S. I. A. Shah and T. Nakahara
Nagoya Math. J.
Vol. 168 (2002), 85–92

MONOGENESIS OF THE RINGS OF INTEGERS IN CERTAIN IMAGINARY ABELIAN FIELDS

SYED INAYAT ALI SHAH AND TORU NAKAHARA*

Abstract. In this paper we consider a subfield K 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 $p > \ell = 3$. Then the theme is to know whether the ring of integers in K has a power basis or does not.

§1. Introduction

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 α generates a power basis of the ring $\boldsymbol{Z}_F$ or simply $\boldsymbol{Z}_F$ has a 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. To determine whether the ring of integers in a field is monogenic or not is proposed as an unsolved problem in [Nar]. This problem is treated by many authors [DK], [Ga], [Gr], [HSW], [N_1], [SN], [T].

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 integers has always a power basis [Li], [W].

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 that $m = 3p^n (n \geq 1)$ with a prime $p > 3$ and the subfield

Received February 21, 2000.
2000 Mathematics Subject Classification: 11R18, 11R04.
*Supported in part by the Japan Society for the Promotion of Science grant (#11640036).

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.

Finally we will give another characterization of fields whose rings of integers do not have any power basis using the decomposition theory of ideals [N$_2$].

§2. Monogenic case

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

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 $G = \mathrm{Gal}(k_m/\boldsymbol{Q}) = \langle\tau\rangle \times \langle\sigma\rangle$ with $\tau^2 = e = \sigma^s$, $s = \phi(m)/2 = 2^{n-2}$ 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 $\langle\sigma^{s/2}\rangle$, $\langle\tau\rangle$ and $H = \langle\sigma^{s/2}\tau\rangle$ respectively. Then K is generated by the Gauss period $\eta = \sum_{\rho\in H}\zeta_m^\rho = \zeta_m - \zeta_m^{-1}$.

We see that $\boldsymbol{Z}_{k_m} = \boldsymbol{Z}[\zeta_m] = \boldsymbol{Z}_K[\zeta_m]$. Then, since $5^{2^{n-1}} \not\equiv -1 \pmod 4$, the relative different $\mathfrak{d}_{k_m/K}$ is given by

$$\left(\zeta_m - \zeta_m^{\sigma^{s/2}\tau}\right)\boldsymbol{Z}_{k_m} = (1-\zeta_m^2)\boldsymbol{Z}_{k_m} = \mathfrak{L}^2,$$

where $\mathfrak{L}$ is the ramified prime ideal $(1-\zeta_m)$ of k_m over 2. From this, it follows that

$$|d(K)| = \sqrt{|d(k_m)|/2^2} = 2^{s(n-1)-1}.$$

On the other hand, by $G/H = \left\{\sigma^j H; 0 \leq j < s\right\}$, the different $\mathfrak{d}_K(\eta)$ of η is given by

$$\prod_{j=1}^{s-1}(\eta - \eta^{\sigma^j}) = \prod_{j=1}^{s-1}\left\{\zeta_m\left(1-\zeta_m^{\sigma^j-1}\right)\left(1+\zeta_m^{-\sigma^j-1}\right)\right\}.$$

Since we observe that

$$\left\{\zeta_m^{\sigma^j},\ -\zeta_m^{-\sigma^j};\ 0 \leq j < s\right\} = \left\{\zeta_m^j;\ 0 < j < m,\ (j,m) = 1\right\},$$
$$\left\{\zeta_m^{\sigma^j-1},\ -\zeta_m^{-\sigma^j-1};\ 0 \leq j < s\right\} = \left\{\zeta_m^j;\ 0 \leq j < m,\ (j,m) \neq 1\right\},$$

