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 $\varepsilon$ of $\mathbb{Q}(\zeta_p)$ which is not in $\mathbb{Z}$, there exist rational integers $a$, $b$ and $c$ satisfying $\varepsilon \equiv a + b(1 - \zeta_p)^c \mod (1 - \zeta_p)^{c+1}$, $ab \not\equiv 0 \mod p$ and $c \not\equiv 0 \mod (p-1)$, where $c$ is uniquely determined by $\varepsilon$. 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 $B_{ipj} \equiv 0 \mod p^{2j+1}$ for $0 \leq j < u_i$ and $B_{ipji} \not\equiv 0 \mod p^{2u_i+1}$, 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

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

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

**Theorem B.** We have

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

Here $h(\cdot)$ denotes the class number of a field $\cdot$ 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 \( \omega \) 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 \( \mathbb{Q}(\zeta_{p^{n+1}})^+ \), \( 0 \leq n \in \mathbb{Z} \), 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

\[
\theta_i^n \equiv a_i + b_i \pi c_i \mod \pi^i + 1, \quad i = 1, \ldots, r,
\]

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

Here \( d = [\mathbb{Q}(\zeta_{p^{n+1}})^+: K_{n+1}] \), \( r = \text{rank } E_{K_{n+1}} = \frac{1}{2d} \varphi(p^{n+1}) - 1 \) and \( \pi \) is the image of \( (1 - \zeta_p^{p+1})(1 - \zeta_p^{-1}) \) 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 \( \varphi_1, \ldots, \varphi_g \) be the primes of \( K_T \) over \( p \), \( \varphi_i' \) \( (i = 1, \ldots, g) \) the primes of \( K \) in the ring \( O_K \) of integers of \( K_\star \) is the group of units of a field \( \star \). Let \( \delta \) be the least natural number \( a \) that satisfies \( e_K/(p - 1) < p^{a-1} \).

Throughout this paper, we assume the following three conditions:

(A1) \( \varphi \) is a principal ideal.

(A2) The exponent of the torsion part of \( E_{K_+}/E_{K_T^+} \) is prime to \( p \).

(A3) The Leopoldt conjecture is valid for \( K \) and \( p \).
Then we may write \( \varphi = (\pi_K) \) 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 \( E \supseteq E_{K_+}^+ \) and \([E_{K_+} : E] < \infty \). Then there exists a basis \( \{\eta_1, \ldots, \eta_r\} \) of \( E^{mp\epsilon_K} E_{K_+} \mod E_{K_+}^+ \) such that

\[
\eta_i \equiv a_i + b_i \pi_K^c \mod \pi_K^{c_i+1}, \quad i = 1, \ldots, r = \text{rank } E_{K_+}/E_{K_+}^+,
\]
where \( a_i \) and \( b_i \) belong to the ring \( O_K \) of integers of \( K_T \), \( a_i \not\equiv 0 \mod p \) and \( a_i \) is a natural number such that \( a_i \not\equiv 0 \mod e_K \).

Further, let \( u_i(E) = \left[ \frac{a_i}{b_i} \right] \) (Gauss symbol) and \( E' \) be a subgroup of \( E \) such that \( E' \supseteq E_{K_+}^+ \) and \([E_{K_+} : E'] < \infty \). Then

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

**Remark 1.** Let \( \eta \) be any element of \( E_{K_+} \setminus K_T \) such that \( \eta^a \in E_{K_+}^+ \) for some natural number \( a \). Then, for any \( \sigma \in \text{Gal}(K/K_T) \), \((\eta^a)^\sigma/\eta^a = (\eta^a)^\sigma/\eta^a = \eta^a/\eta^a = 1 \). So, \( \eta^a \) is an \( \epsilon \)th root of unity. Moreover, when \( K \) is a real or CM-field, \( \eta^a \) is real, hence \( \pm 1 \) and \((\eta^a)^{\epsilon a - 1} = 1 \). Thus, \( \eta^a \in E_{K_+}^+ \) 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 \( E' = C_{K_+}^+ E_{K_+}^+ \), where \( C_K \) is the group of cyclotomic units and \( C_K^+ = C_K \cap K^+ \). Then, since \( v_p([E : E']) = v_p(h(K^+)/h(K_{K_+}^+)) \), we get a generalization of Theorem B:

