Note on Galois descent of a normal integral basis of a cyclic extension of degree p

By Humio Ichimura

Department of Mathematical Sciences, Faculty of Science, Ibaraki University,
Bunkyo 2-1-1, Mito, Ibaraki 310-8512, Japan

(Communicated by Heisuke Hironaka, M.J.A., Nov. 12, 2009)

Abstract: Let p be an odd prime number, and F a number field. We show that when $F/\boldsymbol{Q}$ is unramified at p, any tame cyclic extension N/F of degree p has a normal integral basis if the pushed up extension $N(\zeta_p)/F(\zeta_p)$ has a normal integral basis.

Key words: Normal integral basis; locally free class group.

1. Introduction. Let p be a *fixed* odd prime number. Let Γ be a cyclic group of order p. Let F be a number field, and $K = F(\zeta_p)$ where ζ_p is a primitive p-th root of unity. Gómez Ayala [4, Theorem 2.1] gave a very explicit criterion for a tame Γ-extension over K to have a normal integral basis (NIB for short) in terms of a Kummer generator. Thus, it is natural to ask "does a tame Γ-extension N/F has a NIB if NK/K has a NIB?". Greither [6, Theorem 2.2] gave an affirmative answer to the question when $p = 3$ and $F/\boldsymbol{Q}$ is unramified at 3. The author [10, Theorem 4] removed the assumption that $F/\boldsymbol{Q}$ is unramified at 3. Further, it has an affirmative answer for any p and F when N/F is unramified at all finite primes (Brinkhuis [3], the author [8, 9]). The main purpose of this note is to generalize Greither's result as follows:

Theorem 1. *Let p be an odd prime number, and let F be a number field and $K = F(\zeta_p)$. Assume that $F/\boldsymbol{Q}$ is unramified at p. Then any tame Γ-extension N/F has a NIB if and only if NK/K has a NIB.*

Let F be a number field, $\mathcal{O}_F$ the ring of integers, Cl_F the ideal class group of the Dedekind domain $\mathcal{O}_F$, and $h_F = |Cl_F|$ the class number of F. Let $Cl(\mathcal{O}_F\Gamma)$ be the locally free class group of the group ring $\mathcal{O}_F\Gamma$, and let $Cl^0(\mathcal{O}_F\Gamma)$ be the kernel of the homomorphism $Cl(\mathcal{O}_F\Gamma) \to Cl_F$ induced by the augmentation $\mathcal{O}_F\Gamma \to \mathcal{O}_F$. For a tame Γ-extension N/F, the integer ring $\mathcal{O}_N$ is locally free over $\mathcal{O}_F\Gamma$, and hence it determines a class $[\mathcal{O}_N]$ in $Cl(\mathcal{O}_F\Gamma)$. The class $[\mathcal{O}_N]$ is trivial if and only if the extension N/F has a NIB as Γ is an abelian group. It is known that $[\mathcal{O}_N] \in Cl^0(\mathcal{O}_F\Gamma)$. Hence, Theorem 1 is an immediate consequence of the following

Theorem 2. *Under the setting and the assumption of Theorem* 1*, the natural map*

$$Cl^0(\mathcal{O}_F\Gamma) \to Cl^0(\mathcal{O}_K\Gamma)$$

induced by the scalar extension is injective.

Remarks 1. (I) In general, the locally free class group $Cl^0(\mathcal{O}_F\Gamma)$ is a very complicated object. However, when $F/\boldsymbol{Q}$ is unramified at p, it is shown by Brinkhuis [2, Proposition 2.1] that it is isomorphic to the ray class group $Cl_{K,\pi}$ of $K = F(\zeta_p)$ defined modulo $\pi = \zeta_p - 1$. But, we do not need this fact for proving Theorem 2.

(II) Let L/F be a finite extension of a number field F, and G an arbitrary finite group. Recently, Greither and Johnston [7, Corollary 5.2] showed that the natural map $Cl(\mathcal{O}_FG) \to Cl(\mathcal{O}_LG)$ is injective if $([L : F], |Cl(\mathcal{O}_FG)|) = 1$ and $\mathcal{O}_L$ is free over $\mathcal{O}_F$. Theorem 2 is not contained in this general result. Actually, let F be a number field such that $F/\boldsymbol{Q}$ is unramified at p and $h_F = 1$. Then we have $Cl(\mathcal{O}_F\Gamma) = Cl^0(\mathcal{O}_F\Gamma) \cong Cl_{K,\pi}$. If further $(p-1, h_K) \neq 1$, then the triple (F, K, Γ) does not satisfy the first assumption of [7, Corollary 5.2], while the natural map $Cl(\mathcal{O}_F\Gamma) \to Cl(\mathcal{O}_K\Gamma)$ is injective by Theorem 2. For example, the above conditions on F (and K) are satisfied when $p = 3$ and $F = \boldsymbol{Q}(\sqrt{7})$. (We have $h_K = 2$ in this case.)

