Journal of Number Theory **96**, 326–334 (2002)
doi:10.1006/jnth.2002.2805

On a Problem of Hasse for Certain Imaginary Abelian Fields

Yasuo Motoda

Department of Mathematics, Yatsushiro National College of Technology, Yatsushiro 866-8501, Japan
E-mail: motoda@as.yatsushiro-nct.ac.jp

Toru Nakahara[1]

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

and

Syed Inayat Ali Shah

Shaikh Zayed Islamic Center, University of Peshawar, Pakistan

Communicated by P. Roquette

Received June 26, 2001

DEDICATED TO PROFESSOR KATSUMI SHIRATANI
ON THE OCCASION OF HIS 70TH BIRTHDAY

Let K be the composite field of an imaginary quadratic field $\boldsymbol{Q}(\omega)$ of conductor d and a real abelian field L of conductor f distinct from the rationals $\boldsymbol{Q}$, where $(d,f)=1$. Let Z_K be the ring of integers in K. Then concerning to Hasse's problem we construct new families of infinitely many fields K with the non-monogenic phenomena (1), (2) which supplement (*J. Number Theory* **23** (1986), 347–353; Publ. Math. Fac. Sci Besançon, Theor. Nombres (1984) 25pp) and with monogenic (3).

(1) If $\boldsymbol{Q}(\omega) \neq$ the Gauß field $\boldsymbol{Q}(i)$, then Z_K is of non-monogenesis.

(2) If $\boldsymbol{Q}(\omega)=\boldsymbol{Q}(i)$, then for a sextic field K, Z_K is of non-monogenesis except for two fields K of conductors 28 and 36.

(3) Let $\boldsymbol{Q}(\omega)=\boldsymbol{Q}(i)$. If Z_K has a power basis, then Z_L must have a power basis. Conversely, let L be the maximal real subfield k_f^+ of a cyclotomic field k_f, namely K be the maximal imaginary subfield of k_{4f} of conductor $4f$. Then Z_K has a power basis.

Key Words: Hasse's problem; non-monogenesis; power basis; discriminant; abelian field; imaginary quadratic field.

[1] To whom correspondence should be addressed.

0022-314X/02 $35.00

1. INTRODUCTION

Let K be an algebraic number field over the rationals $\boldsymbol{Q}$. If the ring $Z_K = \boldsymbol{Z}[\alpha]$ of integers in K is generated by an integer α over the ring $\boldsymbol{Z}$ of rational integers, it is said that Z_K has a power basis, Z_K is monogenic or of monogenesis, otherwise Z_K is said to be non-monogenic or of non-monogenesis.

Let k_n be an nth cyclotomic field $\boldsymbol{Q}(\zeta_n)$ over $\boldsymbol{Q}$ and k_n^+ the maximal real subfield of k_n, where ζ_n be a primitive nth root of unity. Gras [4, 5] showed the non-monogenesis of the ring Z_K of integers in cyclic fields K over $\boldsymbol{Q}$ of prime degrees $\ell \geqslant 5$ except for $K = k_{2l+1}^+$, where $2\ell + 1$ is a prime, and subsequently, she proved that there exist only finitely many abelian extensions K over $\boldsymbol{Q}$ of degrees $m \geqslant 5$, $(m, 6) = 1$, whose Z_K have a power basis using the prime decomposition of Gauß sum by Leopoldt [9].

In Theorem 1, we shall give a new family of infinitely many imaginary abelian fields K of degrees $m > 2$ whose rings Z_K are of non-monogenesis applying some evaluation of the different of a number in K [Lemma 1]. In Theorem 2, we shall characterize infinitely many imaginary abelian fields K of degrees $m > 2$ whose rings Z_K are of monogenesis using Lemma 2.

As is well known, Hasse's problem to characterize whether the ring Z_K of integers in a field K is of monogenesis or not is treated by Dummit and Kisilevsky [1], Gras [4], Huard et al. [7], Robertson [10], Schertz [13], Thérond [15] and others. Gaál *et al.* and Győry gave algorithm for determining the power bases of the rings in certain algebraic number fields and several monogenic examples [2, 3, 6]. A survey of researches for integral power bases is given in [6, Remark].

