TOKYO J. MATH.
VOL. 32, NO. 1, 2009

Abelian Number Fields Satisfying the Hilbert-Speiser Condition at $p = 2$ or 3

Yusuke YOSHIMURA

Ibaraki University

(Communicated by T. Kawasaki)

1. Introduction

Let F be a number field and $\mathcal{O}_F$ the ring of integers of F. Let N/F be a finite Galois extension with group G. We say that N/F has a normal integral basis (NIB for short) when $\mathcal{O}_N$ is cyclic over the group ring $\mathcal{O}_F[G]$. Hilbert and Speiser proved that any finite tame abelian extension of the rationals $\mathbf{Q}$ has a NIB. Let p be a prime number. We say that F satisfies the condition (H_p) when any tame cyclic extension N/F of degree p has a NIB. As mentioned above, $\mathbf{Q}$ satisfies (H_p) for any prime number p. On the other hand, Greither *et al.*[4] proved that any number field $F \neq \mathbf{Q}$ does not satisfy (H_p) for infinitely many p. So, it is of interest to determine which number field satisfies (H_p) or not. All imaginary quadratic fields satisfying (H_2) were determined by Carter [1]. There are exactly 3 such fields. All quadratic fields satisfying (H_3) were determined by [1] and Ichimura [2], independently. There are exactly 12 such fields. The purpose of this paper is to determine all imaginary abelian fields satisfying (H_2) and all abelian fields satisfying (H_3). We obtained the following result.

THEOREM.
(I) *Among all imaginary abelian fields F with $[F : \mathbf{Q}] \geq 3$, there exist exactly* 14 *fields satisfying (H_2), which are given in Table* 1 *at the end of this paper.*
(II) *Among all abelian fields F with $[F : \mathbf{Q}] \geq 3$, there exist exactly* 15 *fields satisfying (H_3), which are given in Table* 2.

2. Lemmas

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 $(a) = a\mathcal{O}_F$. In particular, $Cl_F = Cl_F(1)$ is the absolute class group

Received April 3, 2008; revised September 18, 2008

of F. For simplicity, put $[\mathcal{O}_F^\times]_p = \mathcal{O}_F^\times \bmod p$ and

$$V_{F,p} = \frac{(\mathcal{O}_F/p)^\times}{[\mathcal{O}_F^\times]_p}\,.$$

Clearly, this is a subgroup of $Cl_F(p)$. Let $K = F(\zeta_p)$ and $\Delta_F = \mathrm{Gal}(K/F)$. Here, ζ_p is a primitive pth root of unity. Now, the Galois group Δ_F acts on $Cl_K(p)$, and $Cl_K(p)^{\Delta_F}$ denotes the Galois invariant part. We put $\pi = \zeta_p - 1$.

The following three propositions play important roles in the proof of Theorem.

PROPOSITION 1 ([2]). *A number field F satisfies (H_2) if and only if $Cl_F(2)$ is trivial.*

PROPOSITION 2 ([4]). *Let $p \geq 3$. If F satisfies (H_p), then the exponent of $V_{F,p}$ divides $(p-1)^2/2$. In particular, the p-rank of $V_{F,p}$ is zero.*

PROPOSITION 3 ([2, 3]). *Let $p \geq 3$ be a prime number, F a number field and $K = F(\zeta_p)$.*

(I) *When $\zeta_p \in F^\times$, F satisfies (H_p) if and only if $Cl_F(p)$ is trivial.*

(II) *Assume that $[K : F] = 2$. If F satisfies (H_p), then the ray class groups $Cl_K(\pi)$ and $Cl_K(p)^{\Delta_F}$ are trivial. Further, when $p = 3$, the converse holds.*

In the following, we show some lemmas which are necessary to prove Theorem.

LEMMA 1. *Let F be a number field, and $K = F(\zeta_p)$. Assume that $[K : F] \leq 2$. If F satisfies (H_p), then the class number h_F of F is 1.*

PROOF. When $\zeta_p \in F^\times$, the assertion follows immediately from Proposition 1 and Proposition 3 (I). Thus, we deal with the case $[K : F] = 2$. Let H_F be the Hilbert class field of F. From class field theory, $\mathrm{Gal}(H_F/F) \simeq Cl_F$. By Proposition 3 (II), if F satisfies (H_p), then $Cl_K = \{0\}$ and $H_K = K$. It follows that $H_F K = K$. As $[K : F] = 2$, we have $H_F = F$ or K. Clearly, if $H_F = F$, then $h_F = 1$. We discuss the case $H_F = K$.

