Note on imaginary quadratic fields satisfying the Hilbert-Speiser condition at a prime 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., June 12, 2007)

Abstract: Let p be a prime number. A number field F satisfies the condition (H_p) when any tame cyclic extention N/F of degree p has a normal integral basis. For the case $p = 2$, it is shown by Mann that F satisfies (H_2) only when $h_F = 1$ where h_F is the class number of F. We prove that if an imaginary quadratic field F satisfies (H_p) for some p, then $h_F = 1$.

Key words: Hilbert-Speiser number field; imaginary quadratic field.

1. Introduction. 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 (NIB for short). The classical theorem of Hilbert and Speiser asserts that the rationals $\boldsymbol{Q}$ satisfy (H_p) for all prime numbers p. On the other hand, Greither *et al.* [3] recently proved that a number field $F \neq \boldsymbol{Q}$ does not satisfy (H_p) for infinitely many primes p. Thus, it is of interest to determine which number field F satisfies (H_p) or not. In [1, 5, 8], all imaginary quadratic fields F satisfying (H_p) were determined for $p = 2$, 3, 5, 7 and 11. It turned out that all of them satisfy $h_F = 1$. Here, h_F is the class number of F. One naturally asks "can there exist a number field F satisfying (H_p) but $h_F > 1$?" For the case $p = 2$, it is already shown by Mann [9] that if a number field F satisfies (H_2), then $h_F = 1$. More precisely, it is known that F satisfies (H_2) if and only if the ray class group of F defined modulo 2 is trivial [4]. In this note, we give an answer to the above question when F is an imaginary quadratic field.

Theorem. *Let p be a prime number. If an imaginary quadratic field F satisfies the condition (H_p), then $h_F = 1$.*

It is a well known result of Stark [12] that there are exactly nine imaginary quadratic fields F with $h_F = 1$. Hence, we obtain the following

Corollary. *For each prime number p, there exist at most nine imaginary quadratic fields satisfying (H_p).*

2. Proof of Theorem. In view of the result of Mann cited in Section 1, it suffices to deal with the case where p is odd. Let p be a *fixed* odd prime number, and $G = \boldsymbol{F}_p^{\times}$ the multiplicative group of the finite field $\boldsymbol{F}_p$ of p elements. For an integer $i \in \boldsymbol{Z}$ with $p \nmid i$, let σ_i be the corresponding element of $G = \boldsymbol{F}_p^{\times}$. Let $\mathcal{S}_G$ be the classical Stickelberger ideal of the group ring $\boldsymbol{Z}[G]$. Let

$$\theta = \sum_{i=1}^{p-1} \frac{i}{p}\sigma_i^{-1} \in \boldsymbol{Q}[G]$$

be the Stickelberger element of conductor p. It is known that the ideal $\mathcal{S}_G$ is generated over $\boldsymbol{Z}$ by Stickelberger elements

$$(1) \qquad \theta_r = (r - \sigma_r)\theta = \sum_{i=1}^{p-1} \left[\frac{ri}{p}\right] \sigma_i^{-1} \in \boldsymbol{Z}[G]$$

for all $r \in \boldsymbol{Z}$ with $p \nmid r$ (cf. Washington [13, Lemma 6.9]). Here, for a real number x, $[x]$ is the largest integer $\leq x$.

Let F be a number field, and put $K = F(\zeta_p)$ where ζ_p is a primitive p-th root of unity. When $F/\boldsymbol{Q}$ is unramified at p, the Galois group $\mathrm{Gal}(K/F)$ is identified with G through the Galois action on ζ_p. Hence, the group ring $\boldsymbol{Z}[G]$ acts on the ideal class group Cl_K of K. The following is a consequence of a theorem of McCulloh [10].

