J. Math. Soc. Japan
Vol. 48, No. 4, 1996

On a normal integral bases problem over cyclotomic Z_p-extensions

By Humio ICHIMURA

(Received Oct. 28, 1994)

§ 1. Introduction.

Let p be a prime number and K be a number field containing a primitive p-th root of unity. Let $\mathcal{H}(K)$ be the subgroup of $K^\times/K^{\times p}$ consisting of elements $[\alpha]$ $(\in K^\times/K^{\times p})$ for which the extension $K(\alpha^{1/p})$ is unramified over K, and $\mathcal{N}(K)$ be the subset of $\mathcal{H}(K)$ consisting of elements $[\alpha]$ $(\in\mathcal{H}(K))$ for which the unramified cyclic extension $K(\alpha^{1/p})/K$ has a relative normal integral bases. Here, we say that a Galois extension L/E of a number field E has a relative normal integral bases (an RNIB, for short) when the integer ring O_L of L is free over the group ring $O_E[\mathrm{Gal}(L/E)]$. In [3], Childs gave a criterion for a cyclic extension L/K of degree p to be unramified and have an RNIB (see Lemma 5 in § 4), from which it follows that $\mathcal{N}(K)$ is a subgroup of $\mathcal{H}(K)$. He raised the question "what is the quotient group $\mathcal{H}(K)/\mathcal{N}(K)$?". We have been investigating this problem for certain abelian fields ([**14**], [**15**]) in connection with power series associated to certain p-adic L-functions. A similar study is also given in Taylor [**24**] when K is the p-th cyclotomic field $\boldsymbol{Q}(\mu_p)$. In this paper, we shall continue these investigations.

Let p be an odd prime number and k be an imaginary abelian field satisfying the following conditions:

(C1) k contains a primitive p-th root of unity.
(C2) $p\nmid[k:\boldsymbol{Q}]$.
(C3) There is only one prime ideal of k over p.

Let k_∞/k be the cyclotomic $\boldsymbol{Z}_p$-extension and k_n $(n\geqq 0)$ be its n-th layer. We write, for brevity, $\mathcal{H}_n=\mathcal{H}(k_n)$ and $\mathcal{N}_n=\mathcal{N}(k_n)$. The Galois groups $\Delta=\mathrm{Gal}(k/\boldsymbol{Q})$ and $\Gamma=\mathrm{Gal}(k_\infty/k)$ act on these groups in a natural way. In particular, we may decompose these groups by the action of complex conjugation ρ $(\in\Delta)$; $\mathcal{H}_n=\mathcal{H}_n^+\oplus\mathcal{H}_n^-$, $\mathcal{N}_n=\mathcal{N}_n^+\oplus\mathcal{N}_n^-$. As far as normal integral bases problem is concerned, we have nothing to consider on the "odd" part, because we already know that $\mathcal{N}_n^-=\{1\}$ (Brinkhuis [**1**]). As for the "even" part, we have described,

This research was partially supported by Grant-in-Aid for Scientific Research (C) (No. 08640226), Ministry of Education, Science and Culture.

in the previous papers [**14**], [**15**], the Γ-module structure of the quotient group $\mathcal{H}_n^+/\mathcal{N}_n^+$ in terms of power series associated to certain p-adic L-functions under the assumption $p \nmid h(k^+)$ (see Theorem 5 in § 6). Here, $h(k^+)$ denotes the class number of the maximal real subfield k^+ of k. As its application, we have obtained the following

THEOREM 1 ([**15**, Thm. 2]). *Let k be an imaginary abelian field satisfying* (C1), (C2) *and* (C3). *If $p \nmid h(k^+)$, then, $\mathcal{H}_n^+=\mathcal{N}_n^+$ for all sufficiently large n.*

Motivated by this assertion, we shall give some further results on the triviality of $\mathcal{H}_n^+/\mathcal{N}_n^+$ for large n without the assumption $p \nmid h(k^+)$. First, we give a "weak version" of the converse of this theorem. Namely, we prove that if $\mathcal{H}_n^+=\mathcal{N}_n^+$ for all sufficiently large n, then, the Iwasawa λ-invariant of the ideal class group of the maximal real subfield k_∞^+ of k_∞ vanishes (Theorem 2). Next, we give, under some assumptions, a necessary and sufficient condition for $\mathcal{H}_n^+=\mathcal{N}_n^+$ for all sufficiently large n in terms of special values of certain p-adic L-functions (Theorem 3). Finally, returning back to the case $p \nmid h(k^+)$, we give a more "precise" version (Theorem 4) of Theorem 1.

§ 2. Statement of results.

Let k be an imaginary abelian field satisfying (C1), (C2) and (C3). First, we give a "weak version" of the converse of Theorem 1. Let A_n be the Sylow p-subgroup of the ideal class group of k_n, and let $A_\infty=\varprojlim A_n$ be the projective limit w.r.t. the relative norms. Let Ψ be a character of Δ defined and irreducible over $\boldsymbol{Q}_p$, which we call a $\boldsymbol{Q}_p$-character. We fix an irreducible component ψ of Ψ over a fixed algebraic closure Ω_p of $\boldsymbol{Q}_p$. We say that Ψ is even when $\psi(\rho)=1$, ρ being the complex conjugation in Δ. Let e_Ψ be the idempotent of the group ring $\boldsymbol{Z}_p[\Delta]$ corresponding to Ψ. Denote by $\mathcal{O}$ the subring of Ω_p generated over $\boldsymbol{Z}_p$ by the image of ψ. We identify the subring $e_\Psi \boldsymbol{Z}_p[\Delta]$ with $\mathcal{O}$ by the correspondence $e_\Psi \sigma \leftrightarrow \psi(\sigma)$ $(\sigma \in \Delta)$. Let γ be the topological generator of Γ such that $\zeta^\gamma=\zeta^{1+q}$ for all p^a-th roots ζ of unity $(a \geqq 1)$, where q is the least common multiple of p and the conductor of ψ. We identify, as usual, the completed group ring $\mathcal{O}[\![\Gamma]\!]$ with the power series ring $\Lambda=\mathcal{O}[\![t]\!]$ by the correspondence $\gamma \leftrightarrow 1+t$. Thus, for a module X over $\boldsymbol{Z}_p[\Delta][\![\Gamma]\!]$ (e.g., $\mathcal{H}_n$, $\mathcal{N}_n$, A_n, A_∞), its Ψ-component $X(\Psi)=e_\Psi X$ is a module over Λ. By Iwasawa [**19**, Thm. 5], $A_\infty(\Psi)$ is finitely generated and torsion over Λ, hence one can define its characteristic power series. It is the product of a distinguished polynomial and a unit, respectively, of Λ by the theorem of Ferrero-Washington [**5**] on Iwasawa μ-invariants and the Weierstrass preparation theorem. We denote the degree of this distinguished polynomial by λ_Ψ. It is conjectured that $\lambda_\Psi=0$ when Ψ is even ([**19**, page 316], Greenberg [**11**]).

THEOREM 2. *Let k be an imaginary abelian field satisfying* (C1), (C2), (C3) *and let Ψ be a nontrivial even $\boldsymbol{Q}_p$-character of Δ. If $\mathcal{H}_n(\Psi)=\mathcal{N}_n(\Psi)$ for all sufficiently large n, then, we have $\lambda_\Psi=0$.*

REMARK 1. (1) Let k and Ψ be as above. Then, the condition $p \nmid h(k^+)$ implies that $p \nmid h(k_n^+)$ for all n by the criterion of Iwasawa [**16**] on p-divisibility of class numbers, and hence that $\lambda_\Psi=0$. Therefore, Theorem 2 is regarded as a weak version of the converse of Theorem 1. But, the converse of Theorem 1 and that of Theorem 2 do not hold in general as we shall see at the end of § 5.