Assume that F satisfies (H_p) and that $H_F = K$. We compare the p-ranks of $(\mathcal{O}_F/p\mathcal{O}_F)^\times$ and $[\mathcal{O}_F^\times]_p$. First, we calculate the p-rank of $(\mathcal{O}_F/p\mathcal{O}_F)^\times$. Let $p = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_g^{e_g}$ be the prime factorization in F. Let $n = [F : \mathbf{Q}]$ and f_i be the degree of the prime ideal $\mathfrak{p}_i$. We have $n = \sum_{i=1}^{g} e_i f_i$. We have a canonical decomposition

$$(\mathcal{O}_F/p\mathcal{O}_F)^\times \simeq \bigoplus_{i=1}^{g} (\mathcal{O}_F/\mathfrak{p}_i^{e_i})^\times\,.$$

Let $k_i \geq 1$ be the integer such that

$$p(k_i - 1) < e_i \leq pk_i\,. \tag{1}$$

Let

$$X_{k_i} = \{[a]_{\mathfrak{p}_i^{e_i}} \mid a \in \mathcal{O}_F,\, a \equiv 1 \bmod \mathfrak{p}_i^{k_i}\}\,,$$

where $[a]_{\mathfrak{p}_i^{e_i}} \in (\mathcal{O}_F/\mathfrak{p}_i^{e_i})^\times$ denotes the class containing a. For a finite abelian group A and a prime number p, $R_p(A)$ denotes the p-rank of A. By the choice of k_i, we easily see that the exponent of X_{k_i} is p and that $|X_{k_i}| = p^{f_i(e_i-k_i)}$. Thus, we obtain $R_p(X_{k_i}) = f_i(e_i - k_i)$, and

$$R_p\left((\mathcal{O}_F/\mathfrak{p}_i^{e_i})^\times\right) \geq f_i(e_i - k_i)\,.$$

Summing up for all i, we have

$$R_p((\mathcal{O}_F/p)^\times) \geq \sum_{i=1}^{g} f_i(e_i - k_i)\,.$$

Next, we calculate $R_p([\mathcal{O}_F^\times]_p)$. Since $H_F = K = F(\zeta_p)$, all primes of F including the infinite primes are unramified in K. This implies that F is totally imaginary. Therefore, as $\zeta_p \notin F^\times$, we see that

$$R_p([\mathcal{O}_F^\times]_p) \ \leq \frac{n}{2} - 1 = \left(\sum_{i=1}^{g} f_i \frac{e_i}{2}\right) - 1$$

by the Dirichlet unit theorem.

When $e_i \geq 2k_i$ for all $1 \leq i \leq g$, we have

$$\sum_{i=1}^{g} f_i(e_i - k_i) - \left(\left(\sum_{i=1}^{g} f_i e_i/2\right) - 1\right) > 0$$

and hence

$$R_p((\mathcal{O}_F/p)^\times) \geq \sum_{i=1}^{g} f_i(e_i - k_i) > \left(\sum_{i=1}^{g} f_i \frac{e_i}{2}\right) - 1 \geq R_p([\mathcal{O}_F^\times]_p)\,.$$

This contradicts Proposition 2.

Now, we deal with the case $e_i < 2k_i$ for some i. From the assumption, K/F is an unramified extension. The ramification index of p in $\mathbf{Q}(\zeta_p)/\mathbf{Q}$ is $p-1$. Hence, each e_i is divisible by $p-1$. In particular, $e_i \geq p-1$. From $e_i < 2k_i$ and (1) , it follows that

$$k_i < \frac{p}{p-2}\,.$$

We first treat the case $p \geq 5$. By the above inequality, $k_i = 1$. Therefore, $2k_i = 2 > e_i$, which is impossible since $e_i \geq p-1 \geq 4$. Next, let $p = 3$. In this case, $k_i = 1$ or 2 from the above inequality. Then, we see from (1) and $(p-1)|e_i$ that $(k_i, e_i) = (2, 4)$, $(2, 6)$ or $(1, 2)$, which contradicts $e_i < 2k_i$. $\square$

