ACTA ARITHMETICA
136.4 (2009)

On Hilbert–Speiser type imaginary quadratic fields

by

Humio Ichimura (Mito) and Hiroki Sumida-Takahashi (Tokushima)

1. Introduction. 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. By the classical Hilbert–Speiser theorem, the rationals $\mathbb{Q}$ satisfy (H_p) for all p. On the other hand, Greither et al. [3] proved that a number field $F \neq \mathbb{Q}$ does not satisfy (H_p) for infinitely many p using a theorem of McCulloh [8]. Thus, it is of interest which number fields F satisfy (H_p).

In this paper, we deal with imaginary quadratic fields and determine those satisfying (H_p) for each p. When $p = 2, 3, 5, 7$ or 11, all imaginary quadratic fields F satisfying (H_p) were determined in [2, 5, 7]. The number of such F is 3, 4, 2, 1 and 0, respectively. Therefore, it suffices to deal with the case $p \geq 13$. Our result is the following:

Theorem. *For any prime number $p \geq 13$, there exists no imaginary quadratic field satisfying the condition (H_p).*

2. Some known results. In this section, we recall several results which are necessary to prove the Theorem. First, we recall the theorem of McCulloh [8] mentioned in Section 1. Let p be a prime number, and $\Gamma = (\mathbb{Z}/p)^+$ and $G = (\mathbb{Z}/p)^\times$ be the additive group and the multiplicative group of the finite field $\mathbb{Z}/p$, respectively. For a number field F, let $Cl(\mathcal{O}_F\Gamma)$ be the locally free class group of the group ring $\mathcal{O}_F\Gamma$, $\mathcal{O}_F$ being the ring of integers of F, and let $R(\mathcal{O}_F\Gamma)$ be the subset consisting of the locally free classes $[\mathcal{O}_N]$ for all tame Γ extensions N/F. As Γ is an abelian group, F satisfies (H_p) if and only if $R(\mathcal{O}_F\Gamma) = \{0\}$. Let $\mathcal{S}_G$ be the classical Stickelberger ideal of the group ring $\mathbb{Z}G$ associated to the abelian extension $\mathbb{Q}(\zeta_p)/\mathbb{Q}$. For the definition, see [10, Chapter 6]. Through the natural action of G on Γ,

2000 *Mathematics Subject Classification*: 11R33, 11R11.
Key words and phrases: Hilbert–Speiser number field, imaginary quadratic field.

DOI: 10.4064/aa136-4-5

the group ring $\mathbb{Z}G$ acts on $Cl(\mathcal{O}_F\Gamma)$. Then we have

$$R(\mathcal{O}_F\Gamma) = Cl(\mathcal{O}_F\Gamma)^{\mathcal{S}_G}. \tag{1}$$

This theorem of McCulloh plays a crucial role in studying Hilbert–Speiser number fields.

In the following, let F be an imaginary quadratic field, and let χ_F be the associated quadratic character. The following is a consequence of [3, Theorem 1].

LEMMA 1 (cf. [7, Lemma 2]). *Let $p \geq 7$. If F satisfies (H_p), then $\chi_F(p) = 1$.*

We put $K = F(\zeta_p)$ where ζ_p is a primitive pth root of unity. When $\chi_F(p) = 1$, we can identify the Galois group $\mathrm{Gal}(K/F)$ with $G = (\mathbb{Z}/p)^\times$ through the Galois action on ζ_p. Hence, the group ring $\mathbb{Z}G$ acts on several objects associated to K. For a number field N and an integer $\alpha \in \mathcal{O}_N$, let $Cl_{N,\alpha}$ be the ray class group of N defined modulo the principal ideal $\alpha\mathcal{O}_N$. In particular, $Cl_N = Cl_{N,1}$ is the absolute class group of N, and $h_N = |Cl_N|$ is the class number of N. Let $\pi = \zeta_p - 1$. The following is an immediate consequence of (1) combined with [1, Proposition 2.2].

LEMMA 2 (cf. [7, Proposition 5]). *When $\chi_F(p) = 1$, F satisfies (H_p) if and only if $\mathcal{S}_G$ annihilates the ray class group $Cl_{K,\pi}$.*

Using Lemmas 1 and 2, we proved the following assertion in [6].

LEMMA 3. *If F satisfies (H_p), then $h_F = 1$.*

3. Proof of the Theorem. In all the following, let F be an imaginary quadratic field with $\chi_F(p) = 1$ and $h_F = 1$. Let $k = \mathbb{Q}(\zeta_p)$, $K = F \cdot k$ and $K_0 = F \cdot k^+$ where k^+ is the maximal real subfield of k. Let $E_K = \mathcal{O}_K^\times$ be the group of units of K.