(2) Let Ψ_0 be the trivial character of Δ. It follows that $\mathcal{H}_n(\Psi_0)=\{1\}$ and $\lambda_{\Psi_0}=0$ by the Stickelberger theorem for p-cyclotomic fields $\boldsymbol{Q}(\mu_{p^n})$ $(n\geqq 1)$ and the Kummer duality (the formula (6′) of § 4).

Next, let k be an imaginary abelian field satisfying (C1), (C3) and

(C2′) the exponent of Δ is $p-1$.

Then, a $\boldsymbol{Q}_p$-character Ψ of Δ is of degree one, and hence $\phi=\Psi$, $\mathcal{O}=\boldsymbol{Z}_p$. Let Ψ be a nontrivial even $\boldsymbol{Q}_p$-character of Δ. We want to give a necessary and sufficient condition for $\mathcal{H}_n(\Psi)=\mathcal{N}_n(\Psi)$ for all sufficiently large n. This problem is less hard to deal with when the dimension of $\mathcal{H}_n(\Psi)$ over the prime field $\boldsymbol{F}_p$ is small. Denote by Ψ^* the odd $\boldsymbol{Q}_p$-character of Δ defined by

$$\Psi^*(\sigma)=\omega(\sigma)\Psi(\sigma^{-1}) \quad (\sigma\in\Delta). \tag{1}$$

Here, ω is the character of Δ representing the Galois action on p-th roots of unity. Recall that (i) $\dim_{\boldsymbol{F}_p}\mathcal{H}_n(\Psi)$ equals to the p-rank $r(n)$ of $A_n(\Psi^*)$ by the Kummer duality (see the formula (6′) of § 4), and that (ii) $r(n)\leqq\lambda_{\Psi^*}$ for all n and the equality holds for all sufficiently large n (see [**25**, Cor. 13.29]). In particular, we have $\mathcal{H}_n(\Psi)=\mathcal{N}_n(\Psi)=\{1\}$ when $\lambda_{\Psi^*}=0$. Therefore, from the above, the case $\lambda_{\Psi^*}=1$ is the first nontrivial case we have to consider. We prove the following

THEOREM 3. *Let k be an imaginary abelian field satisfying* (C1), (C2′), (C3), *and let Ψ be a nontrivial even $\boldsymbol{Q}_p$-character of Δ such that $\lambda_{\Psi^*}=1$. Then, $\mathcal{H}_n(\Psi)=\mathcal{N}_n(\Psi)$ for all sufficiently large n if and only if $L_p(1,\phi)/|A_0(\Psi)|\equiv 0$* (mod. p). *Here, $L_p(s,\phi)$ is the p-adic L-function associated to ϕ which we are regarding as a primitive Dirichlet character, and $|*|$ denotes the cardinality.*

REMARK 2. Let k and Ψ be as in Theorem 3. It is a direct consequence of Theorems 2 and 3 that $\lambda_\Psi=0$ if $L_p(1,\phi)/|A_0(\Psi)|\equiv 0$ mod. p. A similar sufficient condition for $\lambda_\Psi=0$ is already given in Fukuda-Komatsu [**6**, Thm. 2], Kraft [**21**, Thm. 3] and Taya [**23**, Thm. 2], but without any connection with normal integral bases.

Finally, we return back to the situation of Theorem 1. So, the base field k is an imaginary abelian field satisfying (C1), (C2), (C3) and $p \nmid h(k^+)$. Then,

since $p \nmid h(k_n^+)$ (Remark 1(1)), we have $\mathcal{H}_n^- = \mathcal{R}_n^- = \{1\}$ from the Kummer duality (see (6′) of § 4). We prove the following more precise version of Theorem 1.

THEOREM 4. *Let k be as above. Then, the homomorphism $\mathcal{H}_n/\mathcal{R}_n \to \mathcal{H}_{n+1}/\mathcal{R}_{n+1}$ induced from the inclusion $k_n^\times \to k_{n+1}^\times$ is trivial for all n. Namely, the extension Lk_{n+1}/k_{n+1} does have an RNIB for any unramified cyclic extension L/k_n of degree p and for any n.*

REMARK 3. Theorem 1 follows from Theorem 4 since the p-rank of A_n is bounded as $n \to \infty$ ([**5**]).

The content of this paper is as follows. In § 3, we recall some basic facts on local units and cyclotomic units, which we need in the later sections. We prove Theorems 2, 3 and 4 in § 4, § 5 and § 6 respectively.

§ 3. Cyclotomic units and local units.

Let k be an imaginary abelian field satisfying (C1), (C2), (C3), and let Ψ be a nontrivial even $\boldsymbol{Q}_p$-character of Δ. It follows that there is exactly one prime ideal $\mathfrak{p}_n$ of k_n over p from (C2) and (C3). Let K_n ($\subset \Omega_p$) be the completion of k_n by the prime $\mathfrak{p}_n$, and put $K_\infty = \bigcup K_n$. We regard that k_n is embedded in K_n. Let $\mathcal{U}_n$ be the group of principal units of K_n, and let E_n and C_n be, respectively, the group of units of k_n and the group of cyclotomic units of k_n in the sense of Hasse [**13**] and Gillard [8, § 2-3]. Denote by $\mathcal{E}_n$ and $\mathcal{C}_n$ the closures of $E_n \cap \mathcal{U}_n$ and $C_n \cap \mathcal{U}_n$ in $\mathcal{U}_n$ respectively. Let $\mathcal{U} = \varprojlim \mathcal{U}_n$ and $\mathcal{C} = \varprojlim \mathcal{C}_n$ be the projective limits w.r.t. the relative norms. We identify the Galois groups Δ and Γ with $\mathrm{Gal}(K_0/\boldsymbol{Q}_p)$ and $\mathrm{Gal}(K_\infty/K_0)$ respectively in an obvious way. Hence, we may regard the groups $\mathcal{U}_n$, $\mathcal{U}$ etc. as modules over $\boldsymbol{Z}_p[\Delta][\![\Gamma]\!]$. Therefore, the Ψ-components $\mathcal{U}_n(\Psi)$, $\mathcal{U}(\Psi)$ etc. are regarded as modules over $\Lambda = \mathcal{O}[\![t]\!]$ by the manner we mentioned in § 2. It is known that $\mathcal{U}(\Psi)$ is free and cyclic over Λ (Iwasawa [**17**], Gillard [**10**, Prop. 1]). We fix a generator $\boldsymbol{u} = (\boldsymbol{u}_n)_{n \geq 0}$ of $\mathcal{U}(\Psi)$ over Λ. Iwasawa [**18**] constructed a power series $g_\phi(t) \in \mathcal{O}[\![t]\!]$ such that

$$g_\phi((1+q)^{1-s}-1) = L_p(s, \phi). \tag{2}$$

The following fact due to Iwasawa and Gillard on the quotient Λ-modules $\mathcal{U}(\Psi)/\mathcal{C}(\Psi)$ and $\mathcal{U}_n(\Psi)/\mathcal{C}_n(\Psi)$ plays an important role in our paper. Put $\omega_n = (1+t)^{p^n}-1$.

LEMMA 1. (1) [**10**, Thm. 1] $\mathcal{U}(\Psi)/\mathcal{C}(\Psi) \cong \Lambda/(g_\phi)$.