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

**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 \( f(X) = X^{e_K} + c'_{e_K-1}X^{e_K-1} + \ldots + c'_0X + c'_0 \in \mathbb{Z}[X] \) be the minimal polynomial of \( \pi_K \) which is of Eisenstein type. That is, \( c'_{e_K-1} \equiv \ldots \equiv c'_0 \equiv 0 \mod p \) and \( c'_0 \not\equiv 0 \mod p^2 \). We write \( c_i = -pc_i \) (\( i = 0, 1, \ldots, e_K - 1 \)). Then

\[
\pi_K^{e_K} \equiv pc_0 \mod \pi_K^{e_K+1} \quad \text{and} \quad p \equiv b_0\pi_K^{e_K} \mod \pi_K^{e_K+1},
\]
where \( b_0 \) is the natural number such that \( c_0b_0 \equiv 1 \mod p \) and \( 1 \leq b_0 \leq p-1 \).
For any \( z \in O_K \setminus K_T \) which is prime to \( p \), we define
\[
c(z) = \max\{0 \leq c \in \mathbb{Z} : z \equiv x + y\pi_K^c \mod \pi_K^{c+1} \text{ for some } x, y \in O_{K_T}\}.
\]

It can be easily seen that \( 1 \leq c(z) < \infty \). 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
\[
x_0 \not\equiv 0 \mod \phi_i \ (i = 1, \ldots, g) \quad \text{and} \quad y_0 \not\equiv 0 \mod p.
\]
If \( c(z) \) is a multiple of \( e_K \), then writing \( c(z) = ce_K \) with a natural number \( c \), we have
\[
z \equiv x_0 + y_0\pi_K^{ce_K} \equiv x_0 + y_0p^ec_0 \mod \pi_K^{ce_K+1},
\]
which contradicts the maximality of \( c(z) \). Thus, we get \( c(z) \not\equiv 0 \mod e_K \).

To sum up, we have the following:

**Lemma 1.1.** For any \( z \in O_K \setminus K_T \) which is prime to \( p \),
\[
c(z) = \max\{0 \leq c \in \mathbb{Z} : z \equiv x + y\pi_K^c \mod \pi_K^{c+1} \text{ for some } x, y \in O_{K_T}\}
\]
is a natural number which depends only on \( z \) (it does not depend on the choice of \( \pi_K \)) and \( c(z) \not\equiv 0 \mod e_K \). Let \( x_0 \) and \( y_0 \) be elements in \( O_{K_T} \) giving \( c(z) \). Then \( x_0 \not\equiv 0 \mod \phi_i \ (i = 1, \ldots, g) \) and \( y_0 \not\equiv 0 \mod p \), 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 \( \eta \equiv x + y\pi_K^{c(\eta)} \mod \pi_K^{c(\eta)+1} \) be a congruence giving \( c(\eta) \) according to Lemma 1.1. Then, in the following, we call \( c(\eta) \) the level of \( \eta \) and \((y/x) \mod p \in O_{K_T}/(p)\) the (generalized) Fermat quotient of \( \eta \) and we denote the latter by \( f(\eta) \). Of course they are uniquely determined by \( \eta \).

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 \( c(\eta^a) = c(\eta) \), \( c(\eta^a) = c(\eta) \), \( f(\eta^a) = af(\eta) \) and \( c(\eta^{-1}) = c(\eta) \), \( f(\eta^{-1}) = -f(\eta) \).

(2) Let \( \eta_1 \) and \( \eta_2 \) be elements in \( E_K \setminus K_T \) such that \( c(\eta_1) < c(\eta_2) \). Then \( c(\eta_1\eta_2) = c(\eta_1) \) and \( f(\eta_1\eta_2) = f(\eta_1) \).

(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 \( f(\eta_1) + \ldots + f(\eta_s) \not\equiv 0 \mod p \). Then \( c(\eta_1 \ldots \eta_s) = c(\eta_1) \) and \( f(\eta_1 \ldots \eta_s) = f(\eta_1) + \ldots + f(\eta_s) \).

**Lemma 1.3.** If \( K_V \) is imaginary, then \( \pi_K^l \equiv -\pi_K \mod \pi_K^2 \).
For all natural numbers $u \in E_{K_\nu}$ such that $\pi_K^u = \pi_K u$. We have $\pi_K = (\pi_K^u)^J = (\pi_K u)^J = \pi_K uu^J$. Thus, $uu^J = 1$.

First, we assume $u \not\in K_T$. Let $u \equiv a + b\pi_K^{c(u)} \mod \pi_K^{c(u)+1}$ according to Lemma 1.1. For any $\sigma \in \text{Gal}(K/K_\nu)$, $u^\sigma = u$, $\pi_K^u = \pi_K$ and $u \equiv a^\sigma + b^\sigma \pi_K^{c(u)} \mod \pi_K^{c(u)+1}$. Because $O_{K_\nu}/(\pi_K) = \mathbb{Z}/(p)$, we can always write $u \equiv a + b\pi_K^{c(u)} \mod \pi_K^{c(u)+1}$ where $a, b \in \mathbb{Z}$ are prime to $p$. Then $1 = uu^J \equiv a^2 \mod \pi_K$, so $a \equiv \pm1 \mod p$. Since $\pi_K^J \equiv a\pi_K \mod \pi_K^J$, we have $uu^J \equiv a + ba^{c(u)}\pi_K^{c(u)} \mod \pi_K^{c(u)+1}$. By Lemma 1.2, $f(u^{-1}) = f(u^J) \equiv ba^{c(u)-1} \mod p$ and $f(u^{-1}) = -f(u) \equiv -ba^{-1} \mod p$. This means $a^{c(u)} = -1 \mod p$, so that $a \equiv -1 \mod p$ 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 $u = \pm1$. 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 $c(\eta_\chi) > e_K/(p - 1)$. If $c(\eta) > e_K/(p - 1)$, then $c(\eta_\chi) = c(\eta) + ae_K$ and $f(\eta_\chi) = b_0^a f(\eta)$ for all natural numbers $a$. Here $\delta$ and $b_0$ are as in the introduction.

