การแยกตัวประกอบของจำนวนเฉพาะในฟิลด์ไบควอดราติก

นายชัยยะ เรียบเลิศหิรัญ

สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
สาขาวิชาคณิตศาสตร์ ภาควิชาคณิตศาสตร์
คณะวิทยาศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2549

ISBN 974-14-2618-6

ลิขสิทธิ์ของจุฬาลงกรณ์มหาวิทยาลัย

DECOMPOSITION OF RATIONAL PRIMES IN BIQUADRATIC FIELDS

Mr. Chaiya Riablershirun

สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

A Thesis Submitted in Partial Fulfillment of the Requirements
for the Degree of Master of Science Program in Mathematics
Department of Mathematics
Faculty of Science
Chulalongkorn University
Academic Year 2006

ISBN 974-14-2618-6

Copyright of Chulalongkorn University

Thesis Title	Decomposition of Rational Primes in Biquadratic Fields
By	Mr. Chaiya Riablershirun
Field of Study	Mathematics
Thesis Advisor	Associate Professor Ajchara Harnchoowong, Ph.D.

Accepted by the Faculty of Science, Chulalongkorn University in Partial Fulfillment of the Requirements for the Master's Degree

....Dean of the Faculty of Science

(Professor Piamsak Menasveta, Ph.D.)

Thesis Committee

......Amorn Wasanawichit......Chairman

(Assistant Professor Amorn Wasanawichit, Ph.D.)

......Ajchara Harnchoowong......Thesis Advisor

(Associate Professor Ajchara Harnchoowong, Ph.D.)

......Sajee Pianskool..................Member

(Assistant Professor Sajee Pianskool, Ph.D.)

สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

ชัยยะ เรียบเลิศหิรัญ: การแยกตัวประกอบของจำนวนเฉพาะในฟิลด์ไบควอดราติก
(DECOMPOSITION OF RATIONAL PRIMES IN BIQUADRATIC FIELDS)
อ. ที่ปรึกษา : รศ. ดร.อัจฉรา หาญชูวงศ์, 42 หน้า. ISBN. 974-14-2618-6

วงของจำนวนเต็มของสนามจำนวนอาจจะไม่เป็นโดเมนที่แยกตัวประกอบได้อย่างเดียว นั่นคือ สมาชิกที่ไม่เป็นศูนย์และไม่เป็นสมาชิกหน่วยอาจจะเขียนอยู่ในรูปผลคูณที่แตกต่างกันของสมาชิกที่ลดทอนไม่ได้แต่สำหรับระดับอุดมคติ เราจะได้ว่าทุกอุดมคติแท้ที่ไม่เป็นศูนย์สามารถแทนเป็นผลคูณของอุดมคติเฉพาะได้แบบเดียว การศึกษาการแยกตัวประกอบของจำนวนเฉพาะตรรกยะในหลากหลายชนิดของสนามจำนวนเป็นหัวข้อที่น่าสนใจหัวข้อหนึ่ง การแยกตัวประกอบของจำนวนเฉพาะตรรกยะในสนามกำลังสองได้คำนวณอย่างสมบูรณ์แล้ว

ในวิทยานิพนธ์ฉบับนี้ เราจะคำนวณการแยกตัวประกอบของจำนวนเฉพาะตรรกยะในสนามไบควอดราติก $K = \mathbb{Q}(\sqrt{m}, \sqrt{n})$ โดยที่ m, n เป็นจำนวนเต็มกำลังสองเสรี

สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

ภาควิชา ...คณิตศาสตร์... ลายมือชื่อนิสิต..
สาขาวิชา ...คณิตศาสตร์... ลายมือชื่ออาจารย์ที่ปรึกษา..
ปีการศึกษา ......2549......

4772268523 : MAJOR MATHEMATICS
KEY WORDS : BIQUADRATIC FIELDS / DECOMPOSITION

CHAIYA RIABLERSHIRUN : DECOMPOSITION OF RATIONAL PRIMES IN BIQUADRATIC FIELDS THESIS ADVISOR : ASSOC. PROF. AJCHARA HARNCHOOWONG, Ph.D., 42 pp. ISBN 974-14-2618-6

The ring of integers of a number field may be not a UFD, i.e. a nonzero nonunit element may be written as different products of irreducible elements. But for the ideal levels, we have that every nonzero proper ideal can be represented uniquely as the product of prime ideals. The study of the decomposition of the rational primes in various types of number fields is one of the interesting topics. The decomposition of rational primes in a quadratic field can be determined completely.

In this thesis we will determine the decomposition of rational primes in a biquadratic field $K = \mathbb{Q}(\sqrt{m}, \sqrt{n})$, where m, n are squarefree integers.

สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

Department	...Mathematics...	Student's Signature	Chaiya Riablershirun
Field of Study	...Mathematics...	Advisor's Signature	Ajchara Harnchoowong
Academic Year	.........2006............		

ACKNOWLEDGEMENTS

I am indebted to Associate Professor Dr.Ajchara Harnchoowong, my thesis supervisor, for her kind and helpful advice in preparing and writing my thesis. Moreover, I would like to thank Assistant Professor Dr.Amorn Wasanawichit and Assistant Professor Dr.Sajee Pianskool, the chairman and member of the committee of this thesis. Besides, I feel thankful to all of my teachers who have taught me for my knowledge and skills. Finally, I feel thankful to all of problem which have taught me for presence of mind and responsibility.

In particular, I would like to express my appreciation to my beloved parents for their encouragement throughout my study.

สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

CONTENTS

สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

CHAPTER I

INTRODUCTION

Let K be a number field, i.e. a finite extension over $\mathbb{Q}$. An element $\alpha \in K$ is an *algebraic integer* if and only if α satisfies a monic polynomial in $\mathbb{Z}[x]$. The set of all algebraic integers in K is a subring of K, called *the ring of integers* of K and denoted by $\mathcal{O}_K$. The ring of integers in $\mathbb{Q}$ is $\mathbb{Z}$, sometimes we call elements of $\mathbb{Z}$ rational integers.

$\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank equal to the degree $[K : \mathbb{Q}]$. The study of the form of integral bases in various types of number fields is one of the interesting topics. The form of integral basis in a quadratic field (an extension of degree 2 over $\mathbb{Q}$) can be determined completely (see Theorem 2.1.20). In this thesis we wish to determine the form of integral basis in a biquadratic field.

Even the ring of integers $\mathbb{Z}$ of $\mathbb{Q}$ is a UFD, the ring of integers of a number field may not be a UFD, i.e. a nonzero nonunit element may be written as different products of irreducible elements. But for the ideals level, we have that every nonzero proper ideal can be represented uniquely as the product of prime ideals. For a prime number p, the principal ideal $p\mathbb{Z}$ of $\mathbb{Z}$ generated by p is a prime ideal of $\mathbb{Z}$. But the principal ideal $p\mathcal{O}_K$ of $\mathcal{O}_K$ generated by p may not be a prime ideal of $\mathcal{O}_K$.

The study of the decomposition of the principal ideals generated by rational primes in various types of number fields is one of the interesting topics. The decomposition of the principal ideals generated by rational primes in a quadratic field can be determined completely (see Theorem 2.2.27 and 2.2.28) and the decomposition of the principal ideals generated by rational primes in a cubic field can be

สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

determined completely in [1], [2] and [3].

In this thesis we wish to determine the decomposition of the principal ideals generated by rational primes in a biquadratic field.

สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

CHAPTER II

BASIC DEFINITIONS AND RESULTS OF NUMBER FIELDS

In this chapter, we collect definitions and basic results of number fields, mainly without proofs, to be used throughout the entire thesis. Details and proofs can be found in [4], [5] and [6].

2.1 Rings of Integers and Discriminants

Definition 2.1.1. A *number field* is a finite extension of $\mathbb{Q}$ (in $\mathbb{C}$).

Definition 2.1.2. A *quadratic extension* is a field extension E over F of degree 2, and a *quadratic field* is a quadratic extension of $\mathbb{Q}$.

Let K be a quadratic field. Then $[K:\mathbb{Q}]$=2 and $K=\mathbb{Q}[\alpha]$ where α is a root of monic irreducible polynomial of degree 2, say $f(x)=x^2+ax+b$ where $a,b\in\mathbb{Q}$, i.e, $\alpha=(-a\pm\sqrt{a^2-4b})/2$. Since $a,b\in\mathbb{Q}$, $a^2-4b=d_1/d_2=(d_1d_2/d_2^2)$ for some $d_1,d_2\in\mathbb{Z}$ and then there exist $d,c\in\mathbb{Z}$ such that $d_1d_2=c^2d$ where d is a squarefree integer. Hence $K=\mathbb{Q}[\alpha]=\mathbb{Q}[\sqrt{a^2-4b}]=\mathbb{Q}[\sqrt{d_1d_2}]=\mathbb{Q}[\sqrt{d}]$ for some squarefree integer d.

Definition 2.1.3. Let K be a field and A a subring of K. $\alpha\in K$ is an *algebraic integer* in K if and only if there exist $n\in\mathbb{N}$ and $a_0,a_1,\ldots,a_{n-1}\in\mathbb{Z}$ such that

$$\alpha^n+a_{n-1}\alpha^{n-1}+\ldots+a_1\alpha+a_0=0.$$

Remark 2.1.4. $\alpha\in\mathbb{Q}$ is an algebraic integer if and only if $\alpha\in\mathbb{Z}$.

ศูนย์วิทยทรัพยากร
จุฬาลงกรณ์มหาวิทยาลัย

Definition 2.1.5. The set of all algebraic integers in K is a subring of K, called the *ring of integers* in K and denoted by $\mathcal{O}_K$.

Theorem 2.1.6. *The additive structure of $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank $n(=[K:\mathbb{Q}])$.*

Definition 2.1.7. An *embedding* of L over K in $\mathbb{C}$ is a one to one homomorphism $\sigma : L \to \mathbb{C}$ fixing K pointwise (it is called a K-monomorphism). An *embedding* of L in $\mathbb{C}$ is an embedding of L over $\mathbb{Q}$ in $\mathbb{C}$.

Example 2.1.8. Let $K = \mathbb{Q}[\sqrt{d}]$ where d is a squarefree integer. Then minimal polynomial of $\sqrt{d}$ over $\mathbb{Q}$ are $f(x) = x^2 - d = (x-\sqrt{d})(x+\sqrt{d})$.
Therefore embeddings of K in $\mathbb{C}$ are

$\sigma_1 : \sqrt{d} \mapsto \sqrt{d}$ and fixes $\mathbb{Q}$ pointwise, i.e, σ_1=id,

$\sigma_2 : \sqrt{d} \mapsto -\sqrt{d}$ and fixes $\mathbb{Q}$ pointwise.

Theorem 2.1.9. *Let K and L be number fields with $K \subseteq L$ and $[L:K]=n$. Then there exist n embeddings of L over K in $\mathbb{C}$.*

If L/K is a Galois extension, then all embeddings of L over K are K-automorphisms and the set of all embeddings of L over K is the Galois group of L over K, denoted by $\mathrm{Gal}(L/K)$.

From now on, let L over K be a number field extension of degree n and $\sigma_1 = id_L, \sigma_2, \ldots, \sigma_n$ be all embeddings of L over K.

Definition 2.1.10. For $\alpha \in L$, define the *relative trace* of $\alpha = \mathrm{Tr}_{L/K}(\alpha) = \sigma_1(\alpha) + \sigma_2(\alpha) + \ldots + \sigma_n(\alpha)$ and the *relative norm* of $\alpha = \mathrm{N}_{L/K}(\alpha) = \sigma_1(\alpha)\,\sigma_2(\alpha)\ldots\sigma_n(\alpha)$.

If $K=\mathbb{Q}$, then we write Tr_L and N_L for $\mathrm{Tr}_{L/\mathbb{Q}}$ and $\mathrm{N}_{L/\mathbb{Q}}$ and call the *absolute trace* and *absolute norm*, respectively.