(2) [**10**, Prop. 1, 2 and Thm. 2] *By the correspondence $\boldsymbol{u}_n^g \leftrightarrow g$, we have isomorphisms:*

$$\mathcal{U}_n(\Psi) \cong \Lambda/(\omega_n) \quad \textit{and} \quad \mathcal{C}_n(\Psi) \cong (g_\phi, \omega_n)/(\omega_n).$$

Let $\mathcal{U}_n^{(1)}$ be the subgroup of $\mathcal{U}_n$ consisting of local units u of $\mathcal{U}_n$ such that $u\equiv 1$ modulo the ideal (ζ_0-1), ζ_0 being a primitive p-th root of unity in K_0. Denote by I_n $(n\geqq 1)$ the ideal of Λ generated by p^n and $p^{n-1-j}\cdot t^{p^j}$ $(0\leqq j\leqq n-1)$, and let $I_0=\Lambda$. It follows that I_n contains the ideal (ω_n) from a simple fact ([**15**, Lemma 4]) on binomial coefficients.

LEMMA 2 ([**15**, Prop. 1]). *By the correspondence in the above lemma, we have* $\mathcal{U}_n^{(1)}(\Psi)\cong I_n/(\omega_n)$.

By means of the group C_n of cyclotomic units in the sense of Hasse and Gillard, we have the following analytic class number formula ([**8**, § 2-3]) analogous to the classical one:

$$[E_n : C_n] = h(k_n^+)\times c_n .$$

Here, c_n is an explicitly given integer depending only on the group $\mathrm{Gal}(k_n/\boldsymbol{Q})$, which, because of (C2), is not divisible by p (see [**8**, § 2-3 and § 1]). Hence, we obtain the formula $|A_n^+|=|\mathcal{E}_n/C_n|$. Then, it is quite natural to ask "is the Λ-decomposed version of this formula valid?". As a consequence of the Iwasawa main conjecture (proved by Mazur-Wiles [**22**]), Greenberg [**12**, Prop. 9] (resp. Gillard [**9**, Thm. 3]) proved it when $n=0$ (resp. when n is arbitrary and the Λ-module $A_\infty(\Psi^*)$ is pseudo-isomorphic to $\Lambda/(h)$ for some $h\in\Lambda$). In particular, we have the following

LEMMA 3. *Under the above notations,* $|A_n(\Psi)|$ *equals to the index* $[\mathcal{E}_n(\Psi) : C_n(\Psi)]$ *when* $n=0$ *or* $\lambda_{\Psi^*}=1$.

§ 4. Proof of Theorem 2.

Let k be an imaginary abelian field satisfying (C1), (C2) and (C3). Let M be the maximal pro-p abelian extension over k_∞ unramified outside p, and L be the maximal unramified pro-p abelian extension over k_∞. Put $F=k_\infty(\varepsilon^{1/p^n}\,|\,\varepsilon\in E'_\infty,\ n\geqq 1)$. Here, E'_∞ is the group of p-units of k_∞. The Galois groups of these extensions over k_∞ can be viewed as modules over $\boldsymbol{Z}_p[\Delta][\![\Gamma]\!]$. For a $\boldsymbol{Q}_p$-character Ψ of Δ, let $M(\Psi)$ be the intermediate field of M/k_∞ fixed by Φ-component $\mathrm{Gal}(M/k_\infty)(\Phi)$ for all $\boldsymbol{Q}_p$-characters Φ of Δ different from Ψ. Then $\mathrm{Gal}(M(\Psi)/k_\infty)=\mathrm{Gal}(M/k_\infty)(\Psi)$. Define $L(\Psi)$, $F(\Psi)$ and $(L\cap F)(\Psi)$ in a similar way. In the following, let Ψ be a nontrivial even $\boldsymbol{Q}_p$-character of Δ and Ψ^* be the odd $\boldsymbol{Q}_p$-character associated to Ψ by the relation (1). By the assumptions (C1), (C2) and (C3), we see that the unique prime ideal $\mathfrak{p}_n$ of k_n over p is principal. Therefore, A_n coincides with the Sylow p-subgroup of the p-ideal class group of k_n. Hence, by [**19**, Thm. 16], the Λ-modules $\mathrm{Gal}(M/F)(\Psi^*)$ and $\mathrm{Hom}(\varinjlim A_n(\Psi), \mu_{p^\infty})$ are isomorphic. Here, $\varinjlim A_n$ is the

inductive limit w.r.t. the inclusion map $k_n \to k_m$ $(n<m)$, and μ_{p^∞} is the group of all p-power roots of unity in k_∞. It is known that $\lambda_\Psi=0$ if and only if $\varinjlim A_n(\Psi)=\{1\}$ ([**11**, Prop. 2]). Therefore, to prove Theorem 2, it suffices to show that $M(\Psi^*)=F(\Psi^*)$.

Let $G=\mathrm{Gal}(L/k_\infty)$ and $H=\mathrm{Gal}((L\cap F)/k_\infty)$. To prove that $M(\Psi^*)=F(\Psi^*)$, we need the following

LEMMA 4. *Under the notations as above, both $\mathcal{O}$-modules $G(\Psi^*)$ and $H(\Psi^*)$ are finitely generated and torsion free.*

PROOF. The assertion for $G(\Psi^*)$ is well known (see [**25**, Cor. 13.29]). So, we prove the assertion only for $H(\Psi^*)$. By class field theory, $\mathrm{Gal}(M/L)(\Psi^*)$ is isomorphic over Λ to the projective limit $\varprojlim(\mathcal{U}_n/\mathcal{E}_n)(\Psi^*)$ w.r.t. to the relative norms ([**4**, Thm. 1.1]). Since Ψ^* is odd and $\Psi^*\neq\omega$, we have $\mathcal{E}_n(\Psi^*)=\{1\}$ by the fact ([**25**, Thm. 4.12]) on units of a CM-field. Hence, the Λ-module $\mathrm{Gal}(M/L)(\Psi^*)$ is isomorphic to $\mathcal{U}(\Psi^*)$. But, by [**10**, Prop. 1], the latter module is free and cyclic over Λ. Thus $\mathrm{Gal}(M/L)(\Psi^*)\cong\Lambda$. But, since $\mathrm{Gal}(M/F)(\Psi^*)$ is torsion over Λ ([**19**, Thm. 16]), we see that

$$\mathrm{Gal}(M/L)(\Psi^*)\cap\mathrm{Gal}(M/F)(\Psi^*) = \{1\}.$$

Therefore, we obtain

$$M(\Psi^*) = F(\Psi^*)L(\Psi^*) \tag{3}$$

and

$$\mathrm{Gal}(F(\Psi^*)/(F\cap L)(\Psi^*)) \cong \mathrm{Gal}(M/L)(\Psi^*) \cong \Lambda. \tag{4}$$

By [**19**, Thm. 15], we have an injective homomorphism of $\mathrm{Gal}(F/k_\infty)(\Psi^*)$ into Λ with a finite cokernel. Therefore, by (4), we see that there is an (injective) embedding of $H(\Psi^*)$ into $\Lambda/(h)$ with a finite cokernel for some $h\in\Lambda$. Since the characteristic power series of $G(\Psi^*)$ is not divisible by p ([**5**]) and it is divisible by h, h is not divisible by p. Hence, the $\mathcal{O}$-module $H(\Psi^*)$ is finitely generated and torsion free. □

