YOKOHAMA MATHEMATICAL
JOURNAL VOL. 54, 2007

NOTE ON HILBERT-SPEISER NUMBER FIELDS AT A PRIME p

By

HUMIO ICHIMURA

(Received April 13, 2007)

Abstract. Let p be a prime number. A number field F satisfies the Hilbert-Speiser condition (H_p) when any tame cyclic extension N/F of degree p has a normal integral basis. We show that F satisfies (H_p) only when $F\cap \boldsymbol{Q}(\zeta_p)=\boldsymbol{Q}$ under some assumption on p.

1. Introduction

Let p be a prime number. A number field F satisfies the condition (H_p) when any tame cyclic extension N/F of degree p has a normal integral basis. As is well known, the rationals $\boldsymbol{Q}$ satisfy (H_p) for any p by Hilbert and Speiser. On the other hand, Greither *et al.* [3] proved that $F\neq \boldsymbol{Q}$ does not satisfy (H_p) for infinitely many p. Thus, it is of interest to determine which number field satisfies (H_p) or not. They showed the above assertion after deriving, from a theorem of McCulloh [12], a simple necessary condition for F to satisfy (H_p) (see Lemma 2 in Section 3). Using the necessary condition, we showed in [6, Proposition 2] that if $p\geq 5$ and $\zeta_p\in F^{\times}$, then F does not satisfy (H_p), where ζ_p is a primitive p-th root of unity. For this, see also Herreng [4, Proposition 3.3]. The following more general assertion is easily shown using the necessary condition, and seems to be known to specialists. (Its proof is given at the end of this note.)

PROPOSITION. *Let $p\geq 5$ be a prime number. A number field F does not satisfy (H_p) if $F\cap \boldsymbol{Q}(\zeta_p)$ is an imaginary subfield of $\boldsymbol{Q}(\zeta_p)$.*

The purpose of this note is to deal with the case where $F\cap \boldsymbol{Q}(\zeta_p)$ is a nontrivial real subfield. The following is a consequence of the main theorem.

THEOREM 1. *Let p be a prime number with $23\leq p<2^{10}$ and $p\neq 29$. A number field F does not satisfy (H_p) if $F\cap \boldsymbol{Q}(\zeta_p)$ is a nontrivial real subfield of $\boldsymbol{Q}(\zeta_p)$.*

2000 Mathematics Subject Classification: 11R33, 11R18.
Key words and phrases: Hilbert-Speiser number field, cyclotomic field

From these assertions, we obtain the following:

COROLLARY 1. *Let p be as in Theorem 1. Then, a number field F satisfies (H_p) only when $F \cap \boldsymbol{Q}(\zeta_p) = \boldsymbol{Q}$.*

Let h_p^- be the relative class number of $\boldsymbol{Q}(\zeta_p)$. In our argument, the existence of an odd prime factor of h_p^- is necessary. The condition $p \geq 23$ is equivalent to $h_p^- > 1$ (see Washington [13, Corollary 11.18]). The case $p = 29$ is exceptional since h_p^- is a power of 2 if and only if ($p \leq 19$ or) $p = 29$ by Horie [5].

REMARK 1. (1) Let p be as in Theorem 1. It is known that any subfield $F \neq \boldsymbol{Q}$ of $\boldsymbol{Q}(\zeta_p)$ does not satisfy (H_p) (see Section 4 of [11]). Corollary 1 is a generalization of this.

(2) Imaginary quadratic fields satisfying (H_p) are determined for $p=2$, 3, 5, 7 and 11 ([1, 7, 11]). The numbers of such imaginary quadratic fields are 3, 4, 2, 1, 0, respectively. At present, we have no example of number fields satisfying (H_p) for $p \geq 11$.

(3) When $p = 3$, there exists a number field F with $\zeta_3 \in F^\times$ satisfying (H_3). For example, $F = \boldsymbol{Q}(\zeta_3)$ and $F = \boldsymbol{Q}(\zeta_3, \sqrt{-d})$ with $d = 1, 2, 11$ satisfy (H_3). For this, see [2, p. 110] and [6, Example 1].

