Rep. Fac. Sci. Engrg.
Saga. Univ. Math.
31-1 (2002), 7 ~ 19.

Reports of the Faculty of Science and Engineering,
Saga University, Mathematics, Vol. 31, No. 1, 2002

A Prototype of Certain Abelian Fields whose Rings of Integers Have a Power Basis

By
Syed Inayat Ali SHAH* and Toru NAKAHARA**

Abstract: By our original proof, we show the prototype of our recent works [15], [7] related to a problem of Hasse on the field K whose ring of integers has a power basis or does not. In this note we characterize the field K as a subfield in a cyclotomic field k_m of conductor m such that $[k_m : K] = 2$ in the cases of $m = \ell p^n$ with a prime p, where $\ell = 4$ or $p > \ell = 3$.

Key Words: Hasse's problem, Integral power basis, Cyclotomic fields, Imaginary quadratic field, The conductor-different formula

§1. Introduction

In [11] and [5], W. Narkiewicz and T. Kubota proposed to determine whether the ring of integers in a field is monogenic or not as an unsolved problem. This problem of Hasse is treated by many authors[1], [2], [3], [4], [7-10], [12], [13], [14].

Let F be an algebraic number field over the rationals $\boldsymbol{Q}$. We denote the ring of integers in F by $\boldsymbol{Z}_F$. If we have $\boldsymbol{Z}_F = \boldsymbol{Z}[\alpha]$ for an element α of $\boldsymbol{Z}_F$, then it is said that $\boldsymbol{Z}_F$ has a power basis or F has an integral power basis. The ring $\boldsymbol{Z}_F$ is called monogenic if $\boldsymbol{Z}_F$ has a power basis, otherwise $\boldsymbol{Z}_F$ is said to be non-monogenic.

Set $k_m = \boldsymbol{Q}(\zeta_m)$, where ζ_m is a primitive m-th root of unity. Let G be the galois group $\mathrm{Gal}(k_m/\boldsymbol{Q})$ of k_m over $\boldsymbol{Q}$. If k_m^+ is the maximal real subfield of k_m, then the ring $\boldsymbol{Z}_{k_m^+}$ of

Received May 1, 2002
*Department of Mathematics, University of Peshawar
**Department of Mathematics, Saga University

AMS subject classification: 11R16, 11R18, secondary: 11R04
The second author was supported by a grant (#14540033) from the Japan Society for the Promotion of Science.

integers has always a power basis[13].

In this article we treat certain imaginary abelian subfields K with $[k_m : K] = 2$.

In the next section we consider the case that the conductor $m = 4p^n (n \geq 1)$ with a prime p and will show that the ring $\boldsymbol{Z}_K$ of any subfield K in k_m such that $[k_m : K] = 2$ has a power basis and it is generated by the Gauß period $\eta_H = \sum_{\rho \in H} \zeta_m^\rho$, where H is the subgroup of G corresponding to the field K. On the other hand, in the third section we prove that in the case of $m = 3p^n (n \geq 1)$ with a prime $p > 3$ and the subfield K which is distinct from $k_{m/3}$ and k_m^+, the ring $\boldsymbol{Z}_K$ of integers in K does not have a power basis. We shall prove each theorem using Hasse's conductor-discriminant formula.

Finally we shall determine for the subfields of a cyclotomic frield k_{93} of the conductor $|-3||-31|$ whether each of them has an integral power basis or does not except for two cases among twenty subfields.

§2. Monogenic Case

We start with the following theorems in which the rings of integers have a power basis.

THEOREM 1. *Suppose $m = 2^n \geq 8$ and let K be the imaginary subfield of k_m distinct from $k_{m/2}$ such that $[k_m : K] = 2$. Then the ring $\boldsymbol{Z}_K$ of integers in K coincides with $\boldsymbol{Z}[\eta]$, where η is the Gauß period $\zeta_m - \zeta_m^{-1}$ and the absolute value of the field discriminant of K is equal to $2^{(n-1)\phi(2^{n-1})-1}$.*

Proof. Let $G = \mathrm{Gal}(k_m/\boldsymbol{Q}) =< \tau > \times < \sigma >$ where $\tau^2 = e = \sigma^s$, $s = \phi(m)/2 = 2^{n-2}$ and $\zeta_m^\tau = \bar{\zeta_m}$, $\zeta_m^\sigma = \zeta_m^5$, where $\bar{\alpha}$ means the complex conjugate of a number α and $\phi(\cdot)$ denotes the Euler function. Then $k_{m/2}$, $\boldsymbol{Q}(\zeta_m + \zeta_m^{-1})$ and K are subfields fixed by the subgroups $< \sigma^{s/2} >$, $< \tau >$ and $H =< \sigma^{s/2}\tau >$ respectively. Now the character group of G is $< \lambda > \times < \psi >$, where characters λ and ψ correspond to τ and σ, respectively. We may define $\lambda(\tau) = -1$, $\lambda(\sigma) = 1$ and $\psi(\tau) = 1$, $\psi(\sigma) = \zeta_s$, respectively. Then the subgroup $H =< \sigma^{s/2}\tau >$ is the kernel of a character $\lambda\psi$ and K is generated by the gauss period $\eta = \sum_{\rho \in H} \zeta_m^\rho = \zeta_m - \zeta_m^{-1}$.

