The Prime Ideal Factorization of 2 in Pure Quartic Fields with Index 2

Blair K. Spearman* Kenneth S. Williams†

*Statistics University
†Statistics Carleton University

Copyright ©2006 by the authors. Mathematical Journal of Okayama University is produced by The Berkeley Electronic Press (bepress). http://escholarship.lib.okayama-u.ac.jp/mjou
The Prime Ideal Factorization of 2 in Pure Quartic Fields with Index 2

Blair K. Spearman and Kenneth S. Williams

Abstract

The prime ideal decomposition of 2 in a pure quartic field with field index 2 is determined explicitly.

KEYWORDS: pure quartic field, discriminant, prime decomposition
THE PRIME IDEAL FACTORIZATION OF 2 IN PURE QUARTIC FIELDS WITH INDEX 2

BLAIR K. SPEARMAN AND KENNETH S. WILLIAMS

Abstract. The prime ideal decomposition of 2 in a pure quartic field with field index 2 is determined explicitly.

1. Introduction

Let $K$ be an algebraic number field and $O_K$ its ring of integers. When determining generators of the ideals in the prime ideal factorization of a (rational) prime $p$ in $O_K$, the most difficult case occurs when $p$ divides the field index $i(K)$ of $K$. In this paper we examine the case when $K$ is a pure quartic field. Here $i(K) = 1$ or 2, and we determine explicit generators of the prime ideals in the decomposition of 2 when $i(K) = 2$.

Let $K$ be a pure quartic field. Then there exists a fourth power free integer $m$ such that $K = \mathbb{Q}(m^{1/4})$. It follows from the work of Funakura [1, p. 36] that the field index $i(K)$ of $K$ is given by

$$i(K) = \begin{cases} 2, & \text{if } m \equiv 1 \pmod{16}, \\ 1, & \text{if } m \not\equiv 1 \pmod{16}. \end{cases}$$

From now on we assume that $i(K) = 2$ so that $m \equiv 1 \pmod{16}$, say $m = 16k + 1$. In this case the prime ideal factorization of $<2>$ in $O_K$ is

$$<2> = P_1^2P_2P_3,$$

where $P_1$, $P_2$, $P_3$ are distinct prime ideals, see [1, p. 36]. In this paper we determine explicit generators of $P_1$, $P_2$ and $P_3$.

Theorem. Let $m$ be a fourth power free integer such that $K = \mathbb{Q}(m^{1/4})$ is a pure quartic field with $i(K) = 2$. Then $<2> = P_1^2P_2P_3$, where the
distinct prime ideals $P_1, P_2, P_3$ of $O_K$ are given by

\[
P_1 = < 2, \frac{3}{2} + m^{1/4} + \frac{1}{2} m^{1/2} >,
\]

\[
P_2 = \begin{cases} 
< 2, \frac{5}{4} + \frac{1}{4} m^{1/4} + \frac{1}{4} m^{1/2} + \frac{1}{4} m^{3/4} >, & \text{if } m \equiv 1 \pmod{32}, \\
< 2, \frac{3}{4} + \frac{5}{4} m^{1/4} + \frac{3}{4} m^{1/2} + \frac{1}{4} m^{3/4} >, & \text{if } m \equiv 17 \pmod{32},
\end{cases}
\]

\[
P_3 = \begin{cases} 
< 2, \frac{5}{4} - \frac{1}{4} m^{1/4} + \frac{1}{4} m^{1/2} - \frac{1}{4} m^{3/4} >, & \text{if } m \equiv 1 \pmod{32}, \\
< 2, \frac{3}{4} - \frac{5}{4} m^{1/4} + \frac{3}{4} m^{1/2} - \frac{1}{4} m^{3/4} >, & \text{if } m \equiv 17 \pmod{32}.
\end{cases}
\]

2. Proof of Theorem

Let $L = \mathbb{Q}(m^{1/2})$ so that $\mathbb{Q} \subset L \subset K$ and $[L : \mathbb{Q}] = 2$. Set

\[
Q_1 = < 2, \frac{1 + m^{1/2}}{2} >, \quad Q_2 = < 2, \frac{1 - m^{1/2}}{2} >.
\]

$Q_1$ and $Q_2$ are distinct prime ideals of $O_L$ such that $< 2 > = Q_1 Q_2$. Let $m_2$ be the largest integer such that $m_2^2 | m$. Set $m_1 = m/m_2^2$ so that $m_1$ is a squarefree integer having the same sign as $m$. Clearly $m^{1/2} = m_2 m_1^{1/2}$.