(4) When $p = 5$, we can show that $F = \boldsymbol{Q}(\sqrt{5})$ satisfies (H_5) using the above mentioned theorem of McCulloh by a hard hand-calculation.

2. Main theorem

To state the main result, we first recall the definition and some properties of Stickelbeger ideals of conductor p. Let p be an odd prime number, and $C = \boldsymbol{F}_p^\times$ the multiplicative group of the finite field $\boldsymbol{F}_p$ of p elements. Let $\mathcal{S}_C$ be the classical Stickelberger ideal of the group ring $\boldsymbol{Z}[C]$ (for the definition, see [13, Chap. 6]). Let H be an arbitrary subgroup of C. For an element $\alpha \in \boldsymbol{Z}[C]$, let

$$\alpha_H = \sum_{\sigma \in H} a_\sigma \sigma \in \boldsymbol{Z}[H] \quad \text{with} \quad \alpha = \sum_{\sigma \in C} a_\sigma \sigma$$

be the H-part of α. We define the Stickelberger ideal $\mathcal{S}_H$ of $\boldsymbol{Z}[H]$ by

$$\mathcal{S}_H = \{\alpha_H \mid \alpha \in \mathcal{S}_C\} \subseteq \boldsymbol{Z}[H].$$

Letting ρ be a generator of the cyclic group H, set

$$\mathfrak{n}_H = \begin{cases} 1 + \rho + \rho^2 + \cdots + \rho^{|H|/2-1}, & \text{if } |H| \text{ is even} \\ 1, & \text{if } |H| \text{ is odd.} \end{cases} \tag{1}$$

It is known that $\mathcal{S}_H \subseteq \langle \mathfrak{n}_H \rangle = \mathfrak{n}_H \boldsymbol{Z}[H]$ ([10, Lemma 1]). Further, it is known that the quotient $\langle \mathfrak{n}_H \rangle / \mathcal{S}_H$ is a finite abelian group whose order divides the relative class number h_p^- and that $[\langle \mathfrak{n}_C \rangle : \mathcal{S}_C] = h_p^-$ ([10, Theorem 2]). For a prime number q, let

$$\mathcal{S}_{H,q} = \mathcal{S}_H \otimes \boldsymbol{Z}_q \ (\subseteq \boldsymbol{Z}_q[H]) \quad \text{and} \quad \langle \mathfrak{n}_H \rangle_q = \mathfrak{n}_H \boldsymbol{Z}_q[H].$$

Here, $\boldsymbol{Z}_q$ is the ring of q-adic integers.

Let F be a number field, and $K = F(\zeta_p)$. We regard the Galois group

$$\mathrm{Gal}(K/F) = \mathrm{Gal}(\boldsymbol{Q}(\zeta_p)/F \cap \boldsymbol{Q}(\zeta_p))$$

with a subgroup $H = H_F$ of C through the Galois action on ζ_p. Clearly, the subfield $F \cap \boldsymbol{Q}(\zeta_p)$ of $\boldsymbol{Q}(\zeta_p)$ is real if and only if $|H|$ is even.

Now, the main theorem is stated as follows.

THEOREM 2. *Let p be a prime number with $p \geq 23$ and $p \neq 29$. Let F be a number field such that $F \cap \boldsymbol{Q}(\zeta_p)$ is a nontrivial real subfield of $\boldsymbol{Q}(\zeta_p)$, and let $H = H_F$ be as above. Assume that there exists an odd prime factor q of h_p^- satisfying $\mathcal{S}_{H,q} = \langle \mathfrak{n}_H \rangle_q$. Then, F does not satisfy the condition (H_p).*

Combining this with Proposition, we obtain:

COROLLARY 2. *Let p be a prime number satisfying the assumption of Theorem 2. Then, F satisfies (H_p) only when $F \cap \boldsymbol{Q}(\zeta_p) = \boldsymbol{Q}$.*

For the assumption of Theorem 2, the following assertions are known.