Now, let us prove Theorem 2. Let $\tilde{L}$ be the maximal unramified abelian extension over k_∞ whose Galois group is of exponent p. We have clearly $\mathrm{Gal}(\tilde{L}/k_\infty)=G/G^p$ and $\mathrm{Gal}((\tilde{L}\cap F)/k_\infty)=H/H^p$. Define $\tilde{L}(\Psi^*)$ and $(\tilde{L}\cap F)(\Psi^*)$ similarly to $L(\Psi^*)$ and $(L\cap F)(\Psi^*)$. Hence, we have

$$\mathrm{Gal}(\tilde{L}(\Psi^*)/k_\infty) = (G/G^p)(\Psi^*) \quad\text{and}\quad \mathrm{Gal}((\tilde{L}\cap F)(\Psi^*)/k_\infty) = (H/H^p)(\Psi^*).$$

Let $\mathcal{H}_\infty$ be the subgroup of $k_\infty^\times/k_\infty^{\times p}$ consisting of classes $[\alpha]$ $(\alpha\in k_\infty^\times)$ for which the extension $k_\infty(\alpha^{1/p})/k_\infty$ is unramified. By the Kummer pairing

$$\mathrm{Gal}(\tilde{L}/k_\infty)\times\mathcal{H}_\infty \longrightarrow \mu_p,$$

we obtain (cf. [**25**, Chap. 10])

$$\widetilde{L}(\Psi^*) = k_\infty(\alpha^{1/p} \mid [\alpha] \in \mathcal{H}_\infty(\Psi)) \tag{5}$$

and

$$A_\infty(\Psi^*)/A_\infty(\Psi^*)^p \cong \mathrm{Gal}(L(\Psi^*)/k_\infty) \cong \mathrm{Hom}(\mathcal{H}_\infty(\Psi), \boldsymbol{\mu}_p). \tag{6}$$

The first isomorphism in (6) is due to class field theory. Similarly, we obtain

$$A_n(\Psi^*)/A_n(\Psi^*)^p \cong \mathrm{Hom}(\mathcal{H}_n(\Psi), \mu_p). \tag{6'}$$

Since the p-rank of A_n is bounded as $n \to \infty$ ([**5**]), we see from (6) and (6') that $\mathcal{H}_\infty(\Psi)=\mathcal{H}_n(\Psi)$ for all sufficiently large n under the natural inclusion $\mathcal{H}_m \to \mathcal{H}_\infty$ induced by $k_m^\times \to k_\infty^\times$. Therefore, by the assumption of Theorem 2, we have $\mathcal{H}_\infty(\Psi)=\mathcal{N}_n(\Psi)$ for sufficiently large n. But, by the following lemma (Lemma 5), we have

$$\mathcal{N}_n(\Psi) \subset (E_n k_n^{\times p}/k_n^{\times p})(\Psi).$$

Therefore, we obtain $\widetilde{L}(\Psi^*)=(\widetilde{L} \cap F)(\Psi^*)$ by (5). Hence, $(G/G^p)(\Psi^*)$ and $(H/H^p)(\Psi^*)$ have the same dimension over $\boldsymbol{F}_p$. So, by Lemma 4, we get $G(\Psi^*)=H(\Psi^*)$ and hence $L(\Psi^*) \subset F(\Psi^*)$. Therefore, by (3), we obtain $M(\Psi^*)=F(\Psi^*)$ and hence $\lambda_\Psi=0$. □

LEMMA 5 ([**3**, Thm. B]). *Let K be a number field containing a primitive p-th root ζ_0 of unity. Then, a cyclic extension L/K of degree p is unramified and has an RNIB if and only if L is obtained by adjoining to K a p-th root of a unit ε of K such that $\varepsilon \equiv 1$ modulo the ideal $(\zeta_0-1)^p$.*

We need in § 5 the following fact which follows from the above lemma.

LEMMA 6. *Let k be an imaginary abelian field satisfying* (C1), (C2), (C3), *and let Ψ be a $\boldsymbol{Q}_p$-character of Δ. If $A_0(\Psi)=\{1\}$, then, $\mathcal{H}_0(\Psi)=\mathcal{N}_0(\Psi)$.*

PROOF. Let $\mathcal{N}_0^*$ be the subgroup of $k^\times/k^{\times p}$ consisting of classes $[\varepsilon]$ with $\varepsilon \in E_0$ for which the extension $k(\varepsilon^{1/p})/k$ is unramified. Clearly, we have $\mathcal{N}_0 \subset \mathcal{N}_0^* \subset \mathcal{H}_0$. Let ε be a unit of k such that $k(\varepsilon^{1/p})/k$ is unramified. Let $\mathfrak{p}=\mathfrak{p}_0$ be the unique prime of k over p. Replacing ε by $\varepsilon^{1-N\mathfrak{p}}$ if necessary, we may assume $\varepsilon \equiv 1$ modulo $\mathfrak{p}$, i.e., $\varepsilon \in \mathcal{U}_0$. It follows that $\mathfrak{p}=(\zeta_0-1)$ by (C1), (C2) and (C3). Hence, $\mathcal{U}_0=\mathcal{U}_0^{(1)}$. Further, since $k(\varepsilon^{1/p})/k$ is unramified and $\mathfrak{p}$ is principal, we get $\varepsilon=u^p$ for some $u \in \mathcal{U}_0=\mathcal{U}_0^{(1)}$ by class field theory. Hence, we have $\varepsilon \equiv 1$ modulo $(\zeta_0-1)^p$. Therefore, $\mathcal{N}_0^*=\mathcal{N}_0$ by Lemma 5. For each element $[\alpha]$ of $\mathcal{H}_0$, there exists an ideal $\mathfrak{U}$ of k such that $\mathfrak{U}^p=(\alpha)$. Then, by mapping each $[\alpha]$ $(\in \mathcal{H}_0)$ to the ideal class of $\mathfrak{U}$ with $\mathfrak{U}^p=(\alpha)$, we obtain an exact sequence compatible with the Galois action:

$$\{1\} \longrightarrow \mathcal{N}_0^* \longrightarrow \mathcal{H}_0 \longrightarrow A_0.$$

Therefore, if $A_0(\Psi)=\{1\}$, we have $\mathcal{H}_0(\Psi)=\mathcal{N}_0^*(\Psi)$, and hence $\mathcal{H}_0(\Psi)=\mathcal{N}_0(\Psi)$ as desired. □

REMARK 4. As we mentioned in § 1, we have $\mathcal{N}_n^-=\{1\}$ as a consequence of [1]. This fact also follows from Lemma 5 and the fact [25, Thm. 4.12] on units of a CM-field.

§ 5. Proof of Theorem 3.

§ 5-1. Two Propositions on $\mathcal{H}_n/\mathcal{N}_n$.

In this subsection, we give two propositions on $\mathcal{H}_n/\mathcal{N}_n$, from which Theorem 3 follows immediately. The subsections § 5-2 ~ § 5-4 are devoted to the proof of the propositions.