LEMMA 4. *In the above setting, assume that F satisfies (H_p). Let $\mathfrak{A}$ be an ideal of K_0 relatively prime to p. Then there exists an element $\alpha \in F^\times$ such that $N_{K_0/F}\mathfrak{A} = \alpha\mathcal{O}_F$ and $\alpha \equiv \varepsilon \bmod \pi$ for some unit $\varepsilon \in E_K$.*

Proof. As $h_F = 1$, we have $N_{K_0/F}\mathfrak{A} = \alpha\mathcal{O}_F$ for some $\alpha \in F^\times$. Let $\sigma_i = \bar{i}$ be the element of $G = \mathrm{Gal}(K/F) = (\mathbb{Z}/p)^\times$ corresponding to an integer $i \in \mathbb{Z}$ with $p \nmid i$. Put

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

which belongs to the Stickelberger ideal $\mathcal{S}_G$ (see [10, p. 376]). Noting that θ_2 acts on $K_0^\times$ as the norm $N_{K_0/F}$, we see from Lemma 2 that the ray class

$[N_{K_0/F}\mathfrak{A}\cdot\mathcal{O}_K]=[\alpha\mathcal{O}_K]$ in $Cl_{K,\pi}$ is trivial. Therefore, $\alpha\equiv\varepsilon \bmod \pi$ for some unit $\varepsilon\in E_K$. ∎

As $\chi_F(p)=1$, $(\mathcal{O}_F/p)^\times$ is isomorphic to $(\mathbb{Z}/p)^\times\times(\mathbb{Z}/p)^\times$ as an abelian group. For $\alpha\in F^\times$ with $(\alpha,p)=1$, let $[\alpha]_p\in(\mathcal{O}_F/p)^\times$ be the class containing α. Let H_F be the subgroup of $(\mathcal{O}_F/p)^\times$ generated by the classes $[\alpha]_p$ for all $\alpha\in F^\times$ such that $\alpha\mathcal{O}_F=N_{K_0/F}\mathfrak{A}$ for some ideal $\mathfrak{A}$ of K_0 relatively prime to p. Let J be the complex conjugation of K. For brevity, we write $J=J_{|F}$. As $h_F=1$, the reciprocity law map induces an isomorphism

$$(\mathcal{O}_F/p)^\times/H_F\cong \mathrm{Gal}(K_0/F)$$

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

$$((\mathcal{O}_F/p)^\times)^{J-1}\subseteq H_F. \tag{2}$$

For a number field N, let W_N be the group of roots of unity in N.

LEMMA 5. *Assume that F satisfies (H_p). Then, for any $\alpha\in F^\times$ with $(\alpha,p)=1$, there exists $\eta\in W_F$ such that $\alpha^{(J-1)^2}\equiv\eta \bmod p$.*

Proof. Let $\alpha\in F^\times$ with $(\alpha,p)=1$. By (2) and Lemma 4, $\alpha^{J-1}\equiv \varepsilon \bmod \pi$ for some unit $\varepsilon\in E_K$. We see that $\varepsilon^{J-1}\in W_K$ by a theorem on units of a CM field ([10, Theorem 4.12]). As F is an imaginary quadratic field, we have $W_K=W_F\cdot\langle\zeta_p\rangle$, and hence $\eta=\varepsilon^{(J-1)p}\in W_F$. From this, we obtain

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

However, as $F/\mathbb{Q}$ is unramified at p, this congruence also holds modulo p. ∎

Proof of the Theorem. Write $p=1+2^en$ for some $e\ge 1$ and n odd. Let X be the set of elements of $(\mathcal{O}_F/p)^\times$ whose orders are odd. Let X^- be the (-1)-eigenspace of X under the action of J:

$$X^-=X^{J-1}=X^{(J-1)^2}.$$

Clearly, X^- is a cyclic group of order n. When $F\neq\mathbb{Q}(\sqrt{-3})$, we see from Lemma 5 that $\alpha^{4(J-1)^2}\equiv 1 \bmod p$ for all $\alpha\in F^\times$ relatively prime to p, because the order $|W_F|$ divides 4. This implies that $n=1$. Similarly, when $F=\mathbb{Q}(\sqrt{-3})$, we see that $n=1$ or 3. Therefore, $p=1+2^e$ or $p=1+2^e\cdot 3$, and the latter can only happen when $F=\mathbb{Q}(\sqrt{-3})$. Noting that $\chi_F(p)=1$, let $\wp_1$ and $\wp_2$ be the prime ideals of F over p. Let $a\in\mathbb{Z}$ have order 2^e modulo p. Choose $\alpha\in\mathcal{O}_F$ such that $\alpha\equiv a \bmod \wp_1$ and $\alpha\equiv 1 \bmod \wp_2$. We easily see that $\alpha^{(J-1)^2}\equiv a^2 \bmod \wp_1$. Then Lemma 5 yields $a^8\equiv 1 \bmod p$, which implies that $e\le 3$. Therefore, $p=3,5,7$ or 13. The last two cases can only occur when $F=\mathbb{Q}(\sqrt{-3})$. Since the imaginary quadratic fields F satisfying (H_p) for $p\le 11$ were already determined, we finish the proof of the Theorem by the following lemma. ∎

