Real abelian fields satisfying the Hilbert-Speiser condition for some small primes p

By Humio ICHIMURA

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

(Communicated by Shigefumi MORI, M.J.A., Dec. 14, 2015)

Abstract: For a prime number p, we say that a number field F satisfies the Hilbert-Speiser condition (H_p) if each tame cyclic extension N/F of degree p has a normal integral basis. In this note, we determine the real abelian number fields satisfying (H_p) for odd prime numbers p with $h(\mathbf{Q}(\sqrt{-p})) = 1$.

Key words: Hilbert-Speiser number fields; real abelian fields.

1. Introduction. We say that a finite Galois extension N/F of a number field F with group G has a normal integral basis (NIB for short) when $\mathcal{O}_N$ is cyclic over the group ring $\mathcal{O}_F[G]$. Here, $\mathcal{O}_F$ denotes the ring of integers of F. It is well known that N/F is necessarily tame if it has an NIB. Let p be a prime number, and $\Gamma = (\mathbf{Z}/p\mathbf{Z})^+$ be a cyclic group of order p. We say that a number field F satisfies the Hilbert-Speiser condition (H_p) when each tame Γ-extension N/F has an NIB. There are several results on number fields satisfying (H_p). In particular, all the abelian fields F satisfying (H_3) are determined in Carter [3] and the author [10] when $[F : \mathbf{Q}] = 2$, and by Yoshimura [20] when $[F : \mathbf{Q}] > 2$. The imaginary abelian fields satisfying (H_p) for the case $p \geq 5$ are determined in [11–13]. The number of real (resp. imaginary) abelian fields satisfying (H_3) is 18 (resp. 9). The numbers of imaginary abelian fields satisfying (H_p) are 3, 1 and 0 when $p = 5$, 7, and $p \geq 11$, respectively. The main tools are (i) a theorem of McCulloh [15], (ii) a theorem of Greither *et al.* [6, Corollary 7], and (iii) the complex conjugation acting on several objects associated to the base field F. The first one is of quite fundamental nature and it describes, in the locally free class group $Cl(\mathcal{O}_F[\Gamma])$ associated to the group ring $\mathcal{O}_F[\Gamma]$, the subset of the classes $[\mathcal{O}_N]$ for all tame Γ-extensions N/F. The second one was obtained from this theorem studying the Swan submodule of $Cl(\mathcal{O}_F[\Gamma])$, and it implies that when $p \geq 5$, an imaginary abelian field F satisfies (H_p) only when $F/\mathbf{Q}$ is unramified at p. (See [8, Proposition 3.4], [11, Lemma 2.2], [5, Theorem 1.3]).

Recently, Greither and Johnston ([5, Theorem 1.1]) proved that if $p \geq 7$, a *totally real* number field F satisfies (H_p) only when $F/\mathbf{Q}$ is unramified at p, using [15] with detailed analysis of the group $Cl(\mathcal{O}_F[\Gamma])$ and ramification index. The main purpose of this note is to deal with real abelian fields satisfying (H_p) for those odd prime numbers p with $h(\mathbf{Q}(\sqrt{-p})) = 1$, where $h(\mathbf{Q}(\sqrt{-p}))$ is the class number of $\mathbf{Q}(\sqrt{-p})$. As is well known, the condition on p implies that

$$p = 3,\ 7,\ 11,\ 19,\ 43,\ 67,\ 163.$$

For this, see Cox [4, Theorem 7.30] for instance. First, we show the following result using [15].

Proposition 1. *Let p be a prime number with $p \equiv 3 \bmod 4$. Let F be a number field unramified at p, and let $N = F(\sqrt{-p})$. If F satisfies (H_p), then the exponent of the ideal class group Cl_N of N divides $h(\mathbf{Q}(\sqrt{-p}))$.*

As we mentioned above, the abelian number fields satisfying (H_3) are already determined. So, we let $p \geq 7$. From Proposition 1 and [5, Theorem 1.1] mentioned above, we obtain the following assertion using some computational results on abelian fields.