LEMMA 1. *Let H be a subgroup of $C = \boldsymbol{F}_p^\times$ with $|H|$ even and $H \neq C$.*

(I) *When $|H| = 2, 4, 6$, we have $\mathcal{S}_H = \langle \mathfrak{n}_H \rangle$.*

(II) *When $23 \leq p \leq 499$ and $p \neq 29$, we have $\mathcal{S}_{H,q} = \langle \mathfrak{n}_H \rangle_q$ for some odd prime factor q of h_p^-.*

(III) *For a prime factor q of h_p^- with $q \parallel h_p^-$, we have $\mathcal{S}_{H,q} = \langle \mathfrak{n}_H \rangle_q$ for any H.*

For the assertions (I) and (II), see Theorem 2(III) and Proposition 3 of [10], and for (III), see Corollary 2 of [9]. For prime numbers p with $23 \leq p < 2^{10}$, it is known that $q \parallel h_p^-$ for some odd prime number q except for the case where $p = 29$, 31 or 41 (see the table of Yamamura [14]). Therefore, Theorem 1 is an immediate consequence of Theorem 2 and Lemma 1.

3. Consequences of McCulloh's theorem

To study Hilbert-Speiser number fields, the theorem of McCulloh [12] mentioned in Section 1 plays a fundamental role. In this section, we recall some consequences of the theorem. For a number field F and an integer $a \in \mathcal{O}_F$, let $Cl_{F,a}$ be the ray class group of F defined modulo the integral ideal $a\mathcal{O}_F$, where $\mathcal{O}_F$ is the ring of integers of F. In particular, $Cl_F = Cl_{F,1}$ is the absolute class group of F. Let $\mathcal{O}_F^\times$ be the group of units of F, and let $[\mathcal{O}_F^\times]_p = \mathcal{O}_F^\times \bmod p$ be the subgroup of the multiplicative group $(\mathcal{O}_F/p)^\times$ consisting of the classes containing a unit of F. The quotient $(\mathcal{O}_F/p)^\times/[\mathcal{O}_F^\times]_p$ is a subgroup of the ray class group $Cl_{F,p}$. The following is the necessary condition for (H_p) mentioned in Section 1.

Lemma 2. ([3, Corollary 7]). *If F satisfies the condition (H_p), then the p-part of $(\mathcal{O}_F/p)^\times/[\mathcal{O}_F^\times]_p$ is trivial.*

Lemma 3. ([8, Theorem 5]). *Let F be a number field, and let $K = F(\zeta_p)$ and $H = \mathrm{Gal}(K/F) \subseteq C$. If F satisfies (H_p), then*

$$Cl_{K,\pi}^{\mathcal{S}_H} = \{0\} \quad \text{and} \quad Cl_{K,p}^H \cap Cl_{K,p}^{\mathcal{S}_H} = \{0\}.$$

Here, $\pi = \zeta_p - 1$, and $Cl_{K,p}^H$ is the Galois invariant part. In particular, $\mathcal{S}_H$ kills Cl_K if F satisfies (H_p).

Remark 2. It is known that the converse of Lemma 3 holds when $p = 3$ ([7, Theorem 3]).

4. Proof of Theorem 2

The following lemma is quite easy to show.

Lemma 4. *For an integer $n \geq 2$, let C_n be a cyclic group of order n. Let q be an odd prime number, and let $\Gamma = C_q^{\oplus s}$ with $s \geq 1$. Letting C_2 act on Γ via (-1)-multiplication, let G be the semi-direct product of Γ and C_2 with Γ normal in G. Let J be an element of G of order 2. Then, all elements of G of order 2 are given by*

$$J_\gamma = \gamma^{-1}J\gamma \quad \text{with } \gamma \in \Gamma,$$

and $J_\gamma \neq J_{\gamma'}$ for $\gamma \neq \gamma'$.