Let k be an imaginary abelian field satisfying (C1), (C2′) and (C3), and let Ψ be a nontrivial even $\boldsymbol{Q}_p$-character of Δ. Then, Ψ is of degree one, and hence $\phi=\Psi$, $\mathcal{O}=\boldsymbol{Z}_p$ and $\Lambda=\boldsymbol{Z}_p[\![t]\!]$. Assume that $\lambda_{\Psi^*}=1$. Then, the p-rank of $A_n(\Psi^*)$ is one for all n by [25, Cor. 13.29 and Prop. 13.26] and $\mathcal{O}=\boldsymbol{Z}_p$. Therefore, $\dim_{F_p}\mathcal{H}_n(\Psi)=1$ for all n by (6′) of § 4. Hence, for each integer n_0, we have $\mathcal{H}_n(\Psi)=\mathcal{N}_n(\Psi)$ for all $n\geqq n_0$ if and only if $\mathcal{H}_{n_0}(\Psi)=\mathcal{N}_{n_0}(\Psi)$, or equivalently if and only if $\dim_{F_p}\mathcal{N}_{n_0}(\Psi)=1$. We prove the following

PROPOSITION 1. *Let k be an imaginary abelian field satisfying* (C1), (C2′), *and* (C3), *and let Ψ be a nontrivial even $\boldsymbol{Q}_p$-character of Δ such that $\lambda_{\Psi^*}=1$. Then, $\mathcal{H}_n(\Psi)=\mathcal{N}_n(\Psi)$ for all sufficiently large n if and only if $\mathcal{H}_0(\Psi)=\mathcal{N}_0(\Psi)$.*

We give a necessary and sufficient condition for $\dim_{F_p}\mathcal{N}_0(\Psi)=1$ (without the assumption $\lambda_{\Psi^*}=1$). Such a condition is already obtained by [24, Thm. 2] when $k=\boldsymbol{Q}(\mu_p)$. The following is its generalization.

PROPOSITION 2. *Let k be an imaginary abelian field satisfying* (C1), (C2′) *and* (C3), *and let Ψ be a nontrivial even $\boldsymbol{Q}_p$-character of Δ. Then,* $\dim_{F_p}\mathcal{N}_0(\Psi)\leqq 1$. *Further,* $\dim_{F_p}\mathcal{N}_0(\Psi)=1$ *if and only if* $L_p(1,\phi)/|A_0(\Psi)|\equiv 0 \bmod p$.

§ 5-2. A preliminary lemma.

Let k be an imaginary abelian field satisfying (C1), (C2′), (C3), and let Ψ be a nontrivial even $\boldsymbol{Q}_p$-character of Δ. If $\lambda_\Psi=0$, then, any ideal of k representing an ideal class in $A_0(\Psi)$ is capitulated in k_s for some s ([11, Prop. 2]).

LEMMA 7. *Let k and Ψ be as above. Assume that $\lambda_{\Psi^*}=1$, $\lambda_\Psi=0$ and $A_0(\Psi)\cong\boldsymbol{Z}/p^a\boldsymbol{Z}$ with $a\geqq 1$. Let r be the least nonnegative integer such that any ideal of k representing an ideal class of order p in $A_0(\Psi)$ is capitulated in k_{r+1}. Then, we have $A_n(\Psi)\cong\boldsymbol{Z}/p^{a+n}\boldsymbol{Z}$ (resp. $\boldsymbol{Z}/p^{a+r}\boldsymbol{Z}$) when $0\leqq n\leqq r$ (resp. $n\geqq r+1$).*

PROOF. Though this assertion seems to be more or less known to specialists, we give its proof because we could not find an appropriate reference. First, we give some remarks which follow from the assumptions. Let M and L be as in § 4, and let M_n (resp. L_n) be the maximal abelian extension of k_n contained in M (resp. L). Denote by $M_n(\Psi)$ the intermediate field of M_n/k_∞ fixed by $\mathrm{Gal}(M_n/k_\infty)(\Phi)$ for all $\boldsymbol{Q}_p$-characters Φ of Δ with $\Phi \neq \Psi$. Define $L_n(\Psi)$ in a similar way. From the assumption $\lambda_{\Psi^*}=1$, it follows that the Λ-module $\mathrm{Gal}(M(\Psi)/k_\infty)$ is isomorphic to $\Lambda/(t-\alpha)$ for some $\alpha \in \boldsymbol{Z}_p$ with $p \mid \alpha$ (cf. [**21**, Thm. 1]). Hence, we have

$$\mathrm{Gal}(M_n(\Psi)/k_\infty) \cong \boldsymbol{Z}_p[\![t]\!]/(t-\alpha, \omega_n) \cong \boldsymbol{Z}_p/\alpha p^n \boldsymbol{Z}_p . \tag{7}$$

We must have $\alpha \neq 0$ because $[M_0(\Psi): k_\infty]$ is finite (see [**11**, page 266]) by the Leopoldt conjecture for k and p (proved by Brumer [**2**]). Let p^e ($e \geqq 1$) be the highest power of p dividing α. By class field theory and the assumptions (C2), (C3), there is the canonical isomorphism:

$$\mathrm{Gal}(L_n(\Psi)/k_\infty) \cong A_n(\Psi) . \tag{8}$$

Hence, by (7) and $L_n(\Psi) \subset M_n(\Psi)$, we see that $A_n(\Psi)$ is cyclic. Similarly, we have $a \leqq e$. For $n<m$, denote by $\iota_{n,m}$ the homomorphism $A_n(\Psi) \to A_m(\Psi)$ induced by the inclusion $k_n \to k_m$. From the definition of r and the cyclicity of $A_n(\Psi)$, we see that $\iota_{n,m}$ is injective when $0 \leqq n < m \leqq r$ but $\iota_{r,r+1}$ is not. Further, we have

$$|A_n(\Psi)| \,\Big|\, |A_{n+1}(\Psi)|, \tag{9}$$

since the map $A_{n+1}(\Psi) \to A_n(\Psi)$ induced from the norm map $N_{n+1/n}$ from k_{n+1} to k_n is surjective.

Now, let us prove the first part of the assertion. Assume that $A_n(\Psi) \cong \boldsymbol{Z}/p^{a+n}\boldsymbol{Z}$ for an integer n with $0 \leqq n < r$. Take a prime ideal $\mathfrak{P}$ of k_{n+1} of degree one such that its class $[\mathfrak{P}]_{n+1}$ generates the cyclic group $A_{n+1}(\Psi)$. Here, for an ideal $\mathfrak{U}$ of k_m, $[\mathfrak{U}]_m$ denotes the ideal class of k_m represented by $\mathfrak{U}$. Then, the order of $[\mathfrak{P}]_{n+1}$ is divisible by p^{a+n} by (9) and the assumption of induction. Put $\mathfrak{p}=N_{n+1/n}\mathfrak{P}$. Then, the class $[\mathfrak{p}]_n$ generates $A_n(\Psi)$, and hence, the order of $[\mathfrak{p}]_n$ is p^{a+n}. Hence, the order of $[\mathfrak{p}^{\mathcal{O}_{n+1}}]_{n+1}$ is p^{a+n} because of the injectivity of $\iota_{n,n+1}$. Here, $\mathcal{O}_m$ denotes the ring of integers of k_m. Assume that $[\mathfrak{P}]_{n+1}$ is of order p^{a+n}. Then, $[\mathfrak{p}^{\mathcal{O}_{n+1}}]_{n+1}=[\mathfrak{P}]_{n+1}^c$ for some integer c with $p \nmid c$. Applying the norm map $N_{n+1/n}$, we get $[\mathfrak{p}]_n^p=[\mathfrak{p}]_n^c$. Hence, the order of $[\mathfrak{p}]_n$ is relatively prime to p. This is a contradiction. Assume that the order of $[\mathfrak{P}]_{n+1}$ is divisible by p^{a+n+2}. Then, we see that $a+1 \leqq e$ from (7) and (8), and that there exists an intermediate field H of $M_{n+1}(\Psi)/k_\infty$ such that H is unramified over k_∞ and $[H: k_\infty]=p^{a+n+1}$ from (8). By $a+1 \leqq e$ and (7), we must have $H \subset M_n(\Psi)$, and hence $H \subset L_n(\Psi)$. Therefore, we get $p^{a+n+1} \,|\, |A_n(\Psi)|$ from

(8). This is a contradiction.