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

\begin{equation}
\eta^p = x^p + px^{p-1}y_1\pi_K^{c(\eta)} \\
+ \left(\frac{p}{2}\right) x^{p-2}y_1^2\pi_K^{2c(\eta)} + \ldots + \left(\frac{p}{p-1}\right) x y_1^{p-1} \pi_K^{(p-1)c(\eta)} + y_1^p \pi_K^{pc(\eta)}.
\end{equation}

Since the $\pi_K$-orders of terms on the right hand side are $0, e_K + c(\eta), e_K + 2c(\eta), \ldots, e_K + (p - 1)c(\eta)$ 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,

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

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

For all natural numbers $a$, we get by induction

$$c(\eta_\chi) \geq \min\left\{\frac{e_K}{p-1}, p^a c(\eta)\right\}. $$
Since $c(\eta^p^{d-1}) \geq e_K/(p-1)$, (2) means that
\[ c(\eta^p) \geq \min\{e_K + c(\eta^{p^{d-1}}), pc(\eta^{p^{d-1}})\} > \frac{e_K}{p-1}. \]
When $e_K/(p-1) < c(\eta)$, we have
\[ e_K + c(\eta) < pc(\eta) \quad \text{and} \quad \eta^p \equiv x^p + px^{p-1}y_1 \eta^K c(\eta) \mod \pi_K^{e_K+c(\eta)+1}. \]
Now from (1), we have
\[ (3) \quad \eta^p \equiv x^p + b_0 x^{p-1} y_1 \pi_K^{e_K+c(\eta)+1} \mod \pi_K^{e_K+c(\eta)+1}. \]
So, we conclude that $c(\eta^p) \geq c(\eta) + e_K$.

Suppose $c(\eta^p) > c(\eta) + e_K$. Let $\eta^p \equiv x_2 + y_2 \pi_K^{c(\eta')} \mod \pi_K^{c(\eta') + 1}$ according to Lemma 1.1. Then
\[ x_2 \equiv \eta^p \equiv x_2 + b_0 x^{p-1} y_1 \pi_K^{e_K+c(\eta')} \mod \pi_K^{e_K+c(\eta')+1} \]
and
\[ x_2 - x^p \equiv b_0 x^{p-1} y_1 \pi_K^{e_K+c(\eta')} \mod \pi_K^{e_K+c(\eta')+1}. \]
Take a prime $\varphi'$ dividing $\pi_K$ of $K$ such that $y \not\equiv 0 \mod \varphi'$. Then, from the above, $e_K + c(\eta) = v_{\varphi'}(b_0 x^{p-1} y_1 \pi_K^{e_K+c(\eta)}) = v_{\varphi'}(x_2 - x^p)$. 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),
\[ f(\eta^p) \equiv b_0 \frac{x^{p-1} y_1}{x^p} \equiv b_0 \frac{y_1}{x} \equiv b_0 f(\eta) \mod p. \]
This means that $f(\eta^{p^a}) = b_0^a f(\eta)$ 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 $F_p$-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 $e_i = a_i b_i$ $(\mathbb{Z} \ni a_i \neq 0 \mod p, 0 \leq b_i \in \mathbb{Z}, i = 1, \ldots, s)$. Then from Lemmas 1.2 and 1.4 we have
\[ c(\eta_i^{e_i}) = c(\eta_i^{b_i}) = c(\eta_i) + b_i e_K \quad \text{and} \quad f(\eta_i^{e_i}) = a_i f(\eta_i^{b_i}) = b_i^a a_i f(\eta_i). \]
We denote by $\beta$ 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,
\[ \sum_{i=1}^{t} f(\eta_i^{e_i}) = \sum_{i=1}^{t} b_i^a a_i f(\eta_i) \neq 0 \mod p. \]
Now, \( c(\eta_i^{c_i}) = c(\eta_i) + b_i e_K = c(\eta_i) + \beta e_K \) for all \( i = 1, \ldots, t \). So, from Lemma 1.2, \( c(\prod_{i=1}^t \eta_i^{c_i}) = c(\eta_i) + \beta e_K < c(\eta_i^{c_i}) \) for all \( t + 1 \leq j \leq s \). Therefore, \( c(\prod_{i=1}^s \eta_i^{c_i}) = c(\prod_{i=1}^t \eta_i^{c_i}) = c(\eta_1) + \beta e_K \). This contradicts \( \prod_{i=1}^s \eta_i^{c_i} = 1 \) (whose level is \( \infty \)) 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 \( \eta \equiv x + y \pi_K^{c(\eta)} \mod \pi_K^{c(\eta)+1} \) according to Lemma 1.1. From Lemmas 1.2 and 1.3,

\[
\eta = \eta^J \equiv x^J + y^J(-1)^c(\eta) \pi_K^{c(\eta)} \mod \pi_K^{c(\eta)+1}.
\]