Let p be a prime number with $p \geq 23$ and $p \neq 29$. Let $k = \boldsymbol{Q}(\zeta_p)$, and k^+ its maximal real subfield. Let Cl_k^- be the minus class group of k. Let q be an odd prime number dividing h_p^-, and let M_q^-/k be the class field corresponding to the class group $Cl_k^-/(Cl_k^-)^q$. Then, M_q^- is Galois over any subfield of k. We easily see that there exists an extension E^+/k^+ such that $E^+ \cap k = k^+$ and $E^+k = M_q^-$. Of course, such an extension E^+/k^+ is not uniquely determined. Let $q^s = [M_q^- : k]$.

LEMMA 5. *The unique prime ideal $\wp$ of k^+ over p is decomposed in E^+ as*

$$\wp = \wp_1 \left(\wp_2 \cdots \wp_{(q^s+1)/2}\right)^2,$$

where $\wp_i$'s are prime ideals of E^+ of absolute degree one.

Proof. Let $G = \mathrm{Gal}(M_q^-/k^+)$ and $\Gamma = \mathrm{Gal}(M_q^-/k)$. Then, G is the semi-direct product of Γ and $C_2 = \mathrm{Gal}(k/k^+)$ with C_2 acting on Γ via (-1)-multiplication. Let $\tilde{\wp}$ be the unique prime ideal of k over p. As $\tilde{\wp}$ is principal, it completely decomposes in M_q^-. Let $\mathfrak{P}$ be a prime ideal of M_q^- over $\tilde{\wp}$. Then, all the primes of M_q^- over p are given by $\mathfrak{P}^\gamma$ with $\gamma \in \Gamma$. Let T_γ be the inertia group of $\mathfrak{P}^\gamma$ over k^+, and let $T = T_e$ where e is the identity of Γ. Clearly, $|T_\gamma| = 2$. By Lemma 4, the groups $T_\gamma = \gamma^{-1}T\gamma$ with $\gamma \in \Gamma$ are all the subgroups of G of order 2, and $T_\gamma \neq T_{\gamma'}$ for $\gamma \neq \gamma'$. Hence, we have $T = \mathrm{Gal}(M_q^-/E^+)$ for a suitable choice of $\mathfrak{P}$. It follows that the prime $\mathfrak{P} \cap \mathcal{O}_{E^+}$ is unramified over k^+, and that for $\gamma \neq e$, $\mathfrak{P}^\gamma \cap \mathcal{O}_{E^+}$ is ramified over k^+ with ramification index 2 as $T_\gamma \neq T$. From this, we obtain the assertion since $\mathfrak{P}$ is of absolute degree one. □

LEMMA 6. *Let k_0 be a subfield of k^+. Let E_0/k_0 be an extension such that $E_0 \cap k = k_0$ and $E_0 k = M_q^-$. Then, there exist exactly one real prime and $(q^s - 1)/2$ complex primes of E_0 over each real prime of k_0.*

Proof. Let $G = \mathrm{Gal}(M_q^-/k_0)$, $\Gamma = \mathrm{Gal}(M_q^-/k)$ and $H = \mathrm{Gal}(M_q^-/E_0)$. An element $g \in G$ is uniquely written as $g = \gamma h$ for $\gamma \in \Gamma$ and $h \in H$. Let ∞_0 be a real prime of k_0, and let $\varphi : M_q^- \hookrightarrow \boldsymbol{C}$ be an embedding corresponding to an extension $\widetilde{\infty}$ of ∞_0 to M_q^-. Then, the set of infinite primes of M_q^- over ∞_0 is

$$\{\varphi g, j\varphi g \mid g \in G\}/\sim = \{\varphi\gamma h, j\varphi\gamma h \mid \gamma \in \Gamma, h \in H\}/\sim.$$