we can put

$$X^m - 1 = \Phi_m(X)(X-1)\left(X + \zeta_m^{-2}\right) f(X),$$

where $\Phi_m(X)$ denotes the m-th cyclotomic polynomial and

$$f(X) = \prod_{j=1}^{s-1} \left\{ \left(X - \zeta_m^{\sigma^j - 1}\right)\left(X + \zeta_m^{-\sigma^j - 1}\right) \right\},$$

hence $m = \Phi_m(1)\left(1 - \zeta_m^{2s-2}\right) f(1)$. Then we obtain

$$\mathfrak{d}_K(\eta) \cong f(1) \cong 2^{n-1}/\mathfrak{L}^2,$$

namely

$$|d_K(\eta)| = 2^{s(n-1)-1}.$$

Here the symbol $\alpha \cong \beta$ or $\alpha \cong \mathfrak{A}$ onwards means $(\alpha) = (\beta)$ or $(\alpha) = \mathfrak{A}$ as ideals for numbers α, β and an ideal $\mathfrak{A}$, respectively.

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 $\boldsymbol{Z}_K$ 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 $2^{\phi(p^n)} p^{n\phi(p^n) - p^{n-1} - 1}$.*

Proof. Let $G = \langle\tau\rangle \times \langle\sigma\rangle$ with $\zeta_4^\tau = \bar{\zeta_4}$, $\zeta_{m/4}^\tau = \zeta_{m/4}$ and $\zeta_4^\sigma = \zeta_4$, $\zeta_{m/4}^\sigma = \zeta_{m/4}^r$, where r is a primitive root modulo p^n. We have three subfields $k_{m/4}, k_m^+$ and K of degree $\phi(p^n)$ whose galois groups are $\langle\tau\rangle, \langle\sigma^s\tau\rangle$ and $H = \langle\sigma^s\rangle$ with $s = \phi(m/4)/2$ respectively. 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.

As in the proof of Theorem 1, since $\boldsymbol{Z}_{k_m} = \boldsymbol{Z}_K[\zeta_m]$, the relative different $\mathfrak{d}_{k_m/K}$ is given by

$$\left(\zeta_m - \zeta_m^{\sigma^s}\right) \boldsymbol{Z}_{k_m} = \iota(\zeta - \zeta^{-1}) \boldsymbol{Z}_{k_m} = \mathfrak{P},$$

where $\mathfrak{P}$ is the ramified prime ideal $(1 - \zeta)$ of $k_{m/4}$ over p. Then

$$|d(K)| = \sqrt{|d(k_m)| / \mathrm{N}_{k_m}(\mathfrak{d}_{k_m/K})} = 2^{2s} p^{2ns - (m/4p) - 1}.$$

https://doi.org/10.1017/S0027763000008369 Published online by Cambridge University Press

On the other hand, by $G/H = \left\{\sigma^j H,\ \sigma^j\tau H; 0 \leq j < s\right\}$, the different $\mathfrak{d}_K(\eta)$ of η is given by

$$(\eta - \eta^{\tau})\prod_{j=1}^{s-1}\left\{(\eta - \eta^{\sigma^j})(\eta - \eta^{\sigma^j\tau})\right\}$$
$$= (\iota/\zeta)^{2(s-1)}2\iota(\zeta + \zeta^{-1})\prod_{j=1}^{s-1}\left\{(\zeta^2 - \zeta^{2\sigma^j})(\zeta^2 - \zeta^{-2\sigma^j})\right\}.$$

Since we observe that

$$\left\{\zeta^{2\sigma^j},\ \zeta^{-2\sigma^j};\ 0 \leq j < s\right\} = \left\{\zeta^j;\ 0 < j < m/4,\ (j, m/4) = 1\right\},$$

we can put

$$\Phi_{m/4}(X) = (X - \zeta^2)\left(X - \zeta^{-2}\right)f(X),$$

where

$$f(X) = \prod_{j=1}^{s-1}\left(X - \zeta^{2\sigma^j}\right)\left(X - \zeta^{-2\sigma^j}\right),$$

