ACTA ARITHMETICA
Online First version

Monogenity for certain non-cyclic abelian extension fields

by

Nadia Khan, Toru Nakahara, Hiroshi Sekiguchi
and Tsuyoshi Uehara

To the memory of Prof. Marie-Nicole Gras

Abstract. We prove three results on monogenity of non-cyclic abelian extension fields over the rationals $\mathbb{Q}$. The first one is that for any odd prime cyclotomic field $k_p = \mathbb{Q}(\zeta_p)$ and any quadratic field $k = \mathbb{Q}(\sqrt{\ell})$ of discriminant ℓ prime to p, the non-cyclic abelian field k_pk is non-monogenic if $\ell < -4$ with $\ell \nmid (p \pm 1)$ or $\ell > 4$. The second is that if $k_n^+ = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$ is the maximal real subfield of an nth cyclotomic field with $n \geq 5$, $n \not\equiv 2 \pmod 4$ and if $k = \mathbb{Q}(\sqrt{-m})$ is an imaginary quadratic field of discriminant $-m < -4$ with $(m, n) = 1$, then the composite field $k_n^+ k$ is non-monogenic. The third is that a maximal imaginary subfield $\mathbb{Q}(\zeta_q - \zeta_q^{-1})$ of a cyclotomic field k_q with $q > 4$, $q \equiv 0 \pmod 4$ is monogenic.

1. Introduction. In connection with Hasse's problem to determine the monogenity of an algebraic number field, we consider certain composite abelian extension fields K over the rationals $\mathbb{Q}$. This problem was proposed by W. Narkiewicz in general [8]. Our claims are:

Theorem A. *For an odd prime p let $k_p = \mathbb{Q}(\zeta_p)$ be the pth cyclotomic field, and let $k = \mathbb{Q}(\sqrt{\ell})$ be a quadratic field of discriminant ℓ with $(\ell, p) = 1$. Then the non-cyclic abelian field $K = k_pk = \mathbb{Q}(\zeta_p, \sqrt{\ell})$ is non-monogenic if $\ell < -4$ and $\ell \nmid (p \pm 1)$, and also if $\ell > 4$.*

Theorem B. *For an integer $n \geq 5$ with $n \not\equiv 2 \pmod 4$ let $k_n^+ = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$ be the maximal real subfield of the nth cyclotomic field. Let $k = \mathbb{Q}(\sqrt{-m})$ be an imaginary quadratic field of discriminant $-m < -4$ with $(m, n) = 1$. Then the composite field $K = k_n^+ k = \mathbb{Q}(\zeta_n + \zeta_n^{-1}, \sqrt{-m})$ is non-monogenic.*

2020 *Mathematics Subject Classification*: Primary 11R04; Secondary 11R18, 11R32.
Key words and phrases: non-monogenic field, cyclotomic field, non-cyclic field, field different.
Received 6 February 2025; revised 19 June 2025.
Published online 4 May 2026.

DOI: 10.4064/aa250206-26-7

Theorem C. *Let $q > 4$ be a rational integer divisible by 4 and ζ be a primitive qth root of unity. Then $K = \mathbb{Q}(\zeta - \zeta^{-1})$ is an imaginary subfield of $k_q = \mathbb{Q}(\zeta)$ with $[k_q : K] = 2$ and $Z_K = \mathbb{Z}[\zeta - \zeta^{-1}]$.*

Remark 1.1. In Theorem A we exclude the cases of $k = \mathbb{Q}(\sqrt{-3})$ and $k = \mathbb{Q}(\sqrt{-4})$. Since $\mathbb{Q}(\zeta_p, \sqrt{-3}) = \mathbb{Q}(\zeta_{3p})$ if $p \neq 3$ and $\mathbb{Q}(\zeta_p, \sqrt{-4}) = \mathbb{Q}(\zeta_{4p})$, these fields are monogenic. When k is the Gauß field $\mathbb{Q}(\sqrt{-4})$ and $n \geq 5$ is odd, the assertion for $K = k_n^+ k$ in Theorem B is not true. Indeed, K can be written as

$$\mathbb{Q}((\zeta_n + \zeta_n^{-1})\zeta_4) = \mathbb{Q}(\zeta_n\zeta_4 - \zeta_n^{-1}\zeta_4^{-1}) = \mathbb{Q}(\zeta_{4n} - \zeta_{4n}^{-1}).$$

In general, $\mathbb{Q}(\zeta_q - \zeta_q^{-1})$ is monogenic if $q \equiv 0 \pmod 4$. We will show it in Theorem C.

Let F be an algebraic number field over $\mathbb{Q}$ of degree $[F : \mathbb{Q}] = n$. Let Z_F denote the ring of integers in F, and $\mathbb{Z}$ the ring of rational integers. If there exists $\xi \in F$ such that $Z_F = \mathbb{Z}[\xi] = \mathbb{Z}[1, \xi, \ldots, \xi^{n-1}]$ is of rank n over $\mathbb{Z}$, we say that the field F is *monogenic* or the ring Z_F has a power integral basis. In §2, we give a proof of Theorem A on non-monogenity of real quadratic extensions over a prime cyclotomic field following an idea in [5], which applies the works of Mushtaq Ahmad, Nadia Khan, Hiroshi Sekiguchi, Yasuo Motoda, Mamoona Sultan and the second author [1, 6, 7, 10]. In §3 we prove Theorem B on non-monogenity of imaginary quadratic extensions over the maximal real subfield of a cyclotomic field. Theorem C, proved in §4, involves work on monogenic phenomena of Syed Inayat Ali Shah et al. [9] and is related to work of István Gaál [3]. In §5, we describe two examples of Theorem A. In $(\mathrm{A_I})$ and $(\mathrm{A_{II}})$ we shall introduce the second simplest non-monogenic fields $K = k_7 \cdot k$ with $[K : \mathbb{Q}] = 12$, whose conductors are equal to $7 \cdot 11$ and $7 \cdot 5$ with an imaginary quadratic subfield $k = \mathbb{Q}(\sqrt{-11})$ and a real $k = \mathbb{Q}(\sqrt{5})$, respectively. Based on the experiments and the results in [5] concerning the octic fields $K = k_5 \cdot k$ with $k = \mathbb{Q}(\sqrt{-7})$ and $k = \mathbb{Q}(\sqrt{7})$, we discuss the non-monogenity of the fields of Theorem A and obtain a method of proving it.

