J. Math. Soc. Japan
Vol. 62, No. 1 (2010) pp. 83–94
doi: 10.2969/jmsj/06210083

Hilbert-Speiser number fields and the complex conjugation

By Humio ICHIMURA

(Received Nov. 2, 2008)

Abstract. Let p be a prime number. We say that a number field F satisfies the condition (H_p) when any tame cyclic extension N/F of degree p has a normal integral basis. We determine all the CM Galois extensions $F/\boldsymbol{Q}$ satisfying (H_p) for the case $p \geq 5$, using the action of the complex conjugation on several objects associated to F.

1. Introduction.

Let p be a prime number. We say that a number field F satisfies the Hilbert-Speiser condition (H_p) when any tame cyclic extension N/F of degree p has a (relative) normal integral basis. The rationals $\boldsymbol{Q}$ satisfy the condition (H_p) for all p by a classical theorem of Hilbert and Speiser, while a number field $F \neq \boldsymbol{Q}$ does not satisfy (H_p) for infinitely many p by Greither, Replogle, Rubin and Srivastav [**3**]. There are several results on number fields satisfying or not satisfying this property ([**2**], [**5**], [**8**], [**9**], [**10**], [**12**], [**13**], [**22**]). In particular, in [**13**], we determined all imaginary quadratic fields satisfying (H_p) for each p. In this paper, we deal with a CM Galois extension, and prove the following theorem. Here, a number field F is called a CM Galois extension when F is a CM field and $F/\boldsymbol{Q}$ is a Galois extension. For an integer $n \geq 2$, ζ_n denotes a primitive n-th root of unity.

THEOREM 1.1. *Let p be a prime number with $p \geq 5$ and let $F/\boldsymbol{Q}$ be a nonquadratic* CM *Galois extension. Then F satisfies the condition (H_p) if and only if $F = \boldsymbol{Q}(\zeta_{12})$ and $p = 5$.*

Our method is sketched as follows. Using a theorem of McCulloh [**17**] and several of its known consequences, we show that if a CM Galois extension F satisfies (H_p), then the group W_F of roots of unity in F must be "large" (Lemma 3.1) and at the same time, the minus class group Cl_F^- must be almost trivial (Corollary 4.1). A point of the arguments is the existence of the complex conjugation J acting on several objects associated to F. However, when W_F is

2000 *Mathematics Subject Classification.* Primary 11R33; Secondary 11R18.
Key Words and Phrases. Hilbert-Speiser number field, normal integral basis, CM field.
The author was partially supported by Grant-in-Aid for Scientific Research (C), (No. 19540005), Japan Society for the Promotion of Science.

large, Cl_F^- becomes large. We prove Theorem 1.1 using these facts and some results on class numbers of cyclotomic fields. The arguments in this paper are generalizations of those in the previous papers.

Combined with the result in [**13**] for the imaginary quadratic case, it follows from Theorem 1.1 that there exists no CM Galois extension satisfying (H_p) for $p \geq 11$. In the final section, we give an example of a real abelian field satisfying (H_p) for $p = 11$ or 13.

REMARK 1.

(I) Let $p = 2$ or 3. Yoshimura [**22**] determined all imaginary abelian fields satisfying (H_2) or (H_3) using Yamamura's determination [**21**] of the imaginary abelian fields F with class number one. To determine all CM Galois extensions satisfying (H_2) or (H_3), it would be necessary to know all those with class number one.

(II) In [**1**], Brinkhuis used the complex conjugation to show that an *unramified* abelian extension N/F of CM fields quite rarely has a normal integral basis.

2. McCulloh's theorem.

To study Hilbert-Speiser number fields, a theorem of McCulloh [**17**] mentioned in Section 1 plays an important role. In this section, we recall the theorem and some of its known consequences.

Let p be a prime number, and let $\Gamma = (\boldsymbol{Z}/p)^+$ and $G = (\boldsymbol{Z}/p)^\times$ be the additive group and the multiplicative group of the finite field $\boldsymbol{Z}/p$. For a number field F, let $\mathcal{O}_F$ be the ring of integers of F, and Cl_F the ideal class group of the Dedekind domain $\mathcal{O}_F$. Let $Cl(\mathcal{O}_F\Gamma)$ be the locally free class group of the group ring $\mathcal{O}_F\Gamma$, and $Cl^0(\mathcal{O}_F\Gamma)$ the kernel of the natural map $Cl(\mathcal{O}_F\Gamma) \to Cl_F$ induced from the augmentation $\mathcal{O}_F\Gamma \to \mathcal{O}_F$. Let $R(\mathcal{O}_F\Gamma)$ be the subset of $Cl(\mathcal{O}_F\Gamma)$ consisting of the locally free classes $[\mathcal{O}_N]$ for all tame Γ-extensions N/F. It is known that $R(\mathcal{O}_F\Gamma) \subseteq Cl^0(\mathcal{O}_F\Gamma)$. As Γ is abelian, F satisfies (H_p) if and only if $R(\mathcal{O}_F\Gamma) = \{0\}$. Let $\mathscr{S}_G$ be the classical Stickelberger ideal of the group ring $\boldsymbol{Z}G$ associated to the abelian extension $\boldsymbol{Q}(\zeta_p)/\boldsymbol{Q}$. For the definition, see Washington [**20**, Chapter 6]. Through the natural action of G on Γ, the group ring $\boldsymbol{Z}G$ acts on $Cl(\mathcal{O}_F\Gamma)$. The following is the main theorem of [**17**].