2. NON-MONOGENIC PHENOMENA FOR ABELIAN EXTENSIONS

The following lemma is fundamental for us.

LEMMA 1. *Let f be the conductor of a cyclotomic field k_f, $\prod_p p^e$ be its canonical decomposition and σ be an element of the Galois group G of k_f over $\boldsymbol{Q}$ which generates the Galois subgroup of k_{p^e} over $\boldsymbol{Q}$. Then for any integer R of k_f, $R - R^\sigma$ is divisible by a prime element π_p in k_{p^e} for $\pi_p = 1 - \zeta_{p^e}$.*

Proof. Since p^e and f/p^e are prime to each other, there exist primitive roots ζ_{p^e} and ζ_{f/p^e} such that $\zeta_f = \zeta_{p^e}\zeta_{f/p^e}$. Then $\zeta_f^\sigma = \zeta_{p^e}^\sigma \zeta_{f/p^e}$. Now a number

R in Z_{k_f} is represented by a form $\sum_{1\leqslant j\leqslant n} a_j\zeta_f^j$ with $a_j \in \boldsymbol{Z}$, where n is equal to the value of the Euler function $\phi(f)$. Then $R - R^\sigma = \sum_{1\leqslant j\leqslant n} a_j (\zeta_{p^e}^j - \zeta_{p^e}^{j\sigma})\zeta_{f/p^e}^j$. Since $\zeta_{p^e}^j - \zeta_{p^e}^{j\sigma}$ is divisible by π_p for any $\varrho \in G$, $R - R^\sigma$ is divisible by π_p. ∎

THEOREM 1. *Let K be the composite field of an imaginary quadratic field $\boldsymbol{Q}(\omega)$ and a real abelian field L distinct from the rationals $\boldsymbol{Q}$, whose conductors are prime to each other.*

(1) *If $\boldsymbol{Q}(\omega) \neq \boldsymbol{Q}(i)$ with $i^2 = -1$, then Z_K is of non-monogenesis.*

(2) *If $\boldsymbol{Q}(\omega) = \boldsymbol{Q}(i)$, then for a sextic field K, Z_K is of non-monogenesis except for two fields of conductors* 28 *and* 36.

Proof. Let τ be the generator of Galois group of $\boldsymbol{Q}(\omega)$ over $\boldsymbol{Q}$ and H the Galois group of L over $\boldsymbol{Q}$. Let $d(K)$ and $d(\xi)$ be the field discriminant of K and the discriminant of a number ξ in K, respectively. Then a ring Z_K is of monogenesis if and only if there exists a number ξ in K such that $|d(\xi)| = |d(K)|$. Now put $H^* = H\backslash\{e\}$, where e is the identity in H. Since the Galois group of K over $\boldsymbol{Q}$ is generated by τ and H, we have

$$
\begin{aligned}
|d(\xi)| &= \left|\left(N_K \prod_{\sigma\in H^*} (\xi - \xi^\sigma)\right)(N_K(\xi - \xi^\tau))\left(N_K \prod_{\sigma\in H^*} (\xi - \xi^{\tau\sigma})\right)\right| \\
&= |d(K)||N_K\alpha|\left|N_K \prod_{\sigma\in H^*} (\xi - \xi^{\tau\sigma})\right|
\end{aligned}
$$

for some integer α in K. Therefore if Z_K is of monogenesis, $|N_K \prod_{\sigma\in H^*} (\xi - \xi^{\tau\sigma})| = 1$ should be held. We assume that such ξ exists. Let $\prod_p p^e$ be the canonical decomposition of the conductor f of L. Then an fth root ζ_f of unity can be written as $\prod_p \zeta_{p^e}$ for some p^eth root ζ_{p^e} of unity. Let A be the subgroup of the Galois group G_f of k_f over $\boldsymbol{Q}$, which corresponds to the subfield L of k_f. The group H is isomorphic to the factor group G_f/A. Denote the Galois group of k_{p^e} over $\boldsymbol{Q}$ by A_p with a generator σ_p. Then we have a direct product decomposition $\prod_p A_p$ of G_f. Every σ_p is not contained in A, namely $\bar{\sigma}_p \in H^*$. Because if the group A contains some σ_p, we have $H \cong G_f/A \cong (G_f/\langle\sigma_p\rangle)/(A/\langle\sigma_p\rangle)$, where $\langle\varrho\rangle$ for $\varrho \in G$ denotes the subgroup of G generated by ϱ. This contradicts to the conductor f of L.