Proposition 2. *Let $p \geq 7$ be a prime number with $h(\mathbf{Q}(\sqrt{-p})) = 1$. When $p = 7$ (resp. 11), a real abelian field F satisfies (H_p) if and only if $F = \mathbf{Q}(\sqrt{5})$ or $\mathbf{Q}(\sqrt{13})$ (resp. $F = \mathbf{Q}(\cos 2\pi/7)$). When $p = 19$, 43, 67 or 163, there is no real abelian field satisfying (H_p).*

Remark 1. When $p = 2$, it is known that a number field F satisfies (H_2) if and only if the ray

2010 Mathematics Subject Classification. Primary 11R33, 11R18.

doi: 10.3792/pjaa.92.19

class group of F defined modulo 2 is trivial ([9, Proposition 2]). Imaginary abelian fields satisfying (H_2) are determined in [3] and [20].

2. Proof of Proposition 1. First, we recall the theorem of McCulloh mentioned in §1. Let $G = (\mathbf{Z}/p\mathbf{Z})^\times$ be the multiplicative group, which we naturally identify with the Galois group $\mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q})$. Here, ζ_p is a primitive pth root of unity. We put

$$\theta_G = \frac{1}{p}\sum_{a=1}^{p-1} a\sigma_a^{-1} \in \mathbf{Q}[G]$$

where $\sigma_a = a \bmod p \in G$. Then the Stickelbeger ideal $\mathcal{S}_G$ of the group ring $\mathbf{Z}[G]$ is defined by

$$\mathcal{S}_G = \mathbf{Z}[G] \cap \mathbf{Z}[G]\theta_G.$$

For a number field F, let Cl_F be the ideal class group of F. Further, we denote by $R(\mathcal{O}_F[\Gamma])$ the subset of $Cl(\mathcal{O}_F[\Gamma])$ consisting of the locally free classes $[\mathcal{O}_N]$ for all tame Γ-extensions N/F, and denote by $Cl^0(\mathcal{O}_F[\Gamma])$ the kernel of the map $Cl(\mathcal{O}_F[\Gamma]) \to Cl_F$ induced from the augmentation map $\mathcal{O}_F[\Gamma] \to \mathcal{O}_F$. It is known that $R(\mathcal{O}_F[\Gamma]) \subseteq Cl^0(\mathcal{O}_F[\Gamma])$ and that F satisfies (H_p) if and only if $R(\mathcal{O}_F[\Gamma]) = \{0\}$. The group ring $\mathbf{Z}[G]$ acts on $Cl^0(\mathcal{O}_F[\Gamma])$ through the natural action of $G = (\mathbf{Z}/p\mathbf{Z})^\times$ on the additive group $\Gamma = (\mathbf{Z}/p\mathbf{Z})^+$. Let $Cl^0(\mathcal{O}_F[\Gamma])^{\mathcal{S}_G}$ denote the subgroup of $Cl^0(\mathcal{O}_F[\Gamma])$ generated by the classes c^α for all $c \in Cl^0(\mathcal{O}_F[\Gamma])$ and $\alpha \in \mathcal{S}_G$. The main theorem of [15] asserts that

$$R(\mathcal{O}_F[\Gamma]) = Cl^0(\mathcal{O}_F[\Gamma])^{\mathcal{S}_G}. \tag{1}$$

Let k be an imaginary subfield of $\mathbf{Q}(\zeta_p)$, and let $\Delta = \Delta_k$ be the quotient of $G = \mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q})$ corresponding to k; $\Delta = \mathrm{Gal}(k/\mathbf{Q})$. We denote by $\mathcal{S}_\Delta$ the image of the ideal $\mathcal{S}_G$ under the restriction map $\mathbf{Z}[G] \to \mathbf{Z}[\Delta]$. Let $s_G \in \mathbf{Z}[G]$ (resp. $s_\Delta \in \mathbf{Z}[\Delta]$) be the sum of all elements of G (resp. Δ). Denote by A_G (resp. A_Δ) the elements α of $\mathbf{Z}[G]$ (resp. $\mathbf{Z}[\Delta]$) such that $\alpha(1+J) = a \cdot s_G$ (resp. $a \cdot s_\Delta$) for some $a \in \mathbf{Z}$. Here, J is the complex conjugation in G (resp. Δ). The ideal $\mathcal{S}_G$ (resp. $\mathcal{S}_\Delta$) is contained in A_G (resp. A_Δ) by Sinnott [16, Lemma 2.1]. Denote by h_M the class number of a number field M, and by h_M^- the relative class number when M is an imaginary abelian field. We set $h_p^- = h_M^-$ when $M = \mathbf{Q}(\zeta_p)$. By [16, Theorem 2.1], we have the following class number formulas:

$$[A_G : \mathcal{S}_G] = h_p^- \quad \text{and} \quad [A_\Delta : \mathcal{S}_\Delta] = h_k^-. \tag{2}$$

We see that $A_\Delta = \mathbf{Z}[\Delta]$ when and only when $p \equiv 3 \bmod 4$ and $k = \mathbf{Q}(\sqrt{-p})$. This is a key point of the following argument.

