Imaginary quadratic fields satisfying the Hilbert-Speiser type condition for a small prime p [*]

Humio Ichimura and Hiroki Sumida-Takahashi

Abstract

Let p be a prime number. A number field F satisfies the condition (A_p) when any tame cyclic extension N/F of degree p has a normal integral basis. By Hilbert and Speiser, the rationals $\boldsymbol{Q}$ satisfy (A_p) for all primes p. Greither *et al* proved that $F \neq \boldsymbol{Q}$ does not satisfy (A_p) for infinitely many primes p. It is of interest to determine which number field satisfies (A_p). The imaginary quadratic fields F satisfying (A_2) were determined by Carter. Those satisfying (A_3) were determined by Carter and the first author independently. In this paper, we determine the imaginary quadratic fields F satisfying (A_p) for $p = 5$, 7 or 11.

1 Introduction

Let p be a prime number, and $\Gamma = \Gamma_p$ the cyclic group of order p ; $\Gamma = \boldsymbol{F}_p^+$, where $\boldsymbol{F}_p^+$ is the additive group of the finite field $\boldsymbol{F}_p$ of p elements. We say that a number field F satisfies the condition (A_p) when for any tame Γ-extension N/F, $\mathcal{O}_N$ is cyclic over the group ring $\mathcal{O}_F\Gamma$. Here, $\mathcal{O}_F$ is the ring of integers of F. It is well known by Hilbert and Speiser that the rationals $\boldsymbol{Q}$ satisfy (A_p) for all primes p. In [6, Theorem 1], Greither *et al* gave a necessary condition for a number field F to satisfy (A_p) in terms of (a subgroup of) the ray class group of F defined modulo p, using a theorem of McCulloh [20, 21]. Applying the condition, they proved that $F \neq \boldsymbol{Q}$ does not satisfy (A_p) for infinitely many primes p ([6, Theorem 2]). Thus,

[*] 2000 Mathematics Subject Classification: 11R33, 11R11.

it is of interest to determine which number field F satisfies (A_p). Several authors [3, 4, 11, 12, 13] obtained some results on the problem using the condition (and some other results such as a theorem of Gómez Ayala [5, Theorem 2.1]). For instance, it was shown by Carter [3, Corollary 3] that an imaginary quadratic field $F = \boldsymbol{Q}(\sqrt{-d})$ with $d > 0$ square free satisfies (A_2) if and only if $d = 1$, 3 or 7. Further, all quadratic fields satisfying (A_3) were determined independently in [3, Corollary 5] and [12, Proposition]. There are exactly four imaginary and eight real ones satisfying (A_3). The purpose of this paper is to determine all imaginary quadratic fields satisfying (A_p) for $p = 5$, 7 or 11. The result is as follows:

Theorem 1 *An imaginary quadratic field $F = \boldsymbol{Q}(\sqrt{-d})$ with a square free positive integer d satisfies the condition (A_5) if and only if $d = 1$ or 3. It satisfies (A_7) if and only if $d = 3$. No imaginary quadratic field satisfies (A_{11}).*

As in [6], the above mentioned theorem of McCulloh plays an important role for proving Theorem 1. In Section 2, we recall McCulloh's theorem and its several consequences including the above mentioned condition for (A_p) in [6]. In Section 3, we give some conditions for an imaginary quadratic field to satisfy (A_p) and prove Theorem 1. In Section 4, we review some topics on subfields of the p-cyclotomic field $\boldsymbol{Q}(\zeta_p)$ satisfying (A_p).

2 Consequences of McCulloh's theorem

In this section, we recall a theorem of McCulloh [20, 21] and its several consequences. Let F be a number field. For an integer $a \in \mathcal{O}_F$, let $Cl_F(a)$ be the ray class group of F defined modulo the ideal $a\mathcal{O}_F$. We simply write $Cl_F = Cl_F(1)$, the absolute class group 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 from the augmentation $\mathcal{O}_F\Gamma \to \mathcal{O}_F$. The class group $Cl^0(\mathcal{O}_F\Gamma)$ is known to be a quotient of some copies of the ray class group $Cl_{F(\zeta_p)}(p)$, but it is a quite difficult object in general. Let $R(\mathcal{O}_F\Gamma)$ be the subset of $Cl(\mathcal{O}_F\Gamma)$ consisting of locally free classes $[\mathcal{O}_N]$ for all tame Γ-extensions N/F. It follows that F satisfies (A_p) if and only if $R(\mathcal{O}_F\Gamma) = \{0\}$. It is known that $R(\mathcal{O}_F\Gamma) \subseteq Cl^0(\mathcal{O}_F\Gamma)$. Let $G = \boldsymbol{F}_p^\times$ be the multiplicative group of $\boldsymbol{F}_p$. Through the natural action of G on $\Gamma = \boldsymbol{F}_p^+$, the group ring $\boldsymbol{Z}G$ acts on $Cl(\mathcal{O}_F\Gamma)$. Let $\mathcal{S}_G$ be the classical Stickelberger ideal of the group ring $\boldsymbol{Z}G$. For the definition, see Washington [26, Chapter 6].

Theorem 2 ([21]). *Under the above setting, we have*

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

Let $\mathcal{O}_F^\times$ be the group of units of a number field F. For an integer $a \in \mathcal{O}_F$, let $[\mathcal{O}_F^\times]_a$ be the subgroup of the multiplicative group $(\mathcal{O}_F/a)^\times$ consisting of classes containing a unit of F. The quotient $(\mathcal{O}_F/a)^\times/[\mathcal{O}_F^\times]_a$ is a subgroup of the ray class group $Cl_F(a)$. Greither *et al* [6] proved the following relation between the condition (A_p) and $Cl_F(p)$ from Theorem 2 studying a canonical subgroup of $Cl(\mathcal{O}_F\Gamma)$, called the Swan subgroup.