First, we consider the case where $Q(\omega)$ has an odd conductor m. Then $\boldsymbol{Q}(\omega) = \boldsymbol{Q}(\sqrt{-m})$ and $\{\omega, \omega^\tau\}$ for $\omega = (-1 + \sqrt{-m})/2$ is an integral basis of

$Z_{\boldsymbol{Q}(\omega)}$. Since we can put $\xi = \omega R + \omega^{\tau} S$ for some $R, S \in Z_L$ by [8], it holds that for $\sigma = \sigma_p$,

$$(\xi - \xi^{\tau\sigma})(\xi^{\tau} - \xi^{\sigma}) = \{\omega(R - S^{\sigma}) + \omega^{\tau}(S - R^{\sigma})\}\{\omega(S - R^{\sigma}) + \omega^{\tau}(R - S^{\sigma})\}$$

$$= \omega\omega^{\tau}(s_{\sigma}^2 + t_{\sigma}^2) + \{\omega^2 + (\omega^{\tau})^2\} s_{\sigma} t_{\sigma}$$

$$= \frac{1+m}{4}(s_{\sigma}^2 + t_{\sigma}^2) - \frac{m-1}{2} s_{\sigma} t_{\sigma},$$

where $s_{\sigma} = R - S^{\sigma},\ t_{\sigma} = S - R^{\sigma}$. If $t_{\sigma} = 0$, then we have $\xi - \xi^{\tau\sigma} = \omega(R - R^{\sigma^2})$, which is divisible by a prime factor π_p of p in L by Lemma 1. Thus $|d(\xi)| > |d(K)|$ holds. If $s_{\sigma} = 0$, we have the same conclusion. Next, assume $s_{\sigma} t_{\sigma} \neq 0$. Then it follows that

$$\frac{1+m}{4}(s_{\sigma}^2 + t_{\sigma}^2) - \frac{m-1}{2} s_{\sigma} t_{\sigma} = |s_{\sigma} t_{\sigma}| \left\{ \frac{1+m}{4}\left(\left|\frac{s_{\sigma}}{t_{\sigma}}\right| + \left|\frac{t_{\sigma}}{s_{\sigma}}\right| \right) \mp \frac{m-1}{2} \right\}$$

$$\geqslant |s_{\sigma} t_{\sigma}| \left\{ \frac{1+m}{2} \mp \frac{m-1}{2} \right\}$$

$$\geqslant |s_{\sigma} t_{\sigma}|,$$

where each equality holds if and only if $s_{\sigma} = t_{\sigma}$. Then we obtain $|N_L((\xi - \xi^{\tau\sigma})(\xi^{\tau} - \xi^{\sigma}))| \geqslant |N_L s_{\sigma} t_{\sigma}|$. If $s_{\sigma} \neq t_{\sigma}$, we have $|N_L((\xi - \xi^{\tau\sigma})(\xi^{\tau} - \xi^{\sigma}))| > 1$, namely $|d(\xi)| > |d(K)|$. If $s_{\sigma} = t_{\sigma}$, then we have $\xi - \xi^{\tau\sigma} = (\omega + \omega^{\tau})(R - S^{\sigma}) = -(R - S^{\sigma}) = -(S - R^{\sigma}) = -\frac{1}{2}\{(R+S) - (R+S)^{\sigma}\}$ which contains a prime factor π_p of p. Then $|d(\xi)| > |d(K)|$.

