YOKOHAMA MATHEMATICAL
JOURNAL VOL. 53, 2006

NORMAL INTEGRAL BASES AND RAY CLASS GROUPS, II

By

HUMIO ICHIMURA*

(Received June 15, 2005)

Abstract. Let p be an odd prime number, F a number field, and $K = F(\zeta_p)$. We say that F satisfies the condition (A_p) when any tame cyclic extension N/F of degree p has a normal integral basis (NIB for short), and that it satisfies (B_p) when for any $a \in F^\times$, the cyclic extension $K(a^{1/p})/K$ has a NIB if it is tame. We prove that F satisfies (A_p) only when it satisfies (B_p) under the assumption that the Stickelberger ideal associated to the Galois group $\mathrm{Gal}(K/F)$ is "trivial".

1. Introduction

Let p be an odd prime number, F a number field, and $K = F(\zeta_p)$. Here, ζ_p is a fixed primitive p-th root of unity. We say that F satisfies the condition (A_p) when any tame cyclic extension N/F of degree p has a normal integral basis (NIB for short), and that it satisfies (B_p) when for any $a \in F^\times$, the cyclic extension $K(a^{1/p})/K$ has a NIB if it is tame. It is known that the rationals $\boldsymbol{Q}$ satisfy (A_p) for all p by Hilbert and Speiser, and that $F \neq \boldsymbol{Q}$ does not satisfy (A_p) for infinitely many p by Greither *et al* [5]. Corresponding results for (B_p) were obtained by Kawamoto [12, 13] and the author [7, IV], respectively. When $\zeta_p \in F^\times$, the conditions (A_p) and (B_p) are clearly equivalent. When $\zeta_p \notin F^\times$, the conditions appear, superficially, to be irrelevant to each other. However, in [8, Theorem 2], we proved the following relation between the two conditions.

THEOREM 1. *Let p be an odd prime number, F a number field, and $K = F(\zeta_p)$. Assume that $[K : F] = 2$ and that K/F is totally ramified at least for one prime divisor of F. Then, F satisfies the condition (A_p) only when it satisfies (B_p).*

The purpose of this paper is to relax the assumption $[K : F] = 2$ and generalise the assertion. Let us introduce some notation. The Galois group $\Delta = \mathrm{Gal}(K/F)$ is naturally identified with a subgroup $H = H_F$ of the multi-

*The author was partially supported by Grant-in-Aid for Scientific Research (C) (No.16540033), the Ministry of Education, Culture, Sports, Science and Technology of Japan.
2000 Mathematics Subject Classification: 11R33
Key words and phrases: normal integral basis, ray class group

plicative group $(\boldsymbol{Z}/p)^\times = (\boldsymbol{Z}/p\boldsymbol{Z})^\times$ through the Galois action on ζ_p. For each subgroup H of $(\boldsymbol{Z}/p)^\times$, we defined in [10] a Stickelberger ideal $\mathcal{S}_H$ of the group ring $\boldsymbol{Z}[H]$. When $H = (\boldsymbol{Z}/p)^\times$, it coincides with the classical one given in Washington's textbook [16, Chap. 6]. There are several cases where $\mathcal{S}_H = \boldsymbol{Z}[H]$ (see Lemma 1 in Section 2). For instance, $\mathcal{S}_H = \boldsymbol{Z}[H]$ when $|H| \leq 3$. The following is a generalization of Theorem 1.

THEOREM 2. *Let p, F, K be as in Theorem 1. Let $H = H_F$ be the subgroup of $(\boldsymbol{Z}/p)^\times$ corresponding to $\Delta = \mathrm{Gal}(K/F)$. Assume that $\mathcal{S}_H = \boldsymbol{Z}[H]$. Then, F satisfies the condition (A_p) only when it satisfies (B_p).*

REMARK 1. (1) As we have seen in [8, Remark 3], the condition (A_p) is stronger than (B_p) in general. (2) A p-integer version of Theorem 2 is given in [10, Corollary 4].