In the second edition of his book on monogenity of algebraic number fields István Gaál has given a list of 232 monographs and recent developments on monogenity and power integral bases [2, 4].

2. Proof of Theorem A. The next lemma is fundamental to deciding about monogenity of non-cyclic but abelian fields K. Let $\zeta = \zeta_p$ be a primitive root of unity for an odd prime p. We prove that Z_{k_p} has a relative integral basis $\{1, \zeta\}$ over $Z_{k_p^+}$, where k_p^+ is the maximal real subfield of $k_p = \mathbb{Q}(\zeta)$.

Lemma 2.1. *Let η be the Gauß period $\zeta + \zeta^{-1}$ of length 2. Then*

$$Z_{k_p} = Z_{k_p^+}[1, \zeta] = \mathbb{Z}[1, \eta, \eta^2, \ldots, \eta^{\frac{p-1}{2}-1}][1, \zeta] \quad \textit{as a } \mathbb{Z}\textit{-module.}$$

Proof. We have $Z_{k_p^+} = \mathbb{Z}[1, \eta, \ldots, \eta^{\frac{p-1}{2}-1}]$. Since $Z_{k_p} \supseteq Z_{k_p^+}[1, \zeta]$, we have to show the converse inclusion [11]. We have

$$\begin{aligned} &1, \zeta \in \mathbb{Z}[1, \zeta], \quad \zeta^{-1} = \eta - \zeta, \zeta^2 = \eta\zeta - 1 \in \mathbb{Z}[1, \eta][1, \zeta], \\ &\zeta^{-2} = \eta\zeta^{-1} - 1 = \eta(\eta - \zeta) - 1 \in \mathbb{Z}[1, \eta, \eta^2][1, \zeta], \\ &\zeta^3 = \zeta(\zeta\eta - 1) = \eta^2\zeta - \eta - \zeta \in \mathbb{Z}[1, \eta, \eta^2][1, \zeta] \end{aligned}$$

and

$$\zeta^{-3} = \eta^2\zeta^{-1} - \eta - \zeta^{-1} = \eta^2 \cdot (\eta - \zeta) - \eta - (\eta - \zeta) \in \mathbb{Z}[1, \eta, \eta^2, \eta^3][1, \zeta].$$

Applying $\zeta^{i+1} = \zeta^i\eta - \zeta^{i-1}$ and $\zeta^{-(i+1)} = \zeta^{-i}\eta - \zeta^{-(i-1)}$, by induction we obtain

$$\zeta^i, \zeta^{-(i-1)} \in \mathbb{Z}[1, \eta, \ldots, \eta^{i-1}][1, \zeta] \subseteq \mathbb{Z}[1, \eta, \ldots, \eta^{\frac{p-1}{2}-1}][1, \zeta]$$

for any i with $1 \le i \le \frac{p-1}{2}$. It follows that $Z_{k_p} \subseteq Z_{k_p^+}[1, \zeta]$. ∎

We note that the fields K in Theorems A and B are composed of two monogenic abelian fields with coprime discriminants. We prove:

LEMMA 2.2. *Let $L, M \neq \mathbb{Q}$ be abelian fields with discriminants d_L, d_M such that $(d_L, d_M) = 1$. Assume that $Z_L = \mathbb{Z}[\alpha]$ and $Z_M = \mathbb{Z}[\beta]$ for some integers $\alpha \in Z_L$ and $\beta \in Z_M$. Then for a given integer ξ in the composite field $K = LM$, the ring $\mathbb{Z}[\xi]$ coincides with Z_K if and only if*

$$\frac{\xi - \xi^\sigma}{\alpha - \alpha^\sigma}, \quad \frac{\xi - \xi^\tau}{\beta - \beta^\tau}, \quad \xi - \xi^{\sigma\tau}$$

are all units for any element $\sigma \neq \iota$ of $\mathrm{Gal}(K/M)$ *and any element $\tau \neq \iota$ of* $\mathrm{Gal}(K/L)$*, where ι is the identity element.*

Proof. We know that the discriminant d_K of K is equal to $d_L^m d_M^n$ with $n = [L : \mathbb{Q}]$, $m = [M : \mathbb{Q}]$ and $Z_K = Z_L Z_M$. We put $G_{K/M} = \mathrm{Gal}(K/M)$, $G_{K/L} = \mathrm{Gal}(K/L)$ and $G_K = \mathrm{Gal}(K/\mathbb{Q})$. Since $L \cap M = \mathbb{Q}$, we have $G_K = G_{K/M} G_{K/L}$, and the maps $\sigma \mapsto \sigma|_L$ and $\sigma \mapsto \sigma|_M$ induce isomorphisms $G_{K/M} \cong G_L = \mathrm{Gal}(L/\mathbb{Q})$ and $G_{K/L} \cong G_M = \mathrm{Gal}(M/\mathbb{Q})$. Denote by $d_K(\xi)$ the discriminant of ξ for $K/\mathbb{Q}$. We recall the different

$$\mathfrak{D}_K(\xi) = \prod_{\iota \neq \rho \in G_K} (\xi - \xi^\rho)$$

of $\xi \in Z_K$ for $K/\mathbb{Q}$. It is known that $N_{K/\mathbb{Q}} \mathfrak{D}_K(\xi) = \pm d_K(\xi)$, and $\mathbb{Z}[\xi] = Z_K$ holds if and only if $d_K(\xi) = \pm d_K$ We write $\mathfrak{D}_K(\xi) = ABC$ with

$$A = \prod_{\sigma \neq \iota} (\xi - \xi^\sigma), \quad B = \prod_{\tau \neq \iota} (\xi - \xi^\tau), \quad C = \prod_{\sigma \neq \iota,\, \tau \neq \iota} (\xi - \xi^{\sigma\tau}),$$

where σ, τ range over the non-trivial elements of $G_{K/M}, G_{K/L}$, respectively. Since $\xi = \sum_{i=1}^n a_i \alpha^{i-1} = \sum_{j=1}^m b_j \beta^{j-1}$ with $a_i \in Z_M$ and $b_j \in Z_L$, the numbers