$$R(\mathcal{O}_F\Gamma) = Cl^0(\mathcal{O}_F\Gamma)^{\mathscr{S}_G}. \tag{2.1}$$

The following consequence of (2.1) was proved in [**3**]. Let $E_F = \mathcal{O}_F^\times$ be the group of units of F. For a subgroup E of E_F, let $[E]_p$ be the subgroup of $(\mathcal{O}_F/p)^\times$ consisting of the classes containing units in E.

LEMMA 2.1 ([**3**, Theorem 1]). *Let $p \geq 3$. If F satisfies (H_p), then the exponent of the quotient $(\mathscr{O}_F/p)^\times/[E_F]_p$ divides $(p-1)^2/2$.*

LEMMA 2.2. *Let $p \geq 5$. If a* CM *Galois extension $F/\boldsymbol{Q}$ satisfies (H_p), then p is unramified in F.*

PROOF. Similar assertions are given in [**5**, Proposition 3.4] and [**11**, Proposition]. We can show the assertion similarly by using Lemma 2.1. □

For a number field N and an integer $\alpha \in \mathscr{O}_N$, let $Cl_{N,\alpha}$ be the ray class group of N defined modulo the principal ideal $\alpha\mathscr{O}_N$. In particular, we have $Cl_N = Cl_{N,1}$. Let $K = F(\zeta_p)$ and $\pi = \zeta_p - 1$. In view of Lemma 2.2, we assume that F is a number field *unramified* at p. Then we can identify the Galois group $\mathrm{Gal}(K/F)$ with G through the Galois action on ζ_p. It is known that $Cl^0(\mathscr{O}_F\Gamma)$ is isomorphic to $Cl_{K,\pi}$ as a G-module ([**1**, Proposition 2.1]). Hence, we obtain from (2.1) the following:

LEMMA 2.3. *Let F be a number field unramified at p, and let $K = F(\zeta_p)$. Then F satisfies (H_p) if and only if the Stickelberger ideal $\mathscr{S}_G$ annihilates the ray class group $Cl_{K,\pi}$.*

Next, we collect some facts on the Stickelberger ideal $\mathscr{S}_G$ which are necessary in this paper. Let $k = \boldsymbol{Q}(\zeta_p)$. We are identifying $\mathrm{Gal}(k/\boldsymbol{Q})$ with $G = (\boldsymbol{Z}/p)^\times$ through the Galois action on ζ_p. For an integer i with $p \nmid i$, denote by σ_i the element of G corresponding to i. Let A_G be the ideal of the group ring $\boldsymbol{Z}G$ consisting of the elements α such that $(1+\sigma_{-1})\alpha \in N_G\boldsymbol{Z}$, where N_G is the norm element of $\boldsymbol{Z}G$. Let ρ be a generator of G and put

$$\mathfrak{n}_G = 1 + \rho + \rho^2 + \cdots + \rho^{(p-1)/2-1}.$$

We can easily show that A_G is generated by $\mathfrak{n}_G$ over $\boldsymbol{Z}G$:

$$A_G = \langle \mathfrak{n}_G \rangle.$$

For an integer $n \geq 3$, let h_n^- be the relative class number of the cyclotomic field $\boldsymbol{Q}(\zeta_n)$. By a general theorem of Sinnott [**18**, Theorem 2.1] on Stickelberger ideals, it is known that $\mathscr{S}_G \subseteq A_G$ and that

$$[A_G : \mathscr{S}_G] = h_p^-. \tag{2.2}$$

We put

$$\theta_2 = \sum_{i=1}^{p-1} \left[\frac{2i}{p}\right] \sigma_i^{-1} = \sum_{i=(p+1)/2}^{p-1} \sigma_i^{-1} \in \boldsymbol{Z}G.$$

It is known that θ_2 and N_G belong to $\mathscr{S}_G$. By $N_G \in \mathscr{S}_G$ and Lemma 2.3, we obtain

LEMMA 2.4 ([**12**, Proposition 4]). *Let F be a number field unramified at p, and let $K = F(\zeta_p)$. If F satisfies (H_p), then the natural map $Cl_F \to Cl_K$ is trivial.*

3. Roots of unity.

We collect some notation which we use frequently in this paper. Let F be a CM field and F^+ the maximal real subfield of F. Let Cl_F^- be the kernel of the norm map $Cl_F \to Cl_{F^+}$, namely the minus class group of F, and let $h_F^- = |Cl_F^-|$. Let W_F be the group of roots of unity in F.