Secondly, we treat the case where $\boldsymbol{Q}(\omega)$ has an even conductor $m > 1$. Then $\boldsymbol{Q}(\omega) = \boldsymbol{Q}(\sqrt{-m})$ and $\{1, \omega\}$ for $\omega = \sqrt{-m}$ is an integral basis of $Z_{\boldsymbol{Q}(\omega)}$. Since we can put $\xi = R + \omega S$ for some $R, S \in Z_L$, it holds that $\xi - \xi^{\tau} = 2\omega S$. Then a number S should be a unit of L. By $\xi - \xi^{\tau\sigma} = R - R^{\sigma} + \omega(S + S^{\sigma})$, if $S + S^{\sigma} = 0$, then $\xi - \xi^{\tau\sigma}$ is divisible by a prime factor π_p of p. Hence $|d(\xi)| > |d(K)|$. If $S + S^{\sigma} \neq 0$, then $(\xi - \xi^{\tau\sigma})(\xi^{\tau} - \xi^{\sigma}) \geqslant m(S + S^{\sigma})^2$. Thus we have

$$|N_K(\xi - \xi^{\tau\sigma})| \geqslant |N_L m(S + S^{\sigma})^2| \geqslant m^{[L:\boldsymbol{Q}]} > 1.$$

Then $|d(\xi)| > |d(K)|$.

Finally, we consider the case where $\boldsymbol{Q}(\omega)$ coincides with the Gauß field $\boldsymbol{Q}(i)$ and L is a cubic subfield of k_f of an odd conductor f.

Then we have $H = \{e, \sigma, \sigma^2\}$. For $\varrho \in H$, it holds that

$$(\xi - \xi^{\tau\varrho})(\xi^{\tau} - \xi^{\varrho}) = (R - R^{\varrho})^2 + (S + S^{\varrho})^2.$$

If $S + S^{\varrho} = 0$, then $R - R^{\varrho}$ is divisible by a prime factor π_p in L, where p^e is a prime power factor of f. Here we can consider a representative ϱ as an automorphism $\neq e$ of k_{p^e} over $\boldsymbol{Q}$. Then we may assume $S + S^{\varrho} \neq 0$. If $R - R^{\varrho} \neq 0$ for some $\varrho \in H$, then it holds that $(R - R^{\varrho})^2 + (S + S^{\varrho})^2 \geqslant 2|(R - R^{\varrho})(S + S^{\varrho})|$. Then it follows that $|N_K(\xi - \xi^{\tau\varrho})| \geqslant |N_L 2(R - R^{\varrho})(S + S^{\varrho})| \geqslant 8$. Next, let $R - R^{\varrho} = 0$ for any $\varrho \in H$, namely $R \in \boldsymbol{Z}$. Then $\xi - \xi^{\tau\varrho} = i(S + S^{\varrho})$. Hence if a number ξ generates a power basis of Z_K, the number $S + S^{\varrho}$ should be a unit of L, that is

$$N_L(S + S^{\varrho}) = (S + S^{\varrho})(S^{\varrho} + S^{\varrho^2})(S^{\varrho^2} + S) = \pm 1.$$

On the other hand, as the same evaluation as in the second case, $N_L S = S S^{\varrho} S^{\varrho^2} = \pm 1$ holds. Put $s_1 = S + S^{\varrho} + S^{\varrho^2}$, $s_2 = S S^{\varrho} + S^{\varrho} S^{\varrho^2} + S^{\varrho^2} S$. Then it holds that

$$\begin{aligned} N_L(S + S^{\varrho}) &= (s_1 - S^{\varrho^2})(s_1 - S)(s_1 - S^{\varrho}) \\ &= s_1^3 - s_1^2 s_1 + s_1 s_2 \mp 1 = s_2 s_1 \mp 1 = \pm 1. \end{aligned}$$

Then we have two cases of (i) $s_1 s_2 = 0$ or (ii) $s_1 s_2 = \pm 2$.