After Hilbert [6, Theorem 136] gave his alternative proof of the classical Stickelberger theorem for the ideal class group of the p-cyclotomic field $\boldsymbol{Q}(\zeta_p)$, several authors, in particular McCulloh [14, 15], pursued a relation between Stickelberger ideals and Galois module structure of rings of integers. (For details, see Fröhlich [3, Chapter IV].) We prove Theorem 2 using the main theorem of [15].

2. Stickelberger ideals of conductor p

Let p be an odd prime number, $C = (\boldsymbol{Z}/p)^\times$, and H a subgroup of C. For an integer i, $\bar{i} \in \boldsymbol{Z}/p\boldsymbol{Z}$ denotes the class containing i. We often write an element $\bar{i}$ of C as δ_i. For a real number x, $[x]$ denotes the largest integer $\leq x$. For an integer $r \in \boldsymbol{Z}$, let

$$\theta_r = \theta_{r,H} = \sum_i{}' \left[\frac{ri}{p}\right] \delta_i^{-1} \in \boldsymbol{Z}[H],$$

where in the sum $\sum_i'$, i runs over the integers with $1 \leq i \leq p-1$ and $\bar{i} \in H$. Let $\mathcal{S}_H$ be the submodule of $\boldsymbol{Z}[H]$ generated by θ_r for all r over $\boldsymbol{Z}$:

$$\mathcal{S}_H = \langle \theta_r \mid r \in \boldsymbol{Z} \rangle_{\boldsymbol{Z}}.$$

This is an ideal of $\boldsymbol{Z}[H]$ as $\delta_s\theta_r = \theta_{sr} - r\theta_s$ for $\bar{s} \in H$ (cf. [10, Section 2]). When $H = C$, the ideal $\mathcal{S}_C$ coincides with the classical Stickelberger ideal for the p-cyclotomic field and the one used by McCulloh in [14]. The following assertion was shown in [10, 11].

LEMMA 1. (1) *When* $|H| \leq 3$, $\mathcal{S}_H = \boldsymbol{Z}[H]$ *for any* p. *When* $|H| \geq 4$ *is even,* $\mathcal{S}_H \subsetneqq \boldsymbol{Z}[H]$ *for any* p.

(2) *Let* p *be an odd prime number with* $p \leq 499$, *and* H *a nontrivial subgroup of* $(\boldsymbol{Z}/p)^\times$ *such that* $|H|$ *is odd and* $(p-1)/|H| > 2$. *Then, we have* $\mathcal{S}_H = \boldsymbol{Z}[H]$ *except for the case where* $(p, (p-1)/|H|) = (277, 4)$, $(331, 10)$, $(349, 4)$ *or* $(397, 4)$

(3) *Let* $\ell \geq 5$ *be an odd prime number, and* $g \geq 2$ *an integer. Assume that* $p = (g^\ell - 1)/(g-1)$ *is a prime number, and let* H *be the subgroup of* $(\boldsymbol{Z}/p)^\times$ *of order* ℓ *generated by the class* $\bar{g}$. *Then,* $\mathcal{S}_H = \boldsymbol{Z}[H]$.

For an integer $x \in \boldsymbol{Z}$, let $(x)_p$ be the unique integer with $(x)_p \equiv x \bmod p$ and $0 \leq (x)_p < p$. Clearly, we have

$$x = [x/p]p + (x)_p. \tag{1}$$

We see that

$$\left[\frac{xy(z)_p}{p}\right] = \left[\frac{x(yz)_p}{p}\right] + x\left[\frac{y(z)_p}{p}\right] \tag{2}$$

for $x, y, z \in \boldsymbol{Z}$ applying the formula (1) for the integer $y(z)_p$. Let H be a subgroup of C, and let $d = |H|$, $t = [C : H]$. Let g be a primitive root modulo p, and $\rho = \delta_g \in C$. Then, $C = \langle \rho \rangle$ and $H = \langle \rho^t \rangle$. Using (2), we see that