Lemma 1 ([6, Theorems 5, 6], [8, Propositions 3, 4]). *Assume that $F/\boldsymbol{Q}$ is unramified at p. Then, F satisfies the condition (H_p) only when $\mathcal{S}_G$ annihilates the class group Cl_K and the natural map $Cl_F \to Cl_K$ is trivial.*

In all what follows, let F be an imaginary quadratic field, and put $K = F(\zeta_p)$. The follow-

2000 Mathematics Subject Classiffcation. 11R33, 11R11.

ing lemma is an immediate consequence of [3, Theorem 1]. See also Replogle [11, Theorem 4.3(c)] for a "quantitative" version.

Lemma 2 ([8, Lemma 1])**.** *When $F/\boldsymbol{Q}$ is ramified at p, F satisfies (H_p) if and only if $p=3$ and $F=\boldsymbol{Q}(\sqrt{-3})$.*

In view of this lemma, we may and shall assume that $F/\boldsymbol{Q}$ is unramified at p in the following. Hence, $\mathrm{Gal}(K/F)$ is identified with $G=\boldsymbol{F}_p^{\times}$. We fix a generator ρ of the Galois group G.

Lemma 3 ([8, Lemma 3])**.** *If F satisfies (H_p), then the exponent of Cl_F divides 2.*

Lemma 4 ([8, Lemma 5])**.** *Let p be a prime number with $p\equiv 3 \bmod 4$, and let $E=F(\sqrt{-p})$. If F satisfies the condition (H_p), then the natural map $Cl_F\to Cl_E$ is trivial.*

Proof. We give a proof for a comparison with the case $p\equiv 1 \bmod 4$ (Lemma 7). Let $\mathfrak{A}$ be an ideal of F. By Lemma 1, $\mathfrak{A}\mathcal{O}_K=\alpha\mathcal{O}_K$ for some $\alpha\in K^{\times}$. Hence, it follows that $\mathfrak{A}^{[K:E]}\mathcal{O}_E=\beta\mathcal{O}_E$ with $\beta=N_{K/E}\alpha$. This implies that $\mathfrak{A}\mathcal{O}_E$ is principal since $[K:E]=(p-1)/2$ is odd and $\mathfrak{A}^2$ is principal by Lemma 3. $\square$

Lemma 5. *Under the setting of Lemma 4, assume that $p\geq 7$ and that there exists a prime number q satisfying*

$$q \mid h_E,\quad q\nmid h_k,\quad q\nmid (p-1)/2$$

where $k=\boldsymbol{Q}(\sqrt{-p})$. Then, F does not satisfy (H_p).

Proof. Let $E=F(\sqrt{-p})=F\cdot k$, and let $H=\mathrm{Gal}(K/E)\subseteq G$. Assuming the existence of a prime number q satisfying the conditions, let c be a class in Cl_E of order q. As $q\nmid (p-1)/2$, the lift $\bar{c}$ of c to K is of order q. Assume that F satisfies (H_p). Then, by Lemma 4, the class $c^{1+\rho}=1$ in Cl_E, and hence

$$\bar{c}^{\rho}=\bar{c}^{-1} \tag{2}$$

where ρ is a generator of G. For an integer $r\in\boldsymbol{Z}$, write $\theta_r=x+y\rho$ for some $x,\ y\in\boldsymbol{Z}[H]$. Letting $\iota_H:\boldsymbol{Z}[H]\to\boldsymbol{Z}$ be the augmentation, put $a=\iota_H(x)$ and $b=\iota_H(y)$. As F satisfies (H_p), it follows from Lemma 1 that $\bar{c}^{\theta_r}=1$. Hence, we see from (2) that

$$\bar{c}^{a-b}=1. \tag{3}$$

Let ψ be the quadratic character of conductor p. Then, we see from (1) that

$$a-b=\psi(\theta_r)=(r-\psi(r))\cdot B_{1,\psi}$$

where $B_{1,\psi}$ is the first Bernoulli number. As $p\equiv 3 \bmod 4$, ψ is an odd character and $h_k=-B_{1,\psi}$ by the analytic class number formula ([13, Theorem 4.17]). Hence, it follows that

$$a-b=(\psi(r)-r)\cdot h_k.$$

Noting that $p\geq 7$, we see that the ideal of $\boldsymbol{Z}$ generated by $\psi(r)-r$ for all r with $p\nmid r$ equals $\boldsymbol{Z}$. Therefore, the relation (3) implies $\bar{c}^{h_k}=1$. This is impossible as $\bar{c}$ is of order q and $q\nmid h_k$. $\square$