Proposition 1 ([6, Theorem 1]). *Assume that a number field F satisfies the condition (A_p). Then, the exponent of the quotient $(\mathcal{O}_F/p)^\times/[\mathcal{O}_F^\times]_p$ divides $(p-1)^2/2$ when $p \geq 3$, and $(\mathcal{O}_F/p)^\times = [\mathcal{O}_F^\times]_p$ when $p = 2$.*

The following is obtained from Proposition 1 and [5, Theorem 2.1].

Proposition 2 ([11, Proposition 2]). *A number field F satisfies the condition (A_2) if and only if the ray class group $Cl_F(2)$ is trivial.*

Similar conditions for (A_2) are given also in [3, Theorem 2] and in Herreng [9, Theorem 2.1]. In view of Proposition 2, we let $p \geq 3$ in the following. To give another consequence of Theorem 2, we need to recall a "Stickelberger ideal" associated to a subgroup of G. Let H be a subgroup of G. For an element $\alpha \in \boldsymbol{Z}G$, let

$$\alpha_H = \sum_{\sigma \in H} a_\sigma \sigma \in \boldsymbol{Z}H \quad \text{with} \quad \alpha = \sum_{\sigma \in G} a_\sigma \sigma.$$

In other words, α_H is a H-part of α. In [14], we defined a Stickelberger ideal $\mathcal{S}_H$ of $\boldsymbol{Z}H$ by

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

Several properties of the ideal $\mathcal{S}_H$ are studied in [14, 15, 17, 18]. For an integer $i \in \boldsymbol{Z}$, let $\bar{i}$ be the class in $\boldsymbol{F}_p = \boldsymbol{Z}/p$ containing i. It is known that the ideal $\mathcal{S}_H$ is generated over $\boldsymbol{Z}$ by Stickelberger elements

$$\theta_{H,r} = {\sum_i}' \left[\frac{ri}{p}\right] \cdot \bar{i}^{-1} \in \boldsymbol{Z}H \tag{1}$$

for all integers $r \in \boldsymbol{Z}$. Here, i runs over the integers with $1 \leq i \leq p-1$ and $\bar{i} \in H$, and for a real number x, $[x]$ is the largest integer $\leq x$. Let N_H be the norm element of $\boldsymbol{Z}H$. It follows that

$$N_H = -\theta_{H,-1} \in \mathcal{S}_H.$$

Letting ρ be a generator of H, put

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

As is easily seen, the ideal $\langle \mathfrak{n}_H \rangle = \mathfrak{n}_H \boldsymbol{Z}H$ does not depend on the choice of ρ. It is known that $\mathcal{S}_H \subseteq \langle \mathfrak{n}_H \rangle$ ([18, Lemma 1]) and 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^- of the p-cyclotomic field $\boldsymbol{Q}(\zeta_p)$ ([18, Theorem 2]) :

$$[\langle \mathfrak{n}_H \rangle : \mathcal{S}_H] \mid h_p^-. \qquad (2)$$

Let F be a number field, and $K = F(\zeta_p)$. We naturally identify the Galois group $\mathrm{Gal}(K/F)$ with a subgroup H of G through the Galois action on ζ_p. Then, the group ring $\boldsymbol{Z}H$ acts on several objects associated to K/F. Let $\pi = \zeta_p - 1$. The following assertion was obtained from Theorem 2 and Proposition 1.

Proposition 3 ([13, Theorem 5]). *Let F be a number field, and let $K = F(\zeta_p)$ and $H = \mathrm{Gal}(K/F) \subseteq G$. If F satisfies (A_p), then we have*

$$Cl_K(\pi)^{\mathcal{S}_H} = \{0\} \quad \textit{and} \quad Cl_K(p)^{\mathcal{S}_H} \cap Cl_K(p)^H = \{0\}.$$

Here, $Cl_K(p)^H$ is the Galois invariant part.

It is known that the converse of this assertion holds when $p = 3$ ([12, Theorem 2]). The following is a consequence of Proposition 3.

Proposition 4 *Let F and K be as in Proposition 3. Assume that F satisfies (A_p) and that the norm map $Cl_K \to Cl_F$ is surjective. Then, the natural map $Cl_F \to Cl_K$ is trivial. In particular, the exponent of Cl_F divides $[K : F]$.*

Proof. By the assumption, any ideal class $c \in Cl_F$ is of the form $c = d^{N_H}$ for some $d \in Cl_K$. However, when F satisfies (A_p), the class d^{N_H} is trivial in

Cl_K by Proposition 3 and $N_H \in \mathcal{S}_H$. □

When $F/\boldsymbol{Q}$ is unramified at p, the Galois group $\mathrm{Gal}(K/F)$ is naturally identified with $G = \boldsymbol{F}_p^\times$ through the Galois action on ζ_p. The following is a consequence of Theorem 2.

Proposition 5 *Assume that $F/\boldsymbol{Q}$ is unramified at p, and let $K = F(\zeta_p)$. Then, F satisfies the condition (A_p) if and only if the Stickelberger ideal $\mathcal{S}_G$ annihilates the ray class group $Cl_K(\pi)$.*

Proof. Brinkhuis [2, Proposition (2.2)] proved that the $\boldsymbol{Z}G$-module $Cl^0(\mathcal{O}_F\Gamma)$ is naturally isomorphic to the ray class group $Cl_K(\pi)$ when $F/\boldsymbol{Q}$ is unramified at p. Hence, the assertion follows immedately from Theorem 2. □

Though the following assertion is irrelevant to the proof of Theorem 1, it might be of some interest to the reader. For a CM-field K, let Cl_K^- be the kernel of the norm map $Cl_K \to Cl_{K^+}$ where K^+ is the maximal real subfield of K.