LEMMA 2. *Let F be a number field such that $\zeta_3 \notin F^\times$, and $K = F(\zeta_3)$. Assume that 3 is unramified in $F/\mathbf{Q}$. The Galois invariant part $Cl_K(3)^{\Delta_F}$ is trivial if $Cl_K(\pi)$ is trivial, where $\pi = \zeta_3 - 1$.*

PROOF. Since $Cl_K(\pi)$ is trivial, we have $Cl_K(3) = V_{K,3}$. For an element $\alpha \in \mathcal{O}_K$, $[\alpha]_3$ (resp. $[\alpha]_\pi$) denotes the class in $Cl_K(3)$ (resp. $Cl_K(\pi)$) containing the principal ideal $\alpha\mathcal{O}_K$. Let $[\alpha]_3$ be any element of $V_{K,3}$. As $Cl_K(\pi) = \{0\}$, there exists some unit $\varepsilon \in \mathcal{O}_K^\times$ such that $\alpha \equiv \varepsilon \bmod \pi$. Let $\beta = \varepsilon^{-1}\alpha$. It follows that $[\beta]_3 = [\alpha]_3$ and $\beta = 1 + \pi x$ for some $x \in \mathcal{O}_K$. Noting that $(3) = (\pi^2)$, we see that

$$\beta^3 = 1 + 3\pi x + 3\pi^2 x^2 + \pi^3 x^3 \equiv 1 \mod \pi^3 ,$$

and hence $[\beta]_3^3 = 1$. Thus, the order of $[\beta]_3$ is 1 or 3. Assume that $[\alpha]_3 = [\beta]_3 \in Cl_K(3)^{\Delta_F}$. Then, we see that $\beta^{J-1} = \beta^{1+J}/\beta^2 \equiv \eta \bmod 3$ for some $\eta \in \mathcal{O}_K^\times$. Here, J is the nontrivial element of Δ_F. By the assumption, 3 is unramified in $F/\mathbf{Q}$. Therefore, as $\beta^{1+J} \equiv 1 \bmod \pi$, we find that $\beta^{1+J} \equiv 1 \bmod 3$. As $\beta^2 \equiv \eta^{-1} \bmod 3$, we have $[\beta]_3^2 = 1$. Consequently, we obtain $[\beta]_3 = 1$ and $Cl_K(3)^{\Delta_F}$ is trivial. □

LEMMA 3. *Let F be a number field with $\zeta_3 \notin F^\times$, $K = F(\zeta_3)$ and $\Delta_F = Gal(K/F)$. The group $Cl_K(3)^{\Delta_F}$ is trivial if both Cl_K and $V_{F,3}$ are trivial and $|Cl_K(3)|$ is odd.*

PROOF. We use the same notation as in the proof of Lemma 2. As Cl_K is trivial, we have $Cl_K(3) = V_{K,3}$. For an element $\alpha \in \mathcal{O}_K$ with $(\alpha, 3) = 1$, assume that $[\alpha]_3 \in Cl_K(3)^{\Delta_F}$. Then, there exists a unit $\varepsilon \in \mathcal{O}_K^\times$ such that $\alpha^{1-J} \equiv \varepsilon \bmod 3$. Since $\alpha^{1+J} \in \mathcal{O}_F$ and $V_{F,3}$ is trivial, we find that $\alpha^{1+J} \equiv \eta \bmod 3$ for some $\eta \in \mathcal{O}_F^\times$. Therefore, we have $\alpha^2 \equiv \varepsilon\eta \bmod 3$ and $[\alpha]_3^2 = 1$. As $|Cl_K(3)|$ is odd, we obtain $[\alpha]_3 = 1$. Consequently, $Cl_K(3)^{\Delta_F}$ is trivial. □

3. Proof of Theorem

All imaginary abelian fields F with $h_F = 1$ were determined by Yamamura [6]. Therefore, we can determine imaginary abelian fields F satisfying (H_2) and abelian fields satisfying (H_3) using the results in § 2 and some computation on ray class groups. We practiced the computation using the computational software KASH [5].

