Math. J. Okayama Univ. **61** (2019), 167–172

THE FACTORIZATION OF 2 AND 3 IN CYCLIC QUARTIC FIELDS

This paper is dedicated to the memory of Dr. Blair K. Spearman who passed away on October 1, 2017.

Stephen C. Brown and Chad T. Davis

Abstract. Due to a theorem of Dedekind, factoring ideals generated by prime numbers in number fields is easily done given that said prime number does not divide the index of the field. In this paper, we determine the prime ideal factorizations of both 2 and 3 in cyclic quartic fields whose index is divisible by one of or both of these primes.

1. Introduction

Let K be a number field with ring of integers $\mathcal{O}_K$ and discriminant $d(K)$. For any primitive integer $\theta \in \mathcal{O}_K$, the *index of* θ is defined as

$$i(\theta) = \sqrt{\frac{D(\theta)}{d(K)}}$$

where $D(\theta)$ denotes the discriminant of θ. It is well known that this quantity is always a rational integer (see [4], page 45, exercise 27c). The *index* $i(K)$ *of* K is then defined to be

$$\gcd_{\theta \in \mathcal{O}_K} (i(\theta))$$

where the greatest common divisor is taken over all primitive integers $\theta \in \mathcal{O}_K$. Let $p \in \mathbb{Z}$ be a rational prime and consider the ideal $p\mathcal{O}_K \subseteq \mathcal{O}_K$. A theorem of Dedekind allows us to determine the prime ideal decomposition of $p\mathcal{O}_K$, provided that p does not divide $i(K)$ (see [4], page 79, Theorem 27). If p divides $i(K)$, no such general result is known. However, many specific results on factorizations of $p\mathcal{O}_K$ are known, for instance if $p = 2$ and K is a pure quartic field (see [7]).

Suppose that K is a cyclic quartic field. It is well known that $i(K) \in \{1, 2, 3, 4, 6, 12\}$ (see [1], page 234). In [2], it is shown that K can be expressed uniquely as

$$K = \mathbb{Q}\left(\sqrt{A(D + B\sqrt{D})}\right)$$

where A, B, C, D are rational integers satisfying

(a1) A is squarefree and odd,

Mathematics Subject Classification. Primary 11R16; Secondary 11R27.

Key words and phrases. Cyclic quartic field, Prime ideal factorization.

(a2) $D = B^2 + C^2$ is squarefree and $B, C > 0$,
(a3) $\gcd(A, D) = 1$.

In this paper, we determine explicitly the prime ideal factorizations of both $2\mathcal{O}_K$ and $3\mathcal{O}_K$ when $i(K)$ is divisible by either 2 or 3 (or both). In [6], Spearman and Williams give exact congruence conditions on A, B, C, D that specify the factorization of $i(K)$ (see Theorem 1.3.2 on page 24 and Theorems 1.3.9 and 1.3.10 on page 29 of [6]). In particular, it follows easily that when $4 \mid i(K)$ (resp. $3 \mid i(K)$), then exactly one of $\pm A$ is congruent to C mod 4 (resp. exactly one of B or C is congruent to 0 mod 3). Our main theorem is as follows.

Theorem 1. *Let K be a cyclic quartic field, so that there exist integers A, B, C, D satisfying conditions* (a1)-(a3) *above with $K = \mathbb{Q}\left(\sqrt{A(D+B\sqrt{D})}\right)$. Set*

$$\alpha = \sqrt{A(D+B\sqrt{D})} \qquad \beta = \sqrt{A(D-B\sqrt{D})}. \tag{1.1}$$

Let $\sigma_i : K \hookrightarrow \mathbb{C}, i = 1,2,3,4$ be the embeddings of K in $\mathbb{C}$, and for any ideal $I \subseteq \mathcal{O}_K$, set $\sigma_i(I) = I^{(i)}$. Then