$$\begin{aligned}
\theta_{r,C} &= \sum_{\lambda=0}^{t-1} \rho^{-\lambda} \sum_{i=0}^{d-1} \left[\frac{r(g^{ti+\lambda})_p}{p}\right] \rho^{-ti} \\
&= \sum_{\lambda=0}^{t-1} \rho^{-\lambda} \sum_{i=0}^{d-1} \left\{\left[\frac{rg^\lambda(g^{ti})_p}{p}\right] - r\left[\frac{g^\lambda(g^{ti})_p}{p}\right]\right\} \rho^{-ti} \\
&= \theta_{r,H} + \sum_{\lambda=1}^{t-1} \rho^{-\lambda} \left(\theta_{rg^\lambda,H} - r\theta_{g^\lambda,H}\right) \\
&= \theta_{r,H} + \sum_{\lambda=1}^{t-1} \rho^\lambda s_\lambda \quad \text{for some } s_\lambda \in \mathcal{S}_H.
\end{aligned} \tag{3}$$

This formula is used in the proof of Theorem 2.

3. Proof of Theorem 2

First, let us recall the theorem of McCulloh [15] mentioned in Section 1. Let F be a number field, and G the additive group $(\boldsymbol{Z}/p)^+$. Let $Cl_F = Cl(\mathcal{O}_F)$ be

the ideal class group of $\mathcal{O}_F$, and let $Cl(\mathcal{O}_F G)$ and $R(\mathcal{O}_F G)$ be the locally free class group of the group ring $\mathcal{O}_F G$ and the subset of classes realised by rings of integers of tame G-extensions over F, respectively. Let $Cl^0(\mathcal{O}_F G)$ be the kernel of the homomorphism $Cl(\mathcal{O}_F G) \to Cl_F$ induced from the augmentation map $\mathcal{O}_F G \to \mathcal{O}_F$. The group $C = (\boldsymbol{Z}/p)^\times$ acts on G by multiplication:

$$\sigma^{\delta_i} = \bar{i} \cdot \sigma \quad \text{for } \delta_i \in C,\ \sigma \in G. \tag{4}$$

Via this action, the group ring $\boldsymbol{Z}[C]$ and the Stickelberger ideal $\mathcal{S}_C$ naturally act on $Cl(\mathcal{O}_F G)$ and $Cl^0(\mathcal{O}_F G)$.

THEOREM 3 (McCulloh). *Under the above setting, we have*

$$R(\mathcal{O}_F G) = Cl^0(\mathcal{O}_F G)^{\mathcal{S}_C}.$$

We derive the following assertion from this. For an integer $a \in \mathcal{O}_K$, let $Cl_K(a)$ be the ray class group of K defined modulo the ideal $a\mathcal{O}_K$. Put $\pi = \zeta_p - 1$.

LEMMA 2. *Let F be a number field, $K = F(\zeta_p)$, and $H = \mathrm{Gal}(K/F) \leq C$. If F satisfies the condition (A_p), then $Cl_K(\pi)^{\mathcal{S}_H} = \{0\}$.*

Before showing this, we recall some facts on class groups. Let $\mathcal{O}'_F = \mathcal{O}_F[1/p]$, and $\mathcal{O}_{F,p}$ be the elements of F integral at the primes over p. Clearly, we have $\mathcal{O}_F = \mathcal{O}'_F \cap \mathcal{O}_{F,p}$. Let $I(\mathcal{O}'_F)$ be the group of fractional ideals of $\mathcal{O}'_F$, and P_F the subgroup consisting of principal ideals $\alpha\mathcal{O}'_F$ for units $\alpha \in \mathcal{O}^\times_{F,p}$. The following canonical isomorphism is well known.

