JOURNAL OF NUMBER THEORY **18**, 350–355 (1984)

Cyclic Quartic Fields and Genus Theory of Their Subfields

ZHANG XIANKE

Department of Mathematics, University of Science and Technology of China, Hefei, Anhui, The People's Republic of China

Communicated by D. Zagier

Received June 3, 1982

Let $k = \mathbb{Q}(\sqrt{u})$ ($u \neq 1$ squarefree), K any possible cyclic quartic field containing k. A close relation is established between K and the genus group of k. In particular: (1) Each K can be written uniquely as $K = \mathbb{Q}(\sqrt{vw\eta})$, where η is fixed in k and satisfies $\eta \gg 1$, $(\eta) = \mathfrak{A}^2\sqrt{u}$, $|\mathfrak{A}^2| = |(\sqrt{u})|$, $(v, u) = 1$, $v \in \mathbb{Z}$ is squarefree, $w \mid u$, $0 < w < \sqrt{u}$. Thus if $u \neq a^2 + b^2$, there is no $K \supset k$. If $u = a^2 + b^2$ then for each fixed v there are $2^{g-1} K \supset k$, where g is the number of prime divisors of u. (2) K/k has a relative integral basis (RIB) (i.e., O_K is free over O_k) iff $N(\varepsilon_0) = -1$ and $w = 1$, where ε_0 is the fundamental unit of k, (or, equivalently, iff $K = \mathbb{Q}(\sqrt{v\varepsilon_0\sqrt{u}})$, $(v, u) = 1$). (3) A RIB is constructed explicitly whenever it exists. (4) disc(K) is given. In particular, the following results are special cases of (2): (i) Narkiewicz showed in 1974 that K/k has a RIB if u is a prime; (ii) Edgar and Peterson (*J. Number Theory* **12** (1980), 77–83) showed that for u composite there is at least one $K \supset k$ having no RIB. Besides, it follows from (4) that the classification and integral basis of K given by Albert (*Ann. of Math.* **31** (1930), 381–418) are wrong.

Let $k = \mathbb{Q}(\sqrt{u})$ be arbitrary quadratic field where $u \in \mathbb{Z}$ is squarefree. And let C_k (C_k^0, resp.) be the strict (wide, resp.) ideal class group of k. It is well known that $C_k^0 = C_k/\{1, \Theta\}$, where $\Theta = [(\sqrt{u})]$ is the strict class represented by $(\sqrt{u})$. (For this and genus theory see [4].)

Consider the three sets:

$$\mathscr{K} = \{K \supset k : K \text{ is a cyclic quartic field}\},$$

$$\Sigma = (\theta \in k^*/k^{*2} : N(\theta) \in u \cdot \mathbb{Q}^{*2}\}, \qquad \text{where} \quad N(\theta) = N_{k/\mathbb{Q}}(\theta),$$

$$\mathscr{V} \times \mathscr{B} \qquad \text{where } \mathscr{V} = \{v \in \mathbb{Z} : (v, u) = 1, v \text{ is squarefree}\},$$

$$\mathscr{B} = \{B \in C_k^0 : B^2 = \Theta \text{ in } C_k\}.$$

If $u < 0$, then obviously all three sets are empty. So we assume $u > 0$ and let ε_0 be the fundamental unit of k throughout this paper.

0022-314X/84 $3.00

We will show that for each $\theta \in \Sigma$, (θ) can be written as

$$(\theta) = v\mathfrak{b}^2\sqrt{u}, \tag{1}$$

where $v \in \mathscr{V}'$, $\operatorname{sign}(v) = \operatorname{sign}(\theta)$, $\mathfrak{b}$ is a fractional ideal of k, and $[\mathfrak{b}] = B \in \mathscr{B}$; and that the following maps are well defined:

$$\begin{aligned} &\varphi\colon \mathscr{K} \to \Sigma && \text{where} \quad \varphi^{-1}(\theta) = k(\sqrt{\theta}), \\ &\psi\colon \Sigma \to \mathscr{V}' \times \mathscr{B} && \text{where} \quad \psi(\theta) = (v, [\mathfrak{b}]). \end{aligned} \tag{2}$$

The main results of this paper are the following 4 theorems.

