94. *On a Relative Normal Integral Basis Problem over Abelian Number Fields**)

By Humio ICHIMURA

Department of Mathematics, Yokohama City University

(Communicated by Shokichi IYANAGA, M. J. A., Dec. 13, 1993)

We say that a Galois extension L/K of a number field K with Galois group G has a *relative normal integral basis* (RNIB, for short) when the integer ring O_L of L is free over the group ring $O_K[G]$. Let p be a prime number and assume that K contains a primitive p-th root of unity. In [3], Childs proved that an unramified cyclic extension L/K of degree p has an RNIB if and only if L is obtained by adjoining to K a p-th root of a unit of K satisfying a certain congruence. Let $\mathscr{H}(K)$ be the subgroup of $K^\times/K^{\times p}$ consisting of classes $[\alpha]$ $(\alpha \in K^\times)$ for which $K(\alpha^{1/p})$ is unramified over K, and $\mathscr{N}(K)$ be the subgroup of $\mathscr{H}(K)$ consisting of classes $[\alpha]$ $(\in \mathscr{H}(K))$ for which the unramified cyclic extension $K(\alpha^{1/p})/K$ has an RNIB. Using the above result and tools of Iwasawa theory, we shall describe, in terms of power series attached to p-adic L-functions, the Galois module structure of the quotient $\mathscr{H}(K)/\mathscr{N}(K)$ when the base field K runs over all layers of the cyclotomic $\boldsymbol{Z}_p$-extension of a certain imaginary abelian field (Theorem). As a corollary, we give a necessary and sufficient condition for $\mathscr{H}(K) = \mathscr{N}(K)$ for such K in terms of an Iwasawa invariant and a certain distinguished polynomial. Though there are several results to the effect that relative Galois extensions have no RNIB (e.g. Fröhlich[7, Chap. 6, §3], Cougnard[4], Brinkhuis[1]), there seems to be few results in the other derection. An immediate consequence of the Corollary is that any unramified cyclic extension of degree p over K as above has an RNIB if the base field K is a "sufficiently" high layer. This paper is an announcement of the results generalizing those of our paper [10]. The details will appear elsewhere.

Let p be a fixed odd prime number and k be an imaginary abelian field satisfying the following three 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.

Typical examples of such k are (1) $k = \boldsymbol{Q}(\mu_p)$, and (2) $p = 3$, $k = \boldsymbol{Q}(\sqrt{-3}, \sqrt{d})$ where d is a rational integer with $d \equiv 2 \pmod{3}$. Let k_∞/k be the cyclotomic $\boldsymbol{Z}_p$-extension and k_n be its n-th layer $(n \geq 0)$. Put $\Delta = \mathrm{Gal}(k/\boldsymbol{Q})$ and $\Gamma = \mathrm{Gal}(k_\infty/k)$. We write, for brevity, $\mathscr{H}_n = \mathscr{H}(k_n)$ and $\mathscr{N}_n = \mathscr{N}(k_n)$. The Galois groups Δ and Γ act on these groups naturally. Let Ψ be an irreducible character of Δ over $\boldsymbol{Q}_p$. We call such Ψ a $\boldsymbol{Q}_p$-character. We fix an irreducible component ψ of Ψ over an algebraic closure Ω_p of $\boldsymbol{Q}_p$, which we

*) Partially supported by Grant in Aid for Scientific Research #05640055.

also regard as a primitive Dirichlet character. We say that Ψ is even when the Dirichlet character ψ is even. Let A be the subring of Ω_p generated over $\boldsymbol{Z}_p$ by the image of ψ. Let e_Ψ be the idempotent of the group ring $\boldsymbol{Z}_p[\Delta]$ corresponding to Ψ. For a $\boldsymbol{Z}_p[\Delta]$-module M, we write $M(\Psi) = e_\Psi M$. We identify $e_\Psi \boldsymbol{Z}_p[\Delta]$ with A by $e_\Psi \sigma \leftrightarrow \psi(\sigma)$ $(\sigma \in \Delta)$. Let γ be the topological generator of Γ such that $\zeta^\gamma = \zeta^{1+q_0}$ for all p^a-th roots ζ of unity and for all $a(\geq 1)$, where q_0 is the least common multiple of p and the conductor of ψ. We identify, as usual, the completed group ring $A[[\Gamma]]$ with the power series ring $A[[t]]$ by $\gamma \leftrightarrow 1+t$. Thus, the group $(\mathscr{H}_n/\mathscr{N}_n)(\Psi)$ is a module over $A[[t]]$. When Ψ is nontrivial and even, Iwasawa[12] has constructed a power series $g_\psi(t)$ with coefficients in A such that