(i) If $s_1 = 0$, then a number S is a solution of $x^3 + s_2 x \pm 1 = 0$. Thus $-d(S) = 4s_2^3 + 27$. Since the field discriminant $d(L)$ is equal to f^2, we have $(fa)^2 = -4s_2^3 - 27$, namely $(4fa)^2 = (-4s_2)^3 - 432$. By the transformation $x = \frac{12}{u+v}$, $y = \frac{36(u-v)}{u+v}$, the diophantine equation $y^2 = x^3 - 432$ is birationally equivalent to the Fermat curve $u^3 + v^3 = 1$, whose solutions are of $(\pm 36)^2 = 12^3 - 432$ [14]. Then $f = 3^2, s_2 = -3$. Thus the solutions of the equation $x^3 - 3x + 1 = 0$ are $S = \zeta_9 + \zeta_9^{-1}$ and its conjugates. If $s_2 = 0$, the numbers $\pm 1/S$ are solutions of the same equation as in the case of $s_1 = 0$. Therefore, the field L coincides with the maximal real subfield k_9^+ of conductor 3^2. Then we obtain $Z_K = \boldsymbol{Z}[iS]$ for $S = \zeta_9 + \zeta_9^{-1}$.

(ii) If $s_1 s_2 = \pm 2$, noting the signature of $N_L(S + S^{\sigma})$ coincides with the product of ones of s_1 and s_2, a number S is a solution of one of the following eight cases:

$$
\begin{array}{llll}
x^3 - x^2 + 2x - 1 = 0, & d(S) = -23, & x^3 - x^2 - 2x + 1 = 0, & d(S) = 49, \\
x^3 + x^2 + 2x + 1 = 0, & & x^3 + x^2 - 2x - 1 = 0, & \\
x^3 - 2x^2 + x - 1 = 0, & & x^3 - 2x^2 - x + 1 = 0, & \\
x^3 + 2x^2 + x + 1 = 0, & & x^3 + 2x^2 - x - 1 = 0. &
\end{array}
$$

Each of the latter six equations is obtained from one of the former two ones by a linear fractional transformation. Since the discriminant $d(S)$ of a number S in a cyclic cubic field L must be square, we have a solution $S = \zeta_7 + \zeta_7^{-1}$ of $x^3 + x^2 - 2x - 1 = 0$, which generates the maximal real subfield k_7^+ of conductor 7. Then we obtain $Z_K = \boldsymbol{Z}[iS]$. Therefore we have proved the theorem. ∎

Remark 1. In two cases of the maximal imaginary sextic subfields K of conductors 28 and 36 in k_{28} and k_{36}, the proof of Theorem 1(2) involves that there are generators $\pm iS, \pm i/S$ and their conjugates only for Z_K except for the parallel transformations of them by rational integers. For the cases of cyclotomic fields k_p of the prime conductor p, $p \leqslant 23$, $p \neq 17$, Robertson completely determined the generators of Z_{k_p} in [10].

Remark 2. Let p be an odd prime number greater than three, $n = 3p^m$ and k_n be an nth cyclotomic field $\boldsymbol{Q}(\zeta_n)$ over the rationals $\boldsymbol{Q}$, where ζ_n be a primitive nth root of unity. Let K^- be the imaginary subfield of k_n with $[k_n : K^-] = 2$, which is different to $k_{n/3}$. Then it has been shown that the ring Z_{K^-} of integers has no power basis [12].

By Shah [11], it is given a necessary and sufficient condition Z_K having a power basis for a cyclic sextic field K of a prime conductor, and a problem and a conjecture are proposed as follows:

Problem. Is there no cyclic sextic field K of a prime conductor $p \equiv 1 \pmod 6$ whose ring Z_K of integers is monogenic except for the cyclotomic field k_7 of conductor 7 and the maximal real subfield of k_{13} of conductor 13?

Conjecture. Let p be a prime number and put $m = 3p$ $(p \neq 3)$, $4p$ $(p \neq 7)$ or $m \neq 36$. Then there exists a subfield K of k_m with $[K : \boldsymbol{Q}] = 6$ whose ring Z_K of integers does not have a power basis.

The conjecture above has been solved in general by Theorem 1.