THEOREM 1. *φ is a 1 : 1 map. ψ is a $2^{(N(\varepsilon_0)+1)/2}$: 1 map.*

THEOREM 2. *Every $K \in \mathscr{K}$ can be written uniquely as*

$$K = \mathbb{Q}(\sqrt{vw\eta}), \tag{3}$$

where $\eta \gg 0$ is fixed in $k = \mathbb{Q}(\sqrt{u})$, $(\eta) \in \{\mathfrak{A}^2\sqrt{u} : [\mathfrak{A}]^2 = \Theta\}$, $(v, u) = 1$, $v \in \mathbb{Z}$ is squarefree, $w \in \{u' > 0 : u' \mid u,\ u' \in \mathbb{Z}\}$ modulo the relation $u' \sim u/u'$.

Remark 1. We assume $\eta = \varepsilon_0\sqrt{u}$ whenever $N(\varepsilon_0) = -1$. In general if $u = a^2 + b^2$, a is odd, we may take $\eta = (b + \sqrt{u})\sqrt{u}$.

By genus theory, Θ is a perfect square iff $u = a^2 + b^2$, $a, b \in \mathbb{Z}$. Thus we have

COROLLARY. (i) *If $u \neq a^2 + b^2$, a, $b \in \mathbb{Z}$ (i.e., $u < 0$ or $\exists$ prime $p \equiv 3 (\mathrm{mod}\ 4)$, $p \mid u$) then there is no cyclic quartic field containing k.*

(ii) *If $u = a^2 + b^2$, $a, b \in \mathbb{Z}$, (i.e., $u = p_1 \cdots p_g > 0$, prime $p_i \not\equiv 3 (\mathrm{mod}\ 4)$, $1 \leqslant i \leqslant g$) then for each fixed v there are 2^{g-1} cyclic quartic fields containing k.*

THEOREM 3. *$K \in \mathscr{K}$ has a* relative integral basis (RIB) (*i.e., O_K is free over O_k*) *iff one of the* 3 *equivalent conditions hold*:

(RIB 1) *$N(\varepsilon_0) = -1$ and $w = 1$, where K is as in* (3).

(RIB 2) *$K = \mathbb{Q}(\sqrt{v\varepsilon_0\sqrt{u}})$ for some $v \in \mathbb{Z}$, $(v, u) = 1$.*

(RIB 3) *$B = 1$, where $(v, B) = \psi\varphi(K)$ as in* (2).

COROLLARY. (i) *If $N(\varepsilon_0) = +1$, then no cyclic quartic field K containing k has a* RIB.

(ii) *If $N(\varepsilon_0) = -1$, then for each fixed v exactly one of the 2^{g-1} fields K in* (3) *has a* RIB. *This field is $\mathbb{Q}(\sqrt{v\varepsilon_0\sqrt{u}})$.*

THEOREM 4. *Whenever* $K \in \mathscr{K}$ *has any* RIB, $\{1, \alpha\}$ *is a* RIB, *where*

$$\begin{aligned} \alpha &= \tfrac{1}{2}\left(1 + \sqrt{v\varepsilon_0^3\sqrt{u}}\right) && \text{if } v \equiv \tfrac{1}{2}(u+1) \in \mathbb{Z} \pmod 4, \\ &= \sqrt{v\varepsilon_0\sqrt{u}} && \text{otherwise,} \end{aligned}$$

and $K = \mathbb{Q}(\sqrt{v\varepsilon_0\sqrt{u}})$.

We will use

LEMMA 1. (i) *Let* $\theta \in k^*$, *then* $k(\sqrt{\theta}) \in \mathscr{K}$ *iff* $N(\theta) \in u \cdot Q^{*2}$.

(ii) *Let* $\theta_1, \theta_2 \in k^*$, *then* $k(\sqrt{\theta_1}) = k(\sqrt{\theta_2})$ *iff* $\theta_1 \cdot \theta_2 \in k^{*2}$.

Proof. (i) See [4, pp. 234, 244; or 2]. (ii) is obvious.

Proof of Theorem 1. By Lemma 1, φ is a well-defined 1 : 1 map. As for ψ, for any $\theta \in \Sigma$, we may put

$$(\theta) = \prod_{i=1}^{g} \mathfrak{p}_i^{a_i} \cdot \prod_{i=1}^{r} \mathfrak{q}_i^{b_i} \mathfrak{q}_i'^{b_i'} \cdot \prod_{i=1}^{s} l_i^{c_i} \tag{4}$$