Let us deal with the case $n=r+1$. As we have shown above, we have $A_r(\Psi)\cong \boldsymbol{Z}/p^{a+r}\boldsymbol{Z}$. Hence, by (9), p^{a+r} divides $|A_{r+1}(\Psi)|$. Put $|A_{r+1}(\Psi)|=p^{a+r+l}$ with $l\geqq 0$. We show that $l=0$. Take a prime ideal $\mathfrak{P}$ of k_{r+1} such that the class $[\mathfrak{P}]_{r+1}$ generates $A_{r+1}(\Psi)$. We see that the order of the ideal class $[N_{r+1/r}\mathfrak{P}]_{r+1}$ of k_{r+1} divides p^{a+r-1} because the ideal class $[N_{r+1/r}\mathfrak{P}]_r$ of k_r is of order p^{a+r} and $\iota_{r,r+1}$ is not injective. By the identification of $\boldsymbol{Z}_p[\![\Gamma]\!]$ with $\boldsymbol{Z}_p[\![t]\!]$ via $\gamma\leftrightarrow 1+t$, the norm operator $N_{r+1/r}$ corresponds to the polynomial $\nu=\nu(t)=\omega_{r+1}/\omega_r$. Therefore, the polynomial $p^{a+r-1}\cdot\nu$ annihilates the Λ-module $A_{r+1}(\Psi)$. By (7) and the canonical isomorphism (8), we see that the element t acts on $A_{r+1}(\Psi)$ via the multiplication by α. Hence, if $f(t)$ $(\in \boldsymbol{Z}_p[\![t]\!])$ annihilates $A_{r+1}(\Psi)$, then, $p^{a+r+l}\mid f(\alpha)$ because $A_{r+1}(\Psi)\cong \boldsymbol{Z}/p^{a+r+l}\boldsymbol{Z}$. We easily see that $\nu(\alpha)/p$ is a p-adic unit. Therefore, we have $p^{a+r+l}\mid p^{a+r-1}\cdot p$, hence $l=0$.

Finally, let us prove the assertion when $n\geqq r+2$. Assume that $|A_n(\Psi)|$ is divisible by p^{a+r+1} for some $n\geqq r+2$. Then, by (8), there exists an intermediate field H of $M_n(\Psi)/k_\infty$ such that H/k_∞ is unramified and $[H: k_\infty]=p^{a+r+1}$. Then, we have $H\subset M_{r+1}(\Psi)$ by (7) and $a\leqq e$. Therefore, $H\subset L_{r+1}(\Psi)$. Hence, by (8), $p^{a+r+1}\mid\mid A_{r+1}(\Psi)|$. This is a contradiction. □

§ 5-3. Proof of Proposition 2.

Let k and Ψ be as in Proposition 2. Because of the assumption (C2′), we obtain $\dim_{F_p}(E_0/E_0^p)(\Psi)=1$ from the theorem of Minkowski on units of a Galois extension over $\boldsymbol{Q}$ by using a similar argument as in Iwasawa [**20**, page 119]. Hence, by Lemma 5, we get $\dim_{F_p}\mathcal{N}_0(\Psi)\leqq 1$. Let ε be a unit of k such that its class in E_0/E_0^p generates the cyclic group $(E_0/E_0^p)(\Psi)$ of order p. Replacing ε by $\varepsilon^{1-N\mathfrak{p}}$ if necessary, we may assume $\varepsilon\in\mathcal{U}_0$. Here, $\mathfrak{p}$ is the unique prime ideal of k over p. We see that $\dim_{F_p}\mathcal{N}_0(\Psi)=1$ if and only if $\varepsilon^{e_\Psi}\in\mathcal{U}_0(\Psi)^p$ by a similar argument as the first part of the proof of Lemma 6. On the other hand, we see that $\mathcal{U}_0(\Psi)\cong \boldsymbol{Z}_p$ by $\mathcal{O}=\boldsymbol{Z}_p$ and Lemma 1(2). Therefore, we see that $\dim_{F_p}\mathcal{N}_0(\Psi)=1$ if and only if $p\mid[\mathcal{U}_0(\Psi): \mathcal{E}_0(\Psi)]$. Clearly, we have

$$[\mathcal{U}_0(\Psi): \mathcal{E}_0(\Psi)] = [\mathcal{U}_0(\Psi): C_0(\Psi)]/[\mathcal{E}_0(\Psi): C_0(\Psi)]. \tag{10}$$

By the formula (2), Lemma 1(2) and Lemma 3, the right hand side is divisible by p if and only if so is $L_p(1, \phi)/|A_0(\Psi)|$. □

§ 5-4. Proof of Proposition 1.

Let k and Ψ be as in Proposition 1. By the remark in § 5-1, all we have to do is to prove that $\mathcal{H}_n(\Psi)\neq\mathcal{N}_n(\Psi)$ for all n $(\geqq 0)$ when $\mathcal{H}_0(\Psi)\neq\mathcal{N}_0(\Psi)$. So, we first pick up the cases where $\mathcal{H}_0(\Psi)=\mathcal{N}_0(\Psi)$. Let $g_\phi(t)$ be as before the power series with coefficients in $\boldsymbol{Z}_p$ associated by (2) to the p-adic L-function

$L_p(s, \phi)$. By the Iwasawa main conjecture (proved by Mazur-Wiles [22]), the power series $\dot{g}_\phi(t)=g_\phi((1+q)(1+t)^{-1}-1)$ is a characteristic power series of the torsion Λ-module $A_\infty(\Psi^*)$, which is not a multiple of p by the theorem of [5]. Hence, the assumption $\lambda_{\Psi^*}=1$ implies that g_ϕ equals to $t-\beta$ for some $\beta\in\boldsymbol{Z}_p$ with $p|\beta$ up to multiplication by unit of Λ. The main conjecture also says that g_ϕ is a characteristic power series of $\mathrm{Gal}(M(\Psi)/k_\infty)$. Hence, β is nothing but the α in the proof of Lemma 7. As we have seen there, we have $\beta=\alpha\neq 0$. Let p^e $(e\geqq 1)$ and p^a $(a\geqq 0)$ be the highest powers of p dividing β and $|A_0(\Psi)|$ respectively. By (10), Lemma 1(2) and Lemma 3, we must have $e\geqq a$. By Proposition 2 and the remark in §5-1, we have $\mathcal{H}_0(\Psi)=\mathcal{H}_0(\Psi)$ if and only if $e>a$. Further, we have $\mathcal{H}_0(\Psi)=\mathcal{H}_0(\Psi)$ when $a=0$ by Lemma 6.