We calculate directly the discriminant $d_K(\eta)$ of the Gauß period $\eta = \sum_{\rho\in H} \zeta_m^{\rho}$, which is given by

$$d_K(\eta) = \left(\prod_{i<j,k<l} (\eta^{\tau^i\sigma^k} - \eta^{\tau^j\sigma^l}) \right)^2,$$

where $\tau^i\sigma^k H, \tau^j\sigma^l H \in G/H =< \tau H, \sigma H >$, $n \geq 3$, by way of the different $\mathfrak{d}_K(\eta)$ of η

$$\mathfrak{d}_K(\eta) = \prod_{\rho\in G/H\setminus\{H\}} (\eta - \eta^{\rho}).$$

Then we obtain

$$\eta - \eta^{\tau} = 2(\zeta_m - \zeta_m^{-1}) \cong 2\mathfrak{L}^2.$$

Assume $2^h \| 5^j - 1$ and $2^k \| 5^j + 1$, where $a^e \| b$ for $a, b \in \boldsymbol{Z}$ means that $b \equiv 0 \pmod{a^e}$, but $b \not\equiv 0 \pmod{a^{e+1}}$. Then

$$\begin{aligned}
\eta - \eta^{\sigma^j} &= (\zeta_m - \zeta_m^{-1}) - (\zeta_m^{5^j} - \zeta_m^{-5^j}) \\
&= (\zeta_m - \zeta_m^{-1}) - (\zeta_m^{1+a_h} - \zeta_m^{1+b_k}) \\
&= \zeta_m - \zeta_m^{1+a_h} + \zeta_m^{1+b_k} - \zeta_m^{1+a_h+b_k} \\
&= \zeta_m(1 - \zeta_m^{a_h})(1 + \zeta_m^{b_k}) \\
&= \zeta_m(1 - \zeta_m^{a_h})(1 - \zeta_m^{2^{n-1}+b_k}) \\
&\cong \mathfrak{L}^{2^h}\mathfrak{L}^{2^k},
\end{aligned}$$

where $a_h = 5^j - 1 = 2^h + a_{h+1}(j)2^{h+1} + \cdots$, $b_k = -5^j - 1 = 2^k + b_{k+1}(j)2^{k+1} + \cdots$, and $a_i(j) + b_i(j) = 1$ for $i \geq 1$. Here note that $-1 \equiv 1 + 2 + \cdots + 2^{n-1} \pmod{2^n}$ and one and only one of $5^j - 1$ or $5^j + 1$ is exactly divisible by 2 for $1 \leq j \leq s/2 - 1$. Now, set

$$S_h^- = \{j; 1 \leq j < s/2, 2^h \| 5^j - 1\},\ S_h^+ = \{j; 1 \leq j < s/2, 2^h \| 5^j + 1\}$$

for $1 \leq h \leq n-2$.

Let $\sharp A$ denote the cardinality of a set A. Then it holds that $\sharp S_1^- + \sharp S_1^+ = s/2 - 1$, and $S_2^- = \emptyset$, $S_2^+ = \{j; 1 \leq j < s/2, j : \text{odd}\}$, namely $\sharp S_2^- + \sharp S_2^+ = 2^{n-3-1} = 2^{n-2-h}$. For $h \geq 3$, we have $S_h^- = \{k2^{h-2}; 1 \leq k < 2^{n-3-(h-2)}, k : \text{odd}\}, S_h^+ = \emptyset$, namely $\sharp S_h^- + \sharp S_h^+ = 2^{n-3-(h-2)-1} = 2^{n-2-h}$.

In the case of $\eta - \eta^{\tau\sigma^j} = \eta + \eta^{\sigma^j}$ we have the same evaluation as in $\eta - \eta^{\sigma^j}$. Then by

$$\mathfrak{d}_K(\eta) = 2 \cdot \mathfrak{L}^2 \left(\mathfrak{L}^{2(s/2-1)} \mathfrak{L}^{2^2 \frac{s/2}{\phi(2^2)}} \ \ldots \ \mathfrak{L}^{s/2 \frac{s/2}{\phi(s/2)}} \mathfrak{L}^{s \cdot 1} \right)^2,$$

we obtain

$$\begin{aligned} |d_K(\eta)| &= N_K(\mathfrak{d}_K(\eta)) \\ &= 2^{2^{n-2}} \cdot 2^{\left\{1+(2^{n-2}-2)+(n-4)\cdot 2 \cdot s/2\right\}} \\ &= 2^{s(n-1)-1}, \end{aligned}$$