Remark 2.1.11. For each $\alpha \in L$, $\mathrm{Tr}_{L/K}(\alpha)$ and $\mathrm{N}_{L/K}(\alpha) \in K$. Moreover, if $\alpha \in \mathcal{O}_L$, then $\mathrm{Tr}_L(\alpha)$ and $\mathrm{N}_L(\alpha) \in \mathbb{Z}$.

Example 2.1.12. Let $L = \mathbb{Q}(\sqrt{d})$ and $\alpha = a + b\sqrt{d}$ where $a, b \in \mathbb{Q}$. Then

$$\mathrm{Tr}_{L/\mathbb{Q}}(a + b\sqrt{d}) = (a + b\sqrt{d}) + (a - b\sqrt{d}) = 2a \quad \text{and}$$
$$\mathrm{N}_{L/\mathbb{Q}}(a + b\sqrt{d}) = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - b^2 d.$$

Definition 2.1.13. Let $\alpha_1, \alpha_2, \ldots, \alpha_n \in L$. The *discriminant* of $\alpha_1, \alpha_2, \ldots, \alpha_n$ in L over K denoted by $\mathrm{disc}_{L/K}\ (\alpha_1, \alpha_2, \ldots, \alpha_n) := det[\sigma_i(\alpha_j)]^2$.

Example 2.1.14. Let $K = \mathbb{Q}(\sqrt{d})$.
Then $\mathrm{disc}_{K/\mathbb{Q}}(1, \frac{1+\sqrt{d}}{2}) = d$ and $\mathrm{disc}_{K/\mathbb{Q}}(1, \sqrt{d}) = 4d$.

Proposition 2.1.15. *For any $\alpha_1, \ldots, \alpha_n \in L, \mathrm{disc}_{L/K}(\alpha_1, \ldots, \alpha_n) \in K$. Moreover, if $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_L, \mathrm{disc}_{L/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}$.*

Theorem 2.1.16. *Let K be a number field of degree n over $\mathbb{Q}$. The additive structure of the ring of integers $\mathcal{O}_K$ of K is a free abelian group (or $\mathbb{Z}$-module) of rank n, i.e, it is isomorphic to the direct sum of n subgroups each of which is isomorphic to $\mathbb{Z}$.*

Suppose that $K = \mathbb{Q}(\sqrt{5})$, we have $\{1, \sqrt{5}\}$ is a basis of K over $\mathbb{Q}$, but it is not a $\mathbb{Z}$-basis of $\mathcal{O}_K$ since $\frac{1}{2} + \frac{\sqrt{5}}{2}$, which satisfies $x^2 - x - 1 = 0$, is in $\mathcal{O}_K$ but is not in $\mathbb{Z} \cdot 1 + \mathbb{Z} \cdot \sqrt{5}$.

Definition 2.1.17. A $\mathbb{Z}$-basis $\{\alpha_1, \ldots, \alpha_n\}$ of $\mathcal{O}_K$ is called an *integral basis* of K.

Note. An integral basis of K is also a basis of K over $\mathbb{Q}$.

Proposition 2.1.18. *Let $\{\alpha_1, \ldots, \alpha_n\}$ and $\{\beta_1, \ldots, \beta_n\}$ be any integral bases of K. Then $\mathrm{disc}_K(\alpha_1, \ldots, \alpha_n) = \mathrm{disc}_K(\beta_1, \ldots, \beta_n)$.*

Definition 2.1.19. The *discriminant of the field* $K = \mathrm{disc}_K(\alpha_1, \ldots, \alpha_n)$ where $\{\alpha_1, \ldots, \alpha_n\}$ is an integral basis of K over $\mathbb{Q}$, we denote it by $\mathrm{disc}(K)$ or δ_K.

สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

Theorem 2.1.20. *Let $K = \mathbb{Q}(\sqrt{d})$ where d is a squarefree integer.*
(i) If $d \equiv 1(mod4)$, then

$$\begin{aligned}\mathcal{O}_K &= \left\{\frac{u + v\sqrt{d}}{2}|u, v \in \mathbb{Z}\, and\, u \equiv v(mod2)\right\}\\ &= \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] = \mathbb{Z}\cdot 1 \oplus \mathbb{Z}\cdot\frac{1+\sqrt{d}}{2}\end{aligned}$$

Consequently, $\left\{1, \frac{1+\sqrt{d}}{2}\right\}$ is an integral basis of K and $\delta_K = d$
(ii) If $d \equiv 2$ or $3(mod4)$, then

$$\mathcal{O}_K = \left\{u + v\sqrt{d}|u, v \in \mathbb{Z}\right\} = \mathbb{Z}\cdot 1 \oplus \mathbb{Z}\cdot\sqrt{d}$$

Consequently, $\left\{1, \sqrt{d}\right\}$ is an integral basis of K and $\delta_K = 4d$.

2.2 Prime Decomposition of Ideals

As we have known that the ring of integers $\mathbb{Z}$ in $\mathbb{Q}$ is a UFD. But for general number field K, the ring of integers may not be a UFD.

Example 2.2.1. Let $K = \mathbb{Q}(\sqrt{-5})$. Then by Theorem 2.1.20, $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. $\mathcal{O}_K$ is not a UFD for $2 \cdot 3 = 6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ where $2, 3, 1 + \sqrt{-5}$ and $1 - \sqrt{-5}$ are nonassociate irreducible elements in $\mathcal{O}_K$.

Theorem 2.2.2. *Every nonzero proper ideal in the ring of integers $\mathcal{O}_K$ of a number field K is a prime ideal if and only if it is a maximal ideal.*

Corollary 2.2.3. *If P is a prime ideal in $\mathcal{O}_K$, then $\mathcal{O}_K/P$ is a field.*

Theorem 2.2.4. *Every nonzero proper ideal in $\mathcal{O}_K$ can be written uniquely as a product of prime ideals.*

Recall that $(2)(3) = 6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ in $K = \mathbb{Q}[\sqrt{-5}]$. But for the ideal levels, we will show that they can be represented uniquely as the product of prime ideals.

สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

Example 2.2.5. Let $K = \mathbb{Q}[\sqrt{-5}]$. Then $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$.
Recall that $\mathcal{O}_K$ is not a UFD for $2 \cdot 3 = 6 = (1+\sqrt{-5})(1-\sqrt{-5})$. Pass this to ideals: $\langle 2\rangle \langle 3\rangle = \langle 6\rangle = \left\langle 1+\sqrt{-5}\right\rangle \left\langle 1-\sqrt{-5}\right\rangle$. But

$$\begin{aligned}
\left\langle 2, 1+\sqrt{-5}\right\rangle \left\langle 2, 1+\sqrt{-5}\right\rangle &= \left\langle 4, 2+2\sqrt{-5}, -4+2\sqrt{-5}\right\rangle \\
&= \left\langle 4, 2+2\sqrt{-5}, -6\right\rangle \\
&= \left\langle 2, 2\sqrt{-5}\right\rangle \\
&= \langle 2\rangle \\
\left\langle 3, 1+\sqrt{-5}\right\rangle \left\langle 3, 1-\sqrt{-5}\right\rangle &= \left\langle 9, 3+3\sqrt{-5}, 3-3\sqrt{-5}, 6\right\rangle \\
&= \left\langle 9, 3+3\sqrt{-5}, 6\right\rangle \\
&= \left\langle 3, 3\sqrt{-5}\right\rangle \\
&= \langle 3\rangle \\
\left\langle 2, 1+\sqrt{-5}\right\rangle \left\langle 3, 1+\sqrt{-5}\right\rangle &= \left\langle 6, 2(1+\sqrt{-5}), 3(1+\sqrt{-5}), (1+\sqrt{-5})^2\right\rangle \\
&= \left\langle 1+\sqrt{-5}\right\rangle \\
\left\langle 2, 1+\sqrt{-5}\right\rangle \left\langle 3, 1-\sqrt{-5}\right\rangle &= \left\langle 6, 2(1-\sqrt{-5}), 3(1+\sqrt{-5}), (1-\sqrt{-5})^2\right\rangle \\
&= \left\langle 1-\sqrt{-5}\right\rangle
\end{aligned}$$

Then we obtain that

$$\begin{aligned}
\left\langle 2, 1+\sqrt{-5}\right\rangle^2 \left\langle 3, 1+\sqrt{-5}\right\rangle \left\langle 3, 1-\sqrt{-5}\right\rangle &= \langle 2\rangle \langle 3\rangle \\
&= \langle 6\rangle \\
&= \left\langle 1+\sqrt{-5}\right\rangle \left\langle 1-\sqrt{-5}\right\rangle \\
&= \left\langle 2, 1+\sqrt{-5}\right\rangle^2 \left\langle 3, 1+\sqrt{-5}\right\rangle \left\langle 3, 1-\sqrt{-5}\right\rangle .
\end{aligned}$$

Definition 2.2.6. Let A and B be integral ideals in a number field K. We say that A divides B, denoted by $A \mid B$ if there exists an integral ideal C such that $B = AC$.

Proposition 2.2.7. *Let A and B be integral ideals in a number field K. Then $A \mid B$ if and only if $A \supseteq B$.*

สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

Next, we will define the norm of ideals and use the properties of norm of ideals to check whether an ideal P is a prime ideal or an ideal A divides ideal B. From now on, let K be a number field of degree n over $\mathbb{Q}$.

Definition 2.2.8. The *norm* of a nonzero ideal A in $\mathcal{O}_K$, denoted by $\mathrm{N}(A)$, is defined to be $|\mathcal{O}_K/A|$.

Proposition 2.2.9. *If A is a nonzero ideal of $\mathcal{O}_K$, then A is a free $\mathbb{Z}$-submodule of $\mathcal{O}_K$ of rank n.*

Theorem 2.2.10. *Let A be a nonzero ideal in $\mathcal{O}_K$ with $\mathbb{Z}$-basis $\{\alpha_1, \ldots, \alpha_n\}$. Then*

$$\mathrm{N}(A)^2 = \frac{disc_K(\alpha_1, \ldots, \alpha_n)}{\delta_K}.$$

Corollary 2.2.11. *For any $\alpha \neq 0$ in $\mathcal{O}_K$, $\mathrm{N}(\langle\alpha\rangle)= |\mathrm{N}_K(\alpha)|$.*

Theorem 2.2.12. *For any nonzero ideals A and B, $\mathrm{N}(AB)$=$\mathrm{N}(A)\mathrm{N}(B)$.*

The following corollary is used to check that an ideal A divides an ideal B or not.

Corollary 2.2.13. *If $N(A) \nmid N(B)$, then $A \nmid B$.*

Remark 2.2.14. If P is an ideal such that $N(P) = p$ a prime number, then P is a prime ideal in $\mathcal{O}_K$. The converse is not true, i.e. there is a prime ideal whose norm is not a prime number.

Example 2.2.15. Let $K = \mathbb{Q}[\sqrt{-5}]$.
From Example 2.2.5, we have $\mathrm{N}(\langle 2, 1+\sqrt{-5}\rangle) = 2$, $\mathrm{N}(\langle 3, 1+\sqrt{-5}\rangle)$=3 and $\mathrm{N}(\langle 3, 1+\sqrt{-5}\rangle)$=3. Hence $\langle 2, 1+\sqrt{-5}\rangle$,$\langle 3, 1+\sqrt{-5}\rangle$ and $\langle 3, 1-\sqrt{-5}\rangle$ are prime ideals.

Let $L \supseteq K$ be a finite extension of number fields. Let P be a prime ideal in $\mathcal{O}_K$. Then $P\mathcal{O}_L$ is a nonzero ideal in $\mathcal{O}_L$. It is not necessary a prime ideal in $\mathcal{O}_L$, e.g. let $K = \mathbb{Q}$ and $L = \mathbb{Q}(\sqrt{-5})$. Then $\mathcal{O}_K = \mathbb{Z}$ and $\mathcal{O}_L = \mathbb{Z}[\sqrt{-5}]$. We have $2\mathbb{Z}$ is a prime ideal in $\mathbb{Z}$ but $2\mathcal{O}_L$ is not a prime ideal in $\mathcal{O}_L$ since it is not maximal. For $2\mathcal{O}_L \subsetneq \langle 2, 1+\sqrt{-5}\rangle \subsetneq \mathcal{O}_L$. We will consider the prime factorization of $P\mathcal{O}_L$ in $\mathcal{O}_L$.