Now, assume that $e=a\geqq 1$. We prove $\mathcal{H}_n(\Psi)\neq\mathcal{H}_n(\Psi)$ for all n. By Lemma 1(2) (and $\mathcal{O}=\boldsymbol{Z}_p$), we have

$$\begin{array}{ccccc} \mathcal{U}_n(\Psi)/C_n(\Psi) & \cong & \boldsymbol{Z}_p[\![t]\!]/(t-\beta,\ \omega_n) & \cong & \boldsymbol{Z}/p^{e+n}\boldsymbol{Z} \\ \cup & & \cup & & \cup \\ \overline{\boldsymbol{u}_n^g} & \longleftrightarrow & \bar{g} & \longleftrightarrow & \overline{g(\beta)}\ . \end{array} \tag{11}$$

Here, $\boldsymbol{u}_n$ is as in §3, and $\bar{x}$ denotes the class represented by x. If $\lambda_\Psi\neq 0$, then, we see that $\mathcal{H}_n(\Psi)\neq\mathcal{H}_n(\Psi)$ for all n by using Theorem 2. Hence, we may further assume that $\lambda_\Psi=0$. Let r $(\geqq 0)$ be as in Lemma 7 and n be any integer with $n\geqq r+1$. Then, by Lemma 3, Lemma 7 and (11), we have

$$\mathcal{E}_n(\Psi)=\mathcal{U}_n(\Psi)^{p^{n-r}}\cdot C_n(\Psi) \quad\text{and}\quad \mathcal{E}_n(\Psi)/C_n(\Psi)\cong\boldsymbol{Z}/p^{e+r}\boldsymbol{Z}. \tag{12}$$

In particular, noting that $p|\beta$, we obtain the following isomorphisms induced from the correspondence in Lemma 1(2).

$$\begin{array}{ccccc} \mathcal{E}_{r+1}(\Psi) & \xleftarrow{\sim} & (p,\ t,\ \omega_{r+1})/(\omega_{r+1}) & & (\boldsymbol{u}_{r+1}^g \longleftrightarrow \bar{g}) \\ \cup & & \cup & & \\ \mathcal{E}_{r+1}(\Psi)\cap\mathcal{U}_{r+1}(\Psi)^p & \xleftarrow{\sim} & (p,\ pt,\ \omega_{r+1})/(\omega_{r+1}) & & \\ \cup & & \cup & & \\ \mathcal{E}_{r+1}(\Psi)^p & \xleftarrow{\sim} & (p^2,\ pt,\ \omega_{r+1})/(\omega_{r+1}). & & \end{array}$$

Therefore, we may and shall take a unit ε of k_{r+1} such that, in $\mathcal{U}_{r+1}$, ε^{e_Ψ} is sufficiently close to $\boldsymbol{u}_{r+1}^p$. Then, from the above, we see that the cyclic group $\mathcal{H}_{r+1}(\Psi)$ of order p is generated by the class $[\varepsilon]^{e_\Psi}$. Assume $\mathcal{H}_n(\Psi)=\mathcal{H}_n(\Psi)$ for some n $(\geqq r+1)$. Then, by Lemma 5, we must have $\varepsilon^{e_\Psi}/\eta^p\equiv 1$ modulo $(\zeta_0-1)^p$ for some $\eta\in\mathcal{E}_n(\Psi)$. Therefore, we see that

$$\boldsymbol{u}_{r+1}=v\cdot\eta \text{ for some } v\in\mathcal{U}_n^{(1)}(\Psi) \text{ and } \eta\in\mathcal{E}_n(\Psi). \tag{13}$$

We compare the orders of the classes of both hand sides of (13) in the cyclic group $\mathcal{U}_n(\Psi)/C_n(\Psi)$. By the identification of $\boldsymbol{Z}_p[\![\Gamma]\!]$ with $\boldsymbol{Z}_p[\![t]\!]$ via $\gamma\leftrightarrow 1+t$,

the norm map $N_{n/r+1}$ from $k_n^\times$ to $k_{r+1}^\times$ corresponds to the polynomial

$$S=\sum_{j=0}^{p^{n-r-1}-1}(1+t)^{p^{r+1}j}.$$

In the residue ring $\boldsymbol{Z}_p[\![t]\!]/(t-\beta,\ \omega_n)\cong\boldsymbol{Z}_p/p^{e+n}\boldsymbol{Z}_p$, the class of S is decomposed as the product of p^{n-r-1} and a unit since $S(\beta)$ is p^{n-r-1} times a unit of $\boldsymbol{Z}_p$. Therefore, since $\boldsymbol{u}_{r+1}=N_{n/r+1}\boldsymbol{u}_n=\boldsymbol{u}_n^S$, we see that the order of the class $\bar{\boldsymbol{u}}_{r+1}$ in $\mathcal{U}_n(\Psi)/C_n(\Psi)$ is p^{e+r+1} by (11). On the other hand, we see that the order of the class $\bar{v}$ divides p^e by Lemma 2 and (11) because $p^n\mid p^{n-1-j}\beta^{p^j}$ $(0\leqq j\leqq n-1)$. Further, the order of the class $\bar{\eta}$ divides p^{e+r} by (12). This is a contradiction. Therefore, $\mathcal{H}_n(\Psi)\neq\mathcal{N}_n(\Psi)$ for all $n\geqq r+1$. Hence, $\mathcal{H}_n(\Psi)\neq\mathcal{N}_n(\Psi)$ for all n. □

§5-5. Examples.

The converse of Theorem 1 and that of Theorem 2 do not hold in general as we see in the following examples respectively. Let $p=3$ and $k=\boldsymbol{Q}(\sqrt{-3},\ \sqrt{d})$ where d is a rational integer with $d\equiv 2$ (mod. 3). Let Ψ be the unique nontrivial even $\boldsymbol{Q}_p$-character of Δ. Then, $\mathcal{H}_n(\Psi)=\mathcal{H}_n^+$ and $\mathcal{N}_n(\Psi)=\mathcal{N}_n^+$. Assume $\lambda_{\Psi^*}=1$. Let ε be a fundamental unit of the real quadratic subfield k^+. Then, it follows that $\mathcal{H}_n^+=\mathcal{N}_n^+$ for all sufficiently large n if and only if $\varepsilon^8\equiv 1$ modulo $(\zeta_0-1)^3$ from Proposition 1 (and the remark in §5-1) and Lemma 5.

First, consider the case $d=257$. Then, we have $\varepsilon=16+\sqrt{257}$ and $\varepsilon^8\equiv 1$ (mod. 9). Further, $\lambda_{\Psi^*}=1$ by the table of Fukuda [7] on Iwasawa λ-invariants of imaginary quadratic fields. But, we have $h(k^+)=3$. Next, consider the case $d=443$. Then, we have $\varepsilon=442+21\sqrt{443}$ and $\varepsilon^8\not\equiv 1$ modulo $(\zeta_0-1)^3$. Further, $\lambda_{\Psi^*}=1$ by [7]. But, we have $\lambda_\Psi=0$ by [**11**, page 282].

§6. Proof of Theorem 4.

Let k be an imaginary abelian field satisfying (C1), (C2), (C3) and $p\nmid h(k^+)$. Since $\mathcal{H}_n(\Psi_0)=\mathcal{H}_n^-=\{1\}$ (see §2), it suffices to prove that the homomorphism

$$\rho_n:(\mathcal{H}_n/\mathcal{N}_n)(\Psi)\longrightarrow(\mathcal{H}_{n+1}/\mathcal{N}_{n+1})(\Psi)$$

induced from the inclusion $k_n^\times\to k_{n+1}^\times$ is trivial for any nontrivial even $\boldsymbol{Q}_p$-character Ψ. Let Ψ be any such character and ϕ be a fixed irreducible component of Ψ over Ω_p. To prove Theorem 4, we have to recall the main theorem and a lemma of the preceding paper [**15**]. Define an ideal X_n of $\mathcal{O}[\![t]\!]$ and a $\mathcal{O}[\![t]\!]$-module Y_n by

$$X_n=\{g\in\mathcal{O}[\![t]\!]\mid p\cdot g\in(g_\phi,\ \omega_n)\},$$

$$Y_n=X_n/(X_n\cap I_n,\ g_\phi,\ \omega_n).$$

Put $S_n=\omega_{n+1}/\omega_n$. We see that $g\cdot S_n\in X_{n+1}$ for all $g\in X_n$ and that the homomorphism

$$s_n : Y_n \longrightarrow Y_{n+1}, \quad [g]_n \longrightarrow [g\cdot S_n]_{n+1}$$

is well defined (see [**15**, § 5-1]). Here, $[g]_n$ denotes the element of Y_n represented by $g\in X_n$.