Let F be a CM field unramified at p, and let J be the complex conjugation of the CM field $K = F(\zeta_p)$. Note that J is different from the automorphism $\sigma_{-1} \in G = \mathrm{Gal}(K/F)$. The following assertion is a "minus part" version of Lemma 2.1.

LEMMA 3.1. *Let $p \geq 3$, and let F be a CM field unramified at p. If F satisfies (H_p), then*

$$((\mathscr{O}_F/p)^\times)^{(J-1)^2} \subseteq [W_F]_p.$$

In particular, $((\mathscr{O}_F/p)^\times)^{(J-1)^2}$ is a cyclic group.

PROOF. Let $k = \boldsymbol{Q}(\zeta_p)$ and $K_0 = F \cdot k^+$. Let I_F be the group of ideals of F relatively prime to p, and H_F the subgroup of I_F consisting of ideals $xN_{K_0/F}\mathfrak{A}$ for ideals $\mathfrak{A}$ of K_0 relatively prime to p and elements $x \in F^\times$ with $x \equiv 1 \bmod p$. The reciprocity law induces an isomorphism

$$I_F/H_F \cong \mathrm{Gal}(K_0/F)$$

compatible with the action of the complex conjugation J. As J acts on $\mathrm{Gal}(K_0/F) = \mathrm{Gal}(k^+/\boldsymbol{Q})$ trivially, we obtain

$$I_F^{J-1} \subseteq H_F.$$

Now, let α be an element of $F^\times$ with $(\alpha, p) = 1$. Then, by the above, we have $\alpha^{J-1}\mathscr{O}_F = xN_{K_0/F}\mathfrak{A}$ for some ideal $\mathfrak{A}$ of K_0 and an element $x \in F^\times$ with

$x \equiv 1 \bmod p$. Noting that the element $\theta_2 \in \mathscr{S}_G$ acts on $K_0^\times$ as the norm operator $N_{K_0/F}$, we see from Lemma 2.3 that the ray class $[N_{K_0/F}\mathfrak{A} \cdot \mathscr{O}_K] \in Cl_{K,\pi}$ is trivial. Therefore,

$$\alpha^{J-1} \equiv \epsilon \bmod \pi$$

for some unit $\epsilon \in E_K$. By a theorem of units of a CM field [**20**, Theorem 4.12], we have $\epsilon^{J-1} \in W_K$. We see that $W_K = W_F \cdot \langle \zeta_p \rangle$ as F is unramified at p. Hence, $\epsilon^{(J-1)p} \in W_F$. Let f be the least common multiple of the degrees of the prime ideals of F over p, and put $\eta = \epsilon^{(J-1)p^f} \in W_F$. Then we obtain

$$\alpha^{(J-1)^2} \equiv \alpha^{(J-1)^2 p^f} \equiv \eta \bmod \pi.$$

This congruence holds modulo p as F is unramified at p. Therefore, we obtain the assertion. □

LEMMA 3.2. *Let $p \geq 5$, and let $m \geq 4$ be an even integer with $p \nmid m$. Then $p^{\varphi(m)} = 1 + am$ for some integer $a \geq 3$. Here, $\varphi(*)$ is the Euler function.*

PROOF. We give a proof of this elementary assertion for the sake of completeness. When $m = 2^e$ with $e \geq 2$, we can easily show the assertion by induction on e. So, let us deal with the case where m is not a power of 2. First, let $m = 2m_0$ for some odd integer $m_0 \geq 3$. We have $2^{\varphi(m)} = 2^{\varphi(m_0)} = 1 + am_0$ for some $a \geq 1$. It follows that

$$p^{\varphi(m)} > 4^{\varphi(m)} = 1 + bm_0 \quad \text{with} \quad b = 2a + a^2 m_0 \geq 5.$$