Proposition 6 *Let F be a totally real number field, and $K = F(\zeta_p)$. If F satisfies (A_p), then the exponent of Cl_K^- divides $2h_p^-$.*

Proof. Let $H = \mathrm{Gal}(K/F) \subseteq G$, and let ρ be a generator of H. As F is totally real, $|H|$ is even and $J = \rho^{|H|/2}$ is the complex conjugation in H. We easily see that $(1-\rho)\mathfrak{n}_H = 1 - J$, and that $\mathfrak{n}_H h_p^- \in \mathcal{S}_H$ by (2). Hence, $(1-J)h_p^- \in \mathcal{S}_H$. Assume that F satisfies (A_p). Then, by Proposition 3, $(1-J)h_p^-$ annihilates Cl_K. The assertion follows from this. □

Remark 1. The proof of Proposition 4 relies on the first equality of Proposition 3 shown in the paper [13] which is not yet published. However, when $F/\boldsymbol{Q}$ is unramified at p, we can prove it using Proposition 5 in place of Proposition 3 exactly similarly. And, in the proof of Theorem 1, we can concentrate on imaginary quadratic fields $F/\boldsymbol{Q}$ unramified at p by virtue of Proposition 1, and we do not need the not yet unpublished result. (See the first lemma in the next section.)

3 Imaginary quadratic fields

In this section, let $p \geq 3$ be an odd prime number, and $F = \boldsymbol{Q}(\sqrt{-d})$ an imaginary quadratic field with a square free positive integer d.

Lemma 1 *When p is ramified in $F/\boldsymbol{Q}$, F satisfies (A_p) if and only if $p=3$ and $F=\boldsymbol{Q}(\sqrt{-3})$.*

Proof. The "only if" part is an easy consequence of Proposition 1 since $(\mathcal{O}_F/p)^\times$ is cyclic of order $p(p-1)$ when p ramifies in F. The "if" part is due to [5, p. 110]. $\square$

Lemma 2 (I) *Let $p=3$ or 5. When $F \neq \boldsymbol{Q}(\sqrt{-1})$, $\boldsymbol{Q}(\sqrt{-3})$ and p is inert in F, F does not satisfy (A_p).*

(II) *Let $p \geq 7$. When p is inert in F, F does not satisfy (A_p).*

Proof. This is an easy consequence of Proposition 1 since $(\mathcal{O}_F/p)^\times$ is cyclic of order p^2-1 when p is inert in F. $\square$

In all what follows, we exclude the case where $p=3$ and $F=\boldsymbol{Q}(\sqrt{-3})$, and we let $K=F(\zeta_p)$. Hence, by Lemma 1, if F satisfies (A_p), then $F/\boldsymbol{Q}$ is unramified at p and the Galois group $\mathrm{Gal}(K/F)$ is naturally identified with $G=\boldsymbol{F}_p^\times$.

Lemma 3 *If F satisfies (A_p), then the exponent of the class group Cl_F divides 2.*

Proof. We use a standard argument in [26, pp. 289-290]. Assume that F satisfies (A_p). As $F/\boldsymbol{Q}$ is unramified at p, K/F is totally ramified at the primes over p. Hence, the natural map $Cl_F \to Cl_K$ is trivial by Proposition 4. Let $\mathfrak{A}$ be an arbitrary ideal of F relatively prime to p. We have $\mathfrak{A}\mathcal{O}_K = \alpha\mathcal{O}_K$ for some $\alpha \in K^\times$. Let ρ be a generator of G, and J a generator of $\mathrm{Gal}(F/\boldsymbol{Q}) = \mathrm{Gal}(K/K^+)$ where K^+ is the maximal real subfield of K. As $\mathfrak{A}$ is an ideal of F, we have $\alpha^{1-\rho}=\epsilon \in \mathcal{O}_K^\times$. On the other hand, $\mathfrak{A}^{1+J}=\beta\mathcal{O}_F$ for some $\beta \in \boldsymbol{Q}^\times$. Hence, $\alpha^{1+J}=\beta\eta$ for some unit $\eta \in \mathcal{O}_K^\times$. It follows that

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

as $\beta \in \boldsymbol{Q}^\times$. Putting $\alpha_1 = \alpha^2/\eta$, we have

$$\alpha_1\mathcal{O}_K = \mathfrak{A}^2\mathcal{O}_K. \tag{3}$$

Let

$$\epsilon_1 = \alpha_1^{\rho-1} = \epsilon^{-2}\eta^{1-\rho} \in \mathcal{O}_K^\times. \tag{4}$$

Then, it follows that

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

Hence, ϵ_1 is a root of unity in K by a theorem on units of a CM-field (cf. [26, Theorem 4.12]). Let μ_p be the group of p-th roots of unity in K. We divide the cases according to whether $\epsilon_1 \in \mu_p$ or not.

The case $\epsilon_1 \in \mu_p$. Since the map $\rho - 1 : \mu_p \to \mu_p$ is an isomorphism, we can write $\epsilon_1 = \zeta^{\rho-1}$ for some $\zeta \in \mu_p$. Hence, it follows from (4) that $(\alpha_1/\zeta)^\rho = \alpha_1/\zeta$ and $\alpha_1/\zeta \in F^\times$. Therefore, by (3), $\mathfrak{A}^2$ is a principal ideal of F.