THEOREM 5 ([**15**, Thm. 1]). *Let k and Ψ be as above. Then, there exists an isomorphism ι_n from $(\mathcal{H}_n/\mathcal{N}_n)(\Psi)$ to Y_n as modules over $\mathcal{O}[\![t]\!]$ such that $\iota_{n+1}\circ\rho_n=s_n\circ\iota_n$ for all n.*

Therefore, to prove Theorem 4, it suffices to show that the homomorphism s_n is trivial. For this purpose, we have to know a set of generators of Y_n over $\mathcal{O}[\![t]\!]$. Let h_ϕ be the distinguished polynomial of $\mathcal{O}[t]$ associated to the power series g_ϕ. Since h_ϕ equals to g_ϕ times a unit of $\mathcal{O}[\![t]\!]$ ([**5**]), we may write h_ϕ instead of g_ϕ in the definitions of X_n and Y_n. Put $\lambda=\deg h_\phi$, which does not depend on the choice of the irreducible component ϕ of Ψ. We have $\lambda=\lambda_{\Psi *}$ by the Iwasawa main conjecture. Therefore, when $\lambda=0$, we have $\mathcal{H}_n(\Psi)=\mathcal{N}_n(\Psi)=\{1\}$ by [**25**, Cor. 13.29] and (6′) of § 4. So, we may assume $\lambda\geqq 1$. We put

$$a_n=(h_\phi-t^{\lambda-p^n}\cdot\omega_n)/p \quad \text{or} \quad (\omega_n-t^{p^n-\lambda}\cdot h_\phi)/p$$

according as $p^n\leqq\lambda$ or $p^n\geqq\lambda$. Clearly, the polynomial a_n is an element of X_n.

LEMMA 8 ([**15**, Lemma 3]). *The module Y_n is generated over $\mathcal{O}[\![t]\!]$ by the class of a_n.*

Now, we prove Theorem 4. By Theorem 5 and Lemma 8, it suffices to prove that

$$a_n\cdot S_n\in(X_{n+1}\cap I_{n+1},\ h_\phi,\ \omega_{n+1}). \tag{14}$$

We already have $a_n\cdot S_n\in X_{n+1}$ since $a_n\in X_n$. We see that $S_n=p+\delta$ for some $\delta\in I_{n+1}$ and $\omega_n\in I_{n+1}$ by the equality

$$(1+t)^{p^n}=1+t^{p^n}+\sum_{k=0}^{n-1}t^{p^k}\cdot\sum_{j=p^k}^{p^{k+1}-1}B(p^n,\ j)t^{j-p^k}$$

and a simple fact ([**15**, Lemma 4]) on binomial coefficients $B(p^n,\ j)$. Assume $p^n\leqq\lambda$. Then, since $h_\phi\in X_{n+1}$, we have

$$b=a_n\cdot S_n-h_\phi=-t^{\lambda-p^n}\cdot\omega_n+a_n\delta\in X_{n+1}. \tag{15}$$

On the other hand, we have $b\in I_{n+1}$ because δ, $\omega_n\in I_{n+1}$. Therefore, $b\in X_{n+1}\cap I_{n+1}$, and hence, we obtain the assertion (14) in this case. When $p^n\geqq\lambda$, we obtain (14) by a similar argument, using

$$b' = a_n \cdot S_n + t^{p^{n-\lambda}} \cdot h_\phi = \omega_n + a_n \delta$$

in place of b. This completes the proof of Theorem 4. □

References

[1] J. Brinkhuis, On the Galois module structure over CM-fields, Manuscripta Math., **75** (1992), 333-347.

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

[3] L. N. Childs, The group of unramified Kummer extensions of prime degree, Proc. London Math. Soc., **35** (1977), 407-422.

[4] J. Coates, p-adic L-functions and Iwasawa's theory, Algebraic Number Fields, Durham Symposium 1975, (ed. A. Fröhlich), Academic Press, London, 1977, pp. 269-353.

[5] B. Ferrero and L. C. Washington, The Iwasawa invariant μ_p vanishes for abelian number fields, Ann. of Math., **109** (1979), 377-395.

[6] T. Fukuda and K. Komatsu, On $\boldsymbol{Z}_p$-extensions of real quadratic fields, J. Math. Soc. Japan, **38** (1986), 95-102.

[7] T. Fukuda, Iwasawa λ-invariants of imaginary quadratic fields, J. College Industrial Technology Nihon Univ., **27** (1994), 35-88, (Corrigendum to appear in ibid.).

[8] R. Gillard, Remarques sur les unités cyclotomiques et unités elliptiques, J. Number Theory, **11** (1979), 21-48.

[9] R. Gillard, Unités cyclotomiques, unités semi-locales et $\boldsymbol{Z}_l$-extensions, Ann. Inst. Fourier, **29-1** (1979), 49-79.

[10] R. Gillard, Unités cyclotomiques, unités semi-locales et $\boldsymbol{Z}_l$-extensions II, Ann. Inst. Fourier, **29-4** (1979), 1-15.

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

[12] R. Greenberg, On p-adic L-functions and cyclotomic fields, Nagoya Math. J., **67** (1977), 139-158.

[13] H. Hasse, Über die Klassenzahl Abelscher Zahlkörper, Akademie-Verlag, 1952.

[14] H. Ichimura, On a relative normal integral basis problem over abelian number fields, Proc. Japan Acad., **69** (1993), 413-416.

[15] H. Ichimura, On p-adic L-functions and normal basis of rings of integers, J. Reine Angew. Math., **462** (1995), 169-184.

[16] K. Iwasawa, A note on class numbers of algebraic number fields, Abh. Math. Sem. Univ. Hamburg, **20** (1956), 257-258.

[17] K. Iwasawa, On some modules in the theory of cyclotomic fields, J. Math. Soc. Japan, **16** (1964), 42-82.

[18] K. Iwasawa, Lectures on p-adic L-functions, Ann. of Math. Studies, **74**, Princeton Univ. Press, 1972.

[19] K. Iwasawa, On $\boldsymbol{Z}_l$-extensions of algebraic number fields, Ann. of Math., **98** (1973), 246-326.

[20] K. Iwasawa, A note on cyclotomic fields, Invent. Math., **36** (1976), 115-123.

[21] J. S. Kraft, Iwasawa invariants of CM fields, J. Number Theory, **32** (1989), 65-77.

[22] B. Mazur and A. Wiles, Class fields of abelian extensions of $\boldsymbol{Q}$, Invent. Math., **76** (1984), 179-330.

[23] H. Taya, On the Iwasawa λ-invariants of real quadratic fields, Tokyo J. Math., **16** (1993), 121-130.

[24] M. J. Taylor, The Galois module structure of certain arithmetic principal homogeneous spaces, J. Algebra, **153** (1992), 203-214.
[25] L. C. Washington, Introduction to Cyclotomic Fields, Springer-Verlag, 1982.

Humio ICHIMURA
Department of Mathematics
Yokohama City University
22-2 Seto, Kanazawa-ku
Yokohama 236
Japan