where N_F means the absolute norm of a number from F. This value coincides with the field discriminant $d(K)$ for $K = \boldsymbol{Q}(\zeta_m - \zeta_m^{-1})$, which completes the proof. In fact by Hasse's conductor-discriminant formula, it follows that

$$|d(K)| = \prod_{\chi \in <\lambda\psi>} f_\chi = f_{\psi^0} f_\psi \cdots f_{\psi^{\frac{s}{2}-1}} f_\lambda f_{\lambda\psi} \cdots f_{\lambda\psi^{\frac{s}{2}-1}},$$

where ψ^0 denotes the identity character and f_χ is the conductor of χ in $< \lambda\psi >$. Then $f_{\psi^j} = \dfrac{m}{t_j}$ and $f_{\lambda\psi^j} = \dfrac{m}{t_j}$, where $t_j = \gcd(j, s)$ and $0 \le j \le \dfrac{s}{2} - 1$. Since the number of ψ^j and $\lambda\psi^j$ with $t_j = 2^k$, $0 \le k \le n-3$ is equal to $2\phi\left(\dfrac{s}{2}/t_j\right) = \phi\left(2^{n-2-k}\right)$, we obtain

$$\left(\prod_{j=0}^{\frac{s}{2}-1} f_{\psi^j}\right)\left(\prod_{j=0}^{\frac{s}{2}-1} f_{\lambda\psi^j}\right) = 2^E \quad (s = 2^{n-2} \ \ n \ge 3),$$

where

$$\begin{aligned} E &= \sum_{k=0}^{n-3} (n-k)\phi\left(s/2^k\right) \\ &= n\sum_{k=0}^{n-3} 2^k - \sum_{k=0}^{n-3} k\phi\left(2^{n-2-k}\right) \\ &= n(2^{n-2}-1) - \left((s/2 - 2^{n-4}) + 2(2^{n-4} - 2^{n-5}) + \cdots + (n-3)(2^1 - 1)\right) \\ &= n(2^{n-2}-1) - 2(s/2-1) + n - 3 \\ &= s(n-1) - 1. \end{aligned}$$

THEOREM 2. *Suppose that $m = 4p^n$, where p is an odd prime and let K be the imaginary subfield of k_m distinct from $k_{m/4}$ with $[k_m : K] = 2$. Then the ring Z_K of integers in K coincides with $\boldsymbol{Z}[\eta]$, where η is the Gauß period $\zeta_m - \zeta_m^{-1}$ and the absolute value of the field discriminant of K is equal to $2^{\phi(p^n)}p^{n\phi(p^n)-p^{n-1}-1}$.*

Proof. Since the conductor m of a cyclotomic field k_m is $4p^n$, we have three subfields $k_{m/4}, k_m^+$ and K of degree $\phi(p^n)$ whose galois groups $<\tau>, <\sigma^s\tau>$ and $H = <\sigma^s>$ with $s = \phi(m/4)/2$ respectively, where τ and σ are generators of $\mathrm{Gal}(k_4/\boldsymbol{Q})$ and $\mathrm{Gal}(k_{m/4}/\boldsymbol{Q})$, namely $\zeta_4^\tau = \bar{\zeta}_4,\ \zeta_{m/4}^\tau = \zeta_{m/4}$ and $\zeta_4^\sigma = \zeta_4,\ \zeta_{m/4}^\sigma = \zeta_{m/4}^r$, where r is a primitive root modulo p^n. It is well known that the rings $\boldsymbol{Z}_{k_{m/4}}$ and $\boldsymbol{Z}_{k_m^+}$ are generated by $\zeta_{m/4}$ and $\zeta_m + \zeta_m^{-1}$, respectively [16]. Denote ζ_4 by ι and $\zeta_{m/4}$ by ζ. For $\zeta_m = \iota\zeta$, let $\eta = \sum_{\rho\in H}\zeta_m^\rho = \iota\zeta + \iota\zeta^{-1} = \zeta_m - \zeta_m^{-1}$ be the Gauß period. Then by setting $K = \boldsymbol{Q}(\eta)$, whose galois group $\mathrm{Gal}(K/\boldsymbol{Q})$ is isomorphic to $\{H, \sigma H, \cdots, \sigma^{s-1}H, \tau H, \sigma\tau H, \cdots, \sigma^{s-1}\tau H\}$ and its character group is $\{\mathrm{I}, \psi, \cdots, \psi^{s-1}, \lambda, \lambda\psi, \cdots, \lambda\psi^{s-1}\}$, where I is the identity character, $\psi(\sigma) = \zeta_s, \psi(\tau) = 1$ and $\lambda(\sigma) = 1, \lambda(\tau) = -1$.