(III) Let $R(\mathcal{O}_F\Gamma)$ be the subset of $Cl^0(\mathcal{O}_F\Gamma)$ consisting of the locally free classes $[\mathcal{O}_N]$ for all tame Γ-extensions N/F. In [12], McCulloh characterized the realizable classes $R(\mathcal{O}_F\Gamma)$ in terms of a "Stickelberger ideal" acting on $Cl(\mathcal{O}_F\Gamma)$, from which it fol-

2000 Mathematics Subject Classification. 11R33.

doi: 10.3792/pjaa.85.160

lows that the main part of $R(\mathcal{O}_F\Gamma)$ is contained in the "minus" part of $Cl^0(\mathcal{O}_F\Gamma)$. Therefore, Theorem 2 is an assertion much stronger than Theorem 1, and if one obtains some nice results on the minus part, then it might be possible to obtain a better result on the Galois descent problem.

(IV) Let p be a prime number. We say that a Galois extension N/F has a p-NIB when it has a normal basis with respect to the p-integers $\mathcal{O}'_F = \mathcal{O}_F[1/p]$. One can consider an analogous Galois descent problem; Does a cyclic extension N/F of degree p^n has a p-NIB if the extension $N(\zeta_{p^n})/F(\zeta_{p^n})$ has a p-NIB? Here, ζ_{p^n} is a primitive p^n-th root of unity. When N/F is unramified outside p, a quite general affirmative answer is given in Greither [5, Theorem I.2.1]. However, for the ramified case, the matters are complicated. Such a Galois descent property holds when p does not divide the degree $[F(\zeta_{p^n}) : F]$, but does not hold in general when p divides the degree [11, Theorems 1, 2].

2. A description of locally free class group. In this section, we recall a description of the locally free class group following a convenient exposition in [12, pp. 112–113].

Let p be a *fixed* prime number and F a number field. Let $\mathcal{O}'_F = \mathcal{O}_F[1/p]$ be the ring of p-integers of F, and $\mathcal{O}_{F,p}$ the elements of F integral at the primes over p. Clearly, we have

$$\mathcal{O}_F = \mathcal{O}'_F \cap \mathcal{O}_{F,p}. \tag{1}$$

Let $I(\mathcal{O}'_F\Gamma)$ be the group of fractional $\mathcal{O}'_F\Gamma$-ideals in $F\Gamma$, and let $P(\mathcal{O}'_F\Gamma)$ be the subgroup consisting of principal ideals $\alpha\mathcal{O}'_F\Gamma$ for units $\alpha \in (\mathcal{O}_{F,p}\Gamma)^\times$ ($\subseteq F\Gamma$). Here, for a ring R containing a unity, $R^\times$ denotes the group of invertible elements of R. We have a canonical isomorphism

$$Cl(\mathcal{O}_F\Gamma) \cong I(\mathcal{O}'_F\Gamma)/P(\mathcal{O}'_F\Gamma). \tag{2}$$

Let $K = F(\zeta_p)$. Let χ be a fixed nontrivial K-valued character of Γ, and χ_0 the trivial character of Γ. Let

$$t = t_F = (p-1)/[K : F].$$

Let g be a primitive root modulo p. Then we see that $\chi, \chi^g, \cdots, \chi^{g^{t-1}}$ form a complete set of representatives of the F-equivalent classes of nontrivial K-valued characters of Γ. As usual, we extend a character of Γ to a homomorphism from $F\Gamma$ to K by linearity. We have a Wedderburn decomposition

$$\varphi = \varphi_F : F\Gamma \xrightarrow{\sim} F \oplus K \oplus K \oplus \cdots \oplus K$$

with

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

We easily see that

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

A fractional $\mathcal{O}'_F\Gamma$-ideal in $F\Gamma$ corresponds via φ to a direct product of fractional ideals of the components. Let $I^0(\mathcal{O}'_F\Gamma)$ be the subgroup of $I(\mathcal{O}'_F\Gamma)$ consisting of fractional ideals $A \in I(\mathcal{O}'_F\Gamma)$ for which the first component of $\varphi(A)$ equals the trivial ideal $\mathcal{O}'_F$. Let $P^0(\mathcal{O}'_F\Gamma)$ be the subgroup of $I^0(\mathcal{O}'_F\Gamma)$ consisting of principal ideals $\alpha\mathcal{O}'_F\Gamma$ for units $\alpha \in (\mathcal{O}_{F,p}\Gamma)^\times$ such that $\chi_0(\alpha) = 1$. We easily see that

$$P^0(\mathcal{O}'_F\Gamma) = P(\mathcal{O}'_F\Gamma) \cap I^0(\mathcal{O}'_F\Gamma)$$

using (1). Therefore, the isomorphism (2) induces an isomorphism

$$Cl^0(\mathcal{O}_F\Gamma) \cong I^0(\mathcal{O}'_F\Gamma)/P^0(\mathcal{O}'_F\Gamma).$$