$$g_\psi((1+q_0)^{1-s}-1) = L_p(s, \psi).$$

Here, $L_p(s, \psi)$ is the p-adic L-function associated to the Dirichlet character ψ. Define the ideal X_n of $A[[t]]$ by

$$X_n = \{g \in A[[t]] \mid p \cdot g \in (g_\psi, \omega_n)\}.$$

Here, $\omega_n = (1+t)^{p^n} - 1$. Let $\Lambda_n (n \geq 1)$ be the ideal of $A[[t]]$ generated by p^n, $p^{n-1-j} \cdot t^{p^j}$ $(0 \leq j \leq n-1)$, and $\Lambda_0 = A[[t]]$. Define the $A[[t]]$-module Y_n by

$$Y_n = X_n/(X_n \cap \Lambda_n, g_\psi, \omega_n).$$

Theorem. *Let k be an imaginary abelian field satisfying* (C1), (C2), (C3) *such that p does not divide the class number $h(k^+)$ of its maximal real subfield k^+. Let Ψ be a nontrivial even $\boldsymbol{Q}_p$-character of Δ, and ψ be its irreducible component over Ω_p. Then, there exists an isomorphism ι_n from $(\mathscr{H}_n/\mathscr{N}_n)(\Psi)$ to Y_n over $A[[t]]$ such that the following diagram is commutative*:

$$\begin{array}{ccccccc}
\{[\alpha]_{n+1}\} & \in & (\mathscr{H}_{n+1}/\mathscr{N}_{n+1})(\Psi) & \xrightarrow{\iota_{n+1}} & Y_{n+1} & \ni & [(\sum_{j=0}^{p-1}(1+t)^{p^n \cdot j}) \cdot g]_{n+1} \\
\updownarrow & & \uparrow & & \uparrow & & \updownarrow \\
\{[\alpha]_n\} & \in & (\mathscr{H}_n/\mathscr{N}_n)(\Psi) & \xrightarrow{\iota_n} & Y_n & \ni & [g]_n.
\end{array}$$

Here, $\{[\alpha]_m\}$ *denotes the class in* $\mathscr{H}_m/\mathscr{N}_m$ *represented by an element* $[\alpha]_m$ *of* $\mathscr{H}_m (\alpha \in k_m^\times)$, *and* $[g]_m$ *is the class in* Y_m *represented by* $g (\in X_m)$.

Remark 1. (1) Since $p \nmid h(k^+)$, we see from (C2) and (C3) that $p \nmid h(k_n^+)$ for all $n \geq 0$ by using a theorem of Iwasawa[11]. Therefore, it follows from the Spiegelungsatz that $\mathscr{H}_n^- = \{1\}$.
(2) Let Ψ_0 be the trivial character of Δ. Then, by the Stickelberger theorem for $\boldsymbol{Q}(\mu_{p^n})$ and the Spiegelungsatz, we obtain $\mathscr{H}_n(\Psi_0) = \{1\}$. For a nontrivial even $\boldsymbol{Q}_p$-character Ψ, the Galois module structure of $\mathscr{H}_n(\Psi)$ is described in terms of power series g_ψ by the Iwasawa main conjecture (proved by Mazur-Wiles[14]).