We evaluate the different of the number $\eta = \sum_{\rho\in H}\zeta^\rho = \iota(\zeta + \zeta^{-1})$

$$\mathfrak{d}_K(\eta) = \prod_{\rho H\in G/H\setminus\{H\}} (\eta - \eta^\rho).$$

We see that for $1 \le j \le s-1, (j, p-1) = 1$

$$\begin{aligned}\eta - \eta^{\sigma^j} &= \iota\left(\zeta + \zeta^{-1}\right) - \iota\left(\zeta^{r^j} + \zeta^{-r^j}\right)\\ &= \iota\left(\zeta\left(1 - \zeta^{r^j-1}\right) - \zeta^{-r^j}\left(1 - \zeta^{r^j-1}\right)\right)\\ &= -\iota\zeta^{-r^j}\left(1 - \zeta^{r^j-1}\right)^2\\ &\cong \mathfrak{P}^2\end{aligned}$$

because of $(r^j - 1, p) = 1$. Assume that $j = k\phi(p^u), (k, p) = 1$ for $n \ge u \ge 1$. Then $r^j = r^{k\phi(p^u)} \equiv 1 + ktp^u \pmod{p^{u+1}}$, where we can choose a primitive root r modulo p such that $r^{\phi(p)} = 1 + tp$ and $(t, p) = 1$. Then $(1 - \zeta^{r^j-1})^2 \cong \mathfrak{P}^{2p^u}$. Now the number t_u of exponents j $(1 \le j \le s-1)$ such that $j \equiv 0 \pmod{\phi(p^u)}$ $(1 \le u \le n)$ is $(p^{n-u} - 1)/2$. Then we have

$$\prod_{j=1}^{s-1}(\eta - \eta^{\sigma^j}) \cong \mathfrak{P}^{2E},$$

where

$$\begin{aligned} 2E &= 2\left\{p^0((s-1)-t_1) + p(t_1 - t_2) + \cdots + p^{n-2}(t_{n-2} - t_{n-1}) + p^{n-1}(t_{n-1} - t_n)\right\} \\ &= np^n - (n+1)p^{n-1} - 1 \\ &= n\phi(p^n) - p^{n-1} - 1. \end{aligned}$$

Next by

$$\begin{aligned} \eta - \eta^\tau &= \iota(\zeta + \zeta^{-1}) - \bar{\iota}(\zeta + \zeta^{-1}) \\ &= 2\iota\zeta^{-1}(1 + \zeta^2) \\ &\cong 2 \end{aligned}$$

with $(2, p) = 1$, we see that

$$|N_K(\eta - \eta^\tau)| = 2^{\phi(m)/2} = 2^{\phi(p^n)}.$$

Moreover we see that for $1 \le j \le s-1$,

$$\begin{aligned} \eta - \eta^{\sigma^j\tau} &= \iota(\zeta + \zeta^{-1}) - \bar{\iota}(\zeta^{r^j} + \zeta^{-r^j}) \\ &= \iota\zeta(1 + \zeta^{r^j - 1}) + \iota\zeta^{-r^j}(1 + \zeta^{r^j - 1}) \\ &= \iota\zeta(1 + \zeta^{-r^j - 1})(1 + \zeta^{r^j - 1}) \\ &\cong 1 \end{aligned}$$

with $p^n \not| (r^j \pm 1)$, since we have for $1 \le u \le n$

$$\Phi_{p^u}(-1) = (-1)^{\phi(p^u)} \prod_{(x,p)=1} (1 + \zeta^x) = 1.$$

Thereby we obtain

$$d_K(\eta) \cong \mathrm{N}_K(\mathfrak{d}_K(\eta)) \cong (\mathrm{N}_K\mathfrak{P}^{2E}) \cdot 2^{\phi(m)/2} = 2^{2s}p^{2ns - m/(4p) - 1}.$$

Next the absolute value of the field discriminant $d(K)$ of the field K is equal to

$$\prod_{\chi\in<\lambda\psi>} f_\chi = \left(\prod_{j=0}^{s_n-1} f_{\psi^j}\right)\left(\prod_{j=0}^{s_n-1} f_{\lambda\psi^j}\right).$$

Set $s_j = \phi(p^j)/2$. Then we have

$$\begin{aligned}\prod_{j=1}^{s_n-1} f_{\psi^j} &= \left(\prod_{\substack{j=0\\(j,p^n)=1}}^{s_n-1} f_{\psi^j}\right)\left(\prod_{\substack{j=0\\(j,p^n)=p}}^{s_n-1} f_{\psi^j}\right)\cdots\left(\prod_{\substack{j=0\\(j,p^n)=p^{n-2}}}^{s_n-1} f_{\psi^j}\right)\left(\prod_{\substack{j=0\\(j,p^n)=p^{n-1}}}^{s_n-1} f_{\psi^j}\right)\\ &= (p^n)^{(s_n-1)-(s_{n-1}-1)}\cdot(p^{n-1})^{(s_{n-1}-1)-(s_{n-2}-1)}\cdots(p^2)^{(s_2-1)-(s_1-1)}\cdot p^{s_1-1}\\ &= p^{n(s_n-1)-(s_{n-1}-1)-(s_{n-2}-1)-\cdots-(s_1-1)}\\ &= p^{ns_n-n-s_{n-1}-s_{n-2}-\cdots-s_1+(n-1)}.\end{aligned}$$