(b1) *If $2 \mid\mid i(K)$, then $2\mathcal{O}_K = P_1 P_2$ where*

$$P_1 = \left\langle 2, \frac{1+\sqrt{D}}{2} \right\rangle, P_2 = \left\langle 2, \frac{1-\sqrt{D}}{2} \right\rangle$$

(b2) *If $4 \mid i(K)$, then $2\mathcal{O}_K = \prod_{i=1}^{4} P^{(i)}$ where $P = \langle 2, \theta \rangle$, and*

$$\theta = \begin{cases} \dfrac{A+C+2}{4} + \dfrac{1}{4}(1+\sqrt{D}+\alpha+\beta) & \text{if } A \equiv C \pmod 4 \\[2ex] \dfrac{A-C+2}{4} + \dfrac{1}{4}(1+\sqrt{D}+\alpha-\beta) & \text{if } A \equiv -C \pmod 4 \end{cases}$$

(b3) *If $3 \mid i(K)$, then $3\mathcal{O}_K = \prod_{i=1}^{4} Q^{(i)}$ where $Q = \langle 3, \theta \rangle$ and*

$$\theta = \begin{cases} \sqrt{D}+\alpha-\beta & \text{if } A \equiv 1 \pmod 3, \quad B \equiv 0 \pmod 3 \\ \sqrt{D}+\alpha & \text{if } A \equiv 2 \pmod 3, \quad C \equiv 0 \pmod 3 \end{cases}$$

2. A Few Lemmas

The proof of Theorem 1 will follow from the following series of lemmas.

Lemma 1. *Let K be a cyclic quartic field so that $K = \mathbb{Q}\left(\sqrt{A(D+B\sqrt{D})}\right)$ with A, B, C, D satisfying conditions* (a1)-(a3) *of* §1. *Suppose that* $2 \,||\, i(K)$. *Then*

$$2\mathcal{O}_K = \left\langle 2, \frac{1+\sqrt{D}}{2} \right\rangle \left\langle 2, \frac{1-\sqrt{D}}{2} \right\rangle.$$

Proof. The table on page 234 of [1] implies that the prime ideal factorization of $2\mathcal{O}_K$ is

$$2\mathcal{O}_K = P_1^2 P_2 P_3 \text{ or } 2\mathcal{O}_K = P_1 P_2.$$

As K is normal over $\mathbb{Q}$, the Corollary on page 71 of [4] implies that only the latter case is permissible. By assumption, $2 \,||\, i(K)$, and so Theorem 1.4.2 of [6] implies that $B \equiv 0 \pmod 4$. Furthermore, $D = B^2 + C^2$ and D is square free, hence we see immediately that C must be odd whence $D \equiv 1 \pmod 8$. The quadratic subfield of K is $M = \mathbb{Q}(\sqrt{D})$, thus Theorem 25 of [4] implies that $2\mathcal{O}_M$ factors in this quadratic subfield as

$$2\mathcal{O}_M = \left\langle 2, \frac{1+\sqrt{D}}{2} \right\rangle \left\langle 2, \frac{1-\sqrt{D}}{2} \right\rangle.$$

Since $2\mathcal{O}_K = P_1 P_2$, this factorization lifts to the same one in $\mathcal{O}_K$ which proves the lemma. □

Lemma 2. *Let K be a cyclic quartic field so that $K = \mathbb{Q}\left(\sqrt{A(D+B\sqrt{D})}\right)$ with A, B, C, D satisfying conditions* (a1)-(a3) *of* §1. *Suppose that* $4 \mid i(K)$. *Let θ be defined as in part* (b2) *of Theorem 1. Then $\langle 2, \theta \rangle \subseteq \mathcal{O}_K$ is prime.*

Proof. As $4 \mid i(K)$, Theorem 1.3.10 of [6] implies that either $A \equiv 1 \pmod 8$ and $B \equiv 0 \pmod 8$ or $A \equiv 5 \pmod 8$ and $B \equiv 4 \pmod 8$. As in Lemma 1, C must be odd, hence the Theorem on page 146 of [3] implies that θ is an algebraic integer. There are then 4 possible cases for congruence conditions on A, B, and C.