$$c_\sigma = \frac{\xi - \xi^\sigma}{\alpha - \alpha^\sigma}, \quad c'_\tau = \frac{\xi - \xi^\tau}{\beta - \beta^\tau}$$

are integers for any $\iota \neq \sigma \in G_{K/M}$ and $\iota \neq \tau \in G_{K/L}$. Let c and c' be the product of all c_σ and the product of all c'_τ. By the definition of the different $d_L(\alpha)$ we see that

$$N_{K/M} \prod_{\iota \neq \sigma \in G_{K/M}} (\alpha - \alpha^\sigma) = N_{L/\mathbb{Q}} \prod_{\iota \neq \sigma \in G_L} (\alpha - \alpha^\sigma) = \pm d_L(\alpha) = \pm d_L$$

and $N_{K/\mathbb{Q}} \prod_{\iota \neq \sigma} (\alpha - \alpha^\sigma) = \pm d_L^m$. Hence

$$N_{K/\mathbb{Q}}(A) = N_{K/\mathbb{Q}} \prod_{\iota \neq \sigma \in G_{K/M}} (\alpha - \alpha^\sigma) c_\sigma = \pm d_L^m N_{K/\mathbb{Q}}(c).$$

Similarly, $N_{K/\mathbb{Q}}(B) = \pm d_M^n N_{K/\mathbb{Q}}(c')$. Therefore $d_K(\xi) = \pm d_K = \pm d_L^m d_M^n$ is valid if and only if the norms $N_{K/\mathbb{Q}}(c)$, $N_{K/\mathbb{Q}}(c')$ and $N_{K/\mathbb{Q}}(C)$ are ± 1. This implies the lemma because c_σ, c'_τ and $\xi - \xi^{\sigma\tau}$ are all integers for any $\iota \neq \sigma \in G_{K/M}$ and any $\iota \neq \tau \in G_{K/L}$. ∎

Remark 2.1. Though in this paper we deal with abelian fields only, we shall show that Lemma 2.2 is valid for any composite of two algebraic number fields with coprime discriminants. Let K be an algebraic number field and F its subfield. We denote by $E_{K/F}$ the set of embeddings of K into $\mathbb{C}$ fixing F. Recall that for any $\gamma \in K$ the different

$$\mathfrak{D}_{K/F}(\gamma) = \prod_{\iota \neq \rho \in E_{K/F}} (\gamma - \gamma^\rho)$$

is contained in K, where ι is the identity map of K. Put $E_K = E_{K/\mathbb{Q}}$.

Let $L, M \neq \mathbb{Q}$ be algebraic number fields with coprime discriminants d_L, d_M, and assume that $Z_L = \mathbb{Z}[\alpha]$ and $Z_M = \mathbb{Z}[\beta]$ for some integers $\alpha \in Z_L$ and $\beta \in Z_M$. The discriminant d_K of $K = LM$ is equal to $d_L^m d_M^n$ with $n = [L : \mathbb{Q}]$, $m = [M : \mathbb{Q}]$ and $Z_K = Z_L Z_M$. For any $\sigma \in E_{K/M}$ and any $\tau \in E_{K/L}$ we define an embedding $\rho(\sigma, \tau)$ of K by

$$\Big(\sum_{i=1}^{n} \sum_{j=1}^{m} c_{ij} \alpha^{i-1} \beta^{j-1}\Big)^{\rho(\sigma,\tau)} = \sum_{i=1}^{n} \sum_{j=1}^{m} c_{ij} (\alpha^\sigma)^{i-1} (\beta^\tau)^{j-1}$$

with $c_{ij} \in \mathbb{Q}$. Note that $\rho(\sigma, \iota) = \sigma$ and $\rho(\iota, \tau) = \tau$. Since $L \cap M = \mathbb{Q}$, it follows that $E_K = \{\rho(\sigma, \tau) \mid \sigma \in E_{K/M}, \tau \in E_{K/L}\}$, and the maps $\rho \mapsto \rho|_L$ and $\rho \mapsto \rho|_M$ induce bijections $E_{K/M} \to E_L$ and $E_{K/L} \to E_M$. Replacing $G_{K/M}$, $G_{K/L}$, G_K, G_L, G_M and $\xi^{\sigma\tau}$ with $E_{K/M}$, $E_{K/L}$, E_K, E_L, E_M and $\xi^{\rho(\sigma,\tau)}$, we can use the same arguments as in the proof of the lemma. Notice that A, B, C, c and c' are contained in K. Therefore we find that for a given integer $\xi \in K$ the ring $\mathbb{Z}[\xi]$ coincides with Z_K if and only if

$$\frac{\xi - \xi^\sigma}{\alpha - \alpha^\sigma}, \quad \frac{\xi - \xi^\tau}{\beta - \beta^\tau}, \quad \xi - \xi^{\rho(\sigma,\tau)}$$

are all units for any embedding $\sigma \neq \iota$ in $E_{K/M}$ and any embedding $\tau \neq \iota$ in $E_{K/L}$.

Proof of Theorem A for $\ell < 0$. We treat a non-cyclic abelian field $K = k_p k = \mathbb{Q}(\zeta_p, \sqrt{-m})$, where $k_p = \mathbb{Q}(\zeta_p)$ is the pth cyclotomic field for an odd prime p, and $k = \mathbb{Q}(\sqrt{-m})$ is an imaginary quadratic field of discriminant $\ell = -m$ such that $-m < -4$ and $(m,p) = 1$. We put $\omega = \frac{r+\sqrt{-m}}{2}$, where $r = 1$ if $-m \equiv 1 \pmod 4$ and $r = 0$ otherwise. In this case the integer ring Z_K of K coincides with $\mathbb{Z}[\zeta_p, \omega]$.