On the other hand, $p^{\varphi(m)} = 1 + cm_0$ for some even integer c. From the above inequality, we obtain $c \geq 6$, from which the assertion follows in this case. Next, let $m = 2^{e+1}m_0$ for some $e \geq 1$ and an odd integer $m_0 \geq 3$. We have already shown that $p^{\varphi(2m_0)} = 1 + 2am_0$ for some $a \geq 3$. Hence, it follows that

$$p^{\varphi(m)} = (1 + 2am_0)^{2^e} \geq 1 + 2^{e+1}am_0 = 1 + am.$$

The assertion follows from this. □

LEMMA 3.3. *Let $p \geq 5$. Let $F/\boldsymbol{Q}$ be a nonquadratic* CM *Galois extension unramified at p. Let f^- be the relative degree at F/F^+ of a prime ideal of F over p. Assume that F satisfies (H_p). Then the following assertions hold*:

(I) *$m = |W_F| \geq 4$ and $F = \boldsymbol{Q}(W_F)$.*
(II) *The prime p remains prime in F^+.*

(III) *When* $f^- = 1$ (*resp.* $f^- = 2$), m *is a multiple of* $(p^{\varphi(m)/2} - 1)/2$ (*resp.* $(p^{\varphi(m)/2} + 1)/2$).

PROOF. Let f be the degree of p at $F^+/\boldsymbol{Q}$. We have a canonical decomposition

$$(\mathscr{O}_F/p)^\times \cong \bigoplus_{\wp} (\mathscr{O}_F/\wp)^\times$$

where $\wp$ runs over the prime ideals of F^+ over p and $\mathscr{O}_F/\wp = \mathscr{O}_F/\wp\mathscr{O}_F$. Each component $(\mathscr{O}_F/\wp)^\times$ is invariant under the action of the complex conjugation J. The endomorphism $1 - J$ on $(\mathscr{O}_F/\wp)^\times$ induces an exact sequence

$$1 \to (\mathscr{O}_{F^+}/\wp)^\times \to (\mathscr{O}_F/\wp)^\times \to ((\mathscr{O}_F/\wp)^\times)^{1-J} \to 1.$$

Using this, we easily see that $((\mathscr{O}_F/\wp)^\times)^{1-J}$ is a cyclic group of order $p^f - 1$ (resp. $p^f + 1$) when $f^- = 1$ (resp. 2). As $(J-1)^2 = 2(1-J)$, it follows that $((\mathscr{O}_F/\wp)^\times)^{(1-J)^2}$ is a cyclic group of order $(p^f - 1)/2$ (resp. $(p^f + 1)/2$). As $p \geq 5$, it follows that the last group is nontrivial. However, since $((\mathscr{O}_F/p)^\times)^{(J-1)^2}$ is a cyclic group by Lemma 3.1, we see that the prime number p remains prime in F^+:

$$f = [F^+ : \boldsymbol{Q}].$$

It also follows from Lemma 3.1 that

$$\frac{p^f - 1}{2} \Big| m \quad \text{or} \quad \frac{p^f + 1}{2} \Big| m \tag{3.1}$$

according to whether $f^- = 1$ or 2. If $m = 2$, then we see that $p = 5$ and $f = f^- = 1$, which implies that F is a quadratic field. Thus, we obtain $m \geq 4$. Hence, $\boldsymbol{Q}(W_F)$ is an *imaginary* subfield of F. We put

$$f_0 := \frac{\varphi(m)}{2} = [\boldsymbol{Q}(W_F)^+ : \boldsymbol{Q}].$$

Then, as $\boldsymbol{Q}(W_F)^+ \subseteq F^+$, f is a multiple of f_0. To prove the assertions (I) and (III), it suffices to show that $f = f_0$. Assume, to the contrary, that $f \neq f_0$. We see from (3.1) and Lemma 3.2 that the case $f = 2f_0 = \varphi(m)$ can not happen, and hence $f = f_0 b$ for some $b \geq 3$. Then it follows from (3.1) that

$$\frac{p^{f_0 b} \pm 1}{2} \leq m \leq p^{2f_0} - 1.$$

This is impossible as $b \geq 3$. Therefore, we obtain $f = f_0$. □

Using Lemma 3.1, we can also show the following:

PROPOSITION 3.1. *For each* CM *field F, there exist at most finitely many prime numbers p for which F satisfies (H_p).*

PROOF. Let p be a prime number unramified in F. Let $\wp$ be a prime ideal of F^+ over p, and f the degree of $\wp$. Assume that F satisfies (H_p). Then, similarly as in the proof of Lemma 3.3, we see from Lemma 3.1 that $(p^f - 1)/2$ or $(p^f + 1)/2$ divides the order $|W_F|$. We obtain the assertion because there are at most finitely many primes p satisfying this condition. □

4. Proof of Theorem 1.1.

Let $p \geq 3$ be a prime number. Let F be a CM field unramified at p, and $K = F(\zeta_p)$. Let Cl_F^- be the minus class group of F. The following lemma seems to be known to specialists.