hence $f(\zeta^2) = \Phi'_{m/4}(\zeta^2)\left(\zeta^2 - \zeta^{-2}\right)^{-1}$. Then we obtain

$$\mathfrak{d}_K(\eta) \cong 2\Phi'_{m/4}(\zeta^2)/\left(\zeta - \zeta^{-1}\right) \cong 2p^n\mathfrak{P}^{-p^{n-1}-1},$$

namely

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

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

Remark 1. Using the same way as in [W. Proposition 2.16.], we can give a simple proof of monogenesis of imaginary subfields once we know that they are generated by the Gauß period $\zeta_m - \zeta_m^{-1}$. Our methods of proofs for Theorem 1 and Theorem 2 which give a criterion to $\boldsymbol{Z}_K = \boldsymbol{Z}[\zeta_m - \zeta_m^{-1}]$ can be applied to investigate non-monogenic phenomena in Theorem 3.

https://doi.org/10.1017/S0027763000008369 Published online by Cambridge University Press

§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. Contrary to the theorems in the previous section, the Gauß period does not 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.*

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

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

be the galois group with $\tau^2 = e = \sigma^{\phi(m/3)}$ and $\omega^\tau = \bar{\omega}$, $\omega^\sigma = \omega$, $\zeta^\tau = \zeta$, $\zeta^\sigma = \zeta^r$, where r is a primitive root modulo $p^n = m/3$. Then $\zeta_m^\tau = \bar{\omega} \cdot \zeta$, $\zeta_m^\sigma = \omega \cdot \zeta^r$.

For $s = \phi(m/3)/2$, let $H = \langle\sigma^s\rangle$ 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 $K = \boldsymbol{Q}(\eta)$. Since $\boldsymbol{Z}_K = \boldsymbol{Z}_{k_3} \boldsymbol{Z}_{k_{m/3}}^+ = \omega \boldsymbol{Z}[\gamma] + \omega^\tau \boldsymbol{Z}[\gamma]$, any $\xi \in \boldsymbol{Z}_K$ can be written as $\xi = \omega R + \omega^\tau S$ with $R, S \in \boldsymbol{Z}[\gamma]$, where $\gamma = \zeta + \zeta^{-1}$. Then by $G/H = \left\{\sigma^j H,\ \sigma^j \tau H; 0 \le j < s\right\}$, the different $\mathfrak{d}_K(\xi)$ of ξ is given by

$$\begin{aligned}
&(\xi - \xi^\tau) \prod_{j=1}^{s-1} \left\{(\xi - \xi^{\sigma^j})(\xi - \xi^{\sigma^j \tau})\right\} \\
&\quad = (\omega - \omega^\tau)(R - S) \prod_{j=1}^{s-1} \left\{(\xi - \xi^{\sigma^j \tau})\right\} \prod_{j=1}^{s-1} \left\{\omega(R - R^{\sigma^j}) + \omega^\tau (S - S^{\sigma^j})\right\}.
\end{aligned}$$

Here, we observe that $T - T^\rho$ is always divisible by $\gamma - \gamma^\rho = \zeta - \zeta^\rho + \zeta^{-1} - \zeta^{-\rho}$, which is further divisible by $\mathfrak{P}$, if $T \in \boldsymbol{Z}[\gamma]$ and $\rho \in G$, where $\mathfrak{P}$ is the ramified prime ideal $(1 - \zeta)$ of $k_{m/3}$ over p. Therefore $\mathfrak{d}_K(\xi)$ is a multiple of

$$(1 - \omega)(\xi - \xi^{\sigma\tau}) \prod_{j=1}^{s-1} \left(\gamma - \gamma^{\sigma^j}\right) = (1 - \omega)\,(\xi - \xi^{\sigma\tau})\,\mathfrak{d}_{k_{m/3}^+},$$

namely $d_K(\xi)$ is a multiple of

$$N_K\,(\xi - \xi^{\sigma\tau})\,3^s d\left(k_{m/3}^+\right) = N_K\,(\xi - \xi^{\sigma\tau})\,d(K).$$