Assume that an integer $\xi \in Z_K$ satisfies $\mathbb{Z}[\xi] = Z_K$. Let σ and τ be non-trivial elements of $\mathrm{Gal}(K/k)$ and of $\mathrm{Gal}(K/k_p)$, respectively. In particular, we have $\sqrt{-m}^\tau = -\sqrt{-m}$. Then Lemma 2.2 implies that the partial different $\xi_{\sigma\tau} = \xi - \xi^{\sigma\tau}$ is a unit. Let $k_p^+ = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$. Applying Lemma 2.1 we put

$$\xi = \alpha_0 + \alpha_1\zeta_p + (\beta_0 + \beta_1\zeta_p)\frac{r + \sqrt{-m}}{2}$$

with $\alpha_0, \alpha_1, \beta_0, \beta_1 \in Z_{k_p^+} = \mathbb{Z}[\zeta_p + \zeta_p^{-1}]$. Assume that σ satisfies $\zeta_p^\sigma = \zeta_p^{-1}$. Then

$$\xi_{\sigma\tau} = \xi - \xi^{\sigma\tau} = \frac{2\alpha_1 + r\beta_1}{2}(\zeta_p - \zeta_p^{-1}) + \frac{2\beta_0 + \beta_1(\zeta_p + \zeta_p^{-1})}{2}\sqrt{-m}.$$

We also see from Lemma 2.2 that the ratio

$$\varepsilon = \frac{\xi - \xi^\sigma}{\zeta_p - \zeta_p^\sigma} = \frac{2\alpha_1 + r\beta_1}{2} + \frac{\beta_1}{2}\sqrt{-m}$$

is a unit. Since $\alpha = 2\alpha_1 + r\beta_1$ and β_1 are real, it follows that

$$N_{K/k_p}(\varepsilon) = \varepsilon\varepsilon^\tau = \frac{\alpha^2}{4} + \frac{\beta_1^2}{4}m \geq \frac{m}{4}\beta_1^2.$$

Similarly, $(\varepsilon\varepsilon^\tau)^\rho \geq \frac{m}{4}(\beta_1^\rho)^2$ for any $\rho \in \mathrm{Gal}(k_p/\mathbb{Q})$ and $\alpha, \beta_1 \in k_p^+$. Suppose that $\beta_1 \neq 0$. Since β_1 is an integer and $m > 4$ we obtain

$$N_{K/\mathbb{Q}}(\varepsilon) = N_{k_p/\mathbb{Q}}(\varepsilon\varepsilon^\tau) \geq \left(\frac{m}{4}\right)^{p-1} N_{k_p/\mathbb{Q}}(\beta_1^2) > 1.$$

This contradicts ε being a unit. Therefore $\beta_1 = 0$. Note that $\alpha_1 = \varepsilon$ is a unit. Returning to $\xi_{\sigma\tau}$ we have $\xi_{\sigma\tau} = \xi - \xi^{\sigma\tau} = \alpha_1(\zeta_p - \zeta_p^{-1}) + \beta_0\sqrt{-m}$ and for $\eta = N_{K/k_p}(\xi_{\sigma\tau})$,

$$\eta = \xi_{\sigma\tau} \cdot \xi_{\sigma\tau}^\tau = \alpha_1^2(\zeta_p - \zeta_p^{-1})^2 + \beta_0^2 m.$$

Hence the congruence $\eta \equiv \alpha_1^2(\zeta_p - \zeta_p^{-1})^2 \pmod{m\mathbb{Z}_{k_p^+}}$ holds in k_p^+. Since

$N_{k_p^+/\mathbb{Q}}(\alpha_1^2) = 1$ and

$$N_{k_p^+/\mathbb{Q}}(\zeta_p - \zeta_p^{-1})^2 = \pm N_{k_p/\mathbb{Q}}(\zeta_p - \zeta_p^{-1}) = \pm p,$$

we have $N_{k_p^+/\mathbb{Q}}(\eta) \equiv \pm p \pmod{m}$. We notice that η is a unit in k_p^+ and $N_{k_p^+/\mathbb{Q}}(\eta) = \pm 1$. Hence m divides $p+1$ or $p-1$. Therefore, if $p+1$ and $p-1$ are not divisible by m then K is non-monogenic. Thus we have proved Theorem A when $\ell = -m < 0$. ∎

Proof of Theorem A for $\ell > 0$. Let $k_p = \mathbb{Q}(\zeta_p)$ for an odd prime p and $k = \mathbb{Q}(\sqrt{\ell})$ with $d_k = \ell > 4$ and $(p, \ell) = 1$, and put $K = k_p k$. Assume that K is monogenic and let ξ be an integer in K such that $\mathbb{Z}[\xi] = Z_K$. Let $\ell \equiv 1 \pmod 4$ and put $\omega = \frac{1+\sqrt{\ell}}{2}$. Then ξ can be written as $\xi = \alpha_0 + \alpha_1\zeta_p + (\beta_0 + \beta_1\zeta_p)\omega$ with $\alpha_0, \alpha_1, \beta_0, \beta_1 \in \mathbb{Z}[\zeta_p + \zeta_p^{-1}]$. Let $\sigma \in \mathrm{Gal}(K/k)$ and $\tau \in \mathrm{Gal}(K/k_p)$ be such that $\zeta_p^\sigma = \zeta_p^{-1}$ and $\sqrt{\ell}^{\,\tau} = -\sqrt{\ell}$. Then a partial different satisfies

$$\xi_{\sigma\tau} = \xi - \xi^{\sigma\tau} = \frac{2\alpha_1 + \beta_1}{2}(\zeta_p - \zeta_p^{-1}) + \frac{2\beta_0 + \beta_1(\zeta_p + \zeta_p^{-1})}{2}\sqrt{\ell}.$$

Put $E = 2\alpha_1 + \beta_1$ and $F = 2\beta_0 + \beta_1(\zeta_p + \zeta_p^{-1})$. Since $(\zeta_p - \zeta_p^{-1})^2 < 0$ and $E, F \in \mathbb{R}$, it follows that

$$|N_{K/k_p}(\xi_{\sigma\tau})| = |\xi_{\sigma\tau}\xi_{\sigma\tau}^\tau| = -(\zeta_p - \zeta_p^{-1})^2\frac{E^2}{4} + \frac{F^2}{4}\ell \geq \frac{\ell}{4}F^2.$$

We also see that $|(\xi_{\sigma\tau}\xi_{\sigma\tau}^\tau)^\rho| \geq \frac{\ell}{4}(F^2)^\rho$ for any $\rho \in \mathrm{Gal}(k_p/\mathbb{Q})$.

(i) If $F \neq 0$ then

$$|N_{K/\mathbb{Q}}(\xi_{\sigma\tau})| = |N_{k_p/\mathbb{Q}}(\xi_{\sigma\tau}\xi_{\sigma\tau}^\tau)| \geq \left(\frac{\ell}{4}\right)^{p-1} N_{k_p/\mathbb{Q}}(F^2) > 1$$

because F is an integer and $\ell > 4$. This contradicts $\xi_{\sigma\tau}$ being a unit.