Case 1: Suppose that $A \equiv 1 \pmod 8, B \equiv 0 \pmod 8$, and $A \equiv C \pmod 4$. We have

$$\theta = \frac{A+C+2}{4} + \frac{1}{4}(1+\sqrt{D}+\alpha+\beta)$$

where α and β are given in Equation (1.1). We show that $\langle 2, \theta \rangle$ is prime. Writing $C = A + 4k, A = 1 + 8\ell, B = 8m$ for $k, \ell, m \in \mathbb{Z}$, we have

$$N_{\mathbb{Q}}^{K}(\theta) \equiv 2 + 4k + 4\ell + 8k\ell + 12\ell^2 + 4m^2 \pmod{16}$$

so that $N_{\mathbb{Q}}^{K}(\theta) \equiv 2 \pmod 4$. Thus $N(\theta\mathcal{O}_K) \equiv 2 \pmod 4$ where N denotes the ideal norm in $\mathcal{O}_K$.

Write $\theta\mathcal{O}_K = P_1 \dots P_r$ where the $P_i \subseteq \mathcal{O}_K, i = 1, \dots, r$ are prime ideals. Since $2 \mid\mid N(\theta\mathcal{O}_K)$, the multiplicativity of the norm implies that exactly one of the P_i's has norm equal to 2. Thus $\theta\mathcal{O}_K$ is divisible by a prime ideal lying over 2, and thus we deduce that this prime ideal also divides $\langle 2, \theta \rangle$ since it clearly divides $2\mathcal{O}_K$.

Now it follows from Corollary 2 on page 142 of [5] that $N(\langle 2, \theta \rangle)$ is equal to the greatest common divisor of the norms of all its elements. Thus since $N(2\mathcal{O}_K) = 16$ and $N(\theta\mathcal{O}_K) \equiv 2 \pmod 4$, we deduce that either $N(\langle 2, \theta \rangle) = 1$ or 2. The former case is impossible as $\langle 2, \theta \rangle$ is divisible by a proper prime ideal in $\mathcal{O}_K$, thus $N(\langle 2, \theta \rangle) = 2$ and hence $\langle 2, \theta \rangle$ is prime.

Case 2: Suppose that $A \equiv 1 \pmod 8, B \equiv 0 \pmod 8$ and $A \equiv -C \pmod 4$. We have

$$\theta = \frac{A - C + 2}{4} + \frac{1}{4}(1 + \sqrt{D} + \alpha - \beta).$$

As in Case 1, write $C = -A + 4k, A = 1 + 8\ell, B = 8m$ for $k, \ell, m \in \mathbb{Z}$ to get

$$N_{\mathbb{Q}}^{K}(\theta) \equiv 2 + 12k + 4\ell + 8kl + 12\ell^2 + 4m^2 \pmod{16}$$

so that $N_{\mathbb{Q}}^{K}(\theta) \equiv 2 \pmod 4$. The same argument as in Case 1 implies that $P = \langle 2, \theta \rangle$ is a proper prime ideal.

Case 3: Suppose that $A \equiv 5 \pmod 8, B \equiv 4 \pmod 8$, and $A \equiv C \pmod 4$. As in Case 1, write $C = A + 4k, A = 5 + 8\ell, B = 4 + 8m$ for $k, \ell, m \in \mathbb{Z}$ to get

$$N_{\mathbb{Q}}^{K}(\theta + 2) \equiv 10 + 8k + 8\ell + 12m + 8k\ell + 4\ell^2 + 12m^2 \pmod{16}$$

so that $N_{\mathbb{Q}}^{K}(\theta + 2) \equiv 2 \pmod 4$. The same argument as in Case 1 implies that $P = \langle 2, \theta + 2 \rangle = \langle 2, \theta \rangle$ is a proper prime ideal.