The case $\epsilon_1 \notin \mu_p$. As the class groups of $\boldsymbol{Q}(\sqrt{-1})$ and $\boldsymbol{Q}(\sqrt{-3})$ are trivial, we may as well assume that $F \neq \boldsymbol{Q}(\sqrt{-1})$, $\boldsymbol{Q}(\sqrt{-3})$. Then, the condition $\epsilon_1 \notin \mu_p$ implies that $-\epsilon_1 \in \mu_p$, and hence, $-\epsilon_1 = \zeta^{\rho-1}$ for some $\zeta \in \mu_p$. On the other hand, we have $-1 = (\sqrt{p^*})^{\rho-1}$ where $p^* = p$ if $p \equiv 1 \bmod 4$ and $p^* = -p$ otherwise. Therefore, we see that $\epsilon_1 = (\sqrt{p^*}\zeta)^{\rho-1}$. Hence, it follows from (4) that

$$(\alpha_1/\sqrt{p^*}\zeta)^\rho = \alpha_1/\sqrt{p^*}\zeta \quad \text{and} \quad \alpha_1/\sqrt{p^*}\zeta \in F^\times.$$

This implies that p is ramified in F as $\mathfrak{A}$ is relatively prime to p. This is a contradiction. □

Lemma 3 asserts that if the exponent of Cl_F is greater than 2, then F does not satisfy (A_p) for any prime p. All imaginary quadratic fields F with $Cl_F^2 = \{0\}$ were determined by Weinberger [27, Theorem 1] with possibly one exception. A table of such F's is given in Miyada [22, p. 539]. There are exactly 65 (or possibly 66) such F. In particular, we obtain the following:

Proposition 7 *For each prime number p, there exist at most* 65 (*or possibly* 66) *imaginary quadratic fields satisfying the condition* (A_p).

Lemma 4 *Let $p = 5$, and $E = F(\sqrt{5})$. If F satisfies (A_5), then the natural map $Cl_F \to Cl_E$ is trivial.*

Proof. Assume that F satisfies (A_5). Let ρ be a generator of $G = \mathrm{Gal}(K/F)$. We have $\mathcal{S}_G = \langle 1+\rho \rangle$ by $h_5^- = 1$ and (2). By the assumption and Proposition 3 or 5, $c^{1+\rho} = 1$ for any $c \in Cl_K$. As the norm map $Cl_K \to Cl_E$ is surjective, this relation holds for any $c \in Cl_E$. As the norm map $Cl_E \to Cl_F$ is surjective, any class $d \in Cl_F$ is of the form $d = N_{E/F}(c) = c^{1+\rho}$ for some $c \in Cl_E$. Therefore, we obtain the assertion. □

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

Proof. Assume that F satisfies (A_p). Let $\mathfrak{A}$ be an ideal of F. By Proposition 4, $\mathfrak{A}\mathcal{O}_K = \alpha\mathcal{O}_K$ for some $\alpha \in K^\times$. Hence, $\mathfrak{A}^{[K:E]}\mathcal{O}_E = \beta\mathcal{O}_E$ with $\beta = N_{K/E}(\alpha)$. This implies that $\mathfrak{A}\mathcal{O}_E$ is a principal ideal since $[K : E]$ is odd by the assumption on p and $\mathfrak{A}^2$ is principal in F by Lemma 3. □

Lemma 6 *Let p be a prime number with $p \equiv 3 \bmod 4$ or $p = 5$. If F satisfies (A_p), then Cl_F is isomorphic to the abelian group $(\boldsymbol{Z}/2)^{\oplus R}$ with $R \leq 2$.*

Proof. Let $H_F^{(2)}/F$ be the maximal unramified abelian extension of exponent 2, and let E be as in Lemmas 4 and 5. Assume that F satisfies (A_p). Then, the degree $[H_F^{(2)} : F]$ equals $[H_F^{(2)}E : E]$ since E/F is totally ramified at the primes over p. Let t be the number of prime numbers which ramify in F. Let $\lambda_1, \cdots, \lambda_r$ (resp. $\mu_1, \cdots, \mu_s$) be all the odd prime numbers which ramify in F and congruent to 1 (resp. 3) modulo 4. The 2-rank of Cl_F equals $t - 1$ by a well known theorem on quadratic fields (cf. Hecke [8, Theorem 132]). Hence, by Lemma 3, it suffices to show that $t \leq 3$ since we are assuming that F satisfies (A_p). It is well known and easy to show that

$$H_F^{(2)} = F\left(\sqrt{\lambda_i},\ \sqrt{-\mu_j} \mid 1 \leq i \leq r,\ 1 \leq j \leq s\right).$$

Let ℓ be any one of the prime numbers λ_i and μ_j, and let $\mathfrak{L}$ be the prime ideal of F over ℓ. By Lemmas 4 and 5, the ideal $\mathfrak{L}\mathcal{O}_E$ is principal. This implies that $\ell = \epsilon x^2$ for some unit $\epsilon \in \mathcal{O}_E^\times$ and $x \in E^\times$. Therefore, we obtain

$$H_F^{(2)}E = E\left(\sqrt{\epsilon} \mid \epsilon \in \mathcal{O}_E^\times\right).$$

Now, from the above, it follows that

$$2^{t-1} = [H_F^{(2)} : F] = [H_F^{(2)}E : E] = 1,\ 2 \text{ or } 4$$

since the group $\mathcal{O}_E^\times$ is generated by two elements. Therefore, we obtain $t \leq 3$. □

For a number field N and a prime number q, let $Cl_N[q]$ be the Sylow q-subgroup of the class group Cl_N.