Therefore,

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

When \( K_V \) is real, \( \eta = \eta^J \equiv x^J + y^J \pi_K^{c(\eta)} \mod \pi_K^{c(\eta)+1} \). 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 \( E^{mp^t \epsilon_K} E_{K_T^+} / E_{K_T} \) 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) \( \dim_{p}(O_{K_T}/(p))^+ = \dim_{F_p}(O_{K_T}/(p))^- = d_K/2 \).

(ii) \( E_{K}^+ \subset \text{Ker}(N) \cdot E_{K_T} \) and \( E_{K_T^+}^{[K^+:K_T^+]} \subset \text{Ker}(N^+) \cdot E_{K_T^+} \), 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 \( \eta \) be a non-torsion element of \( E \). If \( v_{\varphi_i}(\log_p \eta) \) is sufficiently large for all primes \( \varphi_i \) (i = 1, \ldots, g) then \( \eta \) is a \( p \)th power in \( E \). Here, we consider \( v_{\varphi_i}(\log_p \eta) \) and \( \log_p \eta \) in the localization of \( K \) with respect to \( \varphi_i \).

**Proof.** If \( \eta \) is not a \( p \)th power in \( E \) then we can take \( u_2, \ldots, u_r \in E \) (\( r = \text{rank}_E E_K \)) such that \( \{ \eta, u_2, \ldots, u_r \} \) generates a subgroup \( E' \) of \( E \) of
finite index prime to $p$. Let $R_p(*)$ be the $p$-adic regulator of $*$ (see Washington [7]). From our assumption, $R_p(E') \equiv 0 \mod \psi_i^c$ for all $\psi_i | p$, where $c$ is sufficiently large. Now,
\[
R_p(E') = [E_K : E] R_p(E'_K) \neq 0
\]
by our assumption (A_3). So, $v_p(R_p(E')) = v_p([E_K : E]) + v_p(R_p(E'_K))$. The right hand side depends only on $E$ 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 $v_{\psi_i'}(\log_p \eta)$ and the level of $\eta$.

**Lemma 2.2.** Let $\eta$ be any element of $E_K \setminus K_T$ and $\psi_i'$ ($i = 1, \ldots, g$) the prime of $K$ over $p$. Suppose $N(\eta) = 1$ and $c(\eta) > e_K/(p - 1)$. Then
\[
v_{\psi_i'}(\log_p \eta) \geq \min\{c(\eta) + 1 - v_p(c_Ke_K), c(\eta)\} \quad \text{for all } \psi_i'.
\]

**Proof.** Let $\eta \equiv x + y\pi_K^{c(\eta)} \mod \pi_K^{c(\eta)+1}$ according to Lemma 1.1. Let $c = c(\eta)$. Fix any prime $\psi_i' | p$. From the assumption, $1 = N(\eta) \equiv x^{e_K} \mod \pi_K^{e_K}$. Observe that the $\pi_K$-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 $x^{e_K} \equiv 1 \mod \pi_K^{c+1}$. As $c > e_K/(p - 1)$, we have $v_{\psi_i'}(\log_p x^{e_K}) \geq c + 1$ (see Lemma 5.5 of Washington [7]). Thus, $v_{\psi_i'}(e_K) + v_{\psi_i'}(\log_p x) \geq c + 1$. From $v_{\psi_i'}(e_K) = v_p(c_Ke_K)$, we obtain $v_{\psi_i'}(\log_p x) \geq c + 1 - v_p(c_Ke_K)$. Thus there exists $y_1 \in O_K$ such that $\eta = x + y_1\pi_K^{e_K}$ and $y_1 \equiv y \mod \pi_K$. Then, since $\log_p \eta = \log_p x + \log_p (1 + y_1\pi_K^{e_K}/x)$, we have
\[
v_{\psi_i'}(\log_p \eta) \geq \min\{v_{\psi_i'}(\log_p x), v_{\psi_i'}(\log_p \left(1 + \frac{y_1}{x}\pi_K^{e_K}\right))\}
\]
\[
\geq \min\{c + 1 - v_p(c_Ke_K), c\}.
\]
The lemma is proved.

