62. Normal Bases and λ-invariants of Number Fields

By Takashi FUKUDA*) and Keiichi KOMATSU**)

(Communicated by Shokichi IYANAGA, M. J. A., Sept. 12, 1991)

Let Q be the rational number field, k be a number field, i.e. a finite algebraic extension of Q, S be a set of prime ideals of k and L a finite algebraic extension of k. We denote by $\mathfrak{O}_L$ the integer ring of L and $v_\mathfrak{p}$ an additive valuation of L with respect to a prime ideal $\mathfrak{p}$ of L. We denote by $\mathfrak{O}_L(S)$ the ring of elements α in L with $v_\mathfrak{p}(\alpha)\geqq 0$ for all prime ideals $\mathfrak{p}$ of L such that $\mathfrak{p}\cap k$ does not belong to S. Now let p be a fixed odd prime number, Z_p the p-adic integer ring and K a Z_p-extension of k. Then there exists a tower of cyclic extensions of k

$$k=K_0\subset K_1\subset\cdots\subset K_n\subset\cdots\subset K$$

such that K_n is an extension of k with the degree $[K_n:k]=p^n$. For the cyclotomic Z_p-extension k_∞ of k, we write $k_n=(k_\infty)_n$.

Recently, Kersten and Michaliček discussed normal bases of p-integer rings of intermediate fields of a Z_p-extension of a CM-field and Vandiver's conjecture. Furthermore, Fleckinger and Nguyen Quang Do have discussed normal bases of p-integer rings of intermediate fields of a Z_p-extension of a number field. In this paper, we investigate normal bases of S-integer rings of intermediate fields of a Z_p-extension of an imaginary quadratic field and the Iwasawa λ-invariant.

Now we define as follows:

Definition (cf. [4]). *We say, a Z_p-extension K/k has a normal S-basis, if each $\mathfrak{O}_{K_n}(S)/\mathfrak{O}_k(S)$ has a normal basis. Namely, there exists an element α_n of $\mathfrak{O}_{K_n}(S)$ such that $\{\alpha_n^\sigma\mid\sigma\in G(K_n/k)\}$ is a free $\mathfrak{O}_k(S)$-basis of $\mathfrak{O}_{K_n}(S)$, where $G(K_n/k)$ is the Galois group of K_n over k.*

Let F be an imaginary quadratic field, F_∞ the cyclotomic Z_p-extension of F and $\zeta_n=\exp(2\pi\sqrt{-1}/p^n)$. We put $k=F(\zeta_1)$ and $\Delta=G(k/F)$. Let δ be the order of Δ and $\chi:\Delta\to Z_p^\times$ the Teichmüller character (a homomorphism such that $\zeta_1^g=\zeta_1^{\chi(g)}$ for all $g\in\Delta$). We define

$$e_i=\frac{1}{\delta}\sum_{g\in\Delta}\chi(g)^i g^{-1}\in Z_p[\Delta]$$

for each integer i. The main purpose of this paper is to prove the following:

Theorem. *Let F be an imaginary quadratic field, p an odd prime number, F_∞, ζ_n, k, Δ and e_i as above. Let k^+ be the maximal real subfield of k, A^+ the p-primary part of the ideal class group of k^+ and S_0 the set of all prime ideals of F each of which has only one prime factor in $k(\zeta_2)$. We*

*) Department of Mathematics, Faculty of Science, Yamagata University.
**) Department of Mathematics, Tokyo University of Agriculture and Technology.

suppose that S_0 contains all prime ideals of F lying above p and that a component $(A^+)^{e_1}$ of Δ-decomposition of A^+ is non-trivial. If there exists a Z_p-extension K of F with $K\cap F_\infty=F$ such that K/F has a normal S_0-basis, then the λ-invariant of the cyclotomic Z_p-extension k_∞^+ of k^+ is non-zero.

In the rest of this paper, we use the same notations as above. Let S be now the set of prime ideals of k lying above primes ideals of S_0. Let E_n be the unit group of $\mathfrak{O}_{k_n}$ and E'_n the unit group of $\mathfrak{O}_{k_n}(S)$. We denote by $N_{n,0}$ the norm of k_n over k. Then we have the following:

Lemma 1. (1) $(E_0/N_{n,0}(E_n))^{e_1}\cong(E_0N_{n,0}(E'_n)/N_{n,0}(E'_n))^{e_1}=(E'_0/N_{n,0}(E'_n))^{e_1}$,
(2) $(E_0/E_0^{p^n})^{e_1}\cong(E_0E_0'^{p^n}/E_0'^{p^n})^{e_1}=(E'_0/E_0'^{p^n})^{e_1}$.