Proof of Theorem for the case $p\equiv 3 \bmod 4$. We use the same notation as in Lemma 5. Let F be an imaginary quadratic field satisfying (H_p). We may as well assume that $p\geq 7$ since the assertion holds when $p=3$. Assume that $h_F\neq 1$. Then, $2 \mid h_F$ by Lemma 3. As E/F is totally ramified at p, it follows that $2 \mid h_E$. It is well known that h_k is odd by genus theory. Hence, the prime $q=2$ satisfies the conditions in Lemma 5. Therefore, F does not satisfy (H_p), a contradiction. $\square$

In all what follows, let p be a prime number with $p\equiv 1 \bmod 4$, and let 2^{e+1} be the highest power of 2 dividing $p-1$. Let k be the intermediate field of $\boldsymbol{Q}(\zeta_p)/\boldsymbol{Q}$ with $[k:\boldsymbol{Q}]=2^e$. Clearly, k is totally real. Let $F=\boldsymbol{Q}(\sqrt{-d})$ be an imaginary quadratic field unramified at p, where d is a square free positive integer with $p\nmid d$. Put

$$E=F\cdot k\subseteq K\quad\text{and}\quad H=\mathrm{Gal}(K/E)\subseteq G.$$

To show Theorem, we may as well assume that $d\neq 1,\ 3$.

Lemma 6. *Under the above setting, we have $\mathcal{O}_E^{\times}=\mathcal{O}_k^{\times}$.*

Proof. Let W be the group of roots of unity in E. As $d\neq 1,\ 3$, we have $W=\{\pm 1\}$. Hence, it suffices to show that the unit index Q_E of E equals 1. Let J be the complex conjugation of E. As is well known, $\epsilon/\epsilon^J\in W$ for any unit $\epsilon\in\mathcal{O}_E^{\times}$ (cf. [13, Lemma 1.6]). Consider the homomorphism

$$\varphi:\mathcal{O}_E^{\times}\to W=W/W^2,\ \epsilon\to\epsilon/\epsilon^J.$$

It is known that $Q_E=1$ if and only if the map φ is trivial (cf. [13, page 40]). Assume to the contrary that φ is nontrivial. Then, $\epsilon^J=-\epsilon$ for some $\epsilon\in\mathcal{O}_E^{\times}$. It follows from Kummer theory that $\epsilon=x\sqrt{-d}$ for some $x\in k^{\times}$ since $E=k(\sqrt{-d})$ and k is the maximal real subfield of E. However, this is impossible since $p\nmid d$ and a prime q dividing d is unramified at k. $\square$

Lemma 7. *Under the above setting, F satisfies (H_p) only when the natural map $Cl_F\to Cl_E$ is trivial.*

Proof. Assume that F satisfies (H_p). By Lemma 1, any ideal class $c \in Cl_K$ satisfies $c^{\theta_2} = 1$. As the norm map $Cl_K \to Cl_E$ is surjective, any ideal class $c \in Cl_E$ satisfies the same relation. We write

$$(4) \qquad \theta_2 = \sum_{i=0}^{2^e-1} x_i \rho^i$$

for some $x_i \in \boldsymbol{Z}[H]$ where ρ is a generator of G. Let $a_i = \iota_H(x_i)$ where ι_H is the augmentation of $\boldsymbol{Z}[H]$. Then, it follows that

$$(5) \qquad c^A = 1 \quad \text{with} \quad A = \sum_{i=0}^{2^e-1} a_i \rho^i$$

for any $c \in Cl_E$. By (1), we easily see that

$$(6) \qquad \sum_{i=0}^{2^e-1} a_i = \sum_{j=0}^{p-1} \left[\frac{2j}{p}\right] = \frac{p-1}{2}.$$