LEMMA 4.1. *Under the above setting, let X_F be the kernel of the natural map $Cl_F^- \to Cl_K$. Then the exponent of X_F divides* 2.

PROOF. We show the assertion using a standard argument in pp. 288–290 of [**20**]. Let ρ be a generator of the Galois group $G = \mathrm{Gal}(K/F)$. Let $\mathfrak{A}$ be an ideal of F such that the ideal class $[\mathfrak{A}]_F$ is contained in the kernel X_F. Then $\mathfrak{A}\mathscr{O}_K = \alpha\mathscr{O}_K$ for some $\alpha \in K^\times$. As $\mathfrak{A}$ is an ideal of F, $\alpha^{\rho-1} = \epsilon$ for some unit $\epsilon \in E_K$. As $[\mathfrak{A}]_F \in Cl_F^-$, it follows that $\mathfrak{A}^{1+J} = \beta\mathscr{O}_F$ for some $\beta \in F^\times$. Therefore, $\alpha^{1+J} = \beta\eta$ for some $\eta \in E_K$, and hence

$$\epsilon^{1+J} = \alpha^{(1+J)(\rho-1)} = (\beta\eta)^{\rho-1} = \eta^{\rho-1}. \tag{4.1}$$

Put $\alpha_1 = \alpha^2/\eta$. Then $\alpha_1\mathscr{O}_K = \mathfrak{A}^2\mathscr{O}_K$, and

$$\epsilon_1 := \alpha_1^{\rho-1} = \alpha^{2(\rho-1)}/\eta^{\rho-1} = \epsilon^2/\eta^{\rho-1} \in E_K.$$

Using (4.1), we see that

$$\epsilon_1^{1+J} = \epsilon^{2(1+J)}\eta^{(1-\rho)(1+J)} = \eta^{(\rho-1)(1-J)}.$$

This implies that $\epsilon_1^{1+J} = \pm 1$. On the other hand, we have $\epsilon_1^2 = \zeta\delta$ for some $\zeta \in W_K$ and a real unit $\delta \in E_{K^+}$ by [**20**, Theorem 4.12]. Then we see that $1 = \epsilon_1^{2(1+J)} = \delta^{1+J} = \delta^2$, and hence $\epsilon_1 \in W_K$. As F is unramified at p, we have $W_K = W_F \cdot \langle \zeta_p \rangle$. As the exponent of X_F divides $p-1$, we may as well replace $\mathfrak{A}$ with $\mathfrak{A}^p$, and ϵ_1 with ϵ_1^p. Therefore, we may as well assume that $\epsilon_1 \in W_F$. Let d be the order of ϵ_1. Then, as $\alpha_1^\rho = \epsilon_1 \alpha_1$, it follows that $a = \alpha_1^d \in F^\times$ and $\mathfrak{A}^{2d} = a\mathcal{O}_F$. We see that the Kummer extension $F(\alpha_1) = F(a^{1/d})$ over F is unramified outside $2d$, and that it is totally ramified at the primes over p as $F(\alpha_1) \subseteq K$. Hence, it follows that $F(\alpha_1) = F$ and $\alpha_1 \in F^\times$. Therefore, $\mathfrak{A}^2$ is a principal ideal of F. □

COROLLARY 4.1. *Under the above setting, if F satisfies (H_p), then the exponent of Cl_F^- divides* 2. *In particular, the relative class number h_F^- is a power of* 2.

PROOF. This follows immediately from Lemmas 2.4 and 4.1. □

PROOF OF THEOREM 1.1 Let $p \geq 5$ and let F be a nonquadratic CM Galois extension satisfying (H_p). Then, by Lemma 3.3 and Corollary 4.1, F coincides with the cyclotomic field $\boldsymbol{Q}(\zeta_m)$ for some *even* integer m and the relative class number h_m^- of $F = \boldsymbol{Q}(\zeta_m)$ is a power of 2. All cyclotomic fields with h_m^- a power of 2 were determined by Masley and Montgomery [**16**] and Horie [**6**]; those with $h_m^- = 1$ by [**16**] and those with $h_m^- > 1$ by [**6**]. There are exactly 33 nonquadratic such ones. The corresponding even integers m are as follows:

$$\begin{aligned} m = {} & 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, \\ & 30, 32, 34, 36, 38, 40, 42, 44, 48, 50, 54, \\ & 56^*, 58^*, 60, 66, 68^*, 70, 78^*, 84, 90, 120^*, 130^*. \end{aligned}$$