Proof of Proposition 1. Let p and F be as in Proposition 1. Assume that F satisfies (H_p); namely that $R(\mathcal{O}_F[\Gamma]) = \{0\}$. Put $K = F(\zeta_p)$, and $\varpi = \varpi_p = \zeta_p - 1$. Since $F/\mathbf{Q}$ is unramified at p, we see that $\mathrm{Gal}(K/F)$ is naturally identified with $G = \mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q})$ and that $Cl^0(\mathcal{O}_F[\Gamma])$ is isomorphic, as a $\mathbf{Z}[G]$-module, to the ray class group $Cl_{K,\varpi}$ of K defined modulo $\varpi\mathcal{O}_K$ by Brinkhuis [1, Proposition 2.1];

$$Cl^0(\mathcal{O}_F[\Gamma]) \cong Cl_{K,\varpi}. \tag{3}$$

Therefore, by (1) and $R(\mathcal{O}_F[\Gamma]) = \{0\}$, the Stickelberger ideal $\mathcal{S}_G$ annihilates $Cl_{K,\varpi}$. In particular, it annihilates the absolute class group Cl_K. Let $k = \mathbf{Q}(\sqrt{-p})$ and $\Delta = \mathrm{Gal}(k/\mathbf{Q})$. We have $N = Fk$, and $\Delta = \mathrm{Gal}(N/F)$ under the identification $G = \mathrm{Gal}(K/F)$. It follows that $\mathcal{S}_\Delta$ annihilates Cl_N since the norm map $Cl_K \to Cl_N$ is surjective by Washington [17, Theorem 10.1]. In our situation, we have $A_\Delta = \mathbf{Z}[\Delta]$ as we mentioned above. Therefore, it follows from (2) that $h(\mathbf{Q}(\sqrt{-p})) \in \mathcal{S}_\Delta$. Thus, multiplication by $h(\mathbf{Q}(\sqrt{-p}))$ annihilates Cl_N. □

Corollary. *Let p and F be as in Proposition 1. Assume that F satisfies (H_p). Then $h_F = 1$ if we further assume that $h(\mathbf{Q}(\sqrt{-p}))$ and $p-1$ are relatively prime.*

Proof. It follows from Proposition 1 that the exponent of Cl_F divides $h(\mathbf{Q}(\sqrt{-p}))$ since the norm map $Cl_N \to Cl_F$ is surjective. On the other hand, we see that

$$s_G = \sum_{\sigma\in G}\sigma = (1+\sigma_{-1})\theta_G \in \mathcal{S}_G.$$

Since F satisfies (H_p), the ideal $\mathcal{S}_G$ annihilates Cl_K as we have seen in the proof of Proposition 1. In particular, s_G annihilates Cl_K. This implies that the exponent of Cl_F divides $p-1$ since the norm map $Cl_K \to Cl_F$ is surjective. Now, we obtain $h_F = 1$ from the second assumption. □

Remark 2. At present, we have no example of an abelian field F which satisfies (H_p) for some p but $h_F > 1$. On the other hand, Byott *et al.* [2, §6.3] give an example of a non-Galois number field F satisfying (H_5) but $h_F = 2$. It is of degree 4 and unramified at 5 over $\mathbf{Q}$, and has exactly 2 real infinite places.

3. Proof of Proposition 2. The following lemmas are consequences of (1), and were shown in [12, Proposition 6] and in [11, Lemma 5.1], respectively.