in k, where $\mathfrak{p}_i^2 = p_i \mid u$, $\mathfrak{q}_i\mathfrak{q}_i' = q_i$ splits in k, l_i is inertial in k, and $a_i, b_i, b_i', c_i \in \mathbb{Z}$. Then from $N(\theta) \in u \cdot \mathbb{Q}^{*2}$, we have $a_i \equiv 1$, $b_i \equiv b_i' \bmod 2$. Thus we have (1), i.e., $(\theta) = v\mathfrak{b}^2\sqrt{u}$. Now changing θ by λ^2 ($\lambda \in k^*$) corresponds to replacing $\mathfrak{b}$ by $(\lambda)\mathfrak{b}$, so $\theta \in \Sigma$ corresponds actually to $B = [\mathfrak{b}] \in C_k^0$. And $B^2 = \Theta$ since $1 = [(\theta)] = [v\mathfrak{b}^2\sqrt{u}] = B^2\Theta$ in C_k. Thus ψ is well defined. To show ψ is surjective, for $(v, B) \in \mathscr{V} \times \mathscr{B}$, we take arbitrary $\mathfrak{b} \in B$. Then $v\mathfrak{b}^2\sqrt{u}$ is a strict principal ideal since $B^2 = \Theta$. Let it be (θ), then $\theta \in \Sigma$ and $\psi(\theta) = (v, B)$. Finally, if $\psi(\theta_1) = \psi(\theta_2)$, then $\theta_2 = \theta_1$ or $\varepsilon_0\theta_1$ since $\operatorname{sign}(\theta_i) = \operatorname{sign}(v)$. If $N(\varepsilon_0) = -1$, $\varepsilon_0\theta_1 \notin \Sigma$. If $N(\varepsilon_0) = +1$, $\varepsilon_0\theta_1 \in \Sigma$. Hence ψ is $2^{(N(\varepsilon_0)+1)/2} : 1$.

Proof of Theorem 2. Theorem 2 follows from Theorem 1 and the fact of genus theory that each of the 2^{g-1} ambiguous ideal classes $C \in C_k$ (i.e., $C^2 = 1$) contains two ambiguous ideals and that the 2^g ambiguous ideals are just

$$\prod_{i=1}^{g} \mathfrak{p}_i^{e_i} \qquad (e_i = 0, 1), \tag{5}$$

where $\mathfrak{p}_i \mid p$, $u = p_1 \cdots p_g$.

Suppose first $N(\varepsilon_0) = -1$, then $C_k^0 = C_k$, $\Theta = 1$. Each $B \in \mathscr{B}$ is an ambiguous class and contains ambiguous ideals $\mathfrak{b}$ and $\sqrt{u}\,\mathfrak{b}$ (within a rational factor). Let $\mathfrak{b}^2 = (w) \mid u$, then $\theta = \psi^{-1}(v, B) = vw\varepsilon_0\sqrt{u} \in \Sigma$.

Now suppose $N(\varepsilon_0) = +1$, then $C_k = C_k^0 \cup \Theta C_k^0$. If $\mathscr{B} \neq \varnothing$, then there is an $A \in C_k$ such that $A^2 = \Theta$ and $\mathscr{B} = \{AG \bmod \Theta : G^2 = 1 \text{ in } C_k\}$ ($\mathscr{B} \neq \varnothing$ iff $u = a^2 + b^2$, $a, b \in \mathbb{Z}$. If a is odd, then $(a, b + \sqrt{u})^2 = (b + \sqrt{u}) \in \Theta$.) Each

G contains ambiguous ideals $\mathfrak{g}$ and $\lambda\mathfrak{g}$ (within a rational factor), where $\varepsilon_0 = \lambda/\lambda'$, $N(\lambda) = u_0 \mid u$. Note that $\lambda^2 = \varepsilon_0 u_0$. Fix $\mathfrak{A} \in A$, then each $B \in \mathscr{B}$ contains 4 ideals $\mathfrak{A}\mathfrak{g}$, $\mathfrak{A}\mathfrak{g}\lambda$, $\mathfrak{A}\mathfrak{g}\sqrt{u}$, $\mathfrak{A}\mathfrak{g}\lambda\sqrt{u}$. Let $\mathfrak{A}^2 = (\alpha)$, $\mathfrak{g}^2 = (w)$ (we may take $\alpha = b + \sqrt{u}$ as stated above). Then $\psi^{-1}(v, B) = vw\alpha\sqrt{u}$ and $\varepsilon_0 \cdot vw\alpha\sqrt{u} = vwu_0\alpha\sqrt{u} \in \Sigma$, since ψ is of 2 : 1.

To prove Theorem 3, we need Lemma 2. The proof is in the Appendix.