For any natural number $c$, we define
\[
F^c_K = \{f(\eta) : \eta \in E_{K^+} \setminus K_T \text{ such that } c(\eta) = c\} \subseteq O_{K_T}(p).
\]

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

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

(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, $F^c_K \subseteq (O_{K_T}, (p))^+ = (O_{K_T}, (p))^+$ and $\dim_{\mathbb{F}_p} F^c_K \leq d_K$.

(IV) If $K_T$ and $K_V$ are real, then $F^c_K \subseteq (O_{K_T}, (p))^+ = (O_{K_T}, (p))^+$ and $\dim_{\mathbb{F}_p} F^c_K \leq d_K$.

**Proof.** (I) Clearly, $K$ is imaginary. Let $\eta \in E_{K^+} \setminus K_T$ and $\eta \equiv x + y\pi_K^{c(\eta)} \mod \pi_K^{c(\eta)+1}$ 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 \( \eta \in E_{K^+}/K_T \) and \( \eta \equiv x + y\pi_{\epsilon K}^{c(\eta)} \) mod \( \pi_{\epsilon K}^{c(\eta) + 1} \) according to Lemma 1.1. Let \( c = c(\eta) \). Because the order of \( J \) is 2, \( \epsilon K \) is clearly even. From Lemma 1.3,

\[
\eta = \eta' \equiv x' + y'(-1)^c\pi_{\epsilon K} \text{ mod } \pi_{\epsilon K}^{c+1}.
\]

Here, \( x' = x \) and \( y' = y \) because \( K_T \) is real. So, \( x + y\pi_{\epsilon K} \equiv x + y(-1)^c\pi_{\epsilon K} \) mod \( \pi_{\epsilon K}^{c+1} \). This means that \( c \) is even.

(IV) It is clear.

Remark 3. We have \( r = \text{rank}_Z(E_{K^+}/E_{K^+}) = \text{rank}_Z E_{K^+} - \text{rank}_Z E_{K^+}/E_{K^+} \).

Hence we easily observe that:

\[
\begin{align*}
r &= \frac{1}{2}d_K(e_K - 1) \quad \text{and dim}_K F^c_K \leq \frac{1}{2}d_K \text{ in the case (I) or (II)}. \\
r &= d_K(\frac{1}{2}e_K - 1) \quad \text{and dim}_K F^c_K \leq d_K \text{ in the case (III)}. \\
r &= d_K(e_K - 1) \quad \text{and dim}_K F^c_K \leq d_K \text{ in the case (IV)}. \\
\end{align*}
\]

Theorem 2.4. Let \( E \supset E_{K^+} \) be a subgroup of \( E_{K^+} \) of finite index. Let \( r = \text{rank}_Z(E_{K^+}/E_{K^+}) \). Then there exists a set of representatives \( \{\eta_1, \ldots, \eta_r\} \) of a basis of \( E^{mp^s\epsilon K} E_{K^+}/E_{K^+} \) such that

1. \( c(\eta_i) > e_K/(p - 1) \) (\( i = 1, \ldots, r \)).
2. \( N^+ (\eta_i) = 1 \) (\( i = 1, \ldots, r \)).
3. \( c_1 \leq c_2 \leq \ldots \leq c_r \) where \( c_i = c(\eta_i) \).
4. Let \( S_j = \{\eta_i : c(\eta_i) \equiv j \text{ mod } e_K\} \) (\( 1 \leq j < e_K \) and \( j \) is even only if \( K_T \) is real and \( K_V \) is imaginary). Then \( \exists S_j = \frac{1}{2}d_K \) (\( d_K \) 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 \( E^m E_{K^+}/E_{K^+} \). Observe that \( E^m E_{K^+}/E_{K^+} \) is torsion-free. From Lemma 1.4, \( c(\xi_i^p) > e_K/(p - 1) \). From (ii), as \( [K^+ : K_T] = e_K \) or \( e_K/2 \), we have \( c(\xi_i^p) = e_{K^+} \in \text{Ker}(N^+) \cdot E_{K^+} \). Therefore,

\[
\xi_i^p = \eta_i u_i \quad \text{with some } \eta_i \in \text{Ker}(N^+) \cap E \text{ and } u_i \in E_{K^+}, \ 1 \leq i \leq r.
\]