Definition 2.2.16. Let $P\mathcal{O}_L = \prod_{i=1}^{g} \mathcal{P}_i^{e_i}$ be the prime decomposition in $\mathcal{O}_L$ where P is a prime ideal in $\mathcal{O}_K$.

(1) g is called the *decomposition number* of P in L.

(2) For each i, e_i is called the *ramification index* of $\mathcal{P}_i$ over P in L over K, denoted by $e(\mathcal{P}_i/P)$.

P is ramified in $\mathcal{O}_L$ (in L) if there exists i such that $e_i > 1$.

P is inert in L if $g = 1$ and $e_1 = 1$, i.e. $P\mathcal{O}_L$ is a prime ideal.

Remark 2.2.17. For P and $\mathcal{P}$ as in Definition 2.2.16, we say that $\mathcal{P}$ *lies over/above* P or P *lies under* $\mathcal{P}$. The field $\mathcal{O}_K/P$ is embedded in the field $\mathcal{O}_L/\mathcal{P}$ so it can be considered as a subfield of $\mathcal{O}_L/\mathcal{P}$.

Definition 2.2.18. The degree of $\mathcal{O}_L/\mathcal{P}_i$ over $\mathcal{O}_K/P$ is called the *residue class degree* or *inertial degree* of $\mathcal{P}_i$ over P, denoted by $f(\mathcal{P}_i/P)$.

Remark 2.2.19. $\mathrm{N}(\mathcal{P}_i) = \mathrm{N}(P)^f$ where $f = f(\mathcal{P}_i/P)$.

Theorem 2.2.20. *Let $L \supseteq K$ be a number field extension of degree n and let $\mathcal{P}_1, \ldots, \mathcal{P}_g$ be primes in $\mathcal{O}_L$ lying above a prime P of $\mathcal{O}_K$ with ramification indices $e_1, \ldots, e_g$ and residue class degrees $f_1, \ldots, f_g$. Then $n = \sum_{i=1}^{g} e_i f_i$.*

Definition 2.2.21. Let $L \supseteq K$ be a number field extension of degree n and P be a prime ideal in $\mathcal{O}_K$ such that $P\mathcal{O}_L = \mathcal{P}_1^{e_1}\mathcal{P}_2^{e_2}\ldots\mathcal{P}_g^{e_g}$ where $\mathcal{P}_i$ are distinct prime ideals of $\mathcal{O}_L$.

(1) P is *totally ramified* in L if $g = 1$ and $e_1 = n$, so $P\mathcal{O}_L = \mathcal{P}_1^n$.

(2) P *splits completely* in L if $g = n$, so $e_i = 1$ and $P\mathcal{O}_L = \mathcal{P}_1 \ldots \mathcal{P}_n$.

Example 2.2.22. From Example 2.2.5 and Definition 2.2.16, $P_2 = 2\mathbb{Z}$ in $\mathbb{Z}$ is ramified in $\mathbb{Q}[\sqrt{-5}]$ while $P_3 = 3\mathbb{Z}$ in $\mathbb{Z}$ splits completely in $\mathbb{Q}[\sqrt{-5}]$.

สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

Theorem 2.2.23. *Let $L \supseteq K$ be a Galois extensions number field of degree n and $\mathcal{P}_i, \mathcal{P}_j$ be primes in $\mathcal{O}_L$ lying above a prime P of $\mathcal{O}_K$. Then $e(\mathcal{P}_i/P) = e(\mathcal{P}_j/P)$ and $f(\mathcal{P}_i/P) = f(\mathcal{P}_j/P)$, i.e. $P\mathcal{O}_L = (\mathcal{P}_1 \dots \mathcal{P}_g)^e$, hence $n = efg$ where $e = e(\mathcal{P}_i/P)$ and $f = f(\mathcal{P}_i/P)$.*

Theorem 2.2.24. *Let p be a prime in $\mathbb{Z}$. Then $p\mathbb{Z}$ is ramified in K if and only if $p|\delta_K$.*

Example 2.2.25. We have seen that in $K = \mathbb{Q}[\sqrt{-5}], 2\mathcal{O}_K = \left\langle 2, 1+\sqrt{-5}\right\rangle^2$ and $3\mathcal{O}_K = \left\langle 3, 1+\sqrt{-5}\right\rangle \left\langle 3, 1-\sqrt{-5}\right\rangle$. Then $2\mathbb{Z}$ is ramified in K while $3\mathbb{Z}$ is not. Notice that $\delta_K = -20$ and $2 \mid \delta_K$ while $3 \nmid \delta_K$.

Definition 2.2.26. Let p be an odd prime and let a be a nonzero integer not a multiple of p. We define the *Legendre symbol* $\left(\frac{a}{p}\right)$ of a, relative to p, as follows:

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \textit{when } a \textit{ is a quadratic residue modulo } p, \\ -1, & \textit{when } a \textit{ is a quadratic nonresidue modulo } p. \end{cases}$$

For typographical reasons, we also use the notation $\left(\frac{a}{p}\right) = (a/p)$. Next, the decomposition of rational primes in quadratic fields can be determined completely as follows.

Theorem 2.2.27. *Let $K = \mathbb{Q}[\sqrt{d}]$ where d is a squarefree integer. Then*

(i) $2\mathbb{Z}$ is totally ramified in $\mathcal{O}_K$ if and only if $d \equiv 2$ or $3 \pmod 4$.

(ii) $2\mathbb{Z}$ splits completely in $\mathcal{O}_K$ if and only if $d \equiv 1 \pmod 8$.

(iii) $2\mathbb{Z}$ is inert in $\mathcal{O}_K$ if and only if $d \equiv 5 \pmod 8$.

Moreover, (i) $2\mathcal{O}_K = \begin{cases} \langle 2, \sqrt{d}\rangle^2 & \textit{if } d \equiv 2 \pmod 4, \\ \langle 2, 1+\sqrt{d}\rangle^2 & \textit{if } d \equiv 3 \pmod 4. \end{cases}$

(ii) $2\mathcal{O}_K = \langle 2, \frac{1+\sqrt{d}}{2}\rangle\langle 2, \frac{1-\sqrt{d}}{2}\rangle$ *if* $d \equiv 1 \pmod 8$.

สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

Theorem 2.2.28. *Let $K = \mathbb{Q}[\sqrt{d}]$ where d is a squarefree integer, p be any odd prime number. Then*

(i) $p\mathbb{Z}$ is totally ramified in $\mathcal{O}_K$ if and only if $p \mid d$.

(ii) $p\mathbb{Z}$ splits completely in $\mathcal{O}_K$ if and only if $p \nmid d$ and $(d/p) = 1$.

(iii) $p\mathbb{Z}$ is inert in $\mathcal{O}_K$ if and only if $p \nmid d$ and $(d/p) = -1$.

Moreover, (i) $p\mathcal{O}_K = \langle p, \sqrt{d}\rangle^2$

(ii) $p\mathcal{O}_K = \langle p, n + \sqrt{d}\rangle\langle p, n - \sqrt{d}\rangle$ if $d \equiv n^2 \pmod{p}$.

From these two theorems we can see that p is ramified in $\mathcal{O}_K$ if and only if $p \mid \delta_K$.

In the next chapter we will find integral bases and discriminants of biquadratic fields.

สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

CHAPTER III

INTEGRAL BASES AND DECOMPOSITION OF RATIONAL PRIMES IN BIQUADRATIC FIELDS

In this chapter, we collect results of biquadratic fields which is an extension of degree 4 over $\mathbb{Q}$ of the form $\mathbb{Q}[\sqrt{m},\sqrt{n}]$ where m, n are distinct squarefree integer. The first section deals with algebraic properties of biquadratic fields . The second section deals with the integral bases and discriminant of biquadratic fields. The third section deals with the decomposition of rational primes in biquadratic fields.

3.1 Algebraic Properties

Let $K = \mathbb{Q}[\sqrt{m},\sqrt{n}]$ be any biquadratic field where m and n are distinct squarefree integers. Let $k = \frac{mn}{d^2}$ where $d = (m,n)$ and since $\sqrt{m} = \frac{d\sqrt{n}\sqrt{k}}{n}$, $\sqrt{n} = \frac{d\sqrt{m}\sqrt{k}}{m}$ and $\sqrt{k} = \frac{\sqrt{m}\sqrt{n}}{d}$, we obtain that $K = \mathbb{Q}[\sqrt{m},\sqrt{n}] = \mathbb{Q}[\sqrt{n},\sqrt{k}] = \mathbb{Q}[\sqrt{k},\sqrt{m}]$. The degree of K over $\mathbb{Q}$ is 4 and a basis of K over $\mathbb{Q}$ is $\{1,\sqrt{m},\sqrt{n},\sqrt{k}\}$. Then every element α of K is written uniquely in the form $\alpha = r_1\cdot 1 + r_2\cdot\sqrt{m} + r_3\cdot\sqrt{n} + r_4\cdot\sqrt{k}$ where $r_i \in \mathbb{Q}$. Since char($\mathbb{Q}$)=0 and K is the splitting filed of the polynomial $(x^2-m)(x^2-n)$ over K, so K is a normal and separable extension, and hence Galois extension over $\mathbb{Q}$ with the Galois group G =Gal($K/\mathbb{Q}$) consists of the following $\mathbb{Q}$-automorphisms of K:

$$\sigma_1 = id.$$

$$\sigma_2 : \sqrt{m} \mapsto \sqrt{m}, \sqrt{n} \mapsto -\sqrt{n},$$

$$\sigma_3 : \sqrt{m} \mapsto -\sqrt{m}, \sqrt{n} \mapsto \sqrt{n},$$

$$\sigma_4 : \sqrt{m} \mapsto -\sqrt{m}, \sqrt{n} \mapsto -\sqrt{n}.$$

สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

All subfields of K of degree 2 over $\mathbb{Q}$ are $\mathbb{Q}[\sqrt{m}]$, $\mathbb{Q}[\sqrt{n}]$ and $\mathbb{Q}[\sqrt{k}]$, and $\mathrm{Gal}(K/\mathbb{Q}[\sqrt{m}]) = \{\sigma_1, , \sigma_2\}$, $\mathrm{Gal}(K/\mathbb{Q}[\sqrt{n}]) = \{\sigma_1, , \sigma_3\}$ and $\mathrm{Gal}(K/\mathbb{Q}[\sqrt{k}]) = \{\sigma_1, , \sigma_4\}$.

3.2 Integral Bases and Discriminants

In this section we will find the integral bases and discriminants for biquadratic fields. First, we will show that 3 cases as follow cover all cases except for rearrangements of m, n and k.

(i) $m \equiv 3, n \equiv k \equiv 2 \pmod 4$.

(ii) $m \equiv 1, n \equiv k \equiv 2$ or $3 \pmod 4$.

(iii) $m \equiv n \equiv k \equiv 1 \pmod 4$.

Since m and n are squarefree integers, $m, n \equiv 1$, 2 or $3 \pmod 4$.

Case1. $m \equiv 3 \pmod 4$ and $n \equiv 3 \pmod 4$.

Since m and n are odd, d is odd and so $d^2 \equiv 1 \pmod 4$. Hence $k \equiv kd^2 = mn \equiv 1 \pmod 4$. This case is supported by (ii).

Case2. $m \equiv 3 \pmod 4$ and $n \equiv 2 \pmod 4$.

Since m is odd, d is odd and so $d^2 \equiv 1 \pmod 4$. Hence $k \equiv kd^2 = mn \equiv 2 \pmod 4$. This case is supported by (i).