Lemma 1 ([12]). *Let F be a totally real number field, p a prime number and $K = F(\zeta_p)$. If F satisfies (H_p), then the exponent of the minus class group Cl_K^- divides $2h_p^-$.*

Lemma 2 ([11]). *Let p be a prime number with $p \equiv 3 \bmod 4$, and let $q = (p-1)/2$. Let F be a totally real number field unramified at p, and let $N = F(\sqrt{-p})$ and $K = F(\zeta_p)$. Assume that the following conditions are satisfied:*

(I) *q is a prime number.*

(II) *The prime number 2 remains prime in $\mathbf{Q}(\zeta_q)$.*

(III) $h_K = h_K^- = 2^{q-1}$.

(IV) $h_N = 1$.

(V) $(\mathcal{O}_K/\varpi)^\times = \mathcal{O}_K^\times \bmod \varpi$ *where* $\varpi = \zeta_p - 1$.

Then F satisfies the condition (H_p).

Proof of Proposition 2. We use the same notation as in §2. Let $p \geq 7$ be a prime number with $h(\mathbf{Q}(\sqrt{-p})) = 1$. Let F be a real abelian field satisfying (H_p), and $N = F(\sqrt{-p})$, $K = F(\zeta_p)$. Then $F/\mathbf{Q}$ is unramified at p by [5, Theorem 1.1], and $h_N = 1$ by Proposition 1. All imaginary abelian fields M with $h_M = 1$ are determined by Yamamura [18]. In our setting where $M = N = F(\sqrt{-p})$, we see that $F/\mathbf{Q}$ is unramified at p and $h_N = 1$ if and only if (i) $p = 7$ and F equals $\mathbf{Q}(\sqrt{5})$, $\mathbf{Q}(\sqrt{13})$, $\mathbf{Q}(\sqrt{61})$ or the cubic cyclic field of conductor 9 or 13 or (ii) $p = 11$ and F equals $\mathbf{Q}(\sqrt{2})$, $\mathbf{Q}(\sqrt{17})$ or the cubic cyclic field of conductor 7.

For each of the above 8 pairs (p, F), we check whether or not the condition (H_p) is satisfied. For these pairs, we have $p = 7$ or 11, and hence $h_p^- = 1$. Therefore, by Lemma 1, h_K^- is necessarily a power of 2 if the condition (H_p) is satisfied. Among the 8 pairs, h_K^- is a power of 2 only when $p = 7$ and $F = \mathbf{Q}(\sqrt{5})$ or $\mathbf{Q}(\sqrt{13})$ or when $p = 11$ and $F = \mathbf{Q}(\cos 2\pi/7)$. We can check this by a table of Hasse [7, Tafel II] (see resp. Yoshino and Hirabayashi [21,22]) on relative class numbers of imaginary abelian fields of conductor f with $f \leq 100$ (resp. $100 < f < 200$), except for the case where $p = 7$ and $F = \mathbf{Q}(\sqrt{61})$. For the exceptional case, we see that $h_K^- = 19$ by a large table of Yamamura [19] on relative class numbers of imaginary abelian fields of non prime power conductor < 10000. For this case, see also Remark 3.

Let us deal with the remaining three cases. When $p = 11$ and $F = \mathbf{Q}(\cos 2\pi/7)$, we have already shown in [11, p. 93] that (H_p) is satisfied using Lemma 2. Let us deal with the case where $p = 7$ and $F = \mathbf{Q}(\sqrt{5})$ or $\mathbf{Q}(\sqrt{13})$. As $p = 7$ remains prime in F, the multiplicative $(\mathcal{O}_K/\varpi)^\times = (\mathcal{O}_F/7)^\times$ is a cyclic group of order 48. Let $\epsilon = (1+\sqrt{5})/2$ or $(3+\sqrt{13})/2$, and $\xi = 1 + \zeta_7$ ($\equiv 2 \bmod \varpi$). These are units of K. We easily see that the orders of the classes $[\epsilon]$ and $[\xi]$ in $(\mathcal{O}_K/\varpi)^\times$ are equal to 16 and 3, respectively. Thus, the condition (V) in Lemma 2 is satisfied in both cases. When $F = \mathbf{Q}(\sqrt{5})$, we have $h_K = 1$ by [18], and hence the ray class group $Cl_{K,\varpi}$ is trivial as (V) is satisfied. Therefore, F satisfies (H_7) by (1) and (3). Finally, let $F = \mathbf{Q}(\sqrt{13})$. The conditions (I) and (II) in Lemma 2 are clearly satisfied. We have $h_{K^+} = 1$ and $h_K^- = 2^2$ by Mäki [14, p. 74] and [7, Tafel II], respectively. Here, K^+ is the maximal real subfield of K. Further, $h_N = 1$ by [18]. Hence, the conditions (III) and (IV) are satisfied. Therefore, F satisfies (H_7) by Lemma 2. □