Proof. Since only one prime ideal of k_n lies above each prime ideal of S, we have $E_0\cap N_{n,0}(E'_n)=N_{n,0}(E_n)$. This shows $(E_0/N_{n,0}(E_n))^{e_1}\cong(E_0N_{n,0}(E'_n)/N_{n,0}(E'_n))^{e_1}$. Let σ be any element of $\Delta=G(k/F)$ and α any element of E'_0. We put $u_\sigma=\alpha^{\sigma-1}$. Then the definition of S, we have $u_\sigma\in E_0$. We denote by $\bar{\alpha}$ the coset $\alpha N_{n,0}(E'_n)$ in the factor group $E'_0/N_{n,0}(E'_n)$. Then we have

$$\bar{\alpha}^{e_1}=\bar{\alpha}^{e_1^2}=(\prod_{\sigma\in\Delta}(\bar{\alpha}\bar{u}_{\sigma-1})^{\chi(\sigma)})^{e_1/\delta}=(\prod_{\sigma\in\Delta}\bar{\alpha}^{\chi(\sigma)})^{e_1/\delta}(\prod_{\sigma\in\Delta}\bar{u}_{\sigma-1}^{\chi(\sigma)})^{e_1/\delta}$$
$$=(\prod_{\sigma\in\Delta}\bar{u}_{\sigma-1}^{\chi(\sigma)})^{e_1/\delta}\in(E_0N_{n,0}(E'_n)/N_{n,0}(E'_n))^{e_1},$$

where χ is the Teichmüller character. This shows $(E_0N_{n,0}(E'_n)/N_{n,0}(E'_n))^{e_1}=(E'_0/N_{n,0}(E'_n))^{e_1}$. In a similar way, we can prove (2).

Lemma 2. *Let* $\mathrm{rank}_p(E_0/E_0^p)^{e_1}$ *denote the dimension of the vector space* $(E_0/E_0^p)^{e_1}$ *over the prime field* $\boldsymbol{F}_p$ *of characteristic* p. *Then we have* $\mathrm{rank}_p(E_0/E_0^p)^{e_1}=2$.

Proof. Let η be a Minkowski unit of k with $N_{k/F}(\eta)=1$. Let H_0 be a subgroup of E_0 generated by $\{\eta^\sigma\mid\sigma\in\Delta=G(k/F)\}$ and W the group of all roots of 1 in k. We put $\bar{E}_0=E_0/W$ and $\bar{H}_0=H_0W/W$. Then by the definition of Minkowski unit, we have $\bar{H}_0\cong\boldsymbol{Z}[\Delta]/\boldsymbol{Z}[\Delta]\sum_{\sigma\in\Delta}\sigma$, where $\boldsymbol{Z}[\Delta]$ is the group ring of Δ over $\boldsymbol{Z}$. Since $\bar{H}_0/\bar{H}_0^p\cong\boldsymbol{F}_p[\Delta]/\boldsymbol{F}_p[\Delta]\sum_{\sigma\in\Delta}\sigma$, we have $(\bar{H}_0/\bar{H}_0^p)^{e_i}\neq1$ for $i\not\equiv0 \pmod{\delta}$, where δ is the order of Δ. Hence we have $(\bar{H}_0/\bar{E}_0^{p^n})^{e_i}\neq1$ for a sufficiently large n and for $i\not\equiv0 \pmod{\delta}$. Since $((\bar{E}_0/\bar{E}_0^{p^n})/(\bar{E}_0/\bar{E}_0^{p^n})^p)^{e_i}\cong(\bar{E}_0/\bar{E}_0^p)^{e_i}\neq1$ for $i\not\equiv0 \pmod{\delta}$ and since $\zeta_1E_0^p\in(E_0/E_0^p)^{e_1}$, we have $\mathrm{rank}_p(E_0/E_0^p)^{e_1}=2$.

Lemma 3. *Let L be a cyclic extension of F with $[L:F]=p$. If there exists an element b of E'_0 with $Lk=k(\sqrt[p]{b})$, then $bE_0'^p\in(E'_0/E_0'^p)^{e_1}$.*

Proof. Let ρ be a generator of $G(Lk/k)$ with $\sqrt[p]{b}^\rho=\sqrt[p]{b}\zeta_1$ and τ an element of $G(Lk/F)$ such that the restriction $\tau|k$ is a generator of $G(k/F)$. Then there exists a rational integer t and an element u of E'_0 with $\sqrt[p]{b}^\tau=\sqrt[p]{b}^tu$. Since we have $\sqrt[p]{b}^{\tau\rho\tau^{-1}}=(\sqrt[p]{b}^tu)^{\rho\tau^{-1}}=(\sqrt[p]{b}^t\zeta_1^tu)^{\tau^{-1}}=\sqrt[p]{b}(\zeta_1^{\tau^{-1}})^t=\sqrt[p]{b}\zeta_1$, we have $\zeta_1^\tau=\zeta_1^t$. Hence we have $t\equiv\chi(\tau) \pmod{p}$. This shows $(bE_0'^p)^\tau=(bE_0'^p)^{\chi(\tau)}$. Namely, we have $bE_0'^p\in(E'_0/E_0'^p)^{e_1}$.