Case 4: Suppose that $A \equiv 5 \pmod 8, B \equiv 4 \pmod 8$ and $A \equiv -C \pmod 4$. As in Case 1, write $C = -A + 4k, A = 5 + 8\ell, B = 4 + 8m$ for $k, \ell, m \in \mathbb{Z}$, to get

$$N_{\mathbb{Q}}^{K}(\theta + 2) \equiv 10 + 8k + 8\ell + 12m + 8k\ell + 4\ell^2 + 12m^2 \pmod{16}$$

so that $N_{\mathbb{Q}}^{K}(\theta + 2) \equiv 2 \pmod 4$. The same argument as in Case 1 implies that $P = \langle 2, \theta + 2 \rangle = \langle 2, \theta \rangle$ is a proper prime ideal. □

Lemma 3. *Let K be a cyclic quartic field so that $K = \mathbb{Q}\left(\sqrt{A(D + B\sqrt{D})}\right)$ with A, B, C, D satisfying conditions* (a1)-(a3) *of* §1. *Suppose that $3 \mid i(K)$. Let θ be defined as in part* (b3) *of Theorem 1. Then $\langle 3, \theta \rangle \subseteq \mathcal{O}_K$ is prime.*

Proof. By assumption, $3 \mid i(K)$, so that Theorem 1.3.9 of [6] implies either $A \equiv 1 \pmod 3$ and $B \equiv 0 \pmod 3$ or $A \equiv 2 \pmod 3$ and $C \equiv 0 \pmod 3$. As in the proof of Lemma 2, we proceed in cases.

Case 1: Suppose that $A \equiv 1 \pmod 3$ and $B \equiv 0 \pmod 3$. Then $C \not\equiv 0 \pmod 3$. Furthermore, the Theorem on page 146 of [3] implies that $\theta = \sqrt{D} + \alpha - \beta$ is an algebraic integer. Write $A = 1 + 3k$, $B = 3\ell$ where $k, \ell \in \mathbb{Z}$. Suppose for the moment that $k \not\equiv 2 \pmod 3$. Then we have

$$N_{\mathbb{Q}}^{K}(\theta) \equiv 3\,C^2(21\,\ell^2 + 26\,C^2 + 23\,C^2 k) \pmod{81}$$

so that $N_{\mathbb{Q}}^{K}(\theta) \equiv 6C^4(k+1) \pmod 9$. As $k \not\equiv 2 \pmod 3$ and $C \not\equiv 0 \pmod 3$, we have that $N_{\mathbb{Q}}^{K}(\theta) \equiv \pm 3 \pmod 9$. The same argument as in Lemma 2 then implies that $\langle 3, \theta \rangle$ is prime. If $k \equiv 2 \pmod 3$, then

$$N_{\mathbb{Q}}^{K}(\theta+3) \equiv 3C(18C^3+15C^3m+25C^2+9C^2m+18C+21C\ell^2+9\ell^2) \pmod{81}$$

where $m \in \mathbb{Z}$ satisfies $k = 2 + 3m$. As $C \not\equiv 0 \pmod 3$, we have $N_{\mathbb{Q}}^{K}(\theta+3) \equiv 3C^3 \equiv \pm 3 \pmod 9$ so that $\langle 3, \theta+3 \rangle = \langle 3, \theta \rangle$ is proper and prime by the same arguments as in Lemma 2.

Case 2: Suppose that $A \equiv 2 \pmod 3$ and $C \equiv 0 \pmod 3$. Then $B \not\equiv 0 \pmod 3$. Furthermore the Theorem on page 146 of [3] implies that $\theta = \sqrt{D} + \alpha$ is an algebraic integer. Write $A = 2 + 3k$, $C = 3\ell$ where $k, \ell \in \mathbb{Z}$. Suppose that $k \not\equiv 1 \pmod 3$. Then we have