Remark 3. Let $K = \mathbf{Q}(\sqrt{61}, \zeta_7)$. We can also show that h_K^- is not a power of 2 as follows: Let $\tilde{h}_K^+$ be the narrow class number of the maximal real subfield K^+. We have $\tilde{h}_K^+ = 1$ by [14, p. 88]. As K/K^+ is ramified only at the unique prime ideal of K^+ over 7 and the infinite prime divisors, we can show that h_K is odd. However, we have $h_K > 1$ by [18], and hence we see that h_K^- $(= h_K)$ is not a 2-power.

Acknowledgement. The author thanks the referee for carefully reading the manuscript and for several valuable comments which improved the presentation of the paper.

References

[1] J. Brinkhuis, Normal integral bases and complex conjugation, J. Reine Angew. Math. **375/376** (1987), 157–166.

[2] N. P. Byott, J. E. Carter, C. Greither and H. Johnston, On the restricted Hilbert-Speiser and Leopoldt properties, Illinois J. Math. **55** (2011), no. 2, 623–639.

[3] 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, Arch. Math. (Basel) **83** (2004), no. 6, vi–vii.

[4] D. A. Cox, *Primes of the form $x^2 + ny^2$*, A Wiley-Interscience Publication, Wiley, New York, 1989.

[5] C. Greither and H. Johnston, On totally real Hilbert-Speiser fields of type C_p, Acta Arith. **138** (2009), no. 4, 329–336.

[6] C. Greither, D. R. Replogle, K. Rubin and A.

Srivastav, Swan modules and Hilbert-Speiser number fields, J. Number Theory **79** (1999), no. 1, 164–173.
[7] H. Hasse, *Über die Klassenzahl abelscher Zahlkörper*, Akademie Verlag, Berlin, 1952.
[8] T. Herreng, Sur les corps de Hilbert-Speiser, J. Théor. Nombres Bordeaux **17** (2005), no. 3, 767–778.
[9] 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.
[10] H. Ichimura, Normal integral bases and ray class groups, Acta Arith. **114** (2004), no. 1, 71–85.
[11] H. Ichimura, Hilbert-Speiser number fields and the complex conjugation, J. Math. Soc. Japan **62** (2010), no. 1, 83–94.
[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), no. 2, 179–191.
[13] H. Ichimura and H. Sumida-Takahashi, On Hilbert-Speiser type imaginary quadratic fields, Acta Arith. **136** (2009), no. 4, 385–389.
[14] S. Mäki, *The determination of units in real cyclic sextic fields*, Lecture Notes in Mathematics, 797, Springer, Berlin, 1980.
[15] L. R. McCulloh, Galois module structure of elementary abelian extensions, J. Algebra **82** (1983), no. 1, 102–134.
[16] W. Sinnott, On the Stickelberger ideal and the circular units of an abelian field, Invent. Math. **62** (1980/81), no. 2, 181–234.
[17] L. C. Washington, *Introduction to cyclotomic fields*, 2nd ed., Graduate Texts in Mathematics, 83, Springer, New York, 1997.
[18] K. Yamamura, The determination of the imaginary abelian number fields with class number one, Math. Comp. **62** (1994), no. 206, 899–921.
[19] K. Yamamura, `http://tnt.math.se.tmu.ac.jp/pub/ac11/rcn/composite/`
[20] Y. Yoshimura, Abelian number fields satisfying the Hilbert-Speiser condition at $p = 2$ or 3, Tokyo J. Math. **32** (2009), no. 1, 229–235.
[21] K. Yoshino and M. Hirabayashi, On the relative class number of the imaginary abelian number field I, Memoirs of the College of Liberal Arts, Kanazawa Medical University **9** (1981), 5–53.
[22] K. Yoshino and M. Hirabayashi, On the relative class number of the imaginary abelian number field II, Memoirs of the College of Liberal Arts, Kanazawa Medical University **10** (1982), 33–81.