3. MONOGENIC PHENOMENA FOR ABELIAN EXTENSIONS

Let K be the composite field of $\boldsymbol{Q}(i)$ and any real subfield L distinct from $\boldsymbol{Q}$ of an odd conductor $f > 1$ of k_f. Assume that the ring Z_K of integers in K has a power basis, that is $|d(\xi)| = |d(K)|$ for some $\xi = R + iS \in Z_K$, where $R, S \in Z_L$. Then we can see that $R \in \boldsymbol{Z}$, and $S,\ S + S^{\varrho}$ are units of L for $\varrho \in H^*$. We have $\xi - \xi^{\varrho} = i(S - S^{\varrho})$. Hence by assumption, it holds that

$$\left| N_K \prod_{\varrho \in H^*} (\xi - \xi^{\varrho}) \right| = |N_L(S - S^{\varrho})|^2 = d(L)^2.$$

Then $Z_L = \boldsymbol{Z}[S]$, namely Z_L has a power basis. Especially, if the extension degree of the field L over $\boldsymbol{Q}$ is a prime $\ell \geqslant 5$, then by Gras [5], f should be a prime of $2l + 1$, namely L is the maximal real subfield k_f^+ of k_f.

Conversely, suppose that a field k_f^+ is the maximal real subfield of k_f of an odd conductor $f > 1$ and let K be the composite field of $\boldsymbol{Q}(i)$ and k_f^+. Then it follows that the maximal real subfield K^+ of K coincides with k_f^+. Put $\xi = iS$ for units $S = \zeta + \zeta^{-1},\ \zeta = \zeta_f$ in k_f^+. Let H be the Galois group of k_f^+ over $\boldsymbol{Q}$. Then we have for an element $\sigma \in H^*,\ \zeta^{\sigma} \neq \zeta^{\pm 1}$. Thus it follows that

$$\begin{aligned} \xi - \xi^{\tau\sigma} &= i(S + S^{\sigma}) \\ &\cong \zeta + \zeta^{-1} + \zeta^{\sigma} + (\zeta^{-1})^{\sigma} \\ &= \zeta(1 + \zeta^{\sigma - 1}) + \zeta^{-\sigma}(1 + \zeta^{\sigma - 1}) \\ &= \zeta^{-\sigma}(1 + \zeta^{\sigma + 1})(1 + \zeta^{\sigma - 1}), \end{aligned}$$

where $\alpha \cong \beta$ for $\alpha, \beta \in K$ means that $(\alpha) = (\beta)$ holds as ideals.

LEMMA 2. *Let g be an odd number > 1 and $(a, g) = 1$. Then for a primitive gth root ζ of unity, $1 + \zeta^a$ is a unit in a cyclotomic field k_g.*

Proof. Let $\Phi_g(X) = \prod_{d|g}(X^d - 1)^{\mu(g/d)}$ be the cyclotomic polynomial of degree $\phi(g)$, where $\phi(\cdot)$ and $\mu(\cdot)$ means the Euler function and the Möbius one, respectively. Let $\prod_p p^e$ be the canonical decomposition of g. Then by

$$\Phi_g(X) = \Phi_{g/p^e}(Y^p) \cdot \Phi_{g/p^e}(Y)^{-1}, \qquad Y = X^{p^{e-1}},$$

we obtain $\Phi_g(-1) = 1$, because of $\Phi_{g/p^e}(-1) \neq 1$. Then a number $1 + \zeta_g^a$ is a unit in k_g for $(a, g) = 1$. ∎

By Lemma 2, each of $1+\zeta^{\sigma+1}$ and $1+\zeta^{\sigma-1}$ is a unit in a cyclotomic field k_g for $g|f$ and $g>2$. Thus $|N_K \prod_{\sigma\in H^*} i(S+S^\sigma)| = 1$. Therefore Z_K is of monogenesis. Then we obtain the theorem.