Here, for those m with $*$-mark, h_m^- is a nontrivial power of 2. Further, p must satisfy the very strong condition (III) in Lemma 3.3. We observe that each of the above m's is a product of powers of at most three prime numbers. Hence, it follows that

$$\frac{\varphi(m)}{m} \geq \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{3}\right) \cdot \left(1 - \frac{1}{5}\right) = \frac{4}{15}.$$

Therefore, if $p \geq 5$ satisfies (III), then

$$5^{2m/15} \leq 2m + 1.$$

We see that this inequality holds only when $m = 8, 10, 12, 14, 16$. Among these five m, the condition (III) is satisfied for a prime $p \geq 5$ when and only when $m = 12$ and $p = 5$. Now, it remains to show that $F = \boldsymbol{Q}(\zeta_{12})$ satisfies (H_5). Let $K = F(\zeta_5) = \boldsymbol{Q}(\zeta_{60})$, and $G = \mathrm{Gal}(K/F) = (\boldsymbol{Z}/5)^{\times}$. By Lemma 2.3, it suffices to show that $Cl_{K,\pi}^{\mathscr{S}_G} = \{0\}$. Let ρ be a generator of G. Then, as $h_5^- = 1$, we have $\mathscr{S}_G = A_G = \langle 1 + \rho \rangle$ by (2.2). On the other hand, Yusuke Yoshimura calculated that $|Cl_{K,\pi}| = 2$ using KASH. Let c be the unique nontrivial element of $Cl_{K,\pi}$. Then, as $c^{\rho} = c$, it follows that $c^{1+\rho} = c^2 = 1$. Therefore, we obtain $Cl_{K,\pi}^{\mathscr{S}_G} = \{0\}$. □

5. Examples.

At present, no example of a number field F satisfying (H_p) for $p \geq 11$ seems to be given in a literature. In this section, we present an example of F satisfying the condition for $p = 11$ or 13.

EXAMPLE.
(I) The real quadratic field $F = \boldsymbol{Q}(\sqrt{5})$ satisfies (H_{13}).
(II) The cyclic cubic field $F = \boldsymbol{Q}(\cos(2\pi/7))$ satisfies (H_{11}).

To deal with the above two examples simultaneously, we need the following lemma, which is given under very strong assumptions. For a number field F, let $h_F = |Cl_F|$ be the class number of F.

LEMMA 5.1. *Let F be a totally real number field unramified at p. Let $K = F(\zeta_p)$, and N be the intermediate field of K/F such that $[N : F]$ is a power of 2 and $[K : N]$ is odd. Assume that the following conditions are satisfied*:

(i) $p = 1 + 2^e q$ *for some* $e \geq 1$ *and some odd prime number* q.
(ii) *The prime* 2 *remains prime in* $\boldsymbol{Q}(\zeta_q)$.
(iii) $h_K = h_K^- = 2^{q-1}$.
(iv) $h_N = 1$.
(v) $(\mathscr{O}_K/\pi)^{\times} = E_K \bmod \pi$.

Then F satisfies the condition (H_p).

PROOF. Let $G = \mathrm{Gal}(K/F)$. By Lemma 2.3 and the assumption (v), it suffices to show that $Cl_K^{\mathscr{S}_G} = \{0\}$. Let ρ be a generator of G, and let $\mathfrak{n}_G$ be the element in $\boldsymbol{Z}G$ defined in Section 2. As $\mathscr{S}_G \subseteq A_G = \langle \mathfrak{n}_G \rangle$, it suffices to show that $\mathfrak{n}_G$ kills Cl_K. As F is totally real, $J = \sigma_{-1} \in G$ is the complex conjugation of the CM field K. We easily see that

$$(\rho - 1)\mathfrak{n}_G = J - 1.$$

Let $\Delta = \mathrm{Gal}(K/N)$. Let $\boldsymbol{Z}_2$ be the ring of 2-adic integers, and let $\bar{\boldsymbol{Q}}_2$ be an algebraic closure of the 2-adic rationals $\boldsymbol{Q}_2$. By (iii), Cl_K is a module over the group ring $\boldsymbol{Z}_2\Delta$. Let χ be a nontrivial $\bar{\boldsymbol{Q}}_2$-valued character of Δ, and χ_0 the trivial character of Δ. By (i), the order of χ equals the prime q. Let $\boldsymbol{Z}_2[\chi] = \boldsymbol{Z}_2[\zeta_q]$ be the subring of $\bar{\boldsymbol{Q}}_2$ generated by the values of χ over $\boldsymbol{Z}_2$. We regard $\boldsymbol{Z}_2[\chi]$ as a module over $\boldsymbol{Z}_2\Delta$ by letting Δ act via χ. Let $Cl_K(\chi_0)$ be the Δ-invariant part of Cl_K, and let $Cl_K(\chi) = Cl_K \otimes \boldsymbol{Z}_2[\chi]$ be the χ-component of Cl_K where the tensor product is taken over $\boldsymbol{Z}_2\Delta$. By the assumptions (i) and (ii), all nontrivial characters of Δ are conjugate to χ over $\boldsymbol{Q}_2$. Hence, we have a canonical isomorphism