3. Proof of Theorem 2. Let p be an odd prime number. We fix a primitive p-th root $\zeta = \zeta_p$ of unity, and put $\pi = \zeta - 1$. Let F be a number field, and $K = F(\zeta)$. Throughout this section, we assume that $[K : F] = p - 1$. Then we have $t_F = 1$ and $t_K = p - 1$. Let χ be a nontrivial K-valued character of Γ, and χ_0 the trivial character of Γ. As $t_F = 1$, all nontrivial characters of Γ are conjugate to χ over F.

Lemma 1. *For $x \in \mathcal{O}_{F,p}^\times$ and $y \in \mathcal{O}_{F,p}[\zeta]^\times$, there exists a unit $\alpha \in (\mathcal{O}_{F,p}\Gamma)^\times$ such that $\chi_0(\alpha) = x$ and $\chi(\alpha) = y$ if and only if $x \equiv y \bmod \pi$.*

Proof. For simplicity, write $\Lambda = \mathcal{O}_{F,p}\Gamma$. Let γ be a generator of Γ. The trivial character χ_0 induces an isomorphism $\Lambda/(\gamma - 1) \cong \mathcal{O}_{F,p}$, and χ induces an isomorphism $\Lambda/(\varphi_p(\gamma)) \cong \mathcal{O}_{F,p}[\zeta]$ as $[K : F] = p - 1$. Here, φ_p is the p-th cyclotomic polynomial. We easily see that $(\gamma - 1) \cap (\varphi_p(\gamma)) = \{0\}$. Hence, we obtain a Milnor square:

$$\begin{array}{ccc} \Lambda & \xrightarrow{\chi_0} & \mathcal{O}_{F,p} \\ {\scriptstyle\chi}\downarrow & & \downarrow{\scriptstyle j_1} \\ \mathcal{O}_{F,p}[\zeta] & \xrightarrow{j_2} & S, \end{array}$$

where $S = \Lambda/(\gamma - 1, \varphi_p(\gamma)) = \mathcal{O}_{F,p}/p$ and the map j_1 (resp. j_2) is the reduction modulo p (resp. π). Here, we are identifying the quotient ring $\mathcal{O}_{F,p}[\zeta]/\pi$ with S by the map

$$\sum_i a_i\zeta^i \bmod \pi \to \sum_i a_i \bmod p$$

with $a_i \in \mathcal{O}_{F,p}$. It is known that this diagram yields the exact sequence:

$$\Lambda^\times \xrightarrow{f} X = \mathcal{O}_{F,p}^\times \times \mathcal{O}_{F,p}[\zeta]^\times \xrightarrow{g} S^\times,$$

where the map f sends $\alpha \in \Lambda^\times$ to $(\chi_0(\alpha), \chi(\alpha))$ and g sends $(x, y) \in X$ to $xy^{-1} \bmod \pi$. For these, see Theorem 5.3 and Example (5.5) in Bass [1, Chapter 9]. The assertion follows from the above exact sequence. □

For a number field F, we put

$$X_{F,p} = \{x \in \mathcal{O}_{K,p} \mid x \equiv 1 \bmod \pi\}$$

with $K = F(\zeta)$. When $F/\boldsymbol{Q}$ is unramified at p, we have $[K : F] = p - 1$ and $\mathcal{O}_{K,p} = \mathcal{O}_{F,p}[\zeta]$. Therefore, Theorem 2 is an immediate consequence of the following

Theorem 3. *Let F be a number field and $K = F(\zeta)$. Assume that $[K : F] = p - 1$ and $X_{F,p} \subseteq \mathcal{O}_{F,p}[\zeta]$. Then the natural map*

$$Cl^0(\mathcal{O}_F\Gamma) \to Cl^0(\mathcal{O}_K\Gamma)$$

is injective.