$$Cl_F \cong I(\mathcal{O}'_F)/P_F. \tag{5}$$

Let $I(\mathcal{O}'_F G)$ be the group of fractional $\mathcal{O}'_F G$-ideals in FG, and $P_{F,G}$ the subgroup consisting of principal ideals $\alpha\mathcal{O}'_F G$ for units $\alpha \in (\mathcal{O}_{F,p}G)^\times$. Via (4), the group ring $\boldsymbol{Z}[C]$ naturally acts on $I(\mathcal{O}'_F G)$ and the quotient $I(\mathcal{O}'_F G)/P_{F,G}$. Similarly to (5), we have the following natural isomorphism compatible with the $\boldsymbol{Z}[C]$-action (see Fröhlich [2, X] or [15, p. 113]).

$$Cl(\mathcal{O}_F G) \cong I(\mathcal{O}'_F G)/P_{F,G}. \tag{6}$$

Proof of Lemma 2. Let χ_0 be the trivial character of G, and χ a fixed nontrivial character of G with values in μ_p. Let $\rho = \delta_g$ be a generator of C where g is a primitive root modulo p. Let $t = [C : H]$. Then, ρ^t is a generator of $H = \mathrm{Gal}(K/F)$ sending ζ_p to $\zeta_p^{g^t}$. For an element $\alpha = \sum_\sigma a_\sigma \sigma$ of FG and a μ_p-valued character ψ of G, let

$$\psi(\alpha) = \sum_\sigma a_\sigma \psi(\sigma).$$

Here, σ runs over G. We have a natural isomorphism of $\mathcal{O}'_F$-algebras

$$\varphi : \mathcal{O}'_F G \to \mathcal{O}'_F \oplus \mathcal{O}'_K \oplus \mathcal{O}'_K \oplus \cdots \oplus \mathcal{O}'_K$$

with

$$\varphi(\alpha) = (\chi_0(\alpha), \chi(\alpha), \chi^g(\alpha), \cdots, \chi^{g^{t-1}}(\alpha)).$$

We easily see that

$$\varphi(\alpha^{\rho^\lambda}) = (\chi_0(\alpha), \chi^{g^\lambda}(\alpha), *\cdots, *) \quad \text{for } 0 \le \lambda \le t-1 \tag{7}$$

and

$$\varphi(\alpha^\delta) = (\chi_0(\alpha), \chi(\alpha)^\delta, \chi^g(\alpha)^\delta, \cdots, \chi^{g^{t-1}}(\alpha)^\delta) \quad \text{for } \delta \in H = \langle \rho^t \rangle. \tag{8}$$

Here, $\chi^{g^\lambda}(\alpha)^\delta$ denotes the Galois action of $\delta \in H$ on $\chi^{g^\lambda}(\alpha) \in K$.

Now, assume that F satisfies (A_p) or equivalently that $R(\mathcal{O}_F G) = \{0\}$. Let $\mathfrak{A}$ be an ideal of $\mathcal{O}'_K$, and A the ideal of $\mathcal{O}'_F G$ with

$$\varphi(A) = \mathcal{O}'_F \oplus \mathfrak{A} \oplus \mathcal{O}'_K \oplus \cdots \oplus \mathcal{O}'_K.$$

Let $r \in \boldsymbol{Z}$ be an arbitrary integer. By Theorem 3 and (6), we have

$$A^{\theta_{r,C}} = \alpha \mathcal{O}'_F G$$

for some unit $\alpha \in (\mathcal{O}_{F,p} G)^\times$. We see from (3), (7) and (8) that

$$\varphi(A^{\theta_{r,C}}) = \mathcal{O}'_F \oplus \mathfrak{A}^{\theta_{r,H}} \oplus \cdots.$$

Therefore, it follows that

$$\mathcal{O}'_F = \chi_0(\alpha)\mathcal{O}'_F \quad \text{and} \quad \mathfrak{A}^{\theta_{r,H}} = \chi(\alpha)\mathcal{O}'_K.$$