$$N_{\mathbb{Q}}^{K}(\theta) \equiv 3B^2(21\ell^2 + 26B^2 + 25B^2 k) \pmod{81}$$

so that $N_{\mathbb{Q}}^{K}(\theta) \equiv 3B^4(2+k) \pmod 9$. Since $k \not\equiv 1 \pmod 3$ and $B \not\equiv 0 \pmod 3$, we see that $N_{\mathbb{Q}}^{K}(\theta) \equiv \pm 3 \pmod 9$, and so the same argument as in Lemma 2 implies that $\langle \theta, 3 \rangle$ is prime. If $k \equiv 1 \pmod 3$, then

$$N_{\mathbb{Q}}^{K}(\theta+3) \equiv 3B(24B^3+21B^3m+20B^2+9B^2m+18B+21B\ell^2+18\ell^2) \pmod{81}$$

where $m \in \mathbb{Z}$ satisfies $k = 1 + 3m$. Since $B \not\equiv 0 \pmod 3$, we then have that $N_{\mathbb{Q}}^{K}(\theta+3) \equiv 6B^3 \equiv \pm 3 \pmod 9$. Thus the same argument as in Lemma 2 implies that $\langle \theta+3, 3 \rangle = \langle \theta, 3 \rangle$ is prime. □

3. Proof of Theorem 1

Proof. Part (a1) of the theorem is Lemma 1. Hence we suppose that $4 \mid i(K)$. The table on page 234 of [1] implies that the prime ideal factorization of $2\mathcal{O}_K$ is $P_1P_2P_3P_4$ for prime ideals $P_i \subseteq \mathcal{O}_K, i = 1, \ldots, 4$. Lemma 2 implies that $P = \langle 2, \theta \rangle$ is a prime ideal lying over 2, hence is one of the prime ideals in the factorization of $2\mathcal{O}_K$. Since K is a Galois extension of $\mathbb{Q}$ (as it is cyclic), Theorem 23 on page 70 of [4] implies that the ideals in the prime ideal factorization of $2\mathcal{O}_K$ are all conjugates of one another. Applying this to the fact that P lies over 2, we have

$$2\mathcal{O}_K = \prod_{i=1}^{4} P^{(i)}$$

which is the desired factorization. The factorization of 3 follows similarly from Lemma 3. □

Acknowledgement

The authors would like to thank the anonymous referee for their helpful suggestions on the first drafts of this paper.

References

[1] H.T. Engstrom, *On the Common Index Divisors of an Algebraic Field*, Trans. Amer. Math. Soc., **32**, no. 2 (1930), 223–237.

[2] K. Hardy; N.M Holtz; R.H. Hudson; D. Richman; K.S. Williams, *Calculation of Class Numbers of Imaginary Cyclic Quartic Fields*, Math. Comp., **49**, no. 180 (1987), 615–620.

[3] R.H. Hudson; K.S. Williams, *The Integers of a Cyclic Quartic Field*, Rocky Mountain J. Math., **20**, no. 1 (1990), 145–150.

[4] D.A. Marcus, *Number Fields*, Unviersitext, *Springer-Verlag, New York-Heidelberg*, 1977.

[5] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers Third Edition*, Springer Monographs in Mathematics, *Springer-Verlag, Berlin*, 2004

[6] B.K. Spearman; K.S. Williams, *The Index of a Cyclic Quartic Field*, Monatsh. Math., **140**, no. 1 (2003), 19–70.

[7] B.K. Spearman; K.S. Williams, *The Prime Ideal Factorization of 2 in Pure Quartic Fields with Index 2*, Math. J. Okayama. Univ., **48**, (2006), 43–46.

Stephen C. Brown
Department of Computer Science, Mathematics, Physics and Statistics
I.K. Barber School of Arts and Sciences
University of British Columbia, Okanagan,
3333 University Way,
Kelowna B.C., Canada, V1V 1V7
e-mail address: stephen.brown@ubc.ca

Chad T. Davis
Department of Computer Science, Mathematics, Physics and Statistics
I.K. Barber School of Arts and Sciences
University of British Columbia, Okanagan,
3333 University Way,
Kelowna B.C., Canada, V1V 1V
e-mail address: chad.davis@ubc.ca

(*Received October 1, 2017*)
(*Accepted February 28, 2018*)