By the theorem of Ferrero-Washington[6] on Iwasawa μ-invariants and the Weierstrass preparation theorem, the power series g_ψ is the product of a distinguished polynomial $h_\psi(t)$ of $A[t]$ and a unit of $A[[t]]$. Put $\lambda = \lambda_\psi = \deg h_\psi$. This does not depend on the choice of an irreducible component ψ of Ψ. When $\lambda_\psi = 0$, it follows from the Iwasawa main conjecture that $\mathscr{H}_n(\Psi) = \{1\}$. Put $H_\psi = h_\psi - t^\lambda$. Some computation on the modules $Y_n (n \geq 0)$ yields the following

Corollary. *Let k be an imaginary abelian field satisfying the assumptions of Theorem, and let Ψ be a nontrivial even $\boldsymbol{Q}_p$-character of Δ such that $\lambda = \lambda_\psi \geq 1$ for its irreducible component ψ over Ω_p. Then, the following holds:*

(a) *When $p^{n-1}(p-1) \geq \lambda$ $(n \geq 1)$, $\mathcal{H}_n(\Psi) = \mathcal{N}_n(\Psi)$.*

(b) *When $p^{n-1}(p-1) < \lambda < p^n$ $(n \geq 2)$, $\mathcal{H}_n(\Psi) = \mathcal{N}_n(\Psi)$ if and only if $t^{p^n-\lambda} \cdot H_\psi \in p\Lambda_n$.*

(c) *When $p^n \leq \lambda$ $(n \geq 0)$, $\mathcal{H}_n(\Psi) = \mathcal{N}_n(\Psi)$ if and only if $H_\psi \in p \cdot \Lambda_n$.*

Remark 2. Since h_ψ is a distinguished polynomial, $H_\psi \in p \cdot \Lambda_0$. So, $\mathcal{H}_0 = \mathcal{N}_0$ for any k satisfying the assumptions of Theorem. But, it can be proved more directly using the result of Childs and the Spiegelungsatz and more or less known that $\mathcal{H}(k) = \mathcal{N}(k)$ for any CM-field k satisfying (C1), $p \nmid h(k^+)$ and such that k is unramified over $\boldsymbol{Q}(\mu_p)$ at the primes over p.

Example 1./Remark 3. Let $k = \boldsymbol{Q}(\mu_p)$. Then, we see, from Corollary, that $\mathcal{H}_n = \mathcal{N}_n$ for all n if $p \nmid h(\boldsymbol{Q}(\cos(2\pi/p)))$ and $\lambda_\psi \leq p-1$ for each nontrivial even character ψ of Δ. By computations on irregular primes and cyclotomic invariants (Ernvall-Metsänkylä[5], Buhler-Crandall-Sompolski[2]), these assumptions are satisfied for $p < 10^6$. In [15], Taylor deals with the case $n = 0$ without the assumption $p \nmid h(\boldsymbol{Q}(\cos(2\pi/p)))$ and obtains a result which contains ours in this case.

Example 2. Let $p = 3$ and $k = \boldsymbol{Q}(\sqrt{-3}, \sqrt{d})$ with $d \equiv 2 \pmod{3}$. Let ψ be the unique nontrivial even character of Δ. Assume that $\lambda = \lambda_\psi \geq 1$ and $3 \nmid h(k^+)$. Then, by the Iwasawa main conjecture (proved by Mazur-Wiles[14]), we see that the dimension of $\mathcal{H}_n$ over $\boldsymbol{Z}/3\boldsymbol{Z}$ is λ (resp. 3^n) when $3^n \geq \lambda$ (resp. $3^n \leq \lambda$). As an example, we have calculated, using our results, the dimension d_n of $\mathcal{H}_n/\mathcal{N}_n$ over $\boldsymbol{Z}/3\boldsymbol{Z}$ for $\lambda \leq 8$. Write $h_\psi = t^\lambda + \sum_{j=0}^{\lambda-1} 3 \cdot a_j \cdot t^j$ with $a_j \in \boldsymbol{Z}_3$. We always have $d_0 = 0$.

$\lambda \leq 2 \Rightarrow d_n = 0 (n \geq 1)$.

$3 \leq \lambda \leq 6$ and $3 \mid a_0 \Rightarrow d_n = 0 (n \geq 1)$.

$3 \leq \lambda \leq 6$ and $3 \nmid a_0 \Rightarrow d_1 = 1,\ d_n = 0\ (n \geq 2)$.