LEMMA 2. *All cyclic quartic fields K can be classified as follows, where $K = \mathbb{Q}(\sqrt{vw\eta})$ as in* (3), $d = 2^\delta v\sqrt{u} = \operatorname{disc}(K/k)$.

class	$u(\text{mod } 2)$	$v(\text{mod } 2)$	relations	δ
1	1	1	$v \equiv \frac{1}{2}(u+1)\ (4)$	0
2	1	1	$-v \equiv \frac{1}{2}(u+1)\ (4)$	2
3	1	0		2
4	0	1		2

Remark 2. Albert [3] classified K and gave an integral basis of K, which was used in [2] to compute (unexplicitly) the discriminant of K to prove the main theorem of [2]. But we have proved that the classification in [3] is wrong and the determinations of integral basis (and, hence, disc(K)) are wrong in 9 of the 16 cases. We have corrected the mistakes of [3] and obtained the (correct) disc(K) and other results in another paper. Keqin has given disc(K) in [6]. To avoid the trouble of transforming different expressions of K, we prefer to give disc(K) in the Appendix by a quick local method.

The following theorem is equivalent to a theorem of Hecke (1912) and Speiser (1909) in [4, p. 222].

THEOREM (Mann [5]). *Let E/F be a quadratic extension of the number field. Then E/F has a relative integral basis iff $E = F(\sqrt{D})$, where $(D) =$ disc(E/F).*

Proof of Theorem 3. By the theorem of Mann, K/k has a relative integral basis iff $K = \mathbb{Q}(\sqrt{vw\eta}) = \mathbb{Q}(\sqrt{d\varepsilon}) = \mathbb{Q}(\sqrt{v\sqrt{u}\,\varepsilon})$ for some unit $\varepsilon = \pm\varepsilon_0^j$ of k (cf. Lemma 2). Thus $\operatorname{sign}(vw\eta) = \operatorname{sign}(v\sqrt{u}\,\varepsilon)$, $N(v\sqrt{u}\,\varepsilon) \in u \cdot \mathbb{Q}^{*2}$. That is $\varepsilon = \varepsilon_0^j$, $N(\varepsilon) = -1$. Therefore, $N(\varepsilon_0) = -1$ and $K = \mathbb{Q}(\sqrt{v\varepsilon_0\sqrt{u}})$.

Proof of Theorem 4. Obviously $\operatorname{disc}\{1, \alpha\} = \operatorname{disc}(K/k)$, so it is sufficient to show $\alpha \in O_K$ when $v \equiv \frac{1}{2}(u+1) \in \mathbb{Z}$ mod 4. Let $\varepsilon_0^3 = s + t\sqrt{u}$, $s, t \in \mathbb{Z}$. By $s^2 - t^2u = -1$, we have $t \equiv s + 1 \equiv 1$ (2) and $s^2 \equiv t^2u - 1 \equiv u - 1$ (8), so $s \equiv \frac{1}{2}(u-1)$ (4), $s + 1 \equiv \frac{1}{2}(u+1) \equiv v$ (4). Thus $\frac{1}{2}(1 - vtu) \equiv \frac{1}{2}(1 - v) \equiv \frac{1}{2}(vs)$

(2). This means $N_{K/k}(\alpha)=\frac{1}{4}(1-v\sqrt{u}\,\varepsilon_0^3)=\frac{1}{4}(1-vtu-vs\sqrt{u})\in O_k$ and $\alpha\in O_K$.

Finally, it is easy to see that the following results about the relative integral basis (RIB) of $K\in\mathscr{K}$ are special cases of our Theorem 3.

(i) Narkiewicz [1] proved that K/k has a RIB if u is a prime.

(ii) Eedgar and Peterson [2] proved that for u composite there is at least one $K\supset k$ having no RIB.

In fact, if u is a prime, it is well known that $N(\varepsilon_0)=-1$. And for each fixed v, there is only $1=2^{g-1}$ field K, which certainly has a RIB. This proves (i). On the other hand, if u is not a prime, then for each fixed v there are $2^{g-1}\geqslant 2$ fields K and at most one of them has a RIB. This proves (ii).

APPENDIX: DISCRIMINANT (PROOF OF LEMMA 2)

We fix a prime $p\in\mathbb{Z}$, and let p_2, p_4 be its prime ideal factors in k and K. Let $p^c \,\|\, \theta=wv\eta$, where $\eta=\alpha\sqrt{u}=(b+\sqrt{u})\sqrt{u}$, $u=a^2+b^2$, as in Remark 1.