THEOREM 2. *Let K be the composite field of the Gauß field $\boldsymbol{Q}(i)$ and a real subfield L of an odd conductor $f>1$ of k_f. Assume that the ring Z_K of integers in K has a power basis, then the ring Z_L of integers in L has also a power basis. Conversely, let L be the maximal real subfield of k_f of an odd conductor $f>1$ and K be the composite field of $\boldsymbol{Q}(i)$ and L. Then the ring Z_K of integers in K has a power basis.*

As an application of Theorem 2 to [4] we obtain

COROLLARY 1. *Let ℓ be a prime number congruent to 7 modulo 30 and $\ell>7$. Then there exist infinitely many abelian fields K of conductor 4ℓ whose integer rings Z_K have no power basis.*

Proof. Choose a proper subfield $\neq \boldsymbol{Q}$ of k_ℓ^+ as a field L in the above theorem and K be the composite field of $\boldsymbol{Q}(i)$ and L. Then by Theorem 2 and [4], the ring Z_K has no power basis. ∎

Remark 3. On the former part of Theorem 2, by [4] if the conductor f of L is a prime such that $f=2\ell+1$, where ℓ is also a prime $\geqslant 5$ and $[L:\boldsymbol{Q}]\geqslant 5$, then the field L coincides with the maximal real subfield k_f^+.

REFERENCES

1. D. S. Dummit and H. Kisilevsky, Indices in cyclic cubic fields, *in* "Number Theory and Algebra," pp. 29–42, Collection of Papers Dedicated to H. B. Mann, A. E. Ross and O. Taussky-Todd, Academic Press, New York/San Francisco/London, 1977.
2. I. Gaál, Computing all power integral bases in orders of totally real cyclic sextic number fields, *Math. Comp.* **65** (1996), 801–822.
3. I. Gaál, A. Pethő, and M. Pohst, On the resolution of index form equations in biquadratic number fields, *J. Number Theory* **38** (1991), 18–34.
4. M.-N. Gras, Non monogénéité de l'anneau des entiers des degré premier $l \geqslant 5$, *J. Number Theory* **23** (1986), 347–353.
5. M.-N. Gras, Non monogénéité de l'anneau des entiers de certaines extensions abéliennes de $\mathbb{Q}$, *Publ. Math. Fac. Sci. Resançon, Théor. Nombres* 1983–1984, Exp. No. 5, (1984), 25pp.
6. K. Győry, Discriminant form and index form equations, *in* "Algebraic Number Theory and Diophantine Analysis" (F. Halter-Koch, and R. F. Tichy, Eds.), pp. 191–214, Walter de Gruyter, Berlin/New York, 2000.
7. J. G. Huard, B. K. Spearman, and K. S. Williams, Integral bases for quartic fields with quadratic subfields, *J. Number Theory* **51** (1995), 87–102.
8. S. Lang, "Algebraic Number Theory," Addison–Wesley Publishing Company, Inc., Reading, MA, 1970.

9. H.-W. Leopoldt, Über die Hauptordnung der ganzen Elemente eines abelschen Zahlkörpers, *J. Reine Angew. Math.* **201** (1959), 119–149.
10. L. Robertson, Power bases for cyclotomic integer rings, *J. Number Theory* **69** (1998), 98–118.
11. S. I. A. Shah, Monogenesis of the ring of integers in a cyclotomic sextic field of a prime conductor, *Rep. Fac. Sci. Eng. Saga Univ. Math.* **29** (2000), 1–9.
12. S. I. A. Shah and T. Nakahara, Monogenesis of the ring of integers in certain imaginary abelian field, *Nagoya Math. J.* **168** (2002), to appear.
13. R. Schertz, Konstruktion von Potenzganzheitsbasen in Strahlklassenkörpern über imaginär-quadraticshen Zahlkörpern, *J. Reine Angew. Math.* **398** (1989), 105–129.
14. J. H. Silverman and J. Tate, ‘‘Rational Points in Elliptic Curves,’’ Undergraduate Texts in Mathematics,’’ Springer/Verlag, Berlin, 1992.
15. J.-D. Thérond, Existence d'une extension cyclique monogéne de discriminant donné, *Arch. Math.* **41**(1983), 243–255.