$\lambda = 7$ and $3 \mid a_0 \Rightarrow d_n = 0 (n \geq 1)$.

$\lambda = 7$ and $3 \nmid a_0 \Rightarrow d_1 = d_2 = 1,\ d_n = 0\ (n \geq 3)$.

$\lambda = 8$ and $3 \mid a_0$, $3 \mid a_1 \Rightarrow d_n = 0\ (n \geq 1)$.

$\lambda = 8$ and $3 \mid a_0$, $3 \nmid a_1 \Rightarrow d_1 = 0,\ d_2 = 1,\ d_n = 0\ (n \geq 3)$.

$\lambda = 8$ and $3 \nmid a_0 \Rightarrow d_1 = 1,\ d_2 = 2,\ d_n = 0\ (n \geq 3)$.

When $\lambda = 7, 8$ and $3 \nmid a_0$, there exists an unramified cyclic extension L/k_1 of degree 3 *without* an RNIB. We see, by using Theorem, that Lk_2/k_2 does have an RNIB for any such L. We have picked up the following values of d from the table of Fukuda[8] on λ-invariants of imaginary quadratic fields, using the computer programs, written by Yamamura, to calculate class numbers of real and imaginary quadratic fields. They satisfy the assumptions $d \equiv 2 (\mathrm{mod.}\ 3)$ and $3 \nmid h(k^+)$.

	$\lambda=1$	$\lambda=2$	$\lambda=3$	$\lambda=4$	$\lambda=5$	$\lambda=6$	$\lambda=7$
$3 \mid a_0$	$d=173$	-1207	878	1541	-10222	-26761	-95569
$3 \nmid a_0$	$d=-31$	62	281	-214	-4006	-5173	14714

Remark 4. The problem we have dealt with is a special case of the following one. For a number field K, a finite set S of prime ideals of K and a finite abelian group G, let H be the group of isomorphism classes of Galois extensions over the S-integer ring of K with group G, and N be the subgroup consisting of classes of those with normal basis. One may ask "What is the group N or H/N?" Basic cases to be considered are (1) $G=\boldsymbol{Z}/p^a\boldsymbol{Z}$ and S is the set of primes over p, and (2) $G=\boldsymbol{Z}/p^a\boldsymbol{Z}$ and S is empty. Though we have a good understanding for the former case (Greither[9], Kersten-Michaliček[13]), we have, so far, few results for the latter case, which include results of Childs and Taylor mentioned previously. We also refer to [1] which studies the action of complex conjugation on N when K is a CM-field or a totally real number field, S is empty and G is any abelian group.

Acknowledgements. The author thanks to N. Suwa for turning his attension to the above problem and for stimulative conversations. He is grateful to T. Fukuda and K. Yamamura, respectively, for permitting him to use the table and the computer programs. He is also grateful to F. Kawamoto for valuable conversations on normal basis.

References

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

[2] J. P. Buhler, R. E. Crandall and R. Sompolski: Irregular primes to one million. Math. Comp., **59**, 712–722 (1992).

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

[4] J. Cougnard: Quelques extensions modérément ramifiées sans base normale. J. London Math. Soc., **31**, 200–204 (1985).

[5] R. Ernvall and T. Metsänkylä: Cyclotomic invariants for primes to one million. Math. Comp., **59**, 249–250 (1992).

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

[7] A. Fröhlich: Galois Module Structure of Algebraic Integers. Springer-Verlag (1983).

[8] T. Fukuda: Iwasawa λ-invariants of imaginary quadratic fields (1992) (unpublished table) (in Japanese).

[9] C. Greither: Cyclic Galois Extensions of Commutative Rings. Lect. Notes in Math., vol. 1534, Springer-Verlag (1992).

[10] H. Ichimura: On a relative normal integral basis problem over cyclotomic fields (1991) (unpublished preprint).

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

[12] K. Iwasawa: Lectures on p-Adic L-Functions. Ann. of Math. Studies, no. 74, Princeton Univ. Press (1972).

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

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

[15] M. J. Taylor: The Galois module structure of certain arithmetic principal homogenous spaces. J. Algebra, **153**, 203–214 (1992).