Then

\[
Q_1 = \begin{cases} 
< 2, \frac{1 + m_1^{1/2}}{2} >, & \text{if } m_2 \equiv 1 \pmod{4}, \\
< 2, \frac{1 - m_1^{1/2}}{2} >, & \text{if } m_2 \equiv 3 \pmod{4}.
\end{cases}
\]

Next, by [2, Table D, cases D1, D2, p. 92], we see that

\[
Q_1 = P_1^2
\]

for some prime ideal $P_1$ of $O_K$. We claim that

\[
P_1 = < 2, \frac{3}{2} + m^{1/4} + \frac{1}{2} m^{1/2} >.
\]

First we show that $P_1$ is a prime ideal of $O_K$. The minimal polynomial of $\theta = \frac{3}{2} + m^{1/4} + \frac{1}{2} m^{1/2}$ over $\mathbb{Q}$ is

\[
g(x) = x^4 - 6x^3 + (13 - 8k)x^2 + (-14 - 8k)x + (6 + 16k + 16k^2).
\]

Hence $N(\theta) = \pm (6 + 16k + 16k^2) \equiv 2 \pmod{4}$. Let $< \theta > = S_1 S_2 \cdots S_r$ be the prime ideal factorization of $< \theta >$ in $O_K$. Hence $N(< \theta >) =$
FACTORIZATION OF 2

As $N(S_1)N(S_2)\cdots N(S_r)$. As $2 \mid N(<\theta>)$ there exists a unique $S = S_i$ such that $2 \mid N(S)$, that is $N(S) = 2$. Thus $<\theta>$ has exactly one prime ideal to exponent 1 in its prime factorization lying above 2. As $P_1 = <2,\theta>$ we deduce that $P_1 = S$ so that $P_1$ is a prime ideal of $O_K$. Next we show that $P_1 \mid Q_1$. We set $\phi = \frac{3}{2} - m^{1/4} + \frac{1}{2}m^{1/2}$. An easy calculation shows that

$$\frac{1 + m^{1/2}}{2} = \theta \phi - (2k + 1)2.$$ 

Hence, as $2 \in P_1$ and $\theta \in P_1$, we deduce that $\frac{1 + m^{1/2}}{2} \in P_1$. Thus we have $Q_1 = <2, \frac{1 + m^{1/2}}{2} > \subseteq P_1$, and so $P_1 \mid Q_1$. As $Q_1$ is the square of a prime ideal in $O_K$, we deduce that $Q_1 = P_1^2$ as asserted.

Let

$$k = \begin{cases} 2g, & \text{if } m \equiv 1 \pmod{32}, \\ 2g + 1, & \text{if } m \equiv 17 \pmod{32}. \end{cases}$$

For $\epsilon = \pm 1$, the minimal polynomial of

$$\alpha(\epsilon) = \begin{cases} \frac{5}{4} + \frac{\epsilon}{4}m^{1/4} + \frac{1}{4}m^{1/2} + \frac{\epsilon}{4}m^{3/4}, & \text{if } m \equiv 1 \pmod{32}, \\ \frac{3}{4} + \frac{5\epsilon}{4}m^{1/4} + \frac{3}{4}m^{1/2} + \frac{\epsilon}{4}m^{3/4}, & \text{if } m \equiv 17 \pmod{32}, \end{cases}$$

is

$$x^4 - 5x^3 + (9 - 12g)x^2 + (-7 + 24g - 64g^2)x + (2 - 12g + 64g^2 - 128g^3),$$

if $m \equiv 1 \pmod{32}$, and

$$x^4 - 3x^3 + (-37 - 76g)x^2 + (-75 - 240g - 192g^2)x + (-38 - 172g - 256g^2 - 128g^3),$$

if $m \equiv 17 \pmod{32}$. Clearly $N(\alpha(\epsilon)) \equiv 2 \pmod{4}$ in both cases, and similarly to the argument above, we deduce that $I_+ = <2,\alpha(1)>$ and $I_- = <2,\alpha(-1)>$ are conjugate prime ideals of $O_K$ lying above 2. If $m \equiv 1 \pmod{32}$ we have

$$\frac{1 - m^{1/2}}{2} = 2(1 - g - gm^{1/2}) - \alpha(1)\alpha(-1) \in I_+ \cap I_-$$

and if $m \equiv 17 \pmod{32}$

$$\frac{1 - m^{1/2}}{2} = 2(-g - (1 + g)m^{1/2}) - \alpha(1)\alpha(-1) \in I_+ \cap I_-.$$
Hence \( \frac{1 - m^{1/2}}{2} \in I_+ \cap I_- \). Thus \( I_+ \) and \( I_- \) are conjugate prime ideals of \( \mathcal{O}_K \) lying above the prime ideal \( Q_2 \) of \( \mathcal{O}_L \). As \( < 2 >= P_1^2P_2P_3 = Q_1Q_2 \) and \( Q_1 = P_1^2 \), we see that \( Q_2 = P_2P_3 \) and that we can take
\[
P_2 = I_+ = < 2, \alpha(1) >
\]
and
\[
P_3 = I_- = < 2, \alpha(-1) >.
\]
This completes the proof.

References


Blair K. Spearman
Department of Mathematics and Statistics
University of British Columbia Okanagan
Kelowna, B.C. Canada V1V 1V7
E-mail address: blair.spearman@ubc.ca

Kenneth S. Williams
School of Mathematics and Statistics
Carleton University
Ottawa, Ontario, Canada K1S 5B6
E-mail address: kwilliam@connect.carleton.ca

(Received May 20, 2005)