Thus

$$\begin{aligned}|d(K)| &= 2^{\phi(p^n)}p^{2(n\phi(p^n)/2-\phi(p^{n-1})/2-\cdots-\phi(p)/2-1)}\\ &= 2^{\phi(p^n)}p^{n\phi(p^n)-p^{n-2}(p-1)-\cdots-(p-1)-2}\\ &= 2^{2s}p^{2ns-m/(4p)-1}.\end{aligned}$$

Therefore we obtain $|d(K)| = |d_K(\eta)|$. This completes a proof of Theorem 2. □

§3. Non-Monogenic Case

We claim that the ring $\boldsymbol{Z}_{k_m^-}$ of integers in an imaginary field k_m^- with $[k_m : k_m^-] = 2$ is non-monogenic for the conductor $m = 3p^n, p$ is a prime > 3. Contrary to the theorems in the previous section, the Gauß period does not necessarily generate a power basis.

THEOREM 3. *Suppose $m = 3p^n$, where p is a prime > 3, and K be the imaginary subfield of k_m distinct from $k_{m/3}$ with $[k_m : K] = 2$. Then the ring $\boldsymbol{Z}_K$ of integers in K does not have a power basis and the absolute value of the field discriminant of K is equal to $N_K(\mathfrak{L}\cdot\mathfrak{P}^{2E}) = 3^{\phi(p^n)/2}p^{n\phi(p^n)-p^{n-1}-1}$.*

Proof. Let $\omega = \zeta_3$, $\zeta = \zeta_{m/3}$. Then $\zeta_m = \omega\cdot\zeta$. For a cyclotomic field $k_m = \boldsymbol{Q}(\zeta_m)$, let

$$G = \mathrm{Gal}(k_m/\boldsymbol{Q}) = <\tau> \times <\sigma>$$

be the galois group with $\tau^2 = e = \sigma^{\phi(m/3)/2}$ and $\omega^\tau = \bar{\omega},\ \omega^\sigma = \omega,\ \ \zeta^\tau = \zeta,\ \zeta^\sigma = \zeta^r$. Then $\zeta_m^\tau = \bar{\omega} \cdot \zeta,\ \ \zeta_m^\sigma = \omega \cdot \zeta^r$. For $s = \phi(m/3)/2$ let $H =< \sigma^s >$ be the subgroup of G corresponding to K and $\eta = \sum_{\rho \in H} \zeta^\rho = \omega(\zeta + \zeta^{-1})$ be the Gauß period. Then $K = \boldsymbol{Q}(\eta)$. Let λ and ψ be characters defined by $\lambda(\tau) = -1, \lambda(\sigma) = 1, \psi(\tau) = 1, \psi(\sigma) = \zeta_s$. Since the group $\mathrm{Gal}(K/\boldsymbol{Q})$ is isomorphic to $\{H, \sigma H, \cdots, \sigma^{s-1}H, \tau H, \tau\sigma, \cdots, \tau\sigma^{s-1}H\}$, by the conductor-discriminant formula we obtain the same absolute value $|d(K)| = 3^s p^{2ns-m/(3p)-1}$ of the field discriminant.

On the other hand, since the set $\left\{\omega^{\tau^i}\gamma^j\right\}_{0\le i\le 1;\ 0\le j\le s-1}$ is an integral basis of $K = \boldsymbol{Q}(\omega\gamma)$ [6], any integer $\xi \in \boldsymbol{Z}_K$ can be written

$$\sum_{j=0}^{s-1} a_j \omega\gamma^j + \sum_{j=0}^{s-1} a_{s+j}\omega^\tau\gamma^j,$$

where $\gamma = \zeta + \zeta^{-1}$. Then for the different of ξ

$$\begin{aligned}\mathfrak{d}_K(\xi) &= \prod_{\rho H \in G/H\setminus\{H\}} (\xi - \xi^\rho) \\ &= (\xi - \xi^\sigma)\cdots(\xi - \xi^{\sigma^{s-1}})(\xi - \xi^\tau)(\xi - \xi^{\tau\sigma})\cdots(\xi - \xi^{\tau\sigma^{s-1}}),\end{aligned}$$

we see that

$$\begin{aligned}\xi - \xi^\tau &= (\omega - \omega^\tau)\left\{\sum_{j=0}^{s-1} a_j\gamma^j - \sum_{j=0}^{s-1} a_{s+j}\gamma^j\right\} \\ &= \alpha(1-\omega) \\ &\cong \alpha\mathfrak{L},\end{aligned}$$

$$\begin{aligned}\xi - \xi^{\sigma^k} &= \omega\sum_{j=0}^{s-1} a_j\left(\gamma^j - \gamma^{j\sigma^k}\right) + \omega^\tau\sum_{j=0}^{s-1} a_{s+j}\left(\gamma^j - \gamma^{j\sigma^k}\right) \\ &= \delta(1-\zeta)^2, \quad 1 \le k \le s-1,\ (k, p-1) = 1\end{aligned}$$