Moreover, by the observation above, we have:

(i) If $R = S^\sigma$, then $\xi - \xi^{\sigma\tau} = \omega^\tau \left(S - S^{\sigma^2}\right) \in \mathfrak{P}$;

(ii) If $S = R^\sigma$, then $\xi - \xi^{\sigma\tau} = \omega \left(R - R^{\sigma^2}\right) \in \mathfrak{P}$;

(iii) If $R - S^\sigma = S - R^\sigma$, then $2(\xi - \xi^{\sigma\tau}) = -(R+S) + (R+S)^\sigma \in \mathfrak{P}$;

(iv) If $R - S^\sigma = R^\sigma - S$, then $(\xi - \xi^{\sigma\tau}) = (\omega - \omega^\tau)(R - S^\sigma) \in (1-\omega)$;

(v) Otherwise, as R, S are totally real, we have

$$\begin{aligned} |N_K(\xi - \xi^{\tau\sigma})| &= \left| N_{k^+_{m/3}} \left((R - S^\sigma)^2 - (R - S^\sigma)(S - R^\sigma) + (S - R^\sigma)^2 \right) \right| \\ &> \left| N_{k^+_{m/3}} \left((R - S^\sigma)(S - R^\sigma) \right) \right| \\ &\geq 1. \end{aligned}$$

This implies that $|N_K(\xi - \xi^{\tau\sigma})| > 1$ whenever $\xi - \xi^{\tau\sigma} \neq 0$. Hence, we find that $|d_K(\xi)| > |d(K)|$ if $d_K(\xi) \neq 0$.

Remark 2. As in the previous section, since $\boldsymbol{Z}_{k_m} = \boldsymbol{Z}_K[\zeta_m]$, the relative different $\mathfrak{d}_{k_m/K}$ is given by

$$\left(\zeta_m - \zeta_m^{\sigma^s}\right) \boldsymbol{Z}_{k_m} = \mathfrak{P}\boldsymbol{Z}_{k_m}.$$

Then

$$|d(K)| = \sqrt{|d(k_m)|/\mathrm{N}_{k_m}(\mathfrak{d}_{k_m/K})} = 3^s p^{2ns-(m/3p)-1}.$$

The following is slightly generalized from [N_2] owing to a remark from L. Washington.

PROPOSITION. *Let K be a galois extension of degree $n > 2$ over $\boldsymbol{Q}$ and ℓ be a prime number of ramification index e and relative degree f for $K/\boldsymbol{Q}$. If either $e\ell^f < n$ or $f > 1$, $e\ell^f \leq n + e - 1$, then $\boldsymbol{Z}_K$ does not have a power basis.*

Proof. Let α be a primitive element of K in $\boldsymbol{Z}_K$. Let the prime ideal decomposition of ℓ in the field K be

$$\ell \cong \prod \mathfrak{L}^e.$$

For any prime ideal $\mathfrak{L}$, we have

$$\alpha^{\mathrm{N}_K \mathfrak{L}} \equiv \alpha \bmod \mathfrak{L}.$$

Then by

$$\alpha^{\mathrm{N}_K \mathfrak{L}} \equiv \alpha \pmod{\prod \mathfrak{L}},$$

we see that

$$(\alpha^{\mathrm{N}_K \mathfrak{L}} - \alpha)^e \equiv 0 \pmod{\ell}.$$

Thus if $e\mathrm{N}_K \mathfrak{L} = e\ell^f < n$, then certainly the number

$$\beta = \ell^{-1}(\alpha^{\mathrm{N}_K \mathfrak{L}} - \alpha)^e = (1/\ell)\alpha^{e\ell^f} \pm \cdots \pm (1/\ell)\alpha^e$$