Lemma 7 *Let $p \geq 7$ be a prime number with $p \equiv 3 \bmod 4$. Let $K = F(\zeta_p)$, and let N be an intermediate field of K/F with $2 \nmid [K:N]$. If the 2-part $Cl_N[2]$ is nontrivial and cyclic as an abelian group, then F does not satisfy (A_p).*

Proof. Assume that $Cl_N[2]$ is nontrivial and cyclic, but that F satisfies (A_p). Let c be a generator of the cyclic group $Cl_N[2]$. Then, we see that

$$c^{\sigma} \equiv c \bmod 2Cl_N[2] \tag{5}$$

for all $\sigma \in G$. As $[K:N]$ is odd, the natural map $Cl_N[2] \to Cl_K$ is injective. Let $\bar{c}$ and $\overline{Cl}_N[2]$ be the images of c and $Cl_N[2]$ under this injection, respectively. As F satisfies (A_p), the Stickelberger element $\theta_{G,2}$ kills $\bar{c}$. We easily see that the augmentation $\boldsymbol{Z}G \to \boldsymbol{Z}$ maps the element $\theta_{G,2}$ to $(p-1)/2$ from the definition (1). Therefore, it follows from (5) that

$$1 = \bar{c}^{\theta_{G,2}} \equiv \bar{c}^{(p-1)/2} \bmod 2\overline{Cl}_N[2].$$

This implies that $c^{(p-1)/2} \in 2Cl_N[2]$ as $Cl_N[2] \to Cl_K$ is injective. Hence, it follows that $c \in 2Cl_N[2]$ as $(p-1)/2$ is odd. This is a contradiction. □

For a number field N, let h_N be the class number of N.

Lemma 8 *Let p be a prime number with $p \equiv 3 \bmod 4$ and $p \leq 19$, and let $E = F(\sqrt{-p})$. If the class number h_E is divisible by an odd prime number q relatively prime to $(p-1)/2$, then F does not satisfy (A_p).*

Proof. As q is relatively prime to $(p-1)/2$, the natural map $Cl_E[q] \to Cl_K$ is injective. Let c be a class in Cl_E of order q, and $\bar{c}$ its lift to K. The class $\bar{c}$ is nontrivial. Let ρ be a generator of $G = \mathrm{Gal}(K/F)$. Assume that F satisfies (A_p). Then, we see that $c^{\rho} = c^{-1}$ since h_F is a power of 2 by Lemma 3. Hence, it follows that

$$\bar{c}^{\rho} = \bar{c}^{-1}. \tag{6}$$

The condition $p \leq 19$ is equivalent to $h_p^- = 1$ (cf. [26, Corollary 11.18]). Hence, by (2), the Stickelberger ideal $\mathcal{S}_G$ is generated by $\mathfrak{n}_G$. Since F satisfies (A_p), we see that $\mathfrak{n}_G$ annihilates Cl_K by Proposition 3 or 5. As $(p-1)/2$ is odd, we see from (6) that

$$1 = \bar{c}^{\mathfrak{n}_G} = \bar{c}^{\{1+(-1)\}+\cdots+\{1+(-1)\}+1} = \bar{c}.$$

This is a contradiction. □

Lemma 9 *Let F be a quadratic field not necessarily imaginary, and let p be a prime number splitting in F. Let $\mathfrak{P}_1$ and $\mathfrak{P}_2$ be the prime ideals of $K = F(\zeta_p)$ over p. Then, the Stickelberger ideal $\mathcal{S}_G$ annihilates $(\mathcal{O}_K/\pi)^\times/[\mathcal{O}_K^\times]_\pi$ if and only if there exists a unit $\epsilon \in \mathcal{O}_K^\times$ satisfying*

$$\epsilon \equiv 1 \bmod \mathfrak{P}_1 \quad \text{and} \quad \epsilon \equiv -1 \bmod \mathfrak{P}_2. \tag{7}$$

Proof. For brevity, put $X = (\mathcal{O}_K/\pi)^\times/[\mathcal{O}_K^\times]_\pi$. We have

$$(\mathcal{O}_K/\pi)^\times = (\mathcal{O}_K/\mathfrak{P}_1)^\times \oplus (\mathcal{O}_K/\mathfrak{P}_2)^\times = \boldsymbol{F}_p^\times \oplus \boldsymbol{F}_p^\times.$$

The Galois group $G = \mathrm{Gal}(K/F)$ fixes the prime ideal $\mathfrak{P}_i$, and it acts trivially on $(\mathcal{O}_K/\mathfrak{P}_i)^\times$. The augmentation $\iota_G : \boldsymbol{Z}G \to \boldsymbol{Z}$ maps both $\mathfrak{n}_G$ and $\theta_{G,2}$ to $(p-1)/2$. Hence, we see from (2) that ι_G maps the ideal $\mathcal{S}_G \subseteq \boldsymbol{Z}G$ onto the ideal of $\boldsymbol{Z}$ generated by $(p-1)/2$. Therefore, it follows that the condition $X^{\mathcal{S}_G} = \{0\}$ is equivalent to

$$(\mathcal{O}_K/\pi)^{\times (p-1)/2} \subseteq [\mathcal{O}_K^\times]_\pi.$$

¿From this, we obtain the assertion. □

Lemma 10 *Let $F = \boldsymbol{Q}(\sqrt{-d})$ be an imaginary quadratic field with a square free positive integer d, and let p be a prime number splitting in F. There exists a unit $\epsilon \in \mathcal{O}_K^\times$ satisfying (7) in the following two cases.*

(I) *$d = 1$,*

(II) *d is a prime number with $d \not\equiv 1 \bmod 4$, and $p \equiv 3 \bmod 4$.*

