Arch. Math., Vol. 48, 322–325 (1987)

0003-889X/87/4804-0322 $ 2.30/0

On the minimum index of a cyclic quartic field

By

TORU NAKAHARA

1. Introduction. Let K be an algebraic number field of finite degree over the rationals $\mathbb{Q}$. We note $\mathbb{Z}$ and $\mathcal{O}_K$ the ring of rational integers and the ring of integers in K respectively. For ξ in $\mathcal{O}_K$ let Ind ξ be the group index $(\mathcal{O}_K : \mathbb{Z}[\xi])$ if ξ is a primitive element of K and 0 otherwise. Then the minimum index $\tilde{m}(K)$ of any field K is defined by the min $\{\mathrm{Ind}\,\eta;\ \eta \in \mathcal{O}_K$ and $\mathbb{Q}(\eta) = K\}$ and the field index $m(K)$ by the g.c.d. $\{\mathrm{Ind}\,\xi;\ \xi \in \mathcal{O}_K\}$.

D. S. Dummit and H. Kisilevsky showed that there exist infinitely many cubic cyclic fields K whose integer rings $\mathcal{O}_K$ have a power basis, i.e. $\tilde{m}(K) = 1$, here we say that $\mathcal{O}_K$ has a power basis when the integer ring $\mathcal{O}_K$ of a field K is equal to the $\mathbb{Z}$-module $\mathbb{Z}[\alpha]$ for a number α in K [1].

To the contrary we shall prove that $\tilde{m}(K)$ is unbounded as K runs through cyclic quartic fields. We use the Gauss sum attached to the quartic character [8].

Recently the related phenomena in the case of cyclic extension $K/\mathbb{Q}$ of prime degree $\geqq 5$, the case of pure quartic fields, the case of non-cyclic but abelian biquadratic fields and more general cases were found by M.-N. Gras, T. Funakura, the author and K. Györy respectively [3], [2], [11], [4], [5].

2. Theorem, Lemma and Remarks. In Section 3 we shall prove the next result:

Theorem. *For any given integer $N > 0$, there exists a cyclic quartic field K such that*

$$\tilde{m}(K) > N \quad \textit{and} \quad m(K) = 1.$$

Remark 1. This theorem means that there does not exist the außerwesentliche Diskriminantenteiler (unessential discriminant divisor) of the field K, but the minimum index $\tilde{m}(K)$ is unbounded as K ranges over suitable cyclic quartic fields.

Remark 2. Our proof of the number of the fields of the theorem deduces due to M. Hall [6] that there exist infinitely many cyclic quartic fields whose integer rings do not have a power basis without using analytic methods [9], [10].

As is well known, if a prime p divides the field index $m(K)$, then p is smaller than the degree of K over Q. The next lemma is a slightly partial refinement of [13].

Lemma ([12]). *For any abelian quartic field K over Q the field index $m(K)$ coincides with one of the $2^e 3^{e'}$ for $e \leqq 2$, $e' \leqq 1$. Especially if the prime 2 is ramified in K, then $e = 0$.*

Remark 3. From the lemma for all the other cases of $m(K) > 1$, we can find fields parallel to ones in the theorem.

3. Proof of the theorem. Let χ be a quartic character with conductor n determined by the biquadratic residue symbol. Let k be the n-th cyclotomic field $\mathbb{Q}(\zeta)$ with $\zeta = \exp(2\pi\sqrt{-1}/n)$. Let G be the Galois group of $k/\mathbb{Q}$. The group $\langle\chi\rangle$ is a cyclic subgroup of order 4 of the character group of G. Let K denote the subfield of k corresponding to the kernel H of χ. As usual we define the Gauss' $\varphi(n)/4$ terms period $\eta = \sum_{\varrho \in H} \zeta^{\varrho}$, where $\varphi(n)$ means the Euler's function. Then we have $K = \mathbb{Q}(\eta)$, and we fix a representative element σ of a generator σH of the Galois group of K over $\mathbb{Q}$ such that $\chi(\sigma) = \sqrt{-1}$. We denote the image of σ^j of $\eta \in K$ by $\eta^{(j)}$. Let $n = \ell m$ be square-free for $\ell = a^2 + 4b^2$, where any prime factor of ℓ is congruent to 1 modulo 4, and $\lambda = a + 2b\sqrt{-1} \equiv 1 \bmod 2(1 - \sqrt{-1})$. Let $\mathbb{Q}(\sqrt{\ell})$ be the real quadratic subfield of K corresponding to the group $\langle\chi^2\rangle$.