and by the same evaluation of $\mathfrak{P}$-exponent of $(\xi - \xi^{\sigma^k})$ in the proof of Theorem 2,

$$\prod_{k=1}^{s-1}(\xi - \xi^{\sigma^k}) \ \cong \beta\mathfrak{P}^{2E}$$

for $\gamma = \zeta + \zeta^{-1}$, some $\alpha, \delta, \beta \in \boldsymbol{Z}_K$, prime ideals $\mathfrak{L} = (1-\omega)$ and $\mathfrak{P} = (1-\zeta)$, where $2E = n\phi(p^n) - p^{n-1} - 1$. Then we have

$$\begin{aligned} |d_K(\xi)| &= \mathrm{N}_K(\mathfrak{d}_K(\xi)) \\ &= \left| N_K\left(\prod_{k=1}^{s-1}(\xi - \xi^{\sigma^k})\right) N_K(\xi - \xi^{\tau}) N_K\left(\prod_{k=1}^{s-1}(\xi - \xi^{\tau\sigma^k})\right)\right| \\ &= \left| N_K(\alpha\beta) d(K) N_K\left(\prod_{k=1}^{s-1}(\xi - \xi^{\tau\sigma^k})\right)\right|. \end{aligned}$$

Here we can confirm the above computation for the field discriminant $d(K)$. Namely, for some ideals $\mathfrak{a}$, $\mathfrak{b}$ we have

$$\mathfrak{d}_{\boldsymbol{Q}(\omega)}(\xi) = \xi - \xi^{\tau} \cong \mathfrak{a}\mathfrak{d}(\boldsymbol{Q}(\omega)), \qquad \mathfrak{d}_{\boldsymbol{Q}(\gamma)}(\xi) = \prod_{k=1}^{s-1}(\xi - \xi^{\sigma^k}) \cong \mathfrak{b}\mathfrak{d}(\boldsymbol{Q}(\gamma)).$$

Moreover we obtain that

$$\mathrm{N}_K(\mathfrak{d}(\boldsymbol{Q}(\omega))\mathfrak{d}(\boldsymbol{Q}(\gamma))) = \mathrm{N}_K\mathfrak{d}(K) = d(K)$$

for linearly disjoint fields $\boldsymbol{Q}(\omega)$ and $\boldsymbol{Q}(\gamma)$ over $\boldsymbol{Q}$.

Then $\boldsymbol{Z}_K = \boldsymbol{Z}[\xi]$ holds if and only if $|d_K(\xi)| = |d(K)|$ and hence it is equivalent to

$$N_K(\alpha\beta) N_K((\xi - \xi^{\tau\sigma}) \cdots (\xi - \xi^{\tau\sigma^{s-1}})) = \pm 1.$$

However we will find that $|N_K(\xi - \xi^{\tau\sigma})| > 1$ for any primitive integer ξ in K. In fact, we write $\xi = \omega R + \omega^{\tau} S$, where $R = \sum_{j=0}^{s-1} a_j \gamma^j$ and $S = \sum_{j=0}^{s-1} a_{s+j}\gamma^j$. In the case of $R - S^{\sigma} \neq 0$, $R^{\sigma} - S \neq 0$ and $R - S^{\sigma} \neq \pm(R^{\sigma} - S)$, we put $A = R - S^{\sigma}$, $B = S - R^{\sigma}$. By $\xi - \xi^{\tau\sigma} = \omega A + \omega^{\tau} B$ we consider the relative norm from K to $\boldsymbol{Q}(\gamma)$. It follows that

$$\begin{aligned} N_{K/\boldsymbol{Q}(\gamma)}(\xi - \xi^{\tau\sigma}) &= (\omega A + \omega^{\tau} B)(\omega^{\tau} A + \omega B) \\ &= A^2 - AB + B^2 \geq A^2 - |AB| + B^2 \geq |AB|, \end{aligned}$$

where the final equality holds only if $|A| = |B|$. Then by assumption, we have

$$\begin{aligned} |N_K(\xi - \xi^{\tau\sigma})| &= \left| N_{\boldsymbol{Q}(\gamma)}(A^2 - AB + B^2)\right| \\ &> \left| N_{\boldsymbol{Q}(\gamma)}(AB)\right| \geq 1. \end{aligned}$$

Next in the case of $R-S^\sigma=0$, assume that $\xi-\xi^{\tau\sigma}\cong S-R^\sigma$ is a unit. Then its conjugate $S^\sigma-R^{\sigma^2}$ is also a unit. However by

$$R-R^{\sigma^2}=\sum_{j=0}^{s-1}a_j\left(\gamma^j-\left(\gamma^{\sigma^2}\right)^j\right)$$

and $\gamma-\gamma^{\sigma^2}=(\zeta+\zeta^{-1})-(\zeta^{r^2}+\zeta^{-r^2})\equiv 0 \pmod{\mathfrak{P}}$, $R-R^{\sigma^2}$ is not a unit, which is a contradiction. In the case of $R^\sigma-S=0$, we can deduce the same contradiction. Next in the case of $R-S^\sigma=R^\sigma-S$, we have $\xi-\xi^{\tau\sigma}=\omega(R-S^\sigma)(1-\omega)\equiv 0 \pmod{\mathfrak{L}}$. Hence $|N_K(\xi-\xi^{\tau\sigma})|>1$.