is in $\boldsymbol{Z}_K$ but outside of $\boldsymbol{Z}[\alpha]$. If $(\alpha, \ell) = 1$, $e\ell^f \leq n + e - 1$, then $\alpha^{-e}\beta \in \boldsymbol{Z}_K$ but $\notin \boldsymbol{Z}[\alpha]$. If $(\alpha, \ell) \neq 1$ and $\boldsymbol{Z}_K = \boldsymbol{Z}[\alpha]$, then $\alpha \equiv 0 \,(\bmod\, \mathfrak{L})$ for a certain $\mathfrak{L}$, hence for any integer $\xi = b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1} \in \boldsymbol{Z}_K$, we have $\xi \equiv b_0 \pmod{\mathfrak{L}}$, namely $f = 1$, which contradicts the hypothesis. Thus there exists an integer of K, but outside of $\boldsymbol{Z}[\alpha]$.

Example. Consider for the case of conductor $m = |5 \cdot (-3)| = 15$ a subfield $K = \boldsymbol{Q}(\sqrt{5}, \sqrt{-3})$ of $k_{15} = \boldsymbol{Q}(\zeta_{15})$ with $[k_{15} : K] = 2$. Since the prime number 2 splits in $\boldsymbol{Q}(\sqrt{-15})$ and $\mathfrak{L}$ is inert in $K/\boldsymbol{Q}(\sqrt{-15})$ for a prime ideal $\mathfrak{L}|2$, the ring $\boldsymbol{Z}_K$ of integers has no power basis by Proposition. Using the Gauß period $\eta = \zeta_3(\zeta_5 + \zeta_5^{-1})$, we have $K = \boldsymbol{Q}(\eta)$. Then the non-monogenesis of the ring $\boldsymbol{Z}_K$ is confirmed by Theorem 3, too. The other examples of prototype are shown in [SN].

Acknowledgements. The authors would like to express their sincere thanks to a referee who indicated a simplified method for the proofs of theorems and improved proposition, Lawrence C. Washington at University of Maryland, Tsuyoshi Uehara at Saga University, Yasuo Motoda at Yatsushiro National College of Technology and Sang Geun Hahn at Korea Adv. Inst. of Sci. & Tech. (KAIST) for their valuable suggestions regarding this work.

References

[DK] Dummit, D. S. and Kisilevsky, H., *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.

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

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

[HSW] Huard, J. G., Spearman, B. K. and Williams, K. S., *Integral Bases for Quartic Fields with Quadratic Subfields*, J. Number Theory, **51** (1995), 87–102.

[Li] Liang, J., *On integral basis of the maximal real subfield of a cyclotomic field*, J. Reine Angew. Math., **286/287** (1976), 223–226.

[N_1] Nakahara, T., *On cyclic biquadratic fields related to a problem of Hasse*, Mh. Math., **94** (1982), 125–132.

[N_2] ———, *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.

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

[SN] Shah, S. I. A., and Nakahara, T., *Non-monogenetic aspect of the rings of integers in certain abelian fields*, the Proceedings of the Jangjeon Mathematical Society, Pusan, Ku-Deok Co.,**1**, 2000, 75–79.

[T] Thérond, J. -D., *Existence d'une extension cyclique monogéne de discriminant donné*, Arch. Math., **41** (1983), 243–255.

[W] Washington, L. C., Introduction to cyclotomic fields, 2nd Edition GTM **83** 1997, Springer-Verlag., New York Heidelberg Berlin.

Syed Inayat Ali Shah
Department of Engineering Systems and Technology
Course of Science and Engineering
Graduate School of Saga University
Saga 840-8502
Japan
shah@ms.saga-u.ac.jp

CURRENT ADDRESS:
Shaikh Zayed Islamic Center
University of Peshawar
The Islamic Republic of Pakistan

Toru Nakahara
Department of Mathematics
Faculty of Science and Engineering
Saga University, Saga 840-8502
Japan
nakahara@ms.saga-u.ac.jp