Here, j is the complex conjugation, and $\sim$ is the obvious equivalence. It follows that the set of infinite primes of E_0 over ∞_0 is

$$\{(\varphi\gamma)_{|E_0}, (j\varphi\gamma)_{|E_0} \mid \gamma \in \Gamma\}/\sim = \{(\varphi\gamma)_{|E_0} \mid \gamma \in \Gamma\}/\sim$$

as H fixes the elements of E_0. Let T_γ be the inertia group over k_0 of the infinite prime $[\varphi\gamma]$ corresponding to the embedding $\varphi\gamma$. As $k_0 \subseteq k^+$, we have $T_\gamma \subseteq \mathrm{Gal}(M_q^-/k^+)$. Hence, T_γ equals the inertia group of $[\varphi\gamma]$ over k^+. By an argument in the proof of Lemma 5, $T_e = \mathrm{Gal}(M_q^-/E_0k^+) \subseteq H$ for a suitable choice of $\widetilde{\infty}$ or φ, and $T_\gamma \neq T_e$ for $\gamma \neq e$. As H is a cyclic group, the last condition implies $T_\gamma \not\subseteq H$. Hence, it follows that the infinite prime of E_0 corresponding to the embedding $\varphi_{|E_0}$ is real, and the other ones are complex. The assertion follows from this. □

Proof of Theorem 2. Let F be a number field, and let $K = F(\zeta_p)$ and $k_0 = F \cap k$. Put

$$H = \mathrm{Gal}(K/F) = \mathrm{Gal}(k/k_0) \subseteq C = \boldsymbol{F}_p^\times.$$

Assume that k_0 is nontrivial and real. Then, $|H| = 2d$ is even, and let J be the element of order 2 of H. Clearly, the restriction $J_{|k}$ is the complex conjugation of k. Let q be an odd prime number dividing h_p^-. Assume that $\mathcal{S}_{H,q} = \langle \mathfrak{n}_H \rangle_q$. Then, by (1), we have

$$1 - J = (1 - \rho)\mathfrak{n}_H \in \mathcal{S}_{H,q}. \tag{2}$$

Assume further that F satisfies (H_p). By Lemma 3, $\mathcal{S}_H$ annihilates the class group Cl_K. Hence, it follows from (2) that $Cl_K(q)^{1-J} = \{0\}$, where $Cl_K(q)$ is the q-part of Cl_K. This implies that the class field M_q^- of k is contained in K. Let E_0 be the subfield of M_q^- fixed by the automorphisms in H. Then, we see that $E_0 \cap k = k_0$ and $E_0k = M_q^-$. Let $n = [F : E_0]$.

Let λ_1 and λ_2 be the p-ranks of the abelian groups $[\mathcal{O}_F^\times]_p$ and $(\mathcal{O}_F/p)^\times$, respectively. In view of Lemma 2, it suffices to show that

$$\lambda_1 < \lambda_2.$$

Let $q^s = [M_q^- : k] = [E_0 : k_0]$. By Lemma 6, the number of complex primes of F is at least

$$\lambda_3 = \frac{p-1}{2d} \times \frac{q^s - 1}{2} \times n.$$

Therefore, as $\zeta_p \notin F^\times$, it follows that

$$\lambda_1 \leq [F : Q] - \lambda_3 - 1 = \frac{(p-1)(q^s+1)n}{4d} - 1$$

from the Dirichlet unit theorem. Let $\wp_0$ be the unique prime ideal of k_0 over p, and let

$$\wp_0 = \wp_1^{e_1} \cdots \wp_r^{e_r}$$

be the prime decomposition in E_0. Here, $\wp_i$ is a prime ideal of E_0 of absolute degree one, and

$$\sum_{i=1}^{r} e_i = q^s. \tag{3}$$

By Lemma 5, at least one of e_i is even. Hence, we may as well assume that $2|e_r$. Let

$$\wp_i = \prod_{j=1}^{g_i} \mathfrak{P}_{i,j}^{e_{i,j}}$$

be the prime decomposition in F. Here, $N_{F/E_0}\mathfrak{P}_{i,j} = \wp_i^{f_{i,j}}$, and

$$\sum_{j=1}^{g_i} e_{i,j} f_{i,j} = n. \tag{4}$$

Let

$$A_i = \bigoplus_{j=1}^{g_i} (1 + \mathfrak{P}_{i,j}^{e_{i,j}e_i}) \quad \text{for } 1 \le i \le r-1$$