(ii) If $F = 0$ then $2\xi_{\sigma\tau} = E(\zeta_p - \zeta_p^{-1}) \equiv 0 \pmod{\mathfrak{P}}$, where $\mathfrak{P} = (1 - \zeta_p)$ is the prime ideal of Z_{k_p} generated by $1 - \zeta_p$. Since $(2, \mathfrak{P}) = 1$, we have $\xi_{\sigma\tau} \equiv 0 \pmod{\mathfrak{P}}$. This is impossible because $\xi_{\sigma\tau}$ is a unit.

Therefore by (i) and (ii) the field K is non-monogenic. We obtain the same conclusion when $\ell \equiv 0 \pmod 4$ and $\omega = \sqrt{\ell}/2$. ∎

Remark 2.2. For a fixed odd prime p there are only a finite number of imaginary quadratic fields $k = \mathbb{Q}(\sqrt{\ell})$ such that $k_p k$ are monogenic, because if the discriminant ℓ of an imaginary quadratic field k is less than $-(p+1)$, then by Theorem A the field $k_p k$ is non-monogenic.

Problem 2.1. Extend Theorem A to the non-cyclic but abelian fields $\mathbb{Q}(\zeta_m, \sqrt{\ell})$ of conductor $\ell \cdot m$ with a squarefree $\ell \neq -4, -3$ and $m = \prod_j p_j^{e_j} \neq 3$ with odd primes p_j.

In [9], the non-monogenity of non-cyclic, but abelian fields of conductor $3 \cdot p^e$ with a prime $p > 3$ is investigated.

Related to Theorem A, we produce a non-monogenic family of non-Galois composite fields $K = LM$ with $(d_L, d_M) = 1$.

NOTE 2.1. *There exist infinitely many non-monogenic, non-Galois sextic fields $K = LM$, where $L = \mathbb{Q}(\sqrt[3]{5})$ and $M = \mathbb{Q}(\sqrt{n})$ for squarefree integers $n \leq -7$ such that $(d_L, d_M) = 1$, $n \equiv 1 \pmod 4$ and $n \equiv \pm 2 \pmod 5$.*

Proof. Let $Z_L = \mathbb{Z}[1, \theta, \theta^2]$ and $Z_M = \mathbb{Z}[1, \omega]$ with $\theta = \sqrt[3]{5}$ and $\omega = \frac{1+\sqrt{n}}{2}$. Due to $(d_L, d_M) = 1$ we have $Z_K = \mathbb{Z}[1, \theta, \theta^2, \omega, \theta\omega, \theta^2\omega]$, and hence $d_K = d_L^2 \cdot d_M^3 = d_L^2 \cdot n^3$ with $d_L = -3^3 5^2$. Let $\mathrm{Iso}(L/\mathbb{Q}) = \langle \sigma \rangle$ and $\mathrm{Gal}(M/\mathbb{Q}) = \langle \tau \rangle$. Then for any integer $\xi \in Z_K$ such that $\xi = \beta_1 + \beta_2\omega$ with $\beta_j \in Z_L$, $j = 1, 2$, using $\omega^\tau = -\omega + 1$ we have the partial different

$$\begin{aligned}\mathfrak{D}_{\sigma\tau}(\xi) &= \xi - \xi^{\sigma\tau} = \beta_1 + \beta_2\omega - (\beta_1^\sigma + \beta_2^\sigma\omega^\tau) \\ &= \beta_1 - \beta_1^\sigma - \beta_2^\sigma + (\beta_2 + \beta_2^\sigma)\omega.\end{aligned}$$

Since $\theta^\sigma = \zeta\theta$ for a cubic root ζ of unity, $\mathfrak{D}_{\sigma\tau}(\xi)$ is contained in $K_1 = K(\zeta)$. Let $\beta_1 = a_0 + a_1\theta + a_2\theta^2$, $\beta_2 = b_0 + b_1\theta + b_2\theta^2$ with $a_i, b_i \in \mathbb{Z}$, and put $\gamma_1 = \beta_1 - \beta_1^\sigma - \beta_2^\sigma$ and $\gamma_2 = \beta_2 + \beta_2^\sigma$. Then $\gamma_1 = -b + \gamma_3\theta$ and $\gamma_2 = 2b + \gamma_4\theta$ with $b = b_0$ and $\gamma_3, \gamma_4 \in Z_{K_1}$. Hence $\mathfrak{D}_{\sigma\tau}(\xi) = b\sqrt{n} + \gamma\theta$ for some $\gamma \in Z_{K_1}$. Assume that $Z_K = \mathbb{Z}[\xi]$. Considering

$$D = N_{K_1/K}(\mathfrak{D}_{\sigma\tau}(\xi)) = \mathfrak{D}_{\sigma\tau}(\xi)\mathfrak{D}_{\sigma\tau}(\xi)^\rho = \mathfrak{D}_{\sigma\tau}(\xi)\mathfrak{D}_{\sigma^2\tau}(\xi) = b^2 n + \delta\theta,$$

where $\mathrm{Gal}(K_1/K) = \langle \rho \rangle$ and $\delta \in Z_K$, we obtain

$$N_{K/M}(D) = (b^3 n)^2 n + 5c + 5d\omega \quad \text{with } c, d \in \mathbb{Z}.$$

Since $\mathfrak{D}_{\sigma\tau}(\xi)$ is a unit of Z_{K_1} by Remark 2.1, it follows that $N_{K/M}(D)$ is a unit of Z_M, and therefore is equal to ± 1. Assume that $b \neq 0$. Hence we see that n is a square residue modulo 5. This contradicts the condition $n \equiv \pm 2 \pmod 5$. If $b = 0$, then $N_{K/M}(D) \equiv 0 \pmod{5Z_M}$, which is impossible. ∎

3. Proof of Theorem B. Let $K = Lk$ be a composite field of the maximal real subfield $L = k_n^+$ of the nth cyclotomic field k_n for $n \geq 5$ with $n \not\equiv 2 \pmod 4$ and an imaginary quadratic field $k = \mathbb{Q}(\sqrt{-m})$ of discriminant $-m = d_k < -4$ such that $(m, n) = 1$. We put $\omega = \frac{r+\sqrt{-m}}{2}$ with $r = 1$ if $-m \equiv 1 \pmod 4$ and $r = 0$ otherwise. Then $Z_K = Z_L Z_k = Z_L[\omega]$. Since $n \not\equiv 2 \pmod 4$, the condition $(m, n) = 1$ is equivalent to the discriminants of L and k being coprime.