At first we consider the case of odd conductor n. Then $\{1, \eta, \eta', \eta''\}$ makes an integral basis of K. Then using the Gauss sum $\tau(\chi) = \sum_{x \in G} \chi(x)\,\zeta^x$ attached to χ and the Jacobi sum $\tau(\chi)^2/\tau(\chi^2)$, from [10] we obtain $\operatorname{Ind}\xi = \sqrt{|d(\xi)/d(K)|} = \sqrt{|(\prod_{i \neq j}(\xi^{(i)} - \xi^{(j)}))/(m^2\ell^3)|}$ $= \sqrt{|c\,\mathrm{N}(\alpha)|}$ for $\xi = x\eta + y\eta' + z\eta''$ in $\mathcal{O}_K$, where

$$\alpha = (cm + d\sqrt{\ell})/2,$$
$$c = ((x - z)^2 - y^2)\,b - (x - z)\,ya,$$
$$d = ((x - y + z)^2 - \chi(-1)\,((x - z)^2 + y^2)\,m)/2.$$

Here $d(\xi)$, $d(K)$ and $\mathrm{N}(\alpha)$ mean the discriminant of ξ, the field discriminant of K and the norm of α with respect to $\mathbb{Q}(\sqrt{\ell})/\mathbb{Q}$ respectively. Let N be a positive integer, ℓ a square-free number $\ell = (12t + 1)^2 + 4 > N$, let g be a quadratic nonresidue modulo ℓ and

$$q_j \equiv \begin{pmatrix} 1 \bmod 4j \\ g \bmod \ell \end{pmatrix} \quad (j = 1, \ldots, N), \qquad q_j > q_{j-1}\,(j \geqq 2).$$

Now we put $m = \prod_{j=1}^{N} q_j$.

Then we have $\left(\frac{\mathrm{N}(\alpha)}{q_j}\right) = \left(\frac{4\mathrm{N}(\alpha)}{q_j}\right) = \left(\frac{-d^2\ell}{q_j}\right) = \left(\frac{\ell}{q_j}\right) = \left(\frac{q_j}{\ell}\right) = \left(\frac{g}{\ell}\right) = -1$, where $\left(\frac{*}{q}\right)$ denotes the Legendre symbol for a prime q and the Jacobi symbol for the others. On the other hand $\left(\frac{\pm j}{q_j}\right) = 1$ $(j = 1, \ldots, N)$. Hence it holds $N < |\mathrm{N}(\alpha)| \leqq \operatorname{Ind}\xi$ for any primitive element ξ in $\mathcal{O}_K$. Then we obtain $\tilde{m}(K) > N$. Finally it is enough for us to evaluate the index $m(K)$ modulo 6 by the lemma. Calculating the value $\chi(-1) = \chi_\ell(-1)\,\psi_m(-1) = (-1)^{\pm 12t}(-1)^{(m-1)/2} = 1$ from [7], we can confirm $\operatorname{Ind}\eta = |\mathrm{N}((m + ((1 - m)/2)\sqrt{\ell})/2)| \equiv (1 - ((12t)^2 + 24t + 5))/4 \equiv 1 \bmod 2$ and $\operatorname{Ind}\eta \equiv \pm 1 \bmod 3$. Thus we get $m(K) = 1$.

Secondly we consider the case of even conductor n. For the case of $n = 16\ell m$ and $2 \nmid \ell m$ we must notice that the integer ring $\mathcal{O}_K$ does not have a normal basis, namely $\mathcal{O}_K = \mathbb{Z}[1, \eta, \eta', \beta]$, $\beta = \sqrt{2\ell}$ [8]. Then we have $\operatorname{Ind}\xi = |c\,\mathrm{N}(\alpha)|$ for $\xi = x\eta + y\eta' + z\beta$, where