Proof. We first show the assertion for the case (II). Let $E = F(\sqrt{-p})$. It is well known that the unit index Q_E of the imaginary abelian field E equals 2 by Hasse [7, p. 76]. We apply the classical argument used for showing $Q_E = 2$. Let $E^+ = \boldsymbol{Q}(\sqrt{pd})$ be the maximal real subfield of E. Let $\mathfrak{Q}_d$ be the prime ideal of E^+ over the prime d ; $(d) = \mathfrak{Q}_d^2$. ¿From the conditions on d and p, we see that the class number of E^+ is odd by genus theory. Hence, there exist integers u, $v \in \boldsymbol{Z}$ such that $u^2 - v^2pd = \pm 4d$. Then, it follows that $u = u'd$ for some $u' \in \boldsymbol{Z}$ and that $\eta = (u'\sqrt{-d}+v\sqrt{-p})/2$ is a unit of $\mathcal{O}_E$. Let $\mathfrak{P}_1$ and $\mathfrak{P}_2$ be the prime ideals of K over p. Let $a \in \boldsymbol{Z}$ be an integer such that $\sqrt{-d} \equiv a \bmod \mathfrak{P}_1$. We see that $\sqrt{-d} \equiv -a \bmod \mathfrak{P}_2$ by taking the conjugate over $\boldsymbol{Q}$. Therefore, it follows that $\eta \equiv b \bmod \mathfrak{P}_1$ and $\eta \equiv -b \bmod \mathfrak{P}_2$ for some integer b with $1 \leq b \leq p-1$. Let $\delta_b = 1+\zeta_p+\cdots+\zeta_p^{b-1}$ be a cyclotomic unit in K. Then, since $\delta_b \equiv b \bmod \pi$, the unit $\epsilon = \eta/\delta_b$ satisfies the condition

(7).

For the case (I), we can similarly show the assertion by taking $\epsilon = \sqrt{-1}$ times a suitable cyclotomic unit of K. □

Proof of Theorem 1. By Lemma 6, we do not need the conditional result of Weinberger [27] mentioned before. The imaginary quadratic fields F with $h_F = 1$ were determined by Stark [24]. Those with $h_F = 2$ were determined independently by Stark [25] and Montgomery and Weinberger [23], and those with $h_F = 4$ were determined by Arno [1]. By genus theory, we can easily pick out those with $Cl_F = (\boldsymbol{Z}/2)^{\oplus 2}$ from Arno's result. Using these results and Lemmas 1 and 2, we obtain the following lists.

Lemma 11 *An imaginary quadratic field $F = \boldsymbol{Q}(\sqrt{-d})$ satisfies (A_5) only when d is one of the following:*

$$\text{(i) } 1,\ 3,\ 11,\ 19;\ \text{(ii) } 6,\ 51,\ 91;\ \text{(iii) } 21.$$

Lemma 12 *An imaginary quadratic field $F = \boldsymbol{Q}(\sqrt{-d})$ satisfies (A_7) only when d is one of the following:*

$$\text{(i) } 3,\ 19;\ \text{(ii) } 5,\ 6,\ 10,\ 13,\ 115,\ 187;\ \text{(iii) } 33,\ 195.$$

Lemma 13 *An imaginary quadratic field $F = \boldsymbol{Q}(\sqrt{-d})$ satisfies (A_{11}) only when d is one of the following:*

$$\text{(i) } 2,\ 7,\ 19,\ 43;\ \text{(ii) } 6,\ 10,\ 13,\ 35,\ 51,\ 123,\ 403;$$

$$\text{(iii) } 21,\ 30,\ 57,\ 85,\ 195,\ 435,\ 483.$$

In the above lists, those F or d in the first groups satisfy $h_F = 1$, those in the second groups $h_F = 2$, and those in the last groups $Cl_F = (\boldsymbol{Z}/2)^{\oplus 2}$, respectively. In the following, let $K = F(\zeta_p)$ and E be the intermediate field of K/F with $[E : F] = 2$. Let ρ be a generator of $G = \mathrm{Gal}(K/F)$. By (2), $\mathcal{S}_G$ is generated by $\mathfrak{n}_G = 1 + \rho + \cdots + \rho^{(p-1)/2-1}$. All the following calculation were done using KASH.

The case $p = 5$. We checked that the natural map $Cl_F \to Cl_E$ is not trivial when $d = 6$, 51, 91 or 21. Hence, by Lemma 4, F does not satisfy (A_5) for these d. When $d = 1$ or 3, we have $Cl_K = \{0\}$. When $d = 1$, we see that $Cl_K(\pi)^{\mathcal{S}_G} = \{0\}$ by Lemmas 9 and 10. When $d = 3$, we checked

$Cl_K(\pi)^{\mathcal{S}_G} = \{0\}$ by explicitly finding a system of fundamental units of K. Hence, by Proposition 5, F satisfies (A_5) for $d = 1$ or 3. When $d = 11$ (resp. 19), we see that $Cl_K = \boldsymbol{Z}/2$ (resp. $\boldsymbol{Z}/4$) and $Cl_K^{\mathcal{S}_G} = \{0\}$. We chose an ideal $\mathfrak{A}$ of K such that the class $[\mathfrak{A}]$ generates the cyclic group Cl_K. We checked that a generator α of the principal ideal $\mathfrak{A}^{1+\rho}$ is not congruent to a unit modulo π. Hence, by Proposition 5, F does not satisfy (A_5) for $d = 11$ or 19.

The case $p = 7$. We checked that the natural map $Cl_F \to Cl_E$ is not trivial when $d = 6$, 33, 195. Hence, by Lemma 5, F does not satisfy (A_7) for these d. For $d = 5$, 10, 115, 187, the 2-part of Cl_K is nontrivial and cyclic, and hence F does not satisfy (A_7) by Lemma 7. When $d = 13$, we found that $Cl_K = \boldsymbol{Z}/2^{\oplus 3} \oplus \boldsymbol{Z}/3$ and $Cl_K^{\mathcal{S}_G} \neq \{0\}$, and hence F does not satisfy (A_7). When $d = 19$, we found that $Cl_K = \boldsymbol{Z}/3$ and $Cl_K^{\mathcal{S}_G} = \{0\}$. We checked that F does not satisfy (A_7) in this case similarly to the case where $p = 5$ and $d = 11$, 19. Finally, when $d = 3$, we found that $Cl_K = \{0\}$, and that $Cl_K(\pi)^{\mathcal{S}_G} = \{0\}$ by Lemmas 9 and 10. Hence, F satisfies (A_7) for $d = 3$.