LEMMA 6. *The field* $F = \mathbb{Q}(\sqrt{-3})$ *does not satisfy* (H_{13}).

Proof. Let $p = 13$. For any imaginary abelian field M, let C_M be the group of circular units of M in the sense of Sinnott [9, p. 119]. The group C_K is generated by C_k, ζ_3 and $1-(\zeta_3\zeta_p)^c$ for integers c with $(c, 3p) = 1$. For $\alpha \in K^\times$ with $(\alpha, p) = 1$, let $[\alpha]_\pi$ be the class in $(\mathcal{O}_K/\pi)^\times$ containing α. For any subgroup E of E_K, let $[E]_\pi$ be the subgroup of $(\mathcal{O}_K/\pi)^\times$ generated by the classes containing an element of E. Since $\zeta_p \equiv 1 \bmod \pi$, the group $[C_K]_\pi$ is generated by $[\zeta_3]_\pi$, $[\sqrt{-3}]_\pi$ and $[a]_\pi$ for integers a with $1 \le a \le p-1$. Hence,

$$[(\mathcal{O}_K/\pi)^\times : [C_K]_\pi] = 2.$$

Let N be the intermediate field of K/F with $[N : F] = 4$. We have $h_K = h_N = 2$ and $h_K^+ = h_N^+ = 1$. For this, see [4, Tafel II] and [10, p. 421]. We see that $[E_K : C_K] = h_K^+ = 1$ by the analytic class number formula [9, Theorem] combined with the formula (4.1) of [9]. Hence,

$$[(\mathcal{O}_K/\pi)^\times : [E_K]_\pi] = 2. \tag{3}$$

Let $\mathfrak{P}_1$ and $\mathfrak{P}_2$ be the prime ideals of K over p, and let $\wp_i = \mathfrak{P}_i \cap \mathcal{O}_N$. As K/F is totally ramified at $\mathfrak{P}_i$, we naturally have

$$(\mathcal{O}_K/\pi)^\times = (\mathcal{O}_N/\wp_1\wp_2)^\times.$$

Now, assume that F satisfies (H_p). Then the Stickelberger ideal $\mathcal{S}_G$ annihilates $Cl_{K,\pi}$ by Lemma 2. As the norm map $Cl_K \to Cl_N$ is surjective, the element $\theta_2 \in \mathcal{S}_G$ kills Cl_N. Let $\mathfrak{A}$ be an ideal of N relatively prime to p such that the ideal class $[\mathfrak{A}] \in Cl_N$ is of order 2. Then $\mathfrak{A}^{\theta_2} = \alpha\mathcal{O}_N$ for some $\alpha \in N^\times$. The element α satisfies $[\alpha]_\pi \in [E_K]_\pi$ as $Cl_{K,\pi}^{\theta_2} = \{0\}$. Choosing an ideal $\mathfrak{A}$, we checked by a KASH calculation that the subgroup of $(\mathcal{O}_N/\wp_1\wp_2)^\times$ generated by the classes containing α and units of N is of index 3. However, as $[\alpha]_\pi \in [E_K]_\pi$, this contradicts (3). ∎

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 cubic cyclic 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*, Academie-Verlag, Berlin, 1952.

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

[6] —, *Note on imaginary quadratic fields satisfying the Hilbert–Speiser condition at a prime p*, Proc. Japan Acad. 83A (2007), 88–91.

[7] 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.
[8] L. R. McCulloh, *Galois module structure of elementary abelian extensions*, J. Algebra 82 (1983), 102–134.
[9] W. Sinnott, *On the Stickelberger ideal and the circular units of a cyclotomic field*, Ann. of Math. 108 (1978), 107–134.
[10] L. C. Washington, *Introduction to Cyclotomic Fields*, 2nd ed., Springer, New York, 1997.

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

Faculty and School of Engineering
The University of Tokushima
2-1, Minami-josanjima-cho
Tokushima, 770-8506, Japan
E-mail: hiroki@pm.tokushima-u.ac.jp

Received on 25.8.2008 (5783)