Finally in the case of $R-S^\sigma=-(R^\sigma-S)$, since

$$\begin{aligned}\alpha &= \xi-\xi^\tau\\ &= \omega(R-S^\sigma)+\omega^\tau(S-R^\sigma)\\ &= \omega(S-R^\sigma)+\omega^\tau(R-S^\sigma),\end{aligned}$$

we have

$$\begin{aligned}2\alpha &= (\omega+\omega^\tau)(R+S-(R+S)^\sigma)\\ &\equiv 0 \pmod{\mathfrak{P}}.\end{aligned}$$

Then in this case also we have $|N_K(\xi-\xi^{\tau\sigma})|>1$. Thus for any integer $\xi\in \boldsymbol{Z}_K$, it can not generate a power basis. □

§4. Examples

We consider all the subfields of the cyclotomic field k_{93} of conductor $|-3||-31|$. According to the same notations as in the previous section, let

$$G=\mathrm{Gal}(k_{93}/\boldsymbol{Q})=<\tau>\times<\sigma>,$$

where $\tau^2=e=\sigma^{2s},\ s=\phi(31)/2$ and $\omega^\tau=\bar{\omega},\ \omega^\sigma=\omega,\ \ \zeta^\tau=\zeta,\ \zeta^\sigma=\zeta^r$ for a primitive cubic root ω of unity, a primitive 31st root ζ of unity and a primitive root r modulo 31.

Let $H^-_{2s/j} =< \sigma^j >$, $H^+_{2s/j} =< \tau\sigma^j >$, $H_{4s/j} =< \tau, \sigma^j >$, $H_1 =< \mathrm{I} >$ be the subgroup of G and K^-_{2j}, K^+_{2j}, K_j, K_{60} be the subfields of k_{93} corresponding to $H^-_{2s/j}$, $H^+_{2s/j}$, $H_{4s/j}$, H_1 for $j|30$, respectively. Let

$$\eta^{\pm}_{2j} = \sum_{\rho \in H^{\pm}_{2s/j}} \zeta^{\rho}_{93},\ \eta_j = \sum_{\rho \in H_{4s/j}} \zeta^{\rho}_{93}$$

of the period length $2s/j$ and $4s/j$, respectively. Then we have twenty subfields of k_{93} and their generators are as follows;

$K_1 = \boldsymbol{Q},\ K^-_2 = \boldsymbol{Q}\left(\sqrt{-3}\right) = k_3,\ K^+_2 = \boldsymbol{Q}\left(\sqrt{93}\right),\ K_2 = \boldsymbol{Q}\left(\sqrt{-31}\right),$

$K_3 = \boldsymbol{Q}\left(\eta_3\right),\ K^-_4 = \boldsymbol{Q}\left(\eta^-_4\right) = \boldsymbol{Q}\left(\sqrt{-3}, \sqrt{-31}\right),\ K_5 = \boldsymbol{Q}\left(\eta_5\right),$

$K^-_6 = \boldsymbol{Q}\left(\eta^-_6\right) = \boldsymbol{Q}\left(\sqrt{-3}, \eta_3\right),\ K^+_6 = \boldsymbol{Q}\left(\eta^+_6\right) = \boldsymbol{Q}\left(\sqrt{93}, \eta_3\right),$

$K_6 = \boldsymbol{Q}\left(\eta_6\right) = \boldsymbol{Q}\left(\sqrt{-31}, \eta_3\right),$

$K^-_{10} = \boldsymbol{Q}\left(\eta^-_{10}\right) = \boldsymbol{Q}\left(\sqrt{-3}, \eta_5\right),\ K^+_{10} = \boldsymbol{Q}\left(\eta^+_{10}\right) = \boldsymbol{Q}\left(\sqrt{93}, \eta_5\right),$

$K_{10} = \boldsymbol{Q}\left(\eta_{10}\right) = \boldsymbol{Q}\left(\sqrt{-31}, \eta_5\right),$

$K^-_{12} = \boldsymbol{Q}\left(\eta^-_{12}\right) = \boldsymbol{Q}\left(\sqrt{-3}, \sqrt{-31}, \eta_3\right),\ K_{15} = \boldsymbol{Q}\left(\eta_{15}\right) = \boldsymbol{Q}\left(\eta_3, \eta_5\right) = k^+_{31},$

$K^-_{20} = \boldsymbol{Q}\left(\eta^-_{20}\right) = \boldsymbol{Q}\left(\sqrt{-3}, \sqrt{-31}, \eta_5\right),$