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

Now we define the condition (C\(_s\)) for \( 1 \leq s < r : \{f(\eta_i) : c(\eta_i) \equiv j \text{ mod } e_K, \ 1 \leq i \leq s\} \) is an \( \mathbb{F}_p \)-independent system for all \( j \) (\( 1 \leq j < e_K, \) \( j \) 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 \( \{f(\eta_i) : c(\eta_i) \equiv l \text{ mod } e_K, \ 1 \leq i \leq s\} \)
∪ \{f(η_{s+1})\} is an $\mathbb{F}_p$-independent system, then $(C_{s+1})$ is valid. If it is not $\mathbb{F}_p$-independent, then
\[
f(η_{s+1}) = \sum_{1 ≤ i ≤ s, c_i ≡ l \mod e_K} a_i b_0^{α_i} f(η_i) \quad \text{with some } a_i ∈ \mathbb{Z},
\]
where $α_i = \frac{1}{ε_K} (c(η_{s+1}) - c(η_i))$. We have $c(η_{s+1}^{a_i p^{α_i}}) = c(η_{s+1})$ and $f(η_{s+1}^{a_i p^{α_i}}) = a_i b_0^{α_i} f(η_i)$. Then
\[
f\left(\prod_{1 ≤ i ≤ s, c_i ≡ l \mod e_K} η_i^{a_i p^{α_i}}\right) = \sum_{1 ≤ i ≤ s, c_i ≡ l \mod e_K} a_i b_0^{α_i} f(η_i) = f(η_{s+1}).
\]
So, letting
\[
η_{s+1}' = η_{s+1} \left(\prod_{1 ≤ i ≤ s, c_i ≡ l \mod e_K} η_i^{a_i p^{α_i}}\right)^{-1},
\]
we get $c(η_{s+1}') > c(η_{s+1})$. Now $\{η_1, ..., η_s, η_{s+1}', η_{s+2}, ..., η_r\}$ is also a set of representatives that satisfies (1) and (2). By means of some permutation of $\{η_{s+1}', η_{s+2}, ..., η_r\}$, we may write it $\{η_{s+1}, η_{s+2}, ..., η_r\}$ again with $c(η_{s+1}) ≤ ... ≤ c(η_r)$. 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 $\{η_1, ..., η_r\}$ as desired.

Note that, in this theorem, the sum of $\# S_j$ for $1 ≤ j < e_K$ ($j$ 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 $E ⊆ E' ⊆ E_{K^+}^+$ and $|E_{K^+} : E'| < ∞$. Let $\{η_i\}$ and $\{θ_i\}$ be as in Theorem 2.4 for $E$ and $E'$, respectively.

For $η ∈ E_{K^+}$, let $η$ denote $η \mod E_{K^+}^+$, and $c(η) = c(η)$ and $f(η) = f(η)$. They are well defined because $c(ηu) = c(η)$ and $f(ηu) = f(η)$ for any $u ∈ E_{K^+}^+$.

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 $R = \{1, ..., r\}$ and $B_l = \{(l - 1)d_0 + 1, ..., ld_0\}$ ($1 ≤ l < e_K$), in the case (I), (II) or (IV) in Lemma 2.3. Moreover we define $B_l$ in the case (III) as follows:

$$B_l = \left\{\left(\frac{l}{2} - 1\right)d_0 + 1, ..., \frac{l}{2}d_0\right\} \quad \text{for } 1 < l < e_K \text{ and } l \text{ even}.$$ 

Then $R$ is the union of all $B_l$.

We permute $η_1, ..., η_r$ and $θ_1, ..., θ_r$ such that $c(η_i) ≡ l \mod e_K$ for all $i ∈ B_l$ and $c(θ_j) ≡ l \mod e_K$ for all $j ∈ B_l$. 

We let, for all \( j = 1, \ldots, r, \)
\[
(5) \quad \bar{\theta}_j = \prod_{i=1}^{r} \tilde{\eta}_i^{a_{ji}p^{e_{ji}}} \quad \text{where } a_{ji} \in \mathbb{Z} \text{ is 0 or prime to } p, \text{ and } 0 \leq e_{ji} \in \mathbb{Z}.
\]

Then
\[
\det(a_{ji}p^{e_{ji}}) = \left[ E^{mp^{\delta_e}K} / E_{K_+}^+ : (E')^{mp^{\delta_e}K} E_{K_+}^+ / E_{K_+}^+ \right]
\]  
\[
= \left[ E^m E_{K_+}^+ / E_{K_+}^+ : (E')^m E_{K_+}^+ / E_{K_+}^+ \right]
\]  
\[
= [E : E'] \times (\text{a natural number prime to } p)
\]

since \( E^m E_{K_+}^+ / E_{K_+}^+ \) and \( (E')^m E_{K_+}^+ / E_{K_+}^+ \) 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 \( E \supset E' \supset E_{K_+}^+ \) 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 \( E \supset E' \supset E_{K_+}^+ \) and \( [E_{K_+} : E'] < \infty \). Let \( \{\eta_j\} \) and \( \{\bar{\theta}_j\} \) be as in Theorem 2A for \( E \) and \( E' \), respectively. Then
\[
v_p([E : E']) = \frac{1}{e_K} \left\{ \sum_{j=1}^{r} c(\bar{\theta}_j) - \sum_{j=1}^{r} c(\eta_j) \right\}.
\]