Assume that an integer $\xi \in Z_K$ satisfies $\mathbb{Z}[\xi] = Z_K$. We write $\xi = \alpha + \beta\omega$ with $\alpha, \beta \in Z_L$. Denote by τ the element of $\mathrm{Gal}(K/L)$ with $\sqrt{-m}^\tau = -\sqrt{-m}$. Let σ be a non-trivial element of $G_{K/k} = \mathrm{Gal}(K/k)$. Then we see by Lemma 2.2 that

$$\xi_{\sigma\tau} = \xi - \xi^{\sigma\tau} = \alpha - \alpha^{\sigma} + \frac{r(\beta - \beta^{\sigma})}{2} + \frac{\beta + \beta^{\sigma}}{2}\sqrt{-m}$$

is a unit.

We claim that $\beta + \beta^{\sigma} \neq 0$ for some $\iota \neq \sigma \in G_{K/k}$. Indeed, if $\beta + \beta^{\sigma} = 0$ for all $\sigma \neq \iota$ then $(\beta^2)^{\sigma} = (\beta^{\sigma})^2 = \beta^2$ for all σ and hence $\beta^2 \in \mathbb{Z}$. On the other hand, Lemma 2.2 also implies that the ratio

$$\beta = \frac{\xi - \xi^{\tau}}{\omega - \omega^{\tau}}$$

is a unit. Since β is real, we deduce $\beta^2 = 1$. Then $\beta + \beta^{\sigma} = \pm 2 \neq 0$ for $\sigma \neq \iota$, which is a contradiction Hence our claim is shown. Next we may assume $\beta + \beta^{\sigma} \neq 0$. Putting $\gamma = \alpha - \alpha^{\sigma} + \frac{r(\beta - \beta^{\sigma})}{2}$ and $\delta = \beta + \beta^{\sigma}$, we obtain

$$\begin{aligned} N_{K/L}(\xi_{\sigma\tau}) = \xi_{\sigma\tau}\xi_{\sigma\tau}^{\tau} &= \left(\gamma + \delta\frac{\sqrt{-m}}{2}\right)\left(\gamma - \delta\frac{\sqrt{-m}}{2}\right) \\ &= \gamma^2 + \frac{m}{4}\delta^2 \geq \frac{m}{4}\delta^2 \end{aligned}$$

because γ, δ are real. For any $\rho \in G_{K/k}$ we also have $\xi_{\sigma\tau}^{\rho}(\xi_{\sigma\tau}^{\rho})^{\tau} \geq \frac{m}{4}(\delta^{\rho})^2$. Since δ is an integer and $m > 4$ it follows that

$$N_{K/\mathbb{Q}}(\xi_{\sigma\tau}) = N_{L/\mathbb{Q}}(\xi_{\sigma\tau}\xi_{\sigma\tau}^{\tau}) \geq \left(\frac{m}{4}\right)^{[L:\mathbb{Q}]} N_{L/\mathbb{Q}}(\delta^2) > 1.$$

This contradicts $\xi_{\sigma\tau}$ being a unit. Hence Theorem B is proved. ∎

Remark 3.1. In Theorem B the field $K = k_n^{+}k$ is a non-cyclic abelian extension of $\mathbb{Q}$ unless $\mathrm{Gal}(k_n^{+}/\mathbb{Q})$ is a cyclic group of odd order. On the other hand, if $n = 2s$ with odd s, then the discriminant d_L of $L = k_n^{+} = k_s^{+}$ is not divisible by 2, and hence the condition $(m, n) = 1$ with $n \not\equiv 2 \pmod 4$ is stronger than $(d_k, d_L) = 1$. We have $k_6^{+} = \mathbb{Q}$ and $K = k_6^{+}k = \mathbb{Q}(\sqrt{-m})$, which are cyclic and monogenic.

Remark 3.2. In [3] I. Gaál considered the monogenity of a composite field $K = LM$ of a totally real number field L and an imaginary quadratic field M such that d_L and $d_M < -4$ are coprime, and proved that K can only be monogenic if L is monogenic. We know that k_n^{+} is monogenic. However, Theorem B gives an example of a monogenic, totally real number field L such that $K = LM$ is non-monogenic.

4. Proof of Theorem C. The case of $q = 2^2p^n$ with an odd prime p in [9, Theorem 2] is generalized in Theorem C.

Proof. Let $q = 2^r n$ with $r \geq 2$ and $(n, 2) = 1$, and take an integer a such that

$$a \equiv 2^{r-1} - 1 \pmod{2^r}, \quad a \equiv -1 \pmod{n}.$$

Then $(a, q) = 1$ and the element $\sigma \in \mathrm{Gal}(k_q/\mathbb{Q})$ induced by $\zeta \mapsto \zeta^a = -\zeta^{-1}$ has order 2. Hence $K = \mathbb{Q}(\zeta - \zeta^{-1})$ is the fixed field of σ. Since the ring of integers in k_q is $\mathbb{Z}[\zeta]$, we have $Z_K = \mathbb{Z}[\zeta] \cap K$. Using $\zeta^i = \zeta^{i-1}(\zeta - \zeta^{-1}) + \zeta^{i-2}$ for $i \geq 2$, we can show by induction on i that

$$\zeta^i \in \mathbb{Z}[\zeta - \zeta^{-1}] + \zeta\mathbb{Z}[\zeta - \zeta^{-1}].$$

This implies

$$\mathbb{Z}[\zeta] = \mathbb{Z}[\zeta - \zeta^{-1}] + \zeta\mathbb{Z}[\zeta - \zeta^{-1}].$$