Case3. $m \equiv 3 \pmod 4$ and $n \equiv 1 \pmod 4$.

Since m and n are odd, d is odd and so $d^2 \equiv 1 \pmod 4$. Hence $k \equiv kd^2 = mn \equiv 3 \pmod 4$. This case is supported by (ii).

Case4. $m \equiv 2 \pmod 4$ and $n \equiv 2 \pmod 4$.

Since $m \equiv 2 \pmod 4$ and $n \equiv 2 \pmod 4$ and d is even, so $\frac{m}{d}$ and $\frac{n}{d}$ are odd. Hence $k = \frac{mn}{d^2} \equiv 1$ or $3 \pmod 4$. This case is supported by (i) or (ii).

Case5. $m \equiv 2 \pmod 4$ and $n \equiv 1 \pmod 4$.

Since n is odd, d is odd and so $d^2 \equiv 1 \pmod 4$. Hence $k \equiv kd^2 = mn \equiv 2 \pmod 4$. This case is supported by (ii).

Case6. $m \equiv 1 \pmod 4$ and $n \equiv 1 \pmod 4$.

Since m and n are odd, d is odd and so $d^2 \equiv 1 \pmod 4$. Hence $k \equiv kd^2 = mn \equiv 1$

สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

(mod 4). This case is supported by (iii).

Hence (i), (ii) and (iii) cover all cases except for rearrangements of m, n and k.

Next, we will find the integral basis of $K = \mathbb{Q}[\sqrt{m}, \sqrt{n}]$ in 3 cases above.

Theorem 3.2.1. *Let $K = \mathbb{Q}[\sqrt{m}, \sqrt{n}]$ where m and n are distinct squarefree integers and $k = \dfrac{mn}{d^2}$ where $d = (m, n)$.*

(i) If $m \equiv 3, n \equiv k \equiv 2 \pmod 4$, then
$\{1, \sqrt{m}, \sqrt{n}, \dfrac{\sqrt{n}+\sqrt{k}}{2}\}$ *is an integral basis of K, i.e.*
$\mathcal{O}_K = \mathbb{Z}\cdot 1 \oplus \mathbb{Z}\cdot\sqrt{m} \oplus \mathbb{Z}\cdot\sqrt{n} \oplus \mathbb{Z}\cdot\dfrac{\sqrt{n}+\sqrt{k}}{2}.$

(ii) If $m \equiv 1, n \equiv k \equiv 2$ or $3 \pmod 4$, then
$\{1, \dfrac{1+\sqrt{m}}{2}, \sqrt{n}, \dfrac{\sqrt{n}+\sqrt{k}}{2}\}$ *is an integral basis of K, i.e.*
$\mathcal{O}_K = \mathbb{Z}\cdot 1 \oplus \mathbb{Z}\cdot\dfrac{1+\sqrt{m}}{2} \oplus \mathbb{Z}\cdot\sqrt{n} \oplus \mathbb{Z}\cdot\dfrac{\sqrt{n}+\sqrt{k}}{2}.$

(iii) If $m \equiv n \equiv k \equiv 1 \pmod 4$, then
$\{1, \dfrac{1+\sqrt{m}}{2}, \dfrac{1+\sqrt{n}}{2}, (\dfrac{1+\sqrt{m}}{2})(\dfrac{1+\sqrt{k}}{2})\}$ *is an integral basis of K, i.e.*
$\mathcal{O}_K = \mathbb{Z}\cdot 1 \oplus \mathbb{Z}\cdot\dfrac{1+\sqrt{m}}{2} \oplus \mathbb{Z}\cdot\dfrac{1+\sqrt{n}}{2} \oplus \mathbb{Z}\cdot(\dfrac{1+\sqrt{m}}{2})(\dfrac{1+\sqrt{k}}{2}).$

Proof. Recall that K has 4 embeddings, namely $\sigma_1 =$id, $\sigma_2 : \sqrt{m} \mapsto \sqrt{m}, \sqrt{n} \mapsto -\sqrt{n}, \sigma_3 : \sqrt{m} \mapsto -\sqrt{m}, \sqrt{n} \mapsto \sqrt{n}$ and $\sigma_4 : \sqrt{m} \mapsto -\sqrt{m}, \sqrt{n} \mapsto -\sqrt{n}$ and all embeddings of K over $\mathbb{Q}[\sqrt{m}]$ are σ_1 and σ_2, of K over $\mathbb{Q}[\sqrt{n}]$ are σ_1 and σ_3 and of K over $\mathbb{Q}[\sqrt{mn}]$ are σ_1 and σ_4.

(i) $m \equiv 3, n \equiv k \equiv 2 \pmod 4$.

Let $\alpha \in \mathcal{O}_K$, so $\alpha = r_0 + r_1\sqrt{m} + r_2\sqrt{n} + r_3\sqrt{k}$ where $r_0, r_1, r_2, r_3 \in \mathbb{Q}$. Then

$$\begin{aligned}
\sigma_2(\alpha) &= r_0 + r_1\sqrt{m} - r_2\sqrt{n} - r_3\sqrt{k},\\
\sigma_3(\alpha) &= r_0 - r_1\sqrt{m} + r_2\sqrt{n} - r_3\sqrt{k},\\
\sigma_4(\alpha) &= r_0 - r_1\sqrt{m} - r_2\sqrt{n} + r_3\sqrt{k}.
\end{aligned}$$

Since $\alpha \in \mathcal{O}_K$, $\mathrm{Tr}_{K/\mathbb{Q}[\sqrt{m}]}(\alpha) \in \mathcal{O}_{\mathbb{Q}[\sqrt{m}]}$, $\mathrm{Tr}_{K/\mathbb{Q}[\sqrt{n}]}(\alpha) \in \mathcal{O}_{\mathbb{Q}[\sqrt{n}]}$, $\mathrm{Tr}_{K/\mathbb{Q}[\sqrt{k}]}(\alpha) \in \mathcal{O}_{\mathbb{Q}[\sqrt{k}]}$.

We express these conditions in terms of the coefficients of α:

$$\begin{aligned}
\mathrm{Tr}_{K/\mathbb{Q}[\sqrt{m}]}(\alpha) &= \alpha + \sigma_2(\alpha) = 2r_0 + 2r_1\sqrt{m} \in \mathcal{O}_{\mathbb{Q}[\sqrt{m}]},\\
\mathrm{Tr}_{K/\mathbb{Q}[\sqrt{n}]}(\alpha) &= \alpha + \sigma_3(\alpha) = 2r_0 + 2r_2\sqrt{n} \in \mathcal{O}_{\mathbb{Q}[\sqrt{n}]},\\
\mathrm{Tr}_{K/\mathbb{Q}[\sqrt{k}]}(\alpha) &= \alpha + \sigma_4(\alpha) = 2r_0 + 2r_3\sqrt{k} \in \mathcal{O}_{\mathbb{Q}[\sqrt{k}]}.
\end{aligned}$$

Taking into account that $\mathcal{O}_{\mathbb{Q}[\sqrt{m}]} = \mathbb{Z}\cdot 1 \oplus \mathbb{Z}\cdot\sqrt{m}$, $\mathcal{O}_{\mathbb{Q}[\sqrt{n}]} = \mathbb{Z}\cdot 1 \oplus \mathbb{Z}\cdot\sqrt{n}$ and $\mathcal{O}_{\mathbb{Q}[\sqrt{k}]} = \mathbb{Z}\cdot 1 \oplus \mathbb{Z}\cdot\sqrt{k}$, then

$$\begin{aligned}
2r_0 + 2r_1\sqrt{m} &\in \mathbb{Z}\cdot 1 \oplus \mathbb{Z}\cdot\sqrt{m},\\
2r_0 + 2r_2\sqrt{n} &\in \mathbb{Z}\cdot 1 \oplus \mathbb{Z}\cdot\sqrt{n},\\
2r_0 + 2r_3\sqrt{k} &\in \mathbb{Z}\cdot 1 \oplus \mathbb{Z}\cdot\sqrt{k}.
\end{aligned}$$

Hence $2r_0 \in \mathbb{Z}, 2r_1 \in \mathbb{Z}, 2r_2 \in \mathbb{Z}$ and $2r_3 \in \mathbb{Z}$. From these relations we deduce $\alpha = r_0 + r_1\sqrt{m} + r_2\sqrt{n} + r_3\sqrt{k} = \frac{1}{2}(w + x\sqrt{m} + y\sqrt{n} + z\sqrt{k})$ for some $w, x, y, z \in \mathbb{Z}$. Since $\alpha \in \mathcal{O}_K$, $\mathrm{N}_{K/\mathbb{Q}[\sqrt{m}]}(\alpha) \in \mathcal{O}_{\mathbb{Q}[\sqrt{m}]}$, $\mathrm{N}_{K/\mathbb{Q}[\sqrt{n}]}(\alpha) \in \mathcal{O}_{\mathbb{Q}[\sqrt{n}]}$, $\mathrm{N}_{K/\mathbb{Q}[\sqrt{k}]}(\alpha) \in \mathcal{O}_{\mathbb{Q}[\sqrt{k}]}$. We express these conditions in terms of the coefficients of α:

$$\begin{aligned}
\mathrm{N}_{K/\mathbb{Q}[\sqrt{m}]}(\alpha) &= \alpha\cdot\sigma_2(\alpha) = \frac{1}{4}(w + x\sqrt{m})^2 - \frac{1}{4}(y\sqrt{n} + z\sqrt{k})^2\\
&= \frac{1}{4}(w^2 + x^2m - y^2n - z^2k) + \frac{1}{4}(2wx\sqrt{m} - 2yz\sqrt{nk})\\
&= \frac{1}{4}(w^2 + x^2m - y^2n - z^2k) + \frac{1}{4}(2wx - 2yz\frac{n}{d})\sqrt{m},\\
\mathrm{N}_{K/\mathbb{Q}[\sqrt{n}]}(\alpha) &= \alpha\cdot\sigma_3(\alpha) = \frac{1}{4}(w + y\sqrt{n})^2 - \frac{1}{4}(x\sqrt{m} + z\sqrt{k})^2\\
&= \frac{1}{4}(w^2 - x^2m + y^2n - z^2k) + \frac{1}{4}(2wy\sqrt{n} - 2xz\sqrt{mk})\\
&= \frac{1}{4}(w^2 - x^2m + y^2n - z^2k) + \frac{1}{4}(2wy - 2xz\frac{m}{d})\sqrt{n},\\
\mathrm{N}_{K/\mathbb{Q}[\sqrt{k}]}(\alpha) &= \alpha\cdot\sigma_4(\alpha) = \frac{1}{4}(w + z\sqrt{k})^2 - \frac{1}{4}(x\sqrt{m} + y\sqrt{n})^2\\
&= \frac{1}{4}(w^2 - x^2m - y^2n + z^2k) + \frac{1}{4}(2wz\sqrt{k} - 2xy\sqrt{mn})\\
&= \frac{1}{4}(w^2 - x^2m - y^2n + z^2k) + \frac{1}{4}(2wz - 2xyd)\sqrt{k}.
\end{aligned}$$

สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

Taking into account that $\mathcal{O}_{\mathbb{Q}[\sqrt{m}]} = \mathbb{Z}\cdot 1 \oplus \mathbb{Z}\cdot\sqrt{m}$, $\mathcal{O}_{\mathbb{Q}[\sqrt{n}]} = \mathbb{Z}\cdot 1 \oplus \mathbb{Z}\cdot\sqrt{n}$ and $\mathcal{O}_{\mathbb{Q}[\sqrt{k}]} = \mathbb{Z}\cdot 1 \oplus \mathbb{Z}\cdot\sqrt{k}$ again, then

$$\begin{aligned}
&\frac{1}{4}(w^2 + x^2m - y^2n - z^2k) + \frac{1}{4}(2wx - 2yz\frac{n}{d})\sqrt{m} \in \mathbb{Z}\cdot 1 \oplus \mathbb{Z}\cdot\sqrt{m},\\
&\frac{1}{4}(w^2 - x^2m + y^2n - z^2k) + \frac{1}{4}(2wy - 2xz\frac{m}{d})\sqrt{n} \in \mathbb{Z}\cdot 1 \oplus \mathbb{Z}\cdot\sqrt{n},\\
&\frac{1}{4}(w^2 - x^2m - y^2n + z^2k) + \frac{1}{4}(2wz - 2xyd)\sqrt{k} \in \mathbb{Z}\cdot 1 \oplus \mathbb{Z}\cdot\sqrt{k}.
\end{aligned}$$

Hence we have

$$\begin{aligned}
&4 \mid (w^2 + x^2m - y^2n - z^2k) && (1)\\
&4 \mid (w^2 - x^2m + y^2n - z^2k) && (2)\\
&4 \mid (w^2 - x^2m - y^2n + z^2k) && (3)\\
&2 \mid (wx - yz\frac{n}{d}) && (4)\\
&2 \mid (wy - xz\frac{m}{d}) && (5)\\
\text{and}\quad &2 \mid (wz - xyd). && (6)
\end{aligned}$$

Since n is even and m is odd, d is odd and $\frac{n}{d}$ is even, by (4) so we have $2 \mid wx$. Hence $2 \mid w$ or $2 \mid x$. By (2) and (3) we have $4 \mid (2w^2 - 2x^2m)$, so $2 \mid (w^2 - x^2m)$. Since one of w or x is divided by 2, and m is odd, then another one must be divided by 2. Hence w and x are even. From (2) we have $4 \mid (y^2n - z^2k)$, which means that $y^2n \equiv z^2k \pmod 4$. Since $n \equiv k \equiv 2 \pmod 4$, we obtain that $2y^2 \equiv 2z^2 \pmod 4$, i.e. $y^2 \equiv z^2 \pmod 2$ which means that $y \equiv z \pmod 2$. Thus in this case, we have that every element in $\mathcal{O}_K$ is of the form $a_0 + a_1\sqrt{m} + \frac{1}{2}(a_2\sqrt{n} + a_3\sqrt{k})$ where $a_i \in \mathbb{Z}$ and $a_2 \equiv a_3 \pmod 2$. Since $a_0 + a_1\sqrt{m} + \frac{1}{2}(a_2\sqrt{n} + a_3\sqrt{k}) = a_0 + a_1\sqrt{m} + \frac{a_2-a_3}{2}\sqrt{n} + a_3(\frac{\sqrt{n}+\sqrt{k}}{2})$,$\mathcal{O}_K \subseteq \mathbb{Z}\cdot 1 \oplus \mathbb{Z}\cdot\sqrt{m} \oplus \mathbb{Z}\cdot\sqrt{n} \oplus \mathbb{Z}\cdot\frac{\sqrt{n}+\sqrt{k}}{2}$. For the converse we can see that $\frac{\sqrt{n}+\sqrt{k}}{2}$ satisfies $(x^2 - (\frac{n+k}{4}))^2 - \frac{nk}{4} \in \mathbb{Z}[x]$. Then $\frac{\sqrt{n}+\sqrt{k}}{2} \in \mathcal{O}_K$. Since $\{1, \sqrt{m}, \sqrt{n}, \frac{\sqrt{n}+\sqrt{k}}{2}\}$ is linearly independent over $\mathbb{Q}$ (so over $\mathbb{Z}$), it is an integral basis of $\mathbb{Q}[\sqrt{m}, \sqrt{n}]$.

สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

(ii) $m \equiv 1, n \equiv k \equiv 2$ or $3 \pmod 4$.

Let $\alpha \in \mathcal{O}_K$, so $\alpha = r_0 + r_1\sqrt{m} + r_2\sqrt{n} + r_3\sqrt{k}$ where $r_0, r_1, r_2, r_3 \in \mathbb{Q}$. Then

$$\begin{aligned}\sigma_2(\alpha) &= r_0 + r_1\sqrt{m} - r_2\sqrt{n} - r_3\sqrt{k},\\ \sigma_3(\alpha) &= r_0 - r_1\sqrt{m} + r_2\sqrt{n} - r_3\sqrt{k},\\ \sigma_4(\alpha) &= r_0 - r_1\sqrt{m} - r_2\sqrt{n} + r_3\sqrt{k}.\end{aligned}$$

Since $\alpha \in \mathcal{O}_K$, $\mathrm{Tr}_{K/\mathbb{Q}[\sqrt{m}]}(\alpha) \in \mathcal{O}_{\mathbb{Q}[\sqrt{m}]}$, $\mathrm{Tr}_{K/\mathbb{Q}[\sqrt{n}]}(\alpha) \in \mathcal{O}_{\mathbb{Q}[\sqrt{n}]}$, $\mathrm{Tr}_{K/\mathbb{Q}[\sqrt{k}]}(\alpha) \in \mathcal{O}_{\mathbb{Q}[\sqrt{k}]}$. We express these conditions in terms of the coefficients of α:

$$\begin{aligned}\mathrm{Tr}_{K/\mathbb{Q}[\sqrt{m}]}(\alpha) = \alpha + \sigma_2(\alpha) = 2r_0 + 2r_1\sqrt{m} &= (2r_0 - 2r_1) + 4r_1(\frac{1+\sqrt{m}}{2}) \in \mathcal{O}_{\mathbb{Q}[\sqrt{m}]},\\ \mathrm{Tr}_{K/\mathbb{Q}[\sqrt{n}]}(\alpha) = \alpha + \sigma_3(\alpha) &= 2r_0 + 2r_2\sqrt{n} \in \mathcal{O}_{\mathbb{Q}[\sqrt{n}]},\\ \mathrm{Tr}_{K/\mathbb{Q}[\sqrt{k}]}(\alpha) = \alpha + \sigma_4(\alpha) &= 2r_0 + 2r_3\sqrt{k} \in \mathcal{O}_{\mathbb{Q}[\sqrt{k}]}.\end{aligned}$$

Taking into account that $\mathcal{O}_{\mathbb{Q}[\sqrt{m}]} = \mathbb{Z}\cdot 1 \oplus \mathbb{Z}\cdot\frac{1+\sqrt{m}}{2}$, $\mathcal{O}_{\mathbb{Q}[\sqrt{n}]} = \mathbb{Z}\cdot 1 \oplus \mathbb{Z}\cdot\sqrt{n}$ and $\mathcal{O}_{\mathbb{Q}[\sqrt{k}]} = \mathbb{Z}\cdot 1 \oplus \mathbb{Z}\cdot\sqrt{k}$, we obtain that

$$\begin{aligned}(2r_0 - 2r_1) + 4r_1(\frac{1+\sqrt{m}}{2}) &\in \mathbb{Z}\cdot 1 \oplus \mathbb{Z}\cdot\frac{1+\sqrt{m}}{2},\\ 2r_0 + 2r_2\sqrt{n} &\in \mathbb{Z}\cdot 1 \oplus \mathbb{Z}\cdot\sqrt{n},\\ 2r_0 + 2r_3\sqrt{k} &\in \mathbb{Z}\cdot 1 \oplus \mathbb{Z}\cdot\sqrt{k}.\end{aligned}$$

Hence $2r_0 - 2r_1 \in \mathbb{Z}, 4r_1 \in \mathbb{Z}, 2r_2 \in \mathbb{Z}$ and $2r_3 \in \mathbb{Z}$. Since $2r_0 - 2r_1 \in \mathbb{Z}$ and $4r_1 \in \mathbb{Z}$, we implies $4r_0 \in \mathbb{Z}$. From these relations we deduce $\alpha = r_0 + r_1\sqrt{m} + r_2\sqrt{n} + r_3\sqrt{k} = \frac{1}{4}(w + x\sqrt{m} + 2y\sqrt{n} + 2z\sqrt{k})$ where $w, x, y, z \in \mathbb{Z}$. Since $\alpha \in \mathcal{O}_K$, $\mathrm{N}_{K/\mathbb{Q}[\sqrt{m}]}(\alpha) \in \mathcal{O}_{\mathbb{Q}[\sqrt{m}]}$, $\mathrm{N}_{K/\mathbb{Q}[\sqrt{n}]}(\alpha) \in \mathcal{O}_{\mathbb{Q}[\sqrt{n}]}$, $\mathrm{N}_{K/\mathbb{Q}[\sqrt{k}]}(\alpha) \in \mathcal{O}_{\mathbb{Q}[\sqrt{k}]}$.

สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

We express these conditions in terms of the coefficients of α:

$$\begin{aligned}
\mathrm{N}_{K/\mathbb{Q}[\sqrt{m}]}(\alpha) &= \alpha\cdot\sigma_2(\alpha) = \frac{1}{16}(w+x\sqrt{m})^2 - \frac{1}{16}(2y\sqrt{n}+2z\sqrt{k})^2\\
&= \frac{1}{16}(w^2+x^2m-4y^2n-4z^2k) + \frac{1}{16}(2wx\sqrt{m}-8yz\sqrt{nk})\\
&= \frac{1}{16}(w^2+x^2m-4y^2n-4z^2k) + \frac{1}{16}(2wx-8yz\frac{n}{d})\sqrt{m}\\
&= \frac{1}{16}(w^2+x^2m-4y^2n-4z^2k-2wx+8yz\frac{n}{d})\\
&\quad + \frac{1}{16}(4wx-16yz\frac{n}{d})(\frac{1+\sqrt{m}}{2}),\\
\mathrm{N}_{K/\mathbb{Q}[\sqrt{n}]}(\alpha) &= \alpha\cdot\sigma_3(\alpha) = \frac{1}{16}(w+2y\sqrt{n})^2 - \frac{1}{16}(x\sqrt{m}+2z\sqrt{k})^2\\
&= \frac{1}{16}(w^2-x^2m+4y^2n-4z^2k) + \frac{1}{16}(4wy\sqrt{n}-4xz\sqrt{mk})\\
&= \frac{1}{16}(w^2-x^2m+4y^2n-4z^2k) + \frac{1}{16}(4wy-4xz\frac{m}{d})\sqrt{n},\\
\mathrm{N}_{K/\mathbb{Q}[\sqrt{k}]}(\alpha) &= \alpha\cdot\sigma_4(\alpha) = \frac{1}{16}(w+2z\sqrt{k})^2 - \frac{1}{16}(x\sqrt{m}+2y\sqrt{n})^2\\
&= \frac{1}{16}(w^2-x^2m-4y^2n+4z^2k) + \frac{1}{16}(4wz\sqrt{k}-4xy\sqrt{mn})\\
&= \frac{1}{16}(w^2-x^2m-4y^2n+4z^2k) + \frac{1}{16}(4wz-4xyd)\sqrt{k}.
\end{aligned}$$

Taking into account that $\mathcal{O}_{\mathbb{Q}[\sqrt{m}]} = \mathbb{Z}\cdot 1 \oplus \mathbb{Z}\cdot\frac{1+\sqrt{m}}{2}$, $\mathcal{O}_{\mathbb{Q}[\sqrt{n}]} = \mathbb{Z}\cdot 1\oplus\mathbb{Z}\cdot\sqrt{n}$ and $\mathcal{O}_{\mathbb{Q}[\sqrt{k}]} = \mathbb{Z}\cdot 1\oplus\mathbb{Z}\cdot\sqrt{k}$ again, then

$$\begin{aligned}
&\frac{1}{16}(w^2+x^2m-4y^2n-4z^2k-2wx+8yz\frac{n}{d})\\
&\qquad + \frac{1}{16}(4wx-16yz\frac{n}{d})(\frac{1+\sqrt{m}}{2}) \in \mathbb{Z}\cdot 1\oplus\mathbb{Z}\cdot\frac{1+\sqrt{m}}{2},\\
&\frac{1}{16}(w^2-x^2m+4y^2n-4z^2k) + \frac{1}{16}(4wy-4xz\frac{m}{d})\sqrt{n} \in \mathbb{Z}\cdot 1\oplus\mathbb{Z}\cdot\sqrt{n},\\
&\frac{1}{16}(w^2-x^2m-4y^2n+4z^2k) + \frac{1}{16}(4wz-4xyd)\sqrt{k} \in \mathbb{Z}\cdot 1\oplus\mathbb{Z}\cdot\sqrt{k}.
\end{aligned}$$

สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

Hence we have

$$16 \mid (w^2 + x^2m - 4y^2n - 4z^2k - 2wx + 8yz\frac{n}{d}) \tag{7}$$

$$16 \mid (w^2 - x^2m + 4y^2n - 4z^2k) \tag{8}$$

$$16 \mid (w^2 - x^2m - 4y^2n + 4z^2k) \tag{9}$$

$$4 \mid (wx - 4yz\frac{n}{d}) \tag{10}$$

$$4 \mid (wy - xz\frac{m}{d}) \tag{11}$$

$$\text{and} \qquad 4 \mid (wz - xyd). \tag{12}$$

From (10) we have $4 \mid wx$. Suppose that w and x do not have same parity, so exactly one of them divided by 4. Without loss of generality say $4 \mid w$. By (11) and (12) we have $4 \mid z$ and $4 \mid y$, respectively. Then w^2, y^2, z^2 are divided by 16, then by (9) we have $16 \mid x^2m$. Since m is odd and $16 \mid x^2m$, this means that w and x have the same parity which is a contradiction. Hence w and x are even. Then $w = 2w'$ and $x = 2x'$ for some $w', x' \in \mathbb{Z}$.

Thus by (7)-(9) we have

$$4 \mid (w'^2 + x'^2m - y^2n - z^2k - 2w'x' + 2yz\frac{n}{d}) \tag{13}$$

$$4 \mid (w'^2 - x'^2m + y^2n - z^2k) \tag{14}$$

$$\text{and} \qquad 4 \mid (w'^2 - x'^2m - y^2n + z^2k). \tag{15}$$

From (14) and (15), we have $4 \mid (2w'^2 - 2x'^2)$, then $2 \mid (w'^2 - x'^2)$ which implies that $w' \equiv x' \pmod 2$. Hence $w'^2 \equiv x'^2 \equiv x'^2m \pmod 4$ and so $4 \mid y^2n - z^2k$. Since $n \equiv k \equiv 2 \pmod 4$ and $4 \mid y^2n - z^2k$, we obtain that $4 \mid 2y^2 - 2z^2$, so $y \equiv z \pmod 2$. In this case, we have that every element in $\mathcal{O}_K$ is of the form $\frac{1}{2}(w' + x'\sqrt{m} + y\sqrt{n} + z\sqrt{k})$ where $w', x', y, z \in \mathbb{Z}$, $w' \equiv x' \pmod 2$ and $y \equiv z \pmod 2$. Since $\frac{1}{2}(w' + x'\sqrt{m} + y\sqrt{n} + z\sqrt{k}) = \frac{w'-x'}{2}(1) + x'(\frac{1+\sqrt{m}}{2}) + \frac{y-z}{2}(\sqrt{n}) + z(\frac{\sqrt{n}+\sqrt{k}}{2}) \in \mathbb{Z}\cdot 1 \oplus \mathbb{Z}\cdot\frac{1+\sqrt{m}}{2} \oplus \mathbb{Z}\cdot\sqrt{n} \oplus \mathbb{Z}\cdot\frac{\sqrt{n}+\sqrt{k}}{2}$. For the converse we can see that $\frac{\sqrt{n}+\sqrt{k}}{2}$ satisfies $(x^2 - (\frac{n+k}{4}))^2 - \frac{nk}{4} \in \mathbb{Z}[x]$. Then $\frac{\sqrt{n}+\sqrt{k}}{2} \in \mathcal{O}_K$. Since $\{1, \frac{1+\sqrt{m}}{2}, \sqrt{n}, \frac{\sqrt{n}+\sqrt{k}}{2}\}$ is linearly independent over $\mathbb{Q}$ (so over $\mathbb{Z}$), it is an integral

ศูนย์วิทยทรัพยากร
จุฬาลงกรณ์มหาวิทยาลัย

basis of $\mathbb{Q}[\sqrt{m}, \sqrt{n}]$.

(iii) $m \equiv n \equiv k \equiv 1 \pmod 4$.

Let $\alpha \in \mathcal{O}_K$, so $\alpha = r_0 + r_1\sqrt{m} + r_2\sqrt{n} + r_3\sqrt{k}$ where $r_0, r_1, r_2, r_3 \in \mathbb{Q}$. Then

$$\begin{aligned}
\sigma_2(\alpha) &= r_0 + r_1\sqrt{m} - r_2\sqrt{n} - r_3\sqrt{k},\\
\sigma_3(\alpha) &= r_0 - r_1\sqrt{m} + r_2\sqrt{n} - r_3\sqrt{k},\\
\sigma_4(\alpha) &= r_0 - r_1\sqrt{m} - r_2\sqrt{n} + r_3\sqrt{k}.
\end{aligned}$$

Since $\alpha \in \mathcal{O}_K$, $\mathrm{Tr}_{K/\mathbb{Q}[\sqrt{m}]}(\alpha) \in \mathcal{O}_{\mathbb{Q}[\sqrt{m}]}$, $\mathrm{Tr}_{K/\mathbb{Q}[\sqrt{n}]}(\alpha) \in \mathcal{O}_{\mathbb{Q}[\sqrt{n}]}$, $\mathrm{Tr}_{K/\mathbb{Q}[\sqrt{k}]}(\alpha) \in \mathcal{O}_{\mathbb{Q}[\sqrt{k}]}$. We express these conditions in terms of the coefficients of α:

$$\begin{aligned}
\mathrm{Tr}_{K/\mathbb{Q}[\sqrt{m}]}(\alpha) &= \alpha + \sigma_2(\alpha) = 2r_0 + 2r_1\sqrt{m} = (2r_0 - 2r_1) + 4r_1(\frac{1+\sqrt{m}}{2}) \in \mathcal{O}_{\mathbb{Q}[\sqrt{m}]},\\
\mathrm{Tr}_{K/\mathbb{Q}[\sqrt{n}]}(\alpha) &= \alpha + \sigma_3(\alpha) = 2r_0 + 2r_2\sqrt{n} = (2r_0 - 2r_2) + 4r_2(\frac{1+\sqrt{n}}{2}) \in \mathcal{O}_{\mathbb{Q}[\sqrt{n}]},\\
\mathrm{Tr}_{K/\mathbb{Q}[\sqrt{k}]}(\alpha) &= \alpha + \sigma_4(\alpha) = 2r_0 + 2r_3\sqrt{k} = (2r_0 - 2r_3) + 4r_3(\frac{1+\sqrt{k}}{2}) \in \mathcal{O}_{\mathbb{Q}[\sqrt{k}]}.
\end{aligned}$$

Taking into account that $\mathcal{O}_{\mathbb{Q}[\sqrt{m}]} = \mathbb{Z}\cdot 1 \oplus \mathbb{Z}\cdot \frac{1+\sqrt{m}}{2}$, $\mathcal{O}_{\mathbb{Q}[\sqrt{n}]} = \mathbb{Z}\cdot 1 \oplus \mathbb{Z}\cdot \frac{1+\sqrt{n}}{2}$ and $\mathcal{O}_{\mathbb{Q}[\sqrt{k}]} = \mathbb{Z}\cdot 1 \oplus \mathbb{Z}\cdot \frac{1+\sqrt{k}}{2}$. We obtain that

$$\begin{aligned}
(2r_0 - 2r_1) + 4r_1(\frac{1+\sqrt{m}}{2}) &\in \mathbb{Z}\cdot 1 \oplus \mathbb{Z}\cdot \frac{1+\sqrt{m}}{2},\\
(2r_0 - 2r_2) + 4r_2(\frac{1+\sqrt{n}}{2}) &\in \mathbb{Z}\cdot 1 \oplus \mathbb{Z}\cdot \frac{1+\sqrt{n}}{2},\\
(2r_0 - 2r_3) + 4r_3(\frac{1+\sqrt{k}}{2}) &\in \mathbb{Z}\cdot 1 \oplus \mathbb{Z}\cdot \frac{1+\sqrt{k}}{2}.
\end{aligned}$$

Hence $2r_0 - 2r_1 \in \mathbb{Z}, 2r_0 - 2r_2 \in \mathbb{Z}, 2r_0 - 2r_3 \in \mathbb{Z}, 4r_1 \in \mathbb{Z}, 4r_2 \in \mathbb{Z}$ and $4r_3 \in \mathbb{Z}$. Since $2r_0 - 2r_1 \in \mathbb{Z}$ and $4r_1 \in \mathbb{Z}$, $4r_0 \in \mathbb{Z}$. From these relations we deduce $\alpha = r_0 + r_1\sqrt{m} + r_2\sqrt{n} + r_3\sqrt{k} = \frac{1}{4}(w + x\sqrt{m} + y\sqrt{n} + z\sqrt{k})$ where $w, x, y, z \in \mathbb{Z}$. Since $\alpha \in \mathcal{O}_K$, $\mathrm{N}_{K/\mathbb{Q}[\sqrt{m}]}(\alpha) \in \mathcal{O}_{\mathbb{Q}[\sqrt{m}]}$, $\mathrm{N}_{K/\mathbb{Q}[\sqrt{n}]}(\alpha) \in \mathcal{O}_{\mathbb{Q}[\sqrt{n}]}$, $\mathrm{N}_{K/\mathbb{Q}[\sqrt{k}]}(\alpha) \in \mathcal{O}_{\mathbb{Q}[\sqrt{k}]}$.

สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

We express these conditions in terms of the coefficients of α:

$$\begin{aligned}
\mathrm{N}_{K/\mathbb{Q}[\sqrt{m}]}(\alpha) = \alpha\cdot\sigma_2(\alpha) &= \frac{1}{16}(w+x\sqrt{m})^2 - \frac{1}{16}(y\sqrt{n}+z\sqrt{k})^2 \\
&= \frac{1}{16}(w^2+x^2m-y^2n-z^2k) + \frac{1}{16}(2wx\sqrt{m}-2yz\sqrt{nk}) \\
&= \frac{1}{16}(w^2+x^2m-y^2n-z^2k) + \frac{1}{16}(2wx-2yz\frac{n}{d})\sqrt{m} \\
&= \frac{1}{16}(w^2+x^2m-y^2n-z^2k-2wx+2yz\frac{n}{d}) \\
&\quad + \frac{1}{16}(4wx-4yz\frac{n}{d})(\frac{1+\sqrt{m}}{2}), \\
\mathrm{N}_{K/\mathbb{Q}[\sqrt{n}]}(\alpha) = \alpha\cdot\sigma_3(\alpha) &= \frac{1}{16}(w+y\sqrt{n})^2 - \frac{1}{16}(x\sqrt{m}+z\sqrt{k})^2 \\
&= \frac{1}{16}(w^2-x^2m+y^2n-z^2k) + \frac{1}{16}(2wy\sqrt{n}-2xz\sqrt{mk}) \\
&= \frac{1}{16}(w^2-x^2m+y^2n-z^2k) + \frac{1}{16}(2wy-2xz\frac{m}{d})\sqrt{n} \\
&= \frac{1}{16}(w^2-x^2m+y^2n-z^2k-2wy+2xz\frac{m}{d}) \\
&\quad + \frac{1}{16}(4wy-4xz\frac{m}{d})(\frac{1+\sqrt{n}}{2}), \\
\mathrm{N}_{K/\mathbb{Q}[\sqrt{k}]}(\alpha) = \alpha\cdot\sigma_4(\alpha) &= \frac{1}{16}(w+z\sqrt{k})^2 - \frac{1}{16}(x\sqrt{m}+y\sqrt{n})^2 \\
&= \frac{1}{16}(w^2-x^2m-y^2n+z^2k) + \frac{1}{16}(2wz\sqrt{k}-2xy\sqrt{mn}) \\
&= \frac{1}{16}(w^2-x^2m-y^2n+z^2k) + \frac{1}{16}(2wz-2xyd)\sqrt{k} \\
&= \frac{1}{16}(w^2-x^2m-y^2n+z^2k-2wz+2xyd) \\
&\quad + \frac{1}{16}(4wz-4xyd)(\frac{1+\sqrt{k}}{2}).
\end{aligned}$$

Taking into account that $\mathcal{O}_{\mathbb{Q}[\sqrt{m}]} = \mathbb{Z}\cdot 1 \oplus \mathbb{Z}\cdot\frac{1+\sqrt{m}}{2}$, $\mathcal{O}_{\mathbb{Q}[\sqrt{n}]} = \mathbb{Z}\cdot 1 \oplus \mathbb{Z}\cdot\frac{1+\sqrt{n}}{2}$ and $\mathcal{O}_{\mathbb{Q}[\sqrt{k}]} = \mathbb{Z}\cdot 1 \oplus \mathbb{Z}\cdot\frac{1+\sqrt{k}}{2}$ again, then

$$\begin{aligned}
&\frac{1}{16}(w^2+x^2m-y^2n-z^2k-2wx+2yz\frac{n}{d}) \\
&\qquad + \frac{1}{16}(4wx-4yz\frac{n}{d})(\frac{1+\sqrt{m}}{2}) \in \mathbb{Z}\cdot 1 \oplus \mathbb{Z}\cdot\frac{1+\sqrt{m}}{2},
\end{aligned}$$

$$\begin{aligned}
&\frac{1}{16}(w^2 - x^2m + y^2n - z^2k - 2wy + 2xz\frac{m}{d}) \\
&\quad + \frac{1}{16}(4wy - 4xz\frac{m}{d})(\frac{1+\sqrt{n}}{2}) \in \mathbb{Z}\cdot 1 \oplus \mathbb{Z}\cdot\frac{1+\sqrt{n}}{2}, \\
&\frac{1}{16}(w^2 - x^2m - y^2n + z^2k - 2wz + 2xyd) \\
&\quad + \frac{1}{16}(4wz - 4xyd)(\frac{1+\sqrt{k}}{2}) \in \mathbb{Z}\cdot 1 \oplus \mathbb{Z}\cdot\frac{1+\sqrt{k}}{2}.
\end{aligned}$$

Hence we have

$$16 \mid (w^2 + x^2m - y^2n - z^2k - 2wx + 2yz\frac{n}{d}) \tag{16}$$

$$16 \mid (w^2 - x^2m + y^2n - z^2k - 2wy + 2xz\frac{m}{d}) \tag{17}$$

$$16 \mid (w^2 - x^2m - y^2n + z^2k - 2wz + 2xyd) \tag{18}$$

$$4 \mid (wx - yz\frac{n}{d}) \tag{19}$$

$$4 \mid (wy - xz\frac{m}{d}) \tag{20}$$

$$\text{and} \qquad 4 \mid (wz - xyd). \tag{21}$$

Case1 w is odd. From (19) and $\frac{n}{d}$ is odd, we obtain that x and yz have the same parity. Suppose that x is even. By (20) and (21) y and z are even, so we have $4 \mid yz$. Through this result to (19) we have that $4 \mid x$. Similarly, by (20) and (21) we have $4 \mid y$ and $4 \mid z$. Then by (16) we obtain that $16 \mid w^2 - 2wx$, i.e. $w^2 - 2wx$ is even which contradicts the fact that w is odd. Thus x is odd. Similarly we can show that y and z are also odd.

Case2 w is even. If one of x, y, z is odd, then anothers are even and similarly to Case1, which leads to a contradiction. Thus x, y, z are even.

Hence in any cases, we have $w \equiv x \equiv y \equiv z \pmod 2$.

In this case, we have that every element in $\mathcal{O}_K$ is of the form $\frac{1}{4}(w + x\sqrt{m} + y\sqrt{n} + z\sqrt{k})$ where $w \equiv x \equiv y \equiv z \pmod 2$.

ศูนย์วิทยทรัพยากร
จุฬาลงกรณ์มหาวิทยาลัย

Since $\frac{1+\sqrt{m}}{2}$ and $\frac{1+\sqrt{k}}{2}$ are in $\mathcal{O}_K$, $\alpha =: \alpha' + z(\frac{1+\sqrt{m}}{2})(\frac{1+\sqrt{k}}{2}) \in \mathcal{O}_K$, we have

$$\begin{aligned}
\alpha' &= \frac{1}{4}(w + x\sqrt{m} + y\sqrt{n} + z\sqrt{k}) - z(\frac{1+\sqrt{m}}{2})(\frac{1+\sqrt{k}}{2}) \\
&= \frac{1}{4}(w + x\sqrt{m} + y\sqrt{n} + z\sqrt{k} - z - z\sqrt{m} - z\sqrt{k} - z\sqrt{mk}) \\
&= \frac{1}{4}((w-z) + (x-z)\sqrt{m} + (y - z\frac{m}{d})\sqrt{n}) \\
&= \frac{1}{2}(\frac{w-z}{2} + \frac{x-z}{2}\sqrt{m} + \frac{y-z\frac{m}{d}}{2}\sqrt{n}).
\end{aligned}$$

Since $w \equiv x \equiv y \equiv z \pmod 2$, $a = \frac{w-z}{2} \in \mathbb{Z}, b = \frac{x-z}{2} \in \mathbb{Z}$ and $c = \frac{y-z\frac{m}{d}}{2} \in \mathbb{Z}$, we have $\alpha' = \frac{1}{2}(a + b\sqrt{m} + c\sqrt{n})$. Claim that $a + b + c \equiv 0 \pmod 2$.

Since $\alpha' \in \mathcal{O}_K$,$\mathrm{N}_{K/\mathbb{Q}[\sqrt{m}]}(\alpha) \in \mathcal{O}_{\mathbb{Q}[\sqrt{m}]}$, $\mathrm{N}_{K/\mathbb{Q}[\sqrt{n}]}(\alpha) \in \mathcal{O}_{\mathbb{Q}[\sqrt{n}]}$, $\mathrm{N}_{K/\mathbb{Q}[\sqrt{k}]}(\alpha) \in \mathcal{O}_{\mathbb{Q}[\sqrt{k}]}$. We express these conditions in terms of the coefficients of α:

$$\begin{aligned}
\mathrm{N}_{K/\mathbb{Q}[\sqrt{m}]}(\alpha') &= \alpha' \cdot \sigma_2(\alpha') = \frac{1}{4}(a + b\sqrt{m})^2 - \frac{1}{4}(c\sqrt{n})^2 \\
&= \frac{1}{4}(a^2 + b^2m - c^2n) + \frac{1}{4}(2ab\sqrt{m}) \\
&= \frac{1}{4}(a^2 + b^2m - c^2n - 2ab) + ab(\frac{1+\sqrt{m}}{2}), \\
\mathrm{N}_{K/\mathbb{Q}[\sqrt{n}]}(\alpha') &= \alpha' \cdot \sigma_3(\alpha') = \frac{1}{4}(a + c\sqrt{n})^2 - \frac{1}{4}(b\sqrt{m})^2 \\
&= \frac{1}{4}(a^2 + b^2m - c^2n) + \frac{1}{4}(2ac\sqrt{n}) \\
&= \frac{1}{4}(a^2 + b^2m - c^2n - 2ac) + ac(\frac{1+\sqrt{n}}{2}), \\
\mathrm{N}_{K/\mathbb{Q}[\sqrt{k}]}(\alpha') &= \alpha' \cdot \sigma_4(\alpha') = \frac{1}{4}(a)^2 - \frac{1}{4}(b\sqrt{m} + c\sqrt{n})^2 \\
&= \frac{1}{4}(a^2 - b^2m - c^2n) - \frac{1}{4}(2bcd\sqrt{k}) \\
&= \frac{1}{4}(a^2 - b^2m - c^2n + 2bcd) - bcd(\frac{1+\sqrt{k}}{2}).
\end{aligned}$$

สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

Taking into account that $\mathcal{O}_{\mathbb{Q}[\sqrt{m}]} = \mathbb{Z}\cdot 1 \oplus \mathbb{Z}\cdot \dfrac{1+\sqrt{m}}{2}$, $\mathcal{O}_{\mathbb{Q}[\sqrt{n}]} = \mathbb{Z}\cdot 1 \oplus \mathbb{Z}\cdot \dfrac{1+\sqrt{n}}{2}$ and $\mathcal{O}_{\mathbb{Q}[\sqrt{k}]} = \mathbb{Z}\cdot 1 \oplus \mathbb{Z}\cdot \dfrac{1+\sqrt{k}}{2}$ again, then

$$4 \mid (a^2 + b^2m - c^2n - 2ab) \tag{22}$$

$$4 \mid (a^2 - b^2m + c^2n - 2ac) \tag{23}$$

$$4 \mid (a^2 - b^2m - c^2n + 2bcd). \tag{24}$$

By (22), (23) and (24),we obtain that

$$\begin{aligned}
&4 \mid (a^2 + b^2m - c^2n - 2ab) - (a^2 - b^2m + c^2n - 2ac) + (a^2 - b^2m - c^2n + 2bcd)\\
&4 \mid (a^2 - b^2m - c^2n - 2ab - 2ac + 2bcd)\\
&4 \mid (a^2 - b^2m - c^2n - 2ab - 2ac + 2bc) + (2bcd - 2bc)\\
&4 \mid (a-b-c)^2 + 2bc(d-1)\\
&4 \mid (a-b-c)^2 \qquad \text{since } d \text{ is odd.}
\end{aligned}$$

Hence $(a-b-c) \equiv 0 \pmod 2$, also we have $(a+b+c) \equiv 0 \pmod 2$.

In this case, we have that every element in $\mathcal{O}_K$ is of the form $\alpha = \alpha' + z(\frac{1+\sqrt{m}}{2})(\frac{1+\sqrt{k}}{2})$, we have

$$\begin{aligned}
\alpha &= \alpha' + z(\frac{1+\sqrt{m}}{2})(\frac{1+\sqrt{k}}{2})\\
&= \frac{1}{2}(a + b\sqrt{m} + c\sqrt{n}) + z(\frac{1+\sqrt{m}}{2})(\frac{1+\sqrt{k}}{2})\\
&= \frac{1}{2}((a-b-c) + (2b)(\frac{1+\sqrt{m}}{2}) + (2c)(\frac{1+\sqrt{n}}{2})) + z(\frac{1+\sqrt{m}}{2})(\frac{1+\sqrt{k}}{2})\\
&= \frac{a-b-c}{2}\cdot 1 + b\cdot(\frac{1+\sqrt{m}}{2}) + c\cdot(\frac{1+\sqrt{n}}{2}) + z(\frac{1+\sqrt{m}}{2})(\frac{1+\sqrt{k}}{2})\\
&\quad \in \mathbb{Z}\cdot 1 \oplus \mathbb{Z}\cdot\frac{1+\sqrt{m}}{2} \oplus \mathbb{Z}\cdot\frac{1+\sqrt{n}}{2} \oplus \mathbb{Z}\cdot(\frac{1+\sqrt{m}}{2})(\frac{1+\sqrt{k}}{2}).
\end{aligned}$$

Hence $\mathcal{O}_K \subseteq \mathbb{Z}\cdot 1 \oplus \mathbb{Z}\cdot \frac{1+\sqrt{m}}{2} \oplus \mathbb{Z}\cdot \frac{1+\sqrt{n}}{2} \oplus \mathbb{Z}\cdot (\frac{1+\sqrt{m}}{2})(\frac{1+\sqrt{k}}{2})$. For the converse we can see that $(\frac{1+\sqrt{m}}{2})(\frac{1+\sqrt{k}}{2}) \in \mathcal{O}_K$, since $\frac{1+\sqrt{m}}{2} \in \mathcal{O}_K$ and $\frac{1+\sqrt{k}}{2} \in \mathcal{O}_K$. Since $\{1, \frac{1+\sqrt{m}}{2}, \frac{1+\sqrt{2}}{2}, (\frac{1+\sqrt{m}}{2})(\frac{1+\sqrt{k}}{2})\}$is linearly independent over $\mathbb{Q}$ (so over $\mathbb{Z}$), it is an integral basis of $\mathbb{Q}[\sqrt{m}, \sqrt{n}]$. The proof is complete. □

Next, we will find the discriminant in all cases.

Lemma 3.2.2. *Let $a, b, c \in \mathbb{R}$. Then* $\begin{vmatrix} 1 & a & b & c \\ 1 & a & -b & -c \\ 1 & -a & b & -c \\ 1 & -a & -b & c \end{vmatrix} = -16abc.$

Proof.

$$\begin{vmatrix} 1 & a & b & c \\ 1 & a & -b & -c \\ 1 & -a & b & -c \\ 1 & -a & -b & c \end{vmatrix} = \left|\begin{matrix} 4 & 0 & 0 & 0 \\ 1 & a & -b & -c \\ 1 & -a & b & -c \\ 1 & -a & -b & c \end{matrix}\right| \begin{matrix} R_1 + R_2 + R_3 + R_4 \\ \\ \\ \\ \end{matrix}$$

$$= \left|\begin{matrix} 4 & 0 & 0 & 0 \\ 2 & 0 & -2b & 0 \\ 2 & -2a & 0 & 0 \\ 1 & -a & -b & c \end{matrix}\right| \begin{matrix} \\ R_2 + R_4 \\ R_3 + R_4 \\ \\ \end{matrix}$$

$$= 4 \begin{vmatrix} 0 & -2b & 0 \\ -2a & 0 & 0 \\ -a & -b & c \end{vmatrix} = 4c \begin{vmatrix} 0 & -2b \\ -2a & 0 \end{vmatrix} = -16abc.$$

□

สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

Theorem 3.2.3. *Let* $K = \mathbb{Q}[\sqrt{m}, \sqrt{n}]$ *where* m *and* n *are distinct squarefree integers and* $k = \dfrac{mn}{d^2}$ *where* $d = (m, n)$.

(i) *If* $m \equiv 3, n \equiv k \equiv 2 \pmod 4$, *then* $\delta_K = 64mnk$,

(ii) *If* $m \equiv 1, n \equiv k \equiv 2$ *or* $3 \pmod 4$, *then* $\delta_K = 16mnk$,

(iii) *If* $m \equiv n \equiv k \equiv 1 \pmod 4$, *then* $\delta_K = mnk$.

Proof. Recall that $\delta_K = \text{disc}_K(\alpha_1, \ldots, \alpha_n)$ where $\{\alpha_1, \ldots, \alpha_n\}$ is an integral basis of K over $\mathbb{Q}$.

Case1. $m \equiv 3, n \equiv k \equiv 2 \pmod 4$.

Then $\{1, \sqrt{m}, \sqrt{n}, \dfrac{\sqrt{n}+\sqrt{k}}{2}\}$ is an integral basis, so we compute discriminant as follows:

$$\delta_K = \begin{vmatrix} 1 & \sqrt{m} & \sqrt{n} & \dfrac{\sqrt{n}+\sqrt{k}}{2} \\ 1 & \sqrt{m} & -\sqrt{n} & \dfrac{-\sqrt{n}-\sqrt{k}}{2} \\ 1 & -\sqrt{m} & \sqrt{n} & \dfrac{\sqrt{n}-\sqrt{k}}{2} \\ 1 & -\sqrt{m} & -\sqrt{n} & \dfrac{-\sqrt{n}+\sqrt{k}}{2} \end{vmatrix}^2$$

$$= \frac{1}{4} \begin{vmatrix} 1 & \sqrt{m} & \sqrt{n} & \sqrt{n}+\sqrt{k} \\ 1 & \sqrt{m} & -\sqrt{n} & -\sqrt{n}-\sqrt{k} \\ 1 & -\sqrt{m} & \sqrt{n} & \sqrt{n}-\sqrt{k} \\ 1 & -\sqrt{m} & -\sqrt{n} & -\sqrt{n}+\sqrt{k} \end{vmatrix}^2$$

$$= \frac{1}{4} \begin{vmatrix} 1 & \sqrt{m} & \sqrt{n} & \sqrt{k} \\ 1 & \sqrt{m} & -\sqrt{n} & -\sqrt{k} \\ 1 & -\sqrt{m} & \sqrt{n} & -\sqrt{k} \\ 1 & -\sqrt{m} & -\sqrt{n} & \sqrt{k} \end{vmatrix}^2 \; C_4 - C_3$$

$$= \frac{1}{4}(-16\sqrt{m}\sqrt{n}\sqrt{k})^2 = 64mnk \quad \text{(by Lemma 3.2.2).}$$

สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

Case2. $m \equiv 1, n \equiv k \equiv 2$ or $3 \pmod 4$.
Then $\{1, \dfrac{1+\sqrt{m}}{2}, \sqrt{n}, \dfrac{\sqrt{n}+\sqrt{k}}{2}\}$ is an integral basis, so we compute discriminant as follows:

$$\begin{aligned}
\delta_K &= \begin{vmatrix} 1 & \dfrac{1+\sqrt{m}}{2} & \sqrt{n} & \dfrac{\sqrt{n}+\sqrt{k}}{2} \\ 1 & \dfrac{1+\sqrt{m}}{2} & -\sqrt{n} & \dfrac{-\sqrt{n}-\sqrt{k}}{2} \\ 1 & \dfrac{1-\sqrt{m}}{2} & \sqrt{n} & \dfrac{\sqrt{n}-\sqrt{k}}{2} \\ 1 & \dfrac{1-\sqrt{m}}{2} & -\sqrt{n} & \dfrac{-\sqrt{n}+\sqrt{k}}{2} \end{vmatrix}^2 \\
&= \frac{1}{16}\begin{vmatrix} 1 & 1+\sqrt{m} & \sqrt{n} & \sqrt{n}+\sqrt{k} \\ 1 & 1+\sqrt{m} & -\sqrt{n} & -\sqrt{n}-\sqrt{k} \\ 1 & 1-\sqrt{m} & \sqrt{n} & \sqrt{n}-\sqrt{k} \\ 1 & 1-\sqrt{m} & -\sqrt{n} & -\sqrt{n}+\sqrt{k} \end{vmatrix}^2 \\
&= \frac{1}{16}\begin{vmatrix} 1 & \sqrt{m} & \sqrt{n} & \sqrt{k} \\ 1 & \sqrt{m} & -\sqrt{n} & -\sqrt{k} \\ 1 & -\sqrt{m} & \sqrt{n} & -\sqrt{k} \\ 1 & -\sqrt{m} & -\sqrt{n} & \sqrt{k} \end{vmatrix}^2 \begin{matrix} \\ C_2 - C_1 \\ C_4 - C_3 \\ \\ \end{matrix} \\
&= \frac{1}{16}(-16\sqrt{m}\sqrt{n}\sqrt{k})^2 = 16mnk \qquad \text{(by Lemma 3.2.2).}
\end{aligned}$$

สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

Case3. $m \equiv n \equiv k \equiv 1 \pmod 4$.

Then $\{1, \dfrac{1+\sqrt{m}}{2}, \dfrac{1+\sqrt{n}}{2}, (\dfrac{1+\sqrt{m}}{2})(\dfrac{1+\sqrt{k}}{2})\}$ is an integral basis, so we compute discriminant as follows:

$$\delta_K = \begin{vmatrix} 1 & \dfrac{1+\sqrt{m}}{2} & \dfrac{1+\sqrt{n}}{2} & (\dfrac{1+\sqrt{m}}{2})(\dfrac{1+\sqrt{k}}{2}) \\ 1 & \dfrac{1+\sqrt{m}}{2} & \dfrac{1-\sqrt{n}}{2} & (\dfrac{1+\sqrt{m}}{2})(\dfrac{1-\sqrt{k}}{2}) \\ 1 & \dfrac{1-\sqrt{m}}{2} & \dfrac{1+\sqrt{n}}{2} & (\dfrac{1-\sqrt{m}}{2})(\dfrac{1-\sqrt{k}}{2}) \\ 1 & \dfrac{1-\sqrt{m}}{2} & \dfrac{1-\sqrt{n}}{2} & (\dfrac{1-\sqrt{m}}{2})(\dfrac{1+\sqrt{k}}{2}) \end{vmatrix}^2$$

$$= \frac{1}{256}\begin{vmatrix} 1 & 1+\sqrt{m} & 1+\sqrt{n} & 1+\sqrt{m}+\sqrt{k}+\sqrt{m}\sqrt{k} \\ 1 & 1+\sqrt{m} & 1-\sqrt{n} & 1+\sqrt{m}-\sqrt{k}-\sqrt{m}\sqrt{k} \\ 1 & 1-\sqrt{m} & 1+\sqrt{n} & 1-\sqrt{m}-\sqrt{k}+\sqrt{m}\sqrt{k} \\ 1 & 1-\sqrt{m} & 1-\sqrt{n} & 1-\sqrt{m}+\sqrt{k}-\sqrt{m}\sqrt{k} \end{vmatrix}^2$$

$$= \frac{1}{256}\begin{vmatrix} 1 & \sqrt{m} & +\sqrt{n} & \sqrt{m}+\sqrt{k}+\dfrac{m}{d}\sqrt{n} \\ 1 & \sqrt{m} & -\sqrt{n} & \sqrt{m}-\sqrt{k}-\dfrac{m}{d}\sqrt{n} \\ 1 & -\sqrt{m} & +\sqrt{n} & -\sqrt{m}-\sqrt{k}+\dfrac{m}{d}\sqrt{n} \\ 1 & -\sqrt{m} & -\sqrt{n} & -\sqrt{m}+\sqrt{k}-\dfrac{m}{d}\sqrt{n} \end{vmatrix}^2 \quad \begin{matrix} C_2 - C_1 \\ C_3 - C_1 \\ C_4 - C_1 \end{matrix}$$

$$= \frac{1}{256}\begin{vmatrix} 1 & \sqrt{m} & +\sqrt{n} & \sqrt{k} \\ 1 & \sqrt{m} & -\sqrt{n} & -\sqrt{k} \\ 1 & -\sqrt{m} & +\sqrt{n} & -\sqrt{k} \\ 1 & -\sqrt{m} & -\sqrt{n} & \sqrt{k} \end{vmatrix}^2 \quad C_4 - C_2 - \frac{m}{d}C_3$$

$$= \frac{1}{256}(-16\sqrt{m}\sqrt{n}\sqrt{k})^2 = mnk \quad \text{(by Lemma 3.2.2).}$$

□

สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

3.3 Decomposition of Rational Primes

In this section we will find the decomposition of rational primes in biquadratic fields. We will use the following theorem from [6] to a biquadratic field which is a quadratic extension of a quadratic field.

Theorem 3.3.1. *[6] Let p be a prime number, F an algebraic number field containing a primitive pth root of unity ζ, $a \in F$ such that a is not the pth power of an element of F, t is a root of $x^p - a$ and $K = F(t)$.*

(i) If $a\mathcal{O}_F = P^eJ$, where J is an ideal of $\mathcal{O}_F$ not a multiple of P and $e > 0$ is an integer not a multiple of p, then P is ramified in K/F.

(ii) Assume that P divides neither $a\mathcal{O}_F$ nor $p\mathcal{O}_F$.

(iia) If the congruence $X^p \equiv a \pmod{P}$ has a solution in $\mathcal{O}_F$, then P splits completely in K/F.

(iib) If the congruence $X^p \equiv a \pmod{P}$ has no solution in $\mathcal{O}_F$, then P is inert in K/F.

(iii) Assume that P does not divide $a\mathcal{O}_F$ but $(1-\zeta)\mathcal{O}_F = P^eJ$ where J is an ideal of $\mathcal{O}_F$ not a multiple of P and $e > 