Kersten and Michaliček obtained the following (cf. [4, p. 373]):

Lemma 4. *Let $k_\infty=\bigcup_{n=0}^\infty k_n$ be the cyclotomic Z_p-extension of k. We suppose that there exists a Z_p-extension $K=\bigcup_{n=0}^\infty K_n$ of k with $K\cap k_\infty=k$ such that K/k has a normal S-basis. Then there exists an element b_n of*

E'_0 with $K_1=k(\sqrt[p]{b_n})$ such that there exists an element v_n of E'_n with $N_{n,0}(v_n)$ $=b_n$ for every natural number n.

We have furthermore

Lemma 5. *If there exists a Z_p-extension K of F with $K\cap F_\infty=F$ such that K/F has a normal S_0-basis, then $(E_0/N_{n,0}(E_n))^{e_1}=1$ for every natural number n.*

Proof. We notice that $Kk\cap k_\infty=k$ follows from $K\cap F_\infty=F$ and that Kk/k has a normal S-basis. It follows from Lemma 1, Lemma 3 and Lemma 4 that there exists an element b_n of E_0 with $b_nE_0^p\in(E_0/E_0^p)^{e_1}$ and with $K_1k=k(\sqrt[p]{b_n})$ such that there exists an element v_n of E_n with $N_{n,0}(v_n)$ $=b_n$ for every natural number n. Since $(E_0/E_0^p)^{e_1}=\langle b_nE_0^p, \zeta_1E_0^p\rangle$ from Lemma 2, $(E_0/N_{n,0}(E_n))^{e_1}=\langle b_nN_{n,0}(E_n), \zeta_1N_{n,0}(E_n)\rangle=1$ for every natural number n.

Proof of Theorem. Let A_n be the p-primary part of the ideal class group of k_n, $\mathrm{Ker}(A_0\to A_n)$ the kernel of a natural embedding of A_0 in A_n and $H^i(G(k_n/k), E_n)$ the cohomology group of the $G(k_n/k)$-module E_n. Then we have an injective morphism

$$1\longrightarrow\mathrm{Ker}(A_0\longrightarrow A_n)\longrightarrow H^1(G(k_n/k), E_n) \quad \text{(cf. [3, p. 267]).}$$

Since Δ is canonically isomorphic to $G(k_\infty/F_\infty)$, we may consider $H^i(G(k_n/k), E_n)$ as Δ-module in a natural way. Then it follows from Herbrand's lemma that the order of $H^0(G(k_n/k), E_n)^{e_1}$ is equal to the order of $H^1(G(k_n/k), E_n)^{e_1}$ (cf. [5, p. 13]). Now, we suppose that there exists a Z_p-extension K of F with $K\cap F_\infty=F$ such that K/F has a normal S_0-basis. Then $H^0(G(k_n/k), E_n)^{e_1}$ $=(E_0/N_{n,0}(E_n))^{e_1}=1$ follows from Lemma 5. Hence we have $H^1(G(k_n/k), E_n)^{e_1}$ $=1$. This shows $\mathrm{Ker}(A_0\to A_n)^{e_1}=1$ (cf. [1]). Hence our theorem follows from [2, Proposition 2] and [6, Theorem 7. 15].

References

[1] V. Fleckinger and T. Nguyen Quang Do: Bases normales unités et conjecture faible de Leopoldt. Manus. Math., **71**, 183–195 (1991).

[2] R. Greenberg: On Iwasawa invariants of totally real number fields. Amer. J. Math., **98**, 263–284 (1976).

[3] K. Iwasawa: On Z_l-extensions of algebraic number fields. Ann. of Math., **98**, 246–326 (1973).

[4] I. Kersten and J. Michaliček: On Vandiver's conjecture and Z_p-extensions of $Q(\zeta_{p^n})$. J. Number Theory, **32**, 371–386 (1989).

[5] J. Neukirch: Class Field Theory. Springer-Verlag, Berlin, Heidelberg, New York, Tokyo (1986).

[6] L. Washington: Introduction to Cyclotomic Fields. Springer-Verlag, Berlin, New York (1982).