For any $\alpha = \beta + \gamma\zeta \in \mathbb{Z}[\zeta]$ with $\beta, \gamma \in \mathbb{Z}[\zeta - \zeta^{-1}]$, we see that $\alpha \in K$ if and only if $\alpha - \alpha^\sigma = \gamma(\zeta + \zeta^{-1}) = 0$, hence $\gamma = 0$, that is, $\alpha = \beta \in \mathbb{Z}[\zeta - \zeta^{-1}]$. This proves that $\mathbb{Z}[\zeta] \cap K = \mathbb{Z}[\zeta - \zeta^{-1}]$. ∎

5. Examples. In this section we provide two typical classes of number fields for which we can apply Theorem A.

($\mathrm{A_I}$) *A field K of degree* 12 *with an imaginary quadratic subfield k.* By Theorem A, we choose an abelian but non-cyclic field K with degree $[K : \mathbb{Q}] = 12$ of conductor $7 \cdot 11$, i.e. $p = 7$ and $-\ell = -11$, which is the second simplest example after the first octic field $k_5 \cdot \mathbb{Q}(\sqrt{-7})$ in [7]. Let K be the composite field of the imaginary quadratic field $k = \mathbb{Q}(\sqrt{-11})$ with $\omega = \frac{1+\sqrt{-11}}{2}$ and the cyclotomic field $K = \mathbb{Q}(\zeta)$ with a primitive 7th root ζ of unity. Then we have $d_K = d_{k_7}^{[k:\mathbb{Q}]} \cdot (-\ell)^{[k_7:\mathbb{Q}]} = (7^5)^2 \cdot (-11)^6$. Here the irreducible polynomial $f(x)$ with $f(\zeta\omega) = 0$ of degree 12 is obtained as follows. Let $h(x) = N_{k_7^+/\mathbb{Q}}(x - \zeta \cdot \omega)$. Then

$$h(x) = (x - \zeta \cdot \omega)(x - \zeta \cdot \omega)^{\sigma^3} = x^2 - (\zeta + \zeta^{-1})\omega x + \omega^2, \qquad \omega^2 = \omega - 3.$$

Let η denote the Gauß period $\zeta + \zeta^{-1}$ satisfying the cubic equation $x^3 + x^2 - 2x - 1 = 0$. Since $\eta = \frac{x^2+\omega-3}{\omega x}$, denote

$$g(x) = (\omega x)^3 \left\{ \left(\frac{x^2 + \omega - 3}{\omega x} \right)^3 + \left(\frac{x^2 + \omega - 3}{\omega x} \right)^2 - 2\frac{x^2 + \omega - 3}{\omega x} - 1 \right\}.$$

Put $f_{\mathrm{I}}(x) = N_{k/\mathbb{Q}}(g(x))$. Here $g(x)$ can be written in the form $g(x) = g_1(x) + \omega g_2(x)$ with polynomials $g_j(x) \in \mathbb{Z}[x]$, $j = 1, 2$. Then $\xi = \zeta\omega$ is a root of an irreducible polynomial

$$\begin{aligned} f_{\mathrm{I}}(x) &= g_1(x)^2 + T_{k/\mathbb{Q}}(\omega)g_1(x)g_2(x) + N_{k/\mathbb{Q}}(\omega)g_2(x)^2 \\ &= (x^6 - 3 \cdot x^4 - 3 \cdot x^3 + 6 \cdot x^2 + 15 \cdot x - 3)^2 \\ &\quad + (x^6 - 3 \cdot x^4 - 3 \cdot x^3 + 6 \cdot x^2 + 15 \cdot x - 3) \\ &\qquad\qquad \cdot (x^5 + x^4 + 2 \cdot x^3 - 9 \cdot x^2 + x + 16) \\ &\quad + 3 \cdot (x^5 + x^4 + 2 \cdot x^3 - 9 \cdot x^2 + x + 16)^2. \end{aligned}$$

Then the polynomial discriminant of $f_{\mathrm{I}}(x)$ is equal to $(3^{15} \cdot 13^5)^2 \cdot d_K$.

(A_{II}) *A field K of degree* 12 *with a real quadratic subfield k.* We select a non-cyclic, but abelian field $K = \mathbb{Q}(\zeta, \sqrt{5})$ of degree $[K : \mathbb{Q}] = 12$ with conductor $7 \cdot 5$, i.e. $p = 7$ and $\ell = 5$, and the field discriminant $d_K = (7^5)^2 \cdot (5)^6$. Let $\xi = \zeta \cdot \omega \in Z_K$. Then ξ is a root of the irreducible polynomial $f_{II}(x) = x^{12} + \cdots \pm 1$, $f_{II}(\xi) = 0$, because $\zeta\omega$ with $\omega = \frac{1+\sqrt{5}}{2}$ is a unit. Then $f_{II}(x)$ is obtained as in (A_I). We have

$$\begin{aligned} g(x) = (&x^6 + x^4 + 3 \cdot x^3 + 2 \cdot x^2 + 3 \cdot x + 5) \\ &+ (x^5 + x^4 + 2 \cdot x^3 + 3 \cdot x^2 + 5 \cdot x + 8)\omega, \end{aligned}$$

and hence

$$\begin{aligned} f_{II}(x) = N_{k/\mathbb{Q}}(g(x)) = &(x^6 + x^4 + 3 \cdot x^3 + 2 \cdot x^2 + 3 \cdot x + 5)^2 \\ &+ T_{k/\mathbb{Q}}(\omega)(x^6 + x^4 + 3 \cdot x^3 + 2 \cdot x^2 + 3 \cdot x + 5) \\ &\qquad \cdot (x^5 + x^4 + 2 \cdot x^3 + 3 \cdot x^2 + 5 \cdot x + 8) \\ &+ N_{k/\mathbb{Q}}(\omega)(x^5 + x^4 + 2 \cdot x^3 + 3 \cdot x^2 + 5 \cdot x + 8)^2. \end{aligned}$$

Then the polynomial discriminant of $f_{II}(x)$ is equal to $(13^5)^2 \cdot d_K$.

All calculations have been made by using GP/PARI.