and

$$A_r = \bigoplus_{j=1}^{g_r} \left(1 + \mathfrak{P}_{r,j}^{e_{r,j}e_r/2}\right),$$

and let

$$B_i = \bigoplus_{j=1}^{g_i} \left(1 + \mathfrak{P}_{i,j}^{e_{i,j}e_i(p-1)/2d}\right) \ (\subseteq A_i)$$

for $1 \le i \le r$. The quotient $C_i = A_i/B_i$ is an abelian group of exponent p, and the product $C_1 \oplus \cdots \oplus C_r$ is naturally contained in $(\mathcal{O}_F/p)^\times$. Hence, it follows from (3) and (4) that

$$\begin{aligned}\lambda_2 &\ge \sum_{i=1}^{r-1}\sum_{j} e_{i,j}f_{i,j}e_i\left(\frac{p-1}{2d}-1\right) + \sum_{j} e_{r,j}f_{r,j}e_r\left(\frac{p-1}{2d}-\frac{1}{2}\right)\\ &= \left(\frac{p-1}{2d}-1\right)q^s n + \frac{ne_r}{2} \ge \left(\frac{p-1}{2d}-1\right)q^s n + n.\end{aligned}$$

Here, the last inequality holds as $2|e_r$. Therefore, we see that

$$\lambda_2 - \lambda_1 \ge \left(\frac{p-1}{4d}-1\right)(q^s-1)n + 1 > 0$$

since $p-1 \ge 4d$ as $k_0 \ne \boldsymbol{Q}$, and we obtain the desired inequality $\lambda_1 < \lambda_2$. □

Proof of Proposition. Since the case $\zeta_p \in F^\times$ is dealt with in [6], we may assume that $\zeta_p \notin F^\times$. As $k_0 = F \cap k$ is imaginary, $[k_0 : \boldsymbol{Q}] = 2e$ is even. Let $n = [F : k_0]$. Let λ_1 and λ_2 be the p-ranks of $[\mathcal{O}_F^\times]_p$ and $(\mathcal{O}_F/p)^\times$, respectively. As $\zeta_p \notin F^\times$, we see that $\lambda_1 \leq en - 1$ by the Dirichlet unit theorem. Noting that p is totally ramified in k_0, we easily see that $\lambda_2 \geq (2e-1)n$. Therefore, $\lambda_1 < \lambda_2$, and the assertion follows from Lemma 2. □

Acknowledgement. The author was partially supported by Grant-in-Aid for Scientific Research (C), No. 19540005, Japan Society for the Promotion of Science.

References

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

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

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

[4] T. Herreng, Sur les corps de Hilbert-Speiser, *J. Théor. Nombres Bordeaux*, **17** (2005), 767–778.

[5] K. Horie, On the class numbers of cyclotomic fields, *Manuscripta Math.*, **65** (1989), 465–477.

[6] H. Ichimura, Note on the ring of integers of a Kummer extension of prime degree, V, *Proc. Japan Acad.*, **78A** (2002), 76–79.

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

[8] H. Ichimura, Normal integral bases and ray class groups, II, *Yokohama Math. J.*, **53** (2006), 75–81.

[9] H. Ichimura, Triviality of Stickelberger ideals of conductor p, *J. Math. Sci. Univ. Tokyo*, **13** (2006), 617–628.

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

[11] H. Ichimura and H. Sumida-Takahashi, Imaginary quadratic fields satisfying the Hilbert-Speiser type condition for a small prime p, *Acta Arith.*, **127** (2007), 179–191.

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

[13] L. C. Washington, Introduction to Cyclotomic Fields (2nd ed.), Springer, New York, 1997.

[14] K. Yamamura, Table of relative class numbers of imaginary abelian number fields of prime power conductors $\leq 2^{10} = 1024$,
available at `ftp://tnt.math.metro-u.ac.jp/pub/table/rcn/`.

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