A number field F satisfies (H_2) only when $h_F = 1$. Using Yamamura's table in [6], we see that there are 163 imaginary abelian fields F with $[F : \mathbf{Q}] \geq 3$ and $h_F = 1$. We computed $Cl_F(2)$ and determined those satisfying (H_2). The result is given in Table 1.

A number field F with $\zeta_3 \in F^\times$ satisfies (H_3) only when $h_F = 1$. By the table of [6], there are 58 abelian fields F satisfying $[F : \mathbf{Q}] \geq 3$, $\zeta_3 \in F^\times$ and $h_F = 1$. We computed $Cl_F(3)$ and determined those satisfying (H_3). There are exactly three F's satisfying (H_3). They are numbered 6, 7, 8 in Table 2.

Now, let F be an abelian field with $[F : \mathbf{Q}] \geq 3$ and $\zeta_3 \notin F^\times$, and let $K = F(\zeta_3)$. By Proposition 3, if F satisfies (H_3), then $Cl_K(\pi) = \{0\}$, and hence $h_K = 1$. By the table of [6], there are 10 fields K satisfying $\zeta_3 \in K$, $h_K = 1$ and $Cl_K(\pi) = \{0\}$. These 10 K's are listed in the second column in Table 3. For each of these K, we gave the subfields F such that $[F : \mathbf{Q}] \geq 3$, $\zeta_3 \notin F^\times$ and $K = F(\zeta_3)$ in the fourth column in Table 3. There are 16 such F's.

We pick out the fields satisfying (H_3) from the F's in Table 3. There are 9 fields F such that 3 is unramified in $F/\mathbf{Q}$ in Table 3. We marked them with $\circ$. By Lemma 2 and Proposition 3, these fields satisfy (H_3).

For the remaining fields F, if F satisfies (H_3), then $h_F = 1$ by Lemma 1. We computed h_F and give the table of the fields with $h_F = 1$. There are exactly 3 such fields. We marked these 3 fields with $\bullet$ in Table 3. The order of the ray class group $Cl_K(3)$ of these fields are 3. For these fields, we see that $Cl_F(3) = V_{F,3} = \{0\}$, and that $Cl_K(3)^{\Delta_F} = \{0\}$ from Lemma 3. Hence, they satisfy (H_3). Consequently, there are exactly 15 abelian fields F with $[F : \mathbf{Q}] \geq 3$ satisfying (H_3), so the proof is completed.

4. Tables

We now give the above mentioned tables. Each field is expressed by the corresponding character group. We use the following notations in order to express generators of associated character groups. χ_4 denotes the unique primitive Dirichlet character of conductor 4. For an odd prime number p, χ_p denotes a primitive Dirichlet character of conductor p and order $p-1$. For a prime power $q = p^m$ $(\neq 4)$, ψ_q denotes an even primitive Dirichlet character of conductor q and of order p^{m-1} or 2^{m-2} according as p is odd or $p = 2$.

4.1. Table 1. Imaginary abelian fields F with $[F : \mathbf{Q}] \geq 3$ satisfying the condition (H_2).

No.	Degree	Generators	Simple expression
1	4	χ_5	$\mathbf{Q}(\zeta_5)$
2		χ_4, ψ_8	$\mathbf{Q}(\sqrt{-1}, \sqrt{2})$
3		χ_3, χ_5^2	$\mathbf{Q}(\zeta_3, \sqrt{5})$
4		χ_4, χ_5^2	$\mathbf{Q}(\sqrt{-1}, \sqrt{5})$
5		χ_7^3, χ_5^2	$\mathbf{Q}(\sqrt{-7}, \sqrt{5})$
6		χ_3, χ_4	$\mathbf{Q}(\zeta_{12})$
7		χ_3, χ_7^3	$\mathbf{Q}(\zeta_3, \sqrt{-7})$
8		χ_4, χ_7^3	$\mathbf{Q}(\sqrt{-1}, \sqrt{-7})$
9	6	χ_7	$\mathbf{Q}(\zeta_7)$
10		$\chi_3\psi_9^2$	$\mathbf{Q}(\zeta_9)$
11		χ_7^3, ψ_9	$\mathbf{Q}(\sqrt{-7}, \cos(2\pi/9))$
12		χ_7^3, χ_{13}^4	
13	8	χ_3, χ_5	$\mathbf{Q}(\zeta_{15})$
14		$\chi_4, \psi_8, \chi_{11}^5$	$\mathbf{Q}(\sqrt{-1}, \sqrt{2}, \sqrt{-11})$