Now we describe how to apply Theorem A to these examples. Let $\zeta = \zeta_n$ be a primitive nth root of unity for $n \geq 3$ with $n \not\equiv 2 \pmod 4$, and put $k_n = \mathbb{Q}(\zeta)$. Let $K = k_n k$ be a composite field of k_n and a quadratic field $k = \mathbb{Q}(\sqrt{m})$ of discriminant $m = d_k$ such that $(m, n) = 1$. We put $\omega = \frac{r+\sqrt{m}}{2}$ with $r = 1$ if $m \equiv 1 \pmod 4$ and $r = 0$ otherwise. Observe that $Z_K = \mathbb{Z}[\zeta\omega]$ if $m = -3, -4$. Furthermore, if $m = -4$ the integer ring of the field $K' = \mathbb{Q}(\zeta + \zeta^{-1}, \omega)$ is $\mathbb{Z}[(\zeta + \zeta^{-1})\omega]$ as mentioned in Remark 1.1. So it seemed to be interesting to search the fields $K = k_n k$ such that $Z_K = \mathbb{Z}[\zeta\omega]$.

Recall that the discriminant d_K is equal to $d_{k_n}^2 d_k^f$ with $f = [K_n : \mathbb{Q}]$ and

$$d_K(\zeta\omega) = d_K N_{K/\mathbb{Q}}(\omega) \prod_{\sigma \neq \iota} N_{K/\mathbb{Q}}(\zeta\omega - \zeta^\sigma\omega^\tau),$$

where σ runs over the non-trivial elements of $\mathrm{Gal}(K/k)$ and τ is the non-trivial element of $\mathrm{Gal}(K/k_n)$. We calculated the values of $d_K(\zeta\omega)$ when $(n, m) = (7, -11)$ and $(n, m) = (7, 5)$ by GP/PARI as follows: $d_K(\zeta\omega) = 3^{30}13^{10}d_K$ if $(n, m) = (7, -11)$ and $d_K(\zeta\omega) = 13^{30}d_K$ if $(n, m) = (7, 5)$. When m is different from $-3, -4$, and 5, it is immediately seen that $N_{K/\mathbb{Q}}(\omega) > 1$ and hence $|d_K(\zeta\omega)| > |d_K|$. If $(n, m) = (7, 5)$ our calculation implies that $|N_{K/\mathbb{Q}}(\zeta\omega - \zeta^\sigma\omega^\tau)| > 1$ for some σ because $N_{K/\mathbb{Q}}(\omega) = 1$. In general, let $m \geq 5$ and σ be such that $\zeta^\sigma = \zeta^{-1}$. Then

$$|(\zeta\omega - \zeta^\sigma\omega^\tau)(\zeta\omega^\tau - \zeta^\sigma\omega)| = \frac{1}{4}|(\zeta - \zeta^{-1})^2 r^2 - (\zeta + \zeta^{-1})^2 m|.$$

Since $(\zeta - \zeta^{-1})^2 < 0$, it follows that

$$|N_{K/\mathbb{Q}}(\zeta\omega - \zeta^\sigma \omega^\tau)| \geq \frac{m}{4} N_{k_n/k}(\zeta + \zeta^{-1})^2 > 1.$$

Hence $|d_K(\zeta\omega)| > |d_K|$ is also valid. Consequently, since $|d_K(\zeta\omega)| > |d_K|$ we have $\mathbb{Z}[\zeta\omega] \neq Z_K$ if $|m| > 4$.

However, our consideration of the norm $N_{K/\mathbb{Q}}(\zeta\omega - \zeta^\sigma\omega^\tau)$ indicated a method of showing $|N_{K/\mathbb{Q}}(\xi - \xi^{\sigma\tau})| > 1$ for a *general* integer $\xi \in Z_K$. Making use of this method we have presented two classes of non-monogenic composite fields $K = k_n k$ as stated in Theorem A. Without these prototypes, it would have been difficult to construct a generalized Theorem A.

Acknowledgements. We thank the referee for valuable remarks. We also appreciate Claude Levesque's [Université Laval] several comments on this article.

Funding. This work is supported by University of Malakand and in part by Sukkur IBA (Institute for Business and Administration) University in the Islamic Republic of Pakistan and the Research Institute for Mathematical Sciences, Kyoto University, Japan.

References

[1] M. Ahmad, A. Hameed, N. Khan and T. Nakahara, *On the monogenity of cyclic sextic fields of composite conductor*, Punjab Univ. J. Math. 50 (2018), 67–73.

[2] I. Gaál, *Diophantine Equations and Power Integral Bases: Theory and Algorithms*, 2nd ed., Birkhäuser/Springer, 2019.

[3] I. Gaál, *Monogenity in totally real extensions of imaginary quadratic fields with an application to simplest quartic fields*, Acta Sci. Math. 89 (2023), 3–12.

[4] I. Gaál, *Monogenity and power integral bases; recent developments*, Axioms 13 (2024), art. 429, 16 pp.

[5] N. Khan, T. Nakahara and H. Sekiguchi, *An ideal theoretic proof on monogenity of cyclic sextic fields of prime power conductor*, J. Number Theory 198 (2019), 43–51.

[6] Y. Motoda, T. Nakahara and S. I. A. Shah, *On a problem of Hasse for certain imaginary abelian fields*, J. Number Theory 96 (2002), 326–334.

[7] T. Nakahara, *Monogenity of certain abelian and non-abelian extension fields*, in: RIMS Kôkyûroku Proc., Kyoto Univ., to appear.

[8] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, 3rd ed., Springer, Berlin, and PWN–Polish Sci. Publ., Warszawa, 2007.

[9] S. I. A. Shah and T. Nakahara, *Monogenesis of the rings of integers in certain imaginary abelian fields*, Nagoya Math. J. 168 (2002), 85–92.

[10] M. Sultan and T. Nakahara, *On certain octic biquartic fields related to a problem of Hasse*, Monatsh. Math. 176 (2015), 153–162.

[11] L. C. Washington, *Introduction to Cyclotomic Fields*, 2nd ed., Grad. Texts in Math. 83, Springer, New York, 1995.

Nadia Khan
Pak-Austria Fachhochschule Institute of Applied Sciences and Technology
Haripur, The Islamic Republic of Pakistan
E-mail: nadiakhan811@gmail.com

Toru Nakahara
Department of Mathematics
University of Malakand
Malakand, The Islamic Republic of Pakistan
E-mail: toru.nakahara@nu.edu.pk

Hiroshi Sekiguchi
Nippon Steel Corpolation
Nagoya, Japan
E-mail: h_sekiguchi@daiichi-tekkou.co.jp

Tsuyoshi Uehara
Saga University
Saga, Japan
E-mail: ueharats0314@gmail.com