The case $p = 11$. For $d = 10$, 35, 21, 30, 57, 85, 195, 435 or 483, we found that the natural map $Cl_F \to Cl_E$ is not trivial. Hence, by Lemma 5, F does not satisfy (A_{11}) for these d. For $d = 6$, 13, 51, 123 or 403, we have $h_E = 2$. Hence, by Lemma 7, F does not satisfy (A_{11}) for these d. For $d = 43$, we have $h_E = 3$, and F does not satisfy (A_{11}) by Lemma 8. Let us deal with the remaining case where $d = 2$, 7 or 19. In these cases, we have $h_E = 1$. In stead of the field $K = F(\zeta_{11})$, we use the subfield $N = F(\cos 2\pi/11)$. We have $h_N = 5$ for $d = 2$ or 7, and $h_N = 55$ for $d = 19$. Let $\mathfrak{A}$ be an ideal of N. If F satisfies (A_{11}), then $\mathfrak{A}^{\mathrm{n}_G}\mathcal{O}_K = \alpha\mathcal{O}_K$ for some $\alpha \in K^\times$ congruent modulo π to a unit of K. Taking the norm to N, it follows that $\mathfrak{A}^{2\mathrm{n}_G} = \beta\mathcal{O}_N$. Here, $\beta = N_{K/N}\alpha$ and is congruent to a unit of N modulo π. For these three d, we chose a nontrivial ideal $\mathfrak{A}$ of N and checked that $\mathfrak{A}^{2\mathrm{n}_G}$ is a principal ideal of $\mathcal{O}_N$ and that its generator is not congruent to a unit of N modulo π after computing a system of fundamental units of N. Therefore, there exists no imaginary quadratic field satisfying (A_{11}). □

Observation/Question. Let p be a prime number. As usual, we put $\tilde{p} = 4$ (resp. p) when $p = 2$ (resp. $p \geq 3$). We have seen that for the first five $\tilde{p}$, the number of imaginary quadratic fields F satisfying (A_p) is 4, 3, 2, 1 and 0, respectively. What is the next term or a general term of this (arithmetic !) progression ?

Remark 2. We can generalize Lemma 3 as follows. For a number field F, let μ_F be the group of roots of unity in F. Let K/F be a finite cyclic extension with both K and F CM-fields. Assume that the following three conditions are satisfied:

(i) $[K:F]$ is even.

(ii) $\mu_F = \{\pm 1\}$ and $\sqrt{-1} \notin \mu_K$, and

(iii) There exists a prime ideal $\wp$ of F over an odd prime number p such that the ramification index of $\wp$ at $F/\boldsymbol{Q}$ is odd and $\wp$ is ramified at the quadratic intermediate field E of K/F.

By the last condition, we can write $E = F(\sqrt{a})$ for some $a \in F^\times$ with $\mathrm{ord}_\wp(a) = 1$. Then, we can show that the exponent of the kernel of the natural map $Cl_F^- \to Cl_K^-$ divides 2 by an argument exactly similar to the proof of Lemma 3 using a inplace of p^*.

Remark 3. If all imaginary abelian fields K of degree $2(p-1)$ for which $Cl_K^{2h_p^-} = \{0\}$ are determined, it would be possible to determine all real quadratic fields satisfying (A_p) for small primes p by virtue of Proposition 6.

4 Subfields of the p-cyclotomic field

In this section, we deal with subfields of the p-cyclotomic field $\boldsymbol{Q}(\zeta_p)$. The following is an immediate consequence of Proposition 1. A more general statement is given in [9, Proposition 3.4]

Proposition 8 *Let p be an odd prime number. An imaginary subfield F of $\boldsymbol{Q}(\zeta_p)$ satisfies (A_p) if and only if $p = 3$ and $F = \boldsymbol{Q}(\zeta_3)$.*

In the following, we summarize what is known or conjectured for the real case. Let $\mathcal{O}_F' = \mathcal{O}_F[1/p]$ be the ring of p-integers of F. We say that F satisfies the condition (A_p') when for any Γ-extension N/F, $\mathcal{O}_N'$ is cyclic over the group ring $\mathcal{O}_F'\Gamma$. It is known that F satisfies (A_p) only when it satisfies (A_p') (see [16, Lemma 7]). The condition (A_p') is more easy to handle with than the difficult one (A_p), and many results on (A_p') are already obtained in [14, 16, 17, 18]. Let $K = F(\zeta_p)$. For instance, it is known that F satisfies (A_p') if $h_K' = 1$, where h_K' is the class number of the Dedekind domain $\mathcal{O}_K'$.

Let $K = \boldsymbol{Q}(\zeta_p)$, and h_p the class number of K. As the unique prime ideal of $\mathcal{O}_K$ over p is principal, we have $h_p = h_K'$. It is well known that $h_p = 1$ if and only if $p \leq 19$ (cf. [26, Theorem 11.1]). Hence, when $p \leq 19$, any subfield F of $K = \boldsymbol{Q}(\zeta_p)$ satisfies (A'_p). When $p \geq 23$, we proposed the following conjecture in [18].

Conjecture 1. Let p be a prime number with $p \geq 23$, and F a subfield of $\boldsymbol{Q}(\zeta_p)$ with $F \neq \boldsymbol{Q}$. If $[F : \boldsymbol{Q}] > 2$ or $p \equiv 1 \bmod 4$, then F does not satisfy the condition (A'_p) except for the case where $p = 29$ and $[F : \boldsymbol{Q}] = 2$ or 7.