4.2. Table 2. Abelian fields F with $[F:\mathbf{Q}] \geq 3$ satisfying the condition (H_3).

No.	Degree	Generators	Simple expression
1	3	ψ_9	$\mathbf{Q}(\cos(2\pi/9))$
2		χ_7^2	$\mathbf{Q}(\cos(2\pi/7))$
3		χ_{13}^4	
4		χ_{31}^{10}	
5		χ_{43}^{14}	
6	4	χ_3, χ_4	$\mathbf{Q}(\zeta_{12})$
7		$\chi_3, \chi_4\psi_8$	$\mathbf{Q}(\zeta_3, \sqrt{-2})$
8		χ_3, χ_{11}^5	$\mathbf{Q}(\zeta_3, \sqrt{-11})$
9		ψ_{16}	$\mathbf{Q}(\cos(2\pi/16))$
10		χ_5	$\mathbf{Q}(\zeta_5)$
11		$\chi_3\chi_5$	$\mathbf{Q}(\cos(2\pi/15))$
12		ψ_8, χ_4	$\mathbf{Q}(\sqrt{2}, \sqrt{-1})$
13		$\psi_8, \chi_4\chi_3$	$\mathbf{Q}(\sqrt{2}, \sqrt{3})$
14	5	χ_{11}^2	$\mathbf{Q}(\cos(2\pi/11))$
15	6	χ_5^2, χ_7^2	$\mathbf{Q}(\sqrt{5}, \cos(2\pi/7))$

4.3. Table 3. Abelian fields $K = F(\zeta_3)$ and F such that $[F:\mathbf{Q}] \geq 3$, $[K:F] = 2$ and $Cl_K(\pi) = \{0\}$.

Degree	Generator of K	Simple expression of K	Generator of F	
6	χ_3, ψ_9	$\mathbf{Q}(\zeta_9)$	ψ_9	•
	χ_3, ψ_7^2	$\mathbf{Q}(\zeta_3, \cos(2\pi/7))$	ψ_7^2	∘
	χ_3, χ_{13}^4		χ_{13}^4	∘
	χ_3, χ_{31}^{10}		χ_{31}^{10}	∘
	χ_3, χ_{43}^{14}		χ_{43}^{14}	∘
8	χ_3, ψ_{16}	$\mathbf{Q}(\zeta_3, \cos(2\pi/16))$	ψ_{16}	∘
			$\chi_3\psi_{16}$	
	χ_3, χ_5	$\mathbf{Q}(\zeta_{15})$	χ_5	∘
			$\chi_3\chi_5$	•
	χ_3, ψ_8, χ_4	$\mathbf{Q}(\sqrt{-3}, \sqrt{2}, \sqrt{-1})$	ψ_8, χ_4	∘
			$\chi_3\psi_8, \chi_4$	
			$\psi_8, \chi_4\chi_3$	•
			$\chi_3\psi_8, \chi_3\chi_4$	
10	χ_3, χ_{11}^2	$\mathbf{Q}(\zeta_3, \cos(2\pi/11))$	χ_{11}^2	∘
12	$\chi_3, \chi_5^2, \chi_7^2$	$\mathbf{Q}(\zeta_3, \sqrt{5}, \cos(2\pi/7))$	χ_5^2, χ_7^2	∘
			$\chi_3\chi_5^2, \chi_7^2$	

ACKNOWLEDGEMENTS. I express deepest gratitude to my thesis advisor, Humio Ichimura, for helpful advice on this paper. Also I thank the referee for carefully reading the original manuscript and pointing out several mistakes. Some calculations were computed using the computer software KASH [5].

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] 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.

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

[4] 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.

[5] M. E. POHST, *et al.* , KANT/KASH, Computer software, 1987–2002.

[6] K. YAMAMURA, The determination of the imaginary abelian number fields with class number one. Math. Comp. **62** (1994), no. 206, 899–921.

Present Address:
GRADUATE SCHOOL OF SCIENCE AND ENGINEERING,
IBARAKI UNIVERSITY,
BUNKYO, MITO, IBARAKI, 310–8512 JAPAN.