Lemma 3.3,

$$c(\theta_i) - c(\eta_i) = l(\theta_i) - l(\eta_i) + e_K\{u(\theta_i) - u(\eta_i)\} \ge 0.$$

So that, $u(\theta_i) \ge u(\eta_i)$ for all $i = 1, \ldots, r$. In addition,

$$\begin{aligned} \sum_{i=1}^r c(\theta_i) - \sum_{i=1}^r c(\eta_i) &= \sum_{i=1}^r \{l(\theta_i) - l(\eta_i)\} + e_K \sum_{i=1}^r \{u(\theta_i) - u(\eta_i)\} \\ &= e_K \sum_{i=1}^r \{u(\theta_i) - u(\eta_i)\}, \end{aligned}$$

because $\sum_{i=1}^r l(\theta_i) = \sum_{i=1}^r l(\eta_i)$ from Theorem 2.4(4).

On the other hand, by Lemma 3.3, we can easily see that the sequence of rational integers $\{c(\eta_1), \ldots, c(\eta_r)\}$, hence $\{u(\eta_1), \ldots, u(\eta_r)\}$, depends only on E. So we may write $u(\eta_i) = u_i(E)$ and $u(\theta_i) = u_i(E')$. Consequently, by means of Theorem 3.2, we have proved the following:

Theorem 3.4. *Let E and E' be subgroups of E_{K^+} such that $E \supset E' \supset E_{K_T^+}$ and $[E_{K^+} : E'] < \infty$. Let $u_i(E)$ and $u_i(E')$ be as above. Then*

$$v_p([E : E']) = \sum_{i=1}^r \{u_i(E') - u_i(E)\}.$$

This is a generalization of Theorems B and D. Now, following Dénes, we may call $u_i(E)$ the p-character of E.

References

[1] A. Brumer, *On the units of algebraic number fields*, Mathematika 14 (1967), 121–124.

[2] P. Dénes, *Über irreguläre Kreiskörper*, Publ. Math. Debrecen 3 (1953), 17–23.

[3] —, *Über Grundeinheitssysteme der irregulären Kreiskörper von besonderen Kongruenzeigenschaften*, ibid. 3 (1954), 195–204.

[4] P. Dénes, *Über den zweiten Faktor der Klassenzahl und den Irregularitätsgrad der irregulären Kreiskörper*, ibid. 4 (1956), 163–170.
[5] F. Kurihara, *On the p-adic expansion of units of cyclotomic fields*, J. Number Theory 32 (1989), 226–253.
[6] L. C. Washington, *Units of irregular cyclotomic fields*, Illinois J. Math. 23 (1979), 635–647.
[7] —, *Introduction to Cyclotomic Fields*, Springer, New York, 1997.

Kanagawa Prefectural Yamato-Higashi High-School
1760 Fukami, Yamato, Kanagawa, 242, Japan
E-mail: tshimada@qa2.so-net.or.jp

Received on 15.7.1997
and in revised form on 3.3.1998 (3216)