$$Cl_K \cong Cl_K(\chi_0) \oplus Cl_K(\chi)$$

of $\boldsymbol{Z}_2\Delta$-modules. (See Tsuji [**19**, Section 2], for this decomposition.) By the assumption (iv), we have $Cl_K(\chi_0) = \{0\}$ and hence, $Cl_K = Cl_K(\chi)$. Let us determine the structure of $Cl_K(\chi)$ over $\boldsymbol{Z}_2[\chi]$. By (ii), $\boldsymbol{Z}_2[\chi] = \boldsymbol{Z}_2^{\oplus(q-1)}$ as modules over $\boldsymbol{Z}_2$. Therefore, it follows from (iii) that

$$Cl_K = Cl_K^- = Cl_K(\chi) \cong \boldsymbol{Z}_2[\chi]/2$$

as $\boldsymbol{Z}_2\Delta$-modules. Hence, we see that $c^{J-1} = 1$ for all $c \in Cl_K$. Further, noting that $\sigma \in \Delta$ acts on $\boldsymbol{Z}_2[\chi]/2$ via $\chi(\sigma)$-multiplication, we can show that if $c \in Cl_K$ satisfies $c^\sigma = c$ for all $\sigma \in \Delta$, then $c = 1$. Now, let c be an arbitrary element of Cl_K. Then, we see that

$$c^{\mathfrak{n}_G(\rho-1)} = c^{J-1} = 1$$

and hence, $(c^{\mathfrak{n}_G})^\rho = c^{\mathfrak{n}_G}$. This implies that $c^{\mathfrak{n}_G} = 1$. □

PROOF OF EXAMPLES. We begin with a simple remark on units of $k = \boldsymbol{Q}(\zeta_p)$. We see that $(\mathscr{O}_k/\pi)^\times = E_k \bmod \pi$ because the cyclotomic unit

$$\xi_a = 1 + \zeta_p + \cdots + \zeta_p^{a-1}$$

satisfies $\xi_a \equiv a \bmod \pi$ for each $2 \le a \le p-1$. Hence, for any divisor d of $p-1$, there exists a unit ϵ of k such that $\epsilon \bmod \pi$ is of order d.

First, let $p = 13$ and $F = \boldsymbol{Q}(\sqrt{5})$. The assumptions (i) and (ii) are satisfied. We see that (iii) and (iv) are satisfied from the table [**4**, Tafel I] and the computation of van der Linden [**15**]. The group $(\mathscr{O}_F/p)^\times = (\mathscr{O}_K/\pi)^\times$ is cyclic of order $2^3 \cdot 3 \cdot 7$. Let $\epsilon = N_{\boldsymbol{Q}(\zeta_{5p})/K}(1 - \zeta_{5p})$ be a cyclotomic unit of K. Using $\zeta_p \equiv 1 \bmod \pi$, we see that

$$\epsilon \equiv \sqrt{5} \cdot \eta \bmod \pi \quad \text{with} \quad \eta = \frac{\sqrt{5} \pm 1}{2}.$$

We see that $\sqrt{5} \bmod \pi$ (resp. $\eta \bmod \pi$) is of order 8 (resp. 28) by some hand calculation. Hence, $\epsilon \bmod \pi$ is of order $2^3 \cdot 7$. Further, as $3|p-1$, there exists a unit δ in $\boldsymbol{Q}(\zeta_p)$ such that $\delta \bmod \pi$ is of order 3 by the above remark. Therefore, the last condition (v) is satisfied.

Next, let $p = 11$ and $F = \boldsymbol{Q}(\cos(2\pi/7))$. The assumptions (i) and (ii) are satisfied. By [**4**, Tafel I] and [**15**], the assumptions (iii) and (iv) are satisfied. The group $(\mathscr{O}_F/p)^\times = (\mathscr{O}_K/\pi)^\times$ is cyclic of order $2 \cdot 5 \cdot 133$. Using KASH, H. Sumida-Takahashi calculated that $[(\mathscr{O}_F/p)^\times : [E_F]_p] = 5$. On the other hand, as $5|p-1$, there exists a unit η in $\boldsymbol{Q}(\zeta_p)$ such that $\eta \bmod \pi$ is of order 5. Therefore, (v) is satisfied. □

Remark 2. The method for determining the Galois module structure of Cl_K in the proof of Lemma 5.1 is a standard one, which originates from Iwasawa [**14**]. For $K = \boldsymbol{Q}(\sqrt{5}, \zeta_{13})$ (resp. $\boldsymbol{Q}(\cos(2\pi/7), \zeta_{11})$), Horie and Ogura [**7**] have already shown that Cl_K is isomorphic to $(\boldsymbol{Z}/2)^{\oplus(q-1)}$ as an abelian group with $q = 3$ (resp. 5).