$$\alpha = cm + d\sqrt{2\ell},$$

$$c = -2xy(a - 2b) + (x^2 - y^2)(a + 2b),$$

$$d = 2z^2 - \chi(-1)(x^2 + y^2)\,m.$$

Let g and q_j $(j = 1, \ldots, N)$ select the same numbers as in the previous case. Now we put $m = \prod_{j=1}^{N} q_j$. Then from $\left(\frac{\mathrm{N}(\alpha)}{q_j}\right) \neq \left(\frac{\pm j}{q_j}\right)$ $(j = 1, \ldots, N)$, it follows $\tilde{m}(K) > N$. Moreover let $3 \nmid a$ and $3 \mid b$, then we have $\operatorname{Ind}\eta \equiv |a(a^2m^2 - 2\ell m^2)| \equiv |a| \not\equiv 0 \bmod 3$, and $\operatorname{Ind}\eta \equiv |c(c^2m^2)| \equiv 1 \bmod 2$. Thus it holds that $m(K) = 1$. For the case of $n = \ell m$, $2 \nmid \ell$ and $m = 4m_0$ we can see that $\mathcal{O}_K = \mathbb{Z}[1, \eta, \eta', \beta]$, $\beta = (1 + \sqrt{\ell})/2$ [8]. Then we get $\operatorname{Ind}\xi = |c\,\mathrm{N}(\alpha)|$ for $\xi = x\eta + y\eta' + z\beta$, where

$$\alpha = 2cm_0 + d\sqrt{\ell},$$

$$c = -xya + (x^2 - y^2)\,2b,$$

$$d = (x^2 + y^2)\,m_0 - \chi(-1)\,z^2.$$

By the same choice of primes q_j $(1 \leqq j \leqq N)$ as the above case, we put $m_0 = 7\prod_{j=1}^{N} q_j$. Hence it holds $m(K) > N$. Moreover let $3 \nmid ab$. Then for $\xi_0 = \eta + \eta'$ and $\xi_1 = \eta + \eta' + \beta$ we get $\operatorname{Ind}\xi_0 \not\equiv 0 \bmod 3$ and $\operatorname{Ind}\xi_1 \not\equiv 0 \bmod 2$. Thus it follows $m(K) = 1$. Therefore we have furnished a proof of the theorem.

References

[1] D. S. DUMMIT and H. KISILEVSKY, Indices in cyclic cubic fields. In: Number Theory and Algebra, H. Zassenhaus ed., New York 29–42 (1977).

[2] T. FUNAKURA, On integral bases of pure quartic fields. Math. J. Okayama Univ. **26**, 27–41 (1984).

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

[4] K. GYÖRY, On discriminants and indices of integers of an algebraic number field. J. Reine Angew. Math. **324**, 114–126 (1981).

[5] K. GYÖRY, Sur les générateurs des ordres monogènes des corps de nombres algébriques. Séminaire de Théorie des Nombres de Bordeaux Année 1983–1984, exposé N° **32**, 1–12 (1984).

[6] M. HALL, Indices in cubic fields. Bull. Amer. Math. Soc. **43**, 104–108 (1937).

[7] H. HASSE, Zahlbericht. Würzburg-Wien 1970.

[8] H. HASSE, Arithmetische Bestimmung von Grundeinheit und Klassenzahl in zyklischen und biquadratischen Zahlkörpern. Abh. Deutsch. Akad. Wiss. Berlin, Math.-Nat. Kl. 2, 3–95 (1950) (= Math. Abhandlungen, hrsg. von H. W. Leopoldt und P. Roquette, Bd. 3, 289–379 Berlin-New York 1975).

[9] T. NAKAHARA, On real quadratic fields whose ideal class groups have a cyclic p-subgroup. Rep. Fac. Sci. Engrg. Saga Univ. Math. **6**, 15–26 (1978).

[10] T. NAKAHARA, On cyclic biquadratic fields related to a problem of Hasse. Monatsh. Math. **94**, 125–132 (1982).
[11] T. NAKAHARA, On the indices and integral bases of non-cyclic but abelian biquadratic fields. Arch. Math. **41**, 504–508 (1983).
[12] T. NAKAHARA, On the indices and integral bases of abelian biquadratic fields. Distribution of values of arithmetic functions (Proc. Sympos. Res. Inst. Math. Sci. Kyoto Univ.) RIMS Kōkyūroku. **517**, 91–100 (1984).
[13] E. von Żyliński, Zur Theorie der außerwesentlichen Diskriminantenteiler algebraischer Körper. Math. Ann. **73**, 273–274 (1913).

Eingegangen am 19. 3. 1986

Anschrift des Autors:

Toru Nakahara
Department of Mathematics
Faculty of Science and Engineering
Saga University
Saga 840
Japan