We have seen in [18, Proposition 4] that the conjecture is valid when $23 \leq p \leq 499$ or when $[K : F] \leq 4$ or $= 6$. A reason that the case $p = 29$ is exceptional is that h_p^- is power of 2 if and only if $p \leq 19$ or $p = 29$ by Horie [10]. When $p = 29$ and $[F : \boldsymbol{Q}] = 2$ or 7, it is known that F satisfies (A'_p) ([18, Proposition 4(II)]). In [16, Theorem 1], we determined all imaginary subfields F of $\boldsymbol{Q}(\zeta_p)$ satisfying (A'_p), and gave an affirmative answer to the conjecture for the imaginary case. In [17], we showed the following assertion for the real case.

Proposition 9 ([17, Proposition 1]). *Let $p \geq 23$. Assume that $q \parallel h_p^-$ for some odd prime number q. Then, any real subfield F of $\boldsymbol{Q}(\zeta_p)$ with $F \neq \boldsymbol{Q}$ does not satisfy (A'_p). (Hence, it does not satisfy (A_p).)*

The assumption in this assertion is satisfied for all primes p with $23 \leq p < 2^{10}$ except for the case where $p = 29$, 31 or 41 by the tables in [26], Lehmer and Masley [19] and Yamamura [28].

Now, we can say that we have enough reasons to propose the following:

Conjecture 2. A real subfield F of $\boldsymbol{Q}(\zeta_p)$ with $F \neq \boldsymbol{Q}$ does not satisfy (A_p) except for the case where $p \leq 19$, or $p = 29$ and $[F : \boldsymbol{Q}] = 2$, 7.

Among the exceptional cases in Conjecture 2, we have checked that $\boldsymbol{Q}(\sqrt{5})$ satisfies (A_5) and that $\boldsymbol{Q}(\cos 2\pi/7)$ does not satisfy (A_7) by computer calculation based upon Theorem 2. The difficult point is that the locally free class group $Cl^0(\mathcal{O}_F\Gamma)$ is very complicated when $F/\boldsymbol{Q}$ is ramified at p.

Acknowledgements. The authors are grateful to the referee for carefully reading the original manuscript and for several kind suggestions. Thanks to the suggestions, we added Remarks 1 and 2 and considerbly improved the proof of Lemma 6. The first author was partially supported by Grant-in-Aid for Scientific Research (C), (No. 16540033), the Ministry of Education, Culture, Sports, Science and Technology of Japan. The second author was partially supported by Grant-in-Aid for Young Scientists, (No. 16740019), the Ministry of Education, Culture, Sports, Science and Technology of Japan.

References

[1] S. Arno, The imaginary quadratic fields of class number 4, Acta Arith., **60** (1992), 321-334.

[2] J. Brinkhuis, Normal integral bases and complex conjugation, J. Reine Angew. Math., **375** (1987), 157-166.

[3] J. E. Carter, Normal integral bases in quadratic and cyclic cubic extensions over quadratic fields, Arch. Math., **81** (2003), 266-271: Erratum, *ibid.*, **83** (2004).

[4] M. Conrad and D. R. Replogle, Nontrivial Galois module structure of cyclotomic fields, Math. Comp., **72** (2003), 891-899.

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

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

[7] H. Hasse, Über die Klassenzahl abelscher Zahlkörper, Akademie-Verlag, Berlin, 1952.

[8] E. Hecke, Lectures on the Theory of Algebraic Numbers, Springer, Berlin-Heidelberg-New York, 1981.

[9] T. Herreng, Sur les corps de Hilbert-Speiser, J. Théor. Nombres Bordeaux, **17** (2005), 767-77.

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

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

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

[13] H. Ichimura, Normal integral bases and ray class groups, II, Yokohama Math. J., in press.

[14] H. Ichimura, Stickelberger ideals and normal bases of rings of p-integers, Math. J. Okayama Univ., in press.

[15] H. Ichimura, A class number formula for the p-cyclotomic field, Arch. Math., in press.

[16] H. Ichimura, Hilbert-Speiser number fields for a prime p inside the p-cyclotomic field, submitted for publication.

[17] H. Ichimura, Triviality of Stickelberger ideals of conductor p, submitted for publication.

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

[19] D. H. Lehmer and J. Masley, Table of the cyclotomic class numbers $h^*(p)$ and their factors for $200 < p < 521$, Math. Comp., **32** (1978), 577-582.

[20] L. R. McCulloh, A Stickelberger condition on Galois module structure for Kummer extensions of prime degree, Algebraic Number Theory (Durham Symposium, ed. A. Fröhlich), 190-204, Academic Press, London, 1977.

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

[22] I. Miyada, On imaginary abelian number fields of type $(2, \cdots, 2)$ with one class in each genus, Manuscripta Math., **88** (1995), 535-540.

[23] H. L. Montgomery and P. J. Weinberger, Notes on small class numbers, Acta Arith., **24** (1973/74), 529-542.

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

[25] H. M. Stark, On complex quadratic fields of class number two, Math. Comp., **29** (1975), 289-302.

[26] L. C. Washington, Introduction to Cyclotomic Fields (2nd ed.), Springer, Berlin-Heidelberg-New York, 1996.

[27] P. J. Weinberger, Exponents of the class groups of complex quadratic fields, Acta Arith., **22** (1973), 117-124.

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

Humio Ichimura
Faculty of Science,
Ibaraki University,
Bunkyo 2-1-1, Mito, Ibaraki, 310-8512,
Japan

Hiroki Sumida-Takahashi
Faculty and School of Engineering,
The University of Tokushima,
2-1, Minami-josanjima-cho, Tokushima, 770-8506,
Japan