$K^-_{30} = \boldsymbol{Q}\left(\eta^-_{30}\right) = \boldsymbol{Q}\left(\sqrt{-3}, \eta_3, \eta_5\right),\ K^+_{30} = \boldsymbol{Q}\left(\eta^+_{30}\right) = \boldsymbol{Q}\left(\sqrt{93}, \eta_3, \eta_5\right) = k^+_{93},$

$K_{30} = \boldsymbol{Q}\left(\eta_{30}\right) = \boldsymbol{Q}\left(\sqrt{-31}, \eta_3, \eta_5\right) = k_{31},$

$K_{60} = \boldsymbol{Q}\left(\zeta_{93}\right) = k_{93}.$

As is well known, the cyclotomic fields k_{93}, k_{31}, k_3, and their maximal real subfields k^+_{93}, k^+_{31}, $\boldsymbol{Q}$, and quadratic subfields K^+_2, K_2 have an integral power basis.

Since $2^5 \equiv 1 \pmod{31}$, the prime number 2 is completely decomposed in the subfield K_6. Then using Proposition [13], the cubic subfield K_3, the biquadratic one K^-_4, three sextic ones K^-_6, K^+_6, K_6 and K^-_{12} have no integral power basis. Next, because two subfields K^-_{10}, K_{10} are the composite fields of an imaginary quadratic field$\neq \boldsymbol{Q}(i)$ and a real abelian field, they have no integral power basis by Theorem 1 [7]. The ring of the maximal imaginary subfield K^-_{30} of k_{31} is non-monogenic by Theorem 3. Finally, since the extension degree of K_5 is a prime $5 > 3$, K_5 has no integral power basis by [3].

On the other hand, we can not determine whether each of the rings of integers in two subfields K^+_{10} and K^-_{20} has a power basis or does not.

References

[1] D. S. DUMMIT and H. KISILEVSKY, *Indices in cyclic cubic fields*, Number Theory and Algebra; Collect. Pap. Dedic. H. B. Mann, A. E. Ross and O. Taussky-Todd, New York San Francisco London, Academic Press, (1977), 29-42

[2] I. GAÁL, *Computing all power integral bases in orders of totally real cyclic sextic number fields*, Math. Comp., **65**(1996), 801-822

[3] M.-N. GRAS, *Non monogénéité de l'anneau des extensions cycliques de* $\mathbb{Q}$ *de degré premier* $\ell \geq 5$, J. Number Theory, **23**(1986), 347-353

[4] K. GYŐRY, *Discriminant form and index form equations*, Algebraic Number Theory and Diophantine Analysis, Halter-Koch, F. and Tichy, R. F. eds., Berlin New York, Walter de Gruyter, (2000), 191-214

[5] T. KUBOTA, Lectures on Number Theory — Metaplectic Theory and Geometric Reciprocity Law — (in Japanese), Makino Shoten, Tokyo, 1999

[6] S. LANG, Algebraic Number Theory, Reading, Massachusetts, Addison-Wesley Publishing Company, INC., 1970

[7] Y. MOTODA, T. NAKAHARA and S. I. A. SHAH, *On a problem of Hasse for certain imaginary abelian fields*, J. Number Theory, (To appear),

[8] T. NAKAHARA, *Examples of algebraic number fields which have not unramified extensions*, Rep. Fac. Sci. Engrg. Saga Univ. Math., **1**(1973), 1-8

[9] T. NAKAHARA, *On cyclic biquadratic fields related to a problem of Hasse*, Mh. Math., **94**(1982), 125-132

[10] T. NAKAHARA, *A simple proof for non-monogenesis of the rings of integers in some cyclic Fields*, The proceedings of the third Conference of the Canadian Number Theory Association, Oxford, Clarendon Press, (1993), 167-173

[11] W. NARKIEWICZ, Elementary and Analytic Theory of Algebraic Numbers, 2nd Edition, Berlin Heidelberg New York, Springer-Verlag; Warszawa, PWN-Polish Scientific Publishers, 1990

[12] S. I. A. SHAH, *Monogenesis of the ring of integers in a cyclotomic sextic field of a prime conductor*, Rep. Fac. Sci. Engrg. Saga Univ. Math., **29**(2000), 1-9

[13] S. I. A. SHAH and T. NAKAHARA, *Monogenesis of the rings of integers in certain imaginary abelian fields*, Nagoya Math. J., **168** (To appear),

[14] L. C. WASHINGTON, Introduction to cyclotomic fields, 2nd Edition, Grad.Texts in Math. **83** New York Heidelberg Berlin, Springer-Verlag, 1997

Syed Inayat Ali SHAH
Shaikh Zayed Islamic Center
University of Peshawar
the Islamic Republic of Pakistan

E-mail: inayat@daak.net

Toru NAKAHARA
Department of Mathematics
Faculty of Science and Engineering
Saga University, Saga 840-8502, Japan

E-mail: nakahara@ms.saga-u.ac.jp