Let ψ be a character of G of order 2^e. Then, ψ is even, and any nontrivial character of G of order dividing 2^e is of the form ψ^j with $1 \le j \le 2^e - 1$. These characters are regarded as those of the Galois group $\mathrm{Gal}(E/F) = G/H$. Let $\zeta = \psi(\rho)$ be a primitive 2^e-th root of unity. We see from (1) that

$$\psi^j(\theta_2) = (2 - \psi^j(2)) \cdot B_{1,\psi^{-j}}$$

where $B_{1,\psi^{-j}}$ is the first Bernoulli number. However, as ψ^j is nontrivial and even, we have $B_{1,\psi^{-j}} = 0$. Hence, it follows from (4) that

$$(7) \quad \psi^j(\theta_2) = \sum_{i=0}^{2^e-1} a_i \zeta^{ij} = 0 \quad \text{for } 1 \le j \le 2^e - 1.$$

From (6) and (7), we obtain

$$a_i = \frac{p-1}{2^{e+1}} \quad (0 \le i \le 2^e - 1).$$

Therefore, by (5), any ideal class $c \in Cl_E$ satisfies the relation

$$(c^{1+\rho+\cdots+\rho^{2^e-1}})^{a_0} = 1.$$

By Lemma 3, the order of the class $N_{E/F}(c) \in Cl_F$ divides 2. Therefore, as a_0 is odd, it follows that

$$c^{1+\rho+\cdots+\rho^{2^e-1}} = 1$$

for all $c \in Cl_E$. As the norm map $Cl_E \to Cl_F$ is surjectve, this implies that the map $Cl_F \to Cl_E$ is trivial. □

Proof of Theorem for the case $p \equiv 1 \bmod 4$. Assume that F satisfies the condition (H_p). Let $-D$ be the discriminant of F. Let us show the following

Claim. For a prime number q dividing D, we have $D/q = a^2$ for some integer $a \in \boldsymbol{Z}$.

Actually: Let q be a prime number dividing D, and let $\mathfrak{Q}$ be the prime ideal of F over q; $q\mathcal{O}_F = \mathfrak{Q}^2$. By Lemma 7, $\mathfrak{Q}\mathcal{O}_E = x\mathcal{O}_E$ for some $x \in E^\times$. Because of Lemma 6, this implies that $q = \epsilon x^2$ for some unit $\epsilon \in \mathcal{O}_k^\times$. Noting that $E = k(\sqrt{-D})$, we see from Kummer theory that $q = \epsilon y^2$ or $q = \epsilon(-D)y^2$ for some $y \in k^\times$. However, the first equality can not hold since $k/\boldsymbol{Q}$ is unramified outside p and $p \nmid D$. It follows from the second equality that D/q is a square in $\boldsymbol{Q}^\times$ by the same reason.

By the Claim, there are only two possibilities for $-D$ according to whether D is even or odd:

$$\text{(i)} - D = -8, \quad \text{(ii)} - D = -\lambda.$$

Here, λ is a prime number with $\lambda \equiv 3 \bmod 4$. When $-D = -8$, we have $h_F = 1$. When $-D = -\lambda$, it is known that h_F is odd by genus theory. This implies $h_F = 1$ since h_F is a 2-power by Lemma 3. □

Remark 1. It is known that if a prime number $p \ge 7$ remains prime in an imaginary quadratic field F, then F does not satisfy (H_p) ([8, Lemma 2], [11, Theorem 4.3(a)]). Therefore, we see from Theorem that there exist infinitely many primes p for which no imaginary quadratic field satisfies (H_p).

Remark 2. An assertion similar to Lemma 1 holds also when $F/\boldsymbol{Q}$ is ramified at p ([6, Theorem 5]).