Remark 3. A table of relative class numbers of imaginary abelian fields of conductor $f \leq 100$ (resp. $100 < f \leq 200$) is given in [**4**, Tafel I] (resp. Yoshino and Hirabayashi [**23**], [**24**]). Using these tables, we observe that for $p \geq 17$, there exists no real abelian field F for which F and $K = F(\zeta_p)$ satisfy the assumptions of Lemma 5.1 and $f_K \leq 200$. Here, f_K is the conductor of K. And, at present, we have no example of a number field F satisfying (H_p) for $p \geq 17$. Does there exist such a number field F?

Acknowledgements. The author thanks Hiroki Sumida-Takahashi and Yusuke Yoshimura for some KASH calculation. The author also thanks the referee for carefully reading the original manuscript and for several valuable comments on it.

References

[1] J. Brinkhuis, Normal integral bases and complex conjugation, J. Reine Angew. Math., **375/376** (1987), 157–166.
[2] J. E. Carter, Normal integral bases in quadratic and cyclic cubic extensions of quadratic fields, Arch. Math. (Basel), **81** (2003), 266–271: Erratum, *ibid.*, **83** (2004), no. 6, vi–vii.
[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] H. Hasse, Über die Klassenzahl abelscher Zahlkörper, Akademie-Verlag, Berlin, 1952.
[5] T. Herreng, Sur les corps de Hilbert-Speiser, J. Théor. Nombres Bordeaux, **17** (2005), 767–778.

[6] K. Horie, On the class numbers of cyclotomic fields, Manuscripta Math., **65** (1989), 465–477.
[7] K. Horie and H. Ogura, On the ideal class groups of imaginary abelian fields with small conductor, Trans. Amer. Math. Soc., **347** (1995), 2517–2532.
[8] H. Ichimura, Note on the ring of integers of a Kummer extension of prime degree, V, Proc. Japan Acad. Ser. A Math. Sci., **78** (2002), 76–79.
[9] H. Ichimura, Normal integral bases and ray class groups, Acta Arith., **114** (2004), 71–85.
[10] H. Ichimura, Note on imaginary quadratic fields satisfying the Hilbert-Speiser condition at a prime p, Proc. Japan Acad. Ser. A Math. Sci., **83** (2007), 88–91.
[11] H. Ichimura, Note on Hilbert-Speiser number fields at a prime p, Yokohama Math. J., **54** (2007), 45–53.
[12] 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.
[13] H. Ichimura and H. Sumida-Takahashi, On Hilbert-Speiser type imaginary quadratic fields, Acta Arith., **136** (2009), 385–389.
[14] K. Iwasawa, A note on ideal class groups, Nagoya Math. J., **27** (1966), 239–247.
[15] F. van der Linden, Class number computations of real abelian number fields, Math. Comp., **39** (1982), 693–707.
[16] J. M. Masley and H. L. Montgomery, Cyclotomic fields with unique factorization, J. Reine Angew. Math., **286/287** (1976), 248–256.
[17] L. R. McCulloh, Galois module structure of elementary abelian extensions, J. Algebra, **82** (1983), 102–134.
[18] W. Sinnott, On the Stickelberger ideal and the circular units of an abelian field, Invent. Math., **62** (1980/81), 181–234.
[19] T. Tsuji, Semi-local units modulo cyclotomic units, J. Number Theory, **78** (1999), 1–16.
[20] L. C. Washington, Introduction to Cyclotomic Fields (2nd ed.), Springer, New York, 1997.
[21] K. Yamamura, The determination of the imaginary abelian number fields with class number one, Math. Comp., **62** (1994), 899–921.
[22] Y. Yoshimura, Abelian number fields satisfying the Hilbert-Speiser condition at $p = 2$ or 3, Tokyo J. Math., **32** (2009), 229–235.
[23] K. Yoshino and M. Hirabayashi, On the relative class number of the imaginary abelian number fields I, Memoirs of the College of Liberal Arts, Kanazawa Medical University, **9** (1981), 5–53.
[24] K. Yoshino and M. Hirabayashi, On the relative class number of the imaginary abelian number fields II, Memoirs of the College of Liberal Arts, Kanazawa Medical University, **10** (1982), 33–81.

Humio ICHIMURA

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