We see that

$$\chi_0(\alpha) \in \mathcal{O}'^\times_F \cap \mathcal{O}^\times_{F,p} = \mathcal{O}^\times_F \quad \text{and} \quad \chi(\alpha) \equiv \chi_0(\alpha) \bmod \pi.$$

This implies that $\theta_{r,H}$ kills the class group $Cl_K(\pi)$. □

The following theorem was proved by Greither *et al* [5, Corollary]. Let $[\mathcal{O}^\times_F]_p$ be the subgroup of the multiplicative group $(\mathcal{O}_F/p)^\times$ consisting of classes containing units of $\mathcal{O}_F$.

THEOREM 4 (Greither *et al.*). *If a number field F satisfies the condition (A_p), then the exponent of the quotient $(\mathcal{O}_F/p)^\times/[\mathcal{O}^\times_F]_p$ divides $(p-1)^2/2$.*

Using Lemma 2 and Theorem 4, we can show the following:

THEOREM 5. *Let F be a number field, $K = F(\zeta_p)$, and $H = \mathrm{Gal}(K/F) \leq C$. If F satisfies the condition (A_p), then we have*

$$Cl_K(\pi)^{S_H} = \{0\} \quad \text{and} \quad Cl_K(p)^H \cap Cl_K(p)^{S_H} = \{0\}.$$

Here, $Cl_K(p)^H$ denotes the Galois invariant part.

Proof. It suffices to show that

$$\mathcal{X} := Cl_K(p)^H \cap Cl_K(p)^{S_H} = \{0\}.$$

As $Cl_K(\pi)^{S_H} = \{0\}$, we see that $Cl_K(\pi^p)^{S_H}$ and hence $\mathcal{X}$ are p-abelian groups. For an integer $a \in \mathcal{O}_K$ and an ideal $\mathfrak{A}$ of $\mathcal{O}_K$ relatively prime to a, let $[\mathfrak{A}]_a$ be the ray class in $Cl_K(a)$ represented by $\mathfrak{A}$. Let c be a ray class in $\mathcal{X}$. As $Cl_K(\pi)^{S_H} = \{0\}$, we see that $c = [\mathfrak{P}]_p$ for some prime ideal $\mathfrak{P}$ of K with $[\mathfrak{P}]_\pi = 1$. Hence, $\mathfrak{P} = \alpha\mathcal{O}_K$ for some integer α. As $c \in Cl_K(p)^H$, we have for each $\delta \in H$, $\alpha^\delta \equiv \epsilon_\delta \alpha \bmod p$ with some unit $\epsilon_\delta \in \mathcal{O}_K^\times$. Therefore, $N_{K/F}\alpha \equiv \epsilon\alpha^d \bmod p$ for some $\epsilon \in \mathcal{O}_K^\times$, where $d = [K : F]$. On the other hand, $(N_{K/F}\alpha)^{(p-1)^2/2}$ is congruent to a unit of K modulo p by Theorem 4. Therefore, we see that the order of $c = [\mathfrak{P}]_p = [\alpha\mathcal{O}_K]_p$ divides $d(p-1)^2/2$. Hence, we obtain $c = 1$ as $\mathcal{X}$ is a p-abelian group. □

As for the condition (B_p), the following assertion holds.