Proof of Theorem 3. Let A be an arbitrary element of $I^0(\mathcal{O}'_F\Gamma)$, and let $\bar{A} = A \cdot \mathcal{O}'_K\Gamma \in I^0(\mathcal{O}'_K\Gamma)$. Let ρ be the generator of the Galois group $\mathrm{Gal}(K/F)$ sending ζ to ζ^g, where g is the primitive root modulo p in Section 2. By the Wedderburn decomposition, we have

$$\varphi_F(A) = \mathcal{O}'_F \oplus \mathfrak{A}$$

and

$$\varphi_K(\bar{A}) = \mathcal{O}'_K \oplus \mathfrak{A} \oplus \mathfrak{A}^\rho \oplus \cdots \oplus \mathfrak{A}^{\rho^{p-2}}$$

as $t_F = 1$ and $t_K = p - 1$. Here, $\mathfrak{A}$ is a fractional ideal of $\mathcal{O}'_K$. Assume that the class $[\bar{A}]_K$ in $Cl^0(\mathcal{O}_K\Gamma) = I^0(\mathcal{O}'_K\Gamma)/P^0(\mathcal{O}'_K\Gamma)$ is trivial. Then there exists a unit $\beta \in (\mathcal{O}_{K,p}\Gamma)^\times$ $(\subseteq K\Gamma)$ such that $\chi_0(\beta) = 1$ and $\bar{A} = \beta\mathcal{O}'_K\Gamma$. In particular, $\chi(\beta)\mathcal{O}'_K = \mathfrak{A}$. Clearly, $\chi(\gamma) \equiv 1 \bmod \pi$ where γ is, as before, a generator of Γ. It follows that $1 = \chi_0(\beta) \equiv \chi(\beta) \bmod \pi$, and hence $\chi(\beta) \in \mathcal{O}_{F,p}[\zeta]$ by the assumption $X_{F,p} \subseteq \mathcal{O}_{F,p}[\zeta]$. Therefore, we see from Lemma 1 that there exists a unit $\alpha \in (\mathcal{O}_{F,p}\Gamma)^\times$ such that $\chi_0(\alpha) = 1$ and $\chi(\alpha) = \chi(\beta)$. Hence, we obtain $A = \alpha\mathcal{O}'_F\Gamma$. □

Remarks 2. (I) Let $p = 3$ and F a number field with $\zeta_3 \notin F$. Then we can easily show that the second condition $X_{F,p} \subseteq \mathcal{O}_{F,p}[\zeta]$ in Theorem 3 is satisfied. Therefore, by Theorem 3, we obtain an alternative proof of [10, Theorem 4] mentioned in Section 1. However, when $p \geq 5$ and $F/\boldsymbol{Q}$ is ramified at p, the condition seems to be quite a hard one.

(II) When $[K : F] < p - 1$ or $X_{F,p} \notin \mathcal{O}_{F,p}[\zeta]$, the author has no idea, at present, as to whether or not the injectivity in Theorem 3 holds.

Acknowledgments. The author is grateful to the referee for valuable suggestions and comments. The proof of Lemma 1 in the former version was elementary but rather complicated. The present simple proof was suggested by the referee. The author was partially supported by Grant-in-Aid for Scientific Research (C), No. 19540005, Japan Society for the Promotion of Science.

References

[1] H. Bass, *Algebraic K-theory*, W. A. Benjamin, Inc., New York, 1968.
[2] J. Brinkhuis, Normal integral bases and complex conjugation, J. Reine Angew. Math. **375/376** (1987), 157–166.
[3] J. Brinkhuis, Normal integral bases and the Spiegelungssatz of Scholz, Acta Arith. **69** (1995), no. 1, 1–9.
[4] E. J. Gómez Ayala, Bases normales d'entiers dans les extensions de Kummer de degré premier, J. Théor. Nombres Bordeaux **6** (1994), no. 1, 95–116.
[5] C. Greither, *Cyclic Galois extensions of commutative rings*, Lecture Notes in Math., 1534, Springer, Berlin, 1992.
[6] C. Greither, On normal integral bases in ray class fields over imaginary quadratic fields, Acta Arith. **78** (1997), no. 4, 315–329.
[7] C. Greither and H. Johnston, Capitulation for locally free class groups of orders of group algebras over number fields, Bull. Lond. Math. Soc. **41** (2009), no. 3, 541–548.
[8] H. Ichimura, On a theorem of Childs on normal bases of rings of integers, J. London Math. Soc. (2) **68** (2003), no. 1, 25–36.
[9] H. Ichimura, Addendum to: "On a theorem of Childs on normal bases of rings of integers" [J. London Math. Soc. (2) **68** (2003), no. 1, 25–36; 1980241], J. London Math. Soc. (2) **69** (2004), no. 2, 303–305.
[10] H. Ichimura, Normal integral bases and ray class groups, Acta Arith. **114** (2004), no. 1, 71–85.
[11] H. Ichimura, On the ring of p-integers of a cyclic p-extension over a number field, J. Théor. Nombres Bordeaux **17** (2005), no. 3, 779–786.
[12] L. R. McCulloh, Galois module structure of elementary abelian extensions, J. Algebra **82** (1983), no. 1, 102–134.