**Proof.** By the properties of level given in Section 1,
\[
c(\bar{\theta}_j) = \min\{c(\bar{\eta}_i^{a_{ji}p^{e_{ji}}}) : 1 \leq i \leq r\}.
\]

Define \( A_j = \{i \in R : c(\bar{\theta}_j) = c(\bar{\eta}_i^{a_{ji}p^{e_{ji}}})\}, 1 \leq j \leq r. \) Clearly, \( A_j \) is non-empty and \( A_j \subset B_l \) if \( j \in B_l \). Further,
\[
f(\bar{\theta}_j) = \sum_{i \in A_j} f(\bar{\eta}_i^{a_{ji}p^{e_{ji}}}) = \sum_{i \in A_j} a_{ji}b_0^{e_{ji}} f(\eta_i) \quad \text{for all } j \in R.
\]

Since \( \{f(\eta_i)\}_{i \in B_l} \) and \( \{f(\bar{\theta}_j)\}_{j \in B_l} \) are \( \mathbb{F}_p \)-independent systems, it follows that
\[
(6) \quad \det(a_{ji}^{e_{ji}}b_0^{e_{ji}})_{j,i \in B_l} \neq 0 \mod p \quad \text{for all } l,
\]
where \( a_{ji}' = a_{ji} \) if \( i \in A_j \) and \( a_{ji}' = 0 \) if \( i \notin A_j \).

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

Then, for each \( l \),
\[
(7) \quad \det(a_{ji}^{e_{ji}}b_0^{e_{ji}})_{j,i \in B_l} = \sum_{\tau_i \in P'_l} \left( \text{sgn}(\tau_i) \cdot \prod_{j \in B_l} a_{j,\tau_i(j)} b_0^{e_{\tau_i(j)}(j)} \right).
\]
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 \( \leq l < e_K \), \( l \) 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 \( \varrho \in P \), \( c(\varrho) < c(\eta_{\varrho}^{\varepsilon_{j\varrho}(j)j}) \) with some \( j \in R \). Therefore, for each \( \varrho \in P \setminus P' \),

\[
\sum_{j=1}^{r} c(\varrho_j) < \sum_{j=1}^{r} c(\eta_{\varrho}^{\varepsilon_{j\varrho}(j)j}).
\]

For \( \varrho \in P' \), by the definition,

\[
\sum_{j=1}^{r} c(\varrho_j) = \sum_{j=1}^{r} c(\eta_{\varrho}^{\varepsilon_{j\varrho}(j)j}).
\]

Since

\[
\sum_{j=1}^{r} c(\eta_{\varrho}^{\varepsilon_{j\varrho}(j)j}) = \sum_{j=1}^{r} \{ c(\eta_{\varrho}(j)) + e_{j\varrho} \} = \sum_{j=1}^{r} c(\eta_{\varrho}(j)) + e_{j\varrho} \sum_{j=1}^{r} e_{j\varrho},
\]

we have

\[
\sum_{j=1}^{r} e_{j\varrho} = \frac{1}{e_K} \left\{ \sum_{j=1}^{r} c(\varrho_j) - \sum_{j=1}^{r} c(\eta_j) \right\} \quad \text{for all } \varrho \in P'.
\]

Similarly, from (8),

\[
\sum_{j=1}^{r} e_{j\varrho} > \frac{1}{e_K} \left\{ \sum_{j=1}^{r} c(\varrho_j) - \sum_{j=1}^{r} c(\eta_j) \right\} \quad \text{for all } \varrho \in P \setminus P'.
\]

From (7) and (9),

\[
\prod_{l} \det(a'_{j'i}, b'_{0j})_{j,i \in B_l} = \sum_{\varrho \in P'} \left( \text{sgn}(\varrho) \cdot \prod_{j=1}^{r} a_{j\varrho}(j) b'_{0j\varrho}^{e_{j\varrho}(j)} \right)
\]

\[
= \sum_{\varrho \in P'} \left( \text{sgn}(\varrho) \cdot \prod_{j=1}^{r} a_{j\varrho}(j) \cdot b'_0 \sum_{j=1}^{r} e_{j\varrho} \cdot \prod_{j=1}^{r} a_{j\varrho}(j) \right)
\]

\[
= b'_0 \frac{1}{e_K} \left( \sum_{j=1}^{r} c(\varrho_j) - \sum_{j=1}^{r} c(\eta_j) \right) \sum_{\varrho \in P'} \left( \text{sgn}(\varrho) \cdot \prod_{j=1}^{r} a_{j\varrho}(j) \right).
\]
Therefore, from (6),

\[
\sum_{\varrho \in P'} \left( \text{sgn}(\varrho) \cdot \prod_{j=1}^{r} a_{j \varrho(j)} \right) \neq 0 \text{ mod } p.
\]