THEOREM 6. *Under the setting of Theorem 5, assume that the natural map $Cl_F(p) \to Cl_K(p)$ is trivial. Then, F satisfies the condition (B_p).*

Proof. A slightly weaker version of Theorem 6 is given in [9, Proposition 1]. Theorem 6 is proved exactly similarly. □

Proof of Theorem 2. Assume that $S_H = \boldsymbol{Z}[H]$ and that F satisfies (A_p). Then, $Cl_K(p)^H$ is trivial by Theorem 5. Hence, F satisfies (B_p) by Theorem 6. □

REMARK 2. The converse of Theorem 5 holds in some cases. (1) When $\zeta_p \in F^\times$, it is shown in [7, V, Proposition 1, 2] that F satisfies (A_p) if and only if $Cl_K(p) = \{0\}$. (2) Let $p = 3$ and $\zeta_3 \notin F^\times$. In this case, we have $S_H = \boldsymbol{Z}[H]$ by Lemma 1. It is shown in [8, Theorem 3] that F satisfies (A_3) if and only if $Cl_K(\pi) = \{0\}$ and $Cl_K(3)^H = \{0\}$. Using this, all quadratic fields satisfying (A_3) were determined ([8, Proposition 1]). Such quadratic fields were determined also by Carter [1] with a different method.

REMARK 3. Gómez Ayala [4, Theorem 2.1] gave a very explicit criterion for a Kummer extension of prime degree to have a NIB in terms of a Kummer generator. It is possible to show Lemma 2 directly from this criterion without using McCulloh's theorem. Actually, in the first version of this paper, the author showed Lemma 2 in this way.

References

[1] J.E. Carter, Normal integral bases in quadratic and cyclic cubic extensions over quadratic fields, *Arch. Math.*, **81** (2003), 266–271; Erratum, *ibid.*, **83** (2004), vol.6, vi–vii.

[2] A. Fröhlich, Locally free modules over arithmetic orders, *J. Reine Angew. Math.*, **274/275** (1975), 112–138.

[3] A. Fröhlich, Galois Module Structure of Algebraic Integers, Springer, Berlin-Heidelberg-New York, 1983.

[4] E.J. Gómez Ayala, Bases normales d'entiers dans les extensions Kummer de degré premier, *J. Théor. Nombres Bordeaux*, **6** (1994), 95–116.

[5] C. Greither, D. Replogle, K. Rubin and A. Srivastav, Swan modules and Hilbert-Speiser number fields, *J. Number Theory*, **79** (1999), 164–173.

[6] D. Hilbert, The Theory of Algebraic Number Fields, Springer, Berlin-Heidelberg-New York, 1998.

[7] H. Ichimura, Note on the ring of integers of a Kummer extension of prime degree, IV, *Proc. Japan Acad.*, **77A** (2001), 92–94; V, *ibid.*, **78A** (2002), 76–79.

[8] H. Ichimura, Normal integral bases and ray class groups, Acta Arith., **114** (2004), 71-85.

[9] H. Ichimura, On a theorem of Kawamoto on normal bases of rings of integers, *Tokyo J. Math.*, **27** (2004), 527–540.

[10] H. Ichimura, Stickelberger ideals and normal bases of rings of p-integers, *Math. J. Okayama Univ.*, in press.

[11] H. Ichimura and H. Sumida-Takahashi, Stickelberger ideals of conductor p and their application, *J. Math. Soc. Japan*, **58** (2006), 885–902.

[12] F. Kawamoto, On normal integral bases, *Tokyo J. Math.*, **7** (1984), 221–231.

[13] F. Kawamoto, Remark on "On normal integral bases", *Tokyo. J. Math.*, **8** (1985), 275.

[14] L.R. McCulloh, A Stickelberger condition on Galois module structure for Kummer extensions of prime degree, Algebraic Number Fields (Durham Symposium, 1975, ed. A. Fröhlich), 561–588, Academic Press, London, 1977.

[15] L.R. McCulloh, Galois module structure of elementary abelian extensions, *J. Algebra*, **82** (1983), 102–134.

[16] L.C. Washington, Introduction to Cyclotomic Fields (2nd ed.), Springer, Berlin-Heidelberg-New York, 1996.

Faculty of Science,
Ibaraki University
Bunkyo 2-1-1, Mito, Ibaraki, 310-8512,
Japan
E-mail: `hichimur@mx.ibaraki.ac.jp`