Remark 3. Let us say that a number field F satisfies the condition $(H_{p,\infty})$ when any tame abelian extension N/F of exponent p has a NIB. When $p = 2$, it is known that F satisfies $(H_{2,\infty})$ if and only if the ray class group $Cl_F(4)$ of F defined modulo 4 is trivial ([4, Proposition 3]). As $Cl_F(4)$ is trivial only when F is totally real ([7, Lemma 4]), there exists no imaginary quadratic field satisfying $(H_{2,\infty})$.

For an odd prime number p and an imaginary quadratic field F with $(p, F) \neq (3, \boldsymbol{Q}(\sqrt{-3}))$, we can show that F satisfies $(H_{p,\infty})$ if and only if it satisfies (H_p), as follows. Let F be an imaginary quadratic field satisfying (H_p), and let N/F be a tame abelian extension of exponent p. By Theorem and $(p, F) \neq (3, \boldsymbol{Q}(\sqrt{-3}))$, p does not divide $h_F \times |\mathcal{O}_F^\times|$. Then, we see from class field theory that N is contained in the composite $M = \prod_i N_i$ of some tame cyclic extensions N_i/F of degree p whose conductors are prime ideals of F different from each other. As $h_F = 1$, the extensions N_i/F are linearly disjoint. Therefore, since each N_i/F has a NIB, the composite M has a NIB by a classical theorem on rings of integers (cf. [2, (2.13)]). Hence, N/F has a NIB as $N \subseteq M$. The author thanks to an anonymous mathematician for pointing out this argument. Formerly, the author showed this assertion for the case $p = 3$ using complicated Kummer theory argument.

Let $p = 3$ and $F = \boldsymbol{Q}(\sqrt{-3})$. We can show that F does not satisfy $(H_{3,\infty})$. Actually, let $\mathfrak{G}$ be a copy of two cyclic groups of order p. Let $Cl(\mathcal{O}_F[\mathfrak{G}])$ be the locally free class group of the group ring $\mathcal{O}_F[\mathfrak{G}]$, and $R(\mathcal{O}_F[\mathfrak{G}])$ the subset of the locally free classes $[\mathcal{O}_N]$ for all tame $\mathfrak{G}$-Galois extensions N/F. Using the main theorem in [10], we can show that $R(\mathcal{O}_F[\mathfrak{G}]) \neq \{0\}$ by some hard hand-calculation. This implies that there exists a tame $\mathfrak{G}$-Galois extension N/F without NIB.

Acknowledgements. 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 quadratic fields, Arch. Math. (Basel) **81** (2003), no. 3, 266–271: Erratum, *ibid.*, **83** (2004), no.6, vi-vii.

[2] A. Fröhlich and M. J. Taylor, *Algebraic number theory*, Cambridge Univ. Press, Cambridge, 1993.

[3] C. Greither *et al.*, Swan modules and Hilbert-Speiser number fields, J. Number Theory **79** (1999), no. 1, 164–173.

[4] 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), no. 6, 76–79.

[5] H. Ichimura, Normal integral bases and ray class groups, Acta Arith. **114** (2004), no. 1, 71–85.

[6] H. Ichimura, Normal integral bases and ray class groups. II, Yokohama Math. J. **53** (2006), no. 1, 75–81.

[7] H. Ichimura and F. Kawamoto, Normal integral basis and ray class group modulo 4, Proc. Japan Acad. Ser. A Math. Sci. **79** (2003), no. 9, 139–141.

[8] 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.

[9] H. B. Mann, On integral bases, Proc. Amer. Math. Soc. **9** (1958), 167–172.

[10] L. R. McCulloh, Galois module structure of elementary abelian extensions, J. Algebra **82** (1983), no. 1, 102–134.

[11] D. R. Replogle, Kernel groups and nontrivial Galois module structure of imaginary quadratic fields, Rocky Mountain J. Math. **34** (2004), no. 1, 309–320.

[12] H. M. Stark, A complete determination of the complex quadratic fields of class-number one, Michigan Math. J. **14** (1967), 1–27.

[13] L. C. Washington, *Introduction to cyclotomic fields*, Second edition, Springer, New York, 1997.