First, we determine whether p_2 divides $(d)=\operatorname{disc}(K/k)$. From a theorem of Hilbert [4, p. 215] we have

(i) If p is odd, then $p_2\mid d$ iff $c\equiv 1 \pmod 2$.

(ii) If $(2,\theta)=1$, then $2_2\mid d$ iff $\theta\equiv x^2 \pmod 4$ has no solution $x\in O_k$.

Thus if p is odd, then $p_2\mid d$ iff $p\mid uv$ since $(\alpha)=\mathfrak{A}^2$. If $2\mid uv$ then certainly $2_2\mid d$. If $u\equiv v\equiv 1$ (2), we assert that $2_2\mid d$ iff $-v\equiv\frac{1}{2}(u+1) \bmod 4$. In fact, from $b\equiv 0$ (2), we have $(2,\theta)=1$, $b^2\equiv u-a^2\equiv u-1$ (8), $b\equiv\frac{1}{2}(u-1)$ (4), and $b\sqrt{u}\equiv b$ (4). Thus, $\eta\equiv b+1\equiv\frac{1}{2}(u+1)$ (4). The assertion follows from that $\theta=wv\eta\equiv -1$ (4) iff $\eta\equiv -v$ (4).

Now, let us determine d (cf. [4, p. 213]). Suppose $p_2\mid d$, $p_2=p_4^2$. Let the local ring $O_K^{p_4}=O_K(O_K-P_4)^{-1}$, and π be its Eisenstein generator (i.e., $\pi=A/B$, $p_4\,\|\, A$). Then the local different $\mathscr{D}_{K/k}^{p_4}=(\pi-\sigma\pi)$, where $(\sigma)=\operatorname{Gal}(K/k)$. If $\pi^s\,\|\,\mathscr{D}_{K/k}^{p_4}$, then the p_2-component of d is $d^{(p_2)}=N_{K/k}p_4^s=p_2^s$.

Obviously, we can find a $\theta^*\equiv\theta \bmod k^{*2}$ such that either $p_2\,\|\,\theta^*$ or $(p_2,\theta^*)=1$. If $p\mid uv$ then from $\alpha=\mathfrak{A}^2$ we evidently have $c\equiv 1$ (2), so $p_2\,\|\,\theta^*$. Thus, we may take $\pi=\sqrt{\theta^*}$. If $p\nmid uv$ (i.e., $p=2$, $u\equiv v\equiv 1$ (2)), then $\Theta\equiv -1$ (4) as stated above. And we may take $\theta^*=\theta$ and $\pi=1+\sqrt{\theta}$ since $2\,\|\,\theta-1$, $2_4\,\|\, 1+\sqrt{\theta}$. In both cases we have $\mathscr{D}_{K/k}^{p_4}=(2\sqrt{\theta^*})$. Thus if p is odd, then $d^{(p_2)}=p_2$. If $p=2$, we have

$$\begin{aligned} d^{(p_2)} &= 2_2^5 && \text{if } u\equiv 0\ (2),\\ &= 2_2^3 && \text{if } u\equiv v+1\equiv 1\ (2),\\ &= 2_2^2 && \text{if } u\equiv v\equiv 1\ (2), -v\equiv\tfrac{1}{2}(u+1)\ (4).\end{aligned}$$

Then Lemma 2 follows from the fact that

$$d = \prod_{\substack{p \\ p_2 | d}} \prod_{p_2 | p} d^{(p_2)}.$$

ACKNOWLEDGMENTS

Thanks are due to my teacher Feng Keqin who suggested and guided this paper. His paper [6] was very helpful to me. The author is also very grateful to Professor D. Zagier whose valuable suggestions greatly simplified the results and proofs and determined the final form of this paper.

REFERENCES

1. W. NARKIEWICZ, "Elementary and Analytic Theory of Algebraic Numbers," PWN, Warsaw, 1974.
2. H. EDGAR AND B. PETERSON, Some contributions to the theory of cyclic quartic extensions of the rationals, *J. Number Theory* **12** (1980), 77–83.
3. A. A. ALBERT, The integers of normal quartic fields, *Ann. of Math.* **31** (1930), 381–418.
4. H. COHN, "A Classical Invitation to Algebraic Numbers and Class Fields," Springer-Verlag, New York/Berlin, 1978.
5. H. MANN, On integral bases, *Proc. Amer. Math. Soc.* **9** (1958), 167–172.
6. F. KEQIN, Explicit description of cyclic quartic fields, to appear.