Now, we have

\[
\text{det}(a_{ji}p_{ji})_{1 \leq j, i \leq r} = \sum_{\varrho \in P'} \left( \text{sgn}(\varrho) \cdot \prod_{j=1}^{r} a_{j \varrho(j)} \right) + \sum_{\varrho \in P' \setminus P'} \left( \text{sgn}(\varrho) \cdot \prod_{j=1}^{r} a_{j \varrho(j)} \right)
\]

\[
= \sum_{\varrho \in P'} \left( \text{sgn}(\varrho) \cdot \prod_{j=1}^{r} a_{j \varrho(j)} \right)
\]

Combining (10)–(12), we get

\[
u_p(\text{det}(a_{ji}p_{ji})_{1 \leq j, i \leq r}) = \frac{1}{e_K} \left\{ \sum_{j=1}^{r} c(\bar{\varrho}_j) - \sum_{j=1}^{r} c(\bar{\eta}_j) \right\}.
\]

The proof is completed by using Lemma 3.1.

**Lemma 3.3.** Let \( E \) and \( E' \) be subgroups of \( E_{K+} \) such that \( E \supset E' \supset E_{K+} \) and \([E_{K+} : E'] < \infty\). Let \( \{\eta_i\} \) and \( \{\theta_i\} \) be as in Theorem 2.4 for \( E \) and \( E' \), respectively. Then \( c(\bar{\theta}_i) \geq c(\bar{\eta}_i) \) for all \( i = 1, \ldots, r \).

**Proof.** Suppose that there exists \( t \) such that \( 1 \leq t \leq r \) and \( c(\bar{\theta}_t) < c(\bar{\eta}_t) \).

For each \( l \) \((1 \leq l \leq e_K - 1, \ l \) is even in the case (III)), we define

\[
T_l = \{ \bar{\theta}_h : 1 \leq h \leq t, \ c(\bar{\theta}_h) \equiv l \text{ mod } e_K \}.
\]

Then \( \{\bar{\theta}_1, \ldots, \bar{\theta}_t\} = \bigcup_{l} T_{l} \) (disjoint union) and \( t = \sum_{l} n_T_{l} \). Fix any \( l \). Then each \( f(\bar{\theta}_h) \ (\bar{\theta}_h \in T_l) \) is a linear combination of \( f(\bar{\eta}_1), \ldots, f(\bar{\eta}_{t-1}) \) because \( c(\bar{\theta}_1) \leq \ldots \leq c(\bar{\theta}_t) < c(\bar{\eta}_t) \leq \ldots \leq c(\bar{\eta}_r) \). For each \( l \) \((1 \leq l \leq e_K - 1, \ l \) is even in the case (III)), we define

\[
T_{l}' = \{ \bar{\eta}_i : 1 \leq i \leq t - 1, \ c(\bar{\eta}_i) \equiv l \text{ mod } e_K \}.
\]
Then \( \{\bar{\eta}_1, \ldots, \bar{\eta}_{t-1}\} = \bigcup_l T'_l \) (disjoint union) and \( t - 1 = \sum_l \sharp T'_l \). Now \( f(\bar{\theta}_h) (\bar{\theta}_h \in T_1) \) is a linear combination of \( \{f(\bar{\eta}_i) : \bar{\eta}_i \in T'_1\} \). Therefore, from Theorem 2.4(4), we have \( \sharp T_l \leq \sharp T'_l \) for any \( l \), and hence \( \sum_l \sharp T_l \leq \sum_l \sharp T'_l \). This is a contradiction.

Note that, in Theorem 3.2, it does not necessarily hold that
\[
c(\bar{\theta}_i) \equiv c(\bar{\eta}_i) \mod e_K \quad \text{for all } i = 1, \ldots, r,
\]
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:
\[
c(\eta_i) = l(\eta_i) + u(\eta_i) e_K, \quad 1 \leq l(\eta_i) < e_K, \quad 0 \leq u(\eta_i) \in \mathbb{Z}, \quad 1 \leq i \leq r.
\]
Let \( l(\theta_i) \) and \( u(\theta_i) \) be defined in the same way for \( \theta_i \). From Lemma 3.3,
\[
c(\theta_i) - c(\eta_i) = l(\theta_i) - l(\eta_i) + e_K \{u(\theta_i) - u(\eta_i)\} \geq 0.
\]
So that, \( u(\theta_i) \geq u(\eta_i) \) for all \( i = 1, \ldots, r \). In addition,
\[
\sum_{i=1}^r c(\theta_i) - \sum_{i=1}^r c(\eta_i) = \sum_{i=1}^r \{l(\theta_i) - l(\eta_i)\} + e_K \sum_{i=1}^r \{u(\theta_i) - u(\eta_i)\}
\]
\[
= e_K \sum_{i=1}^r \{u(\theta_i) - u(\eta_i)\},
\]
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 \( E \supset E' \supset E_{K+} \) 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**


Received on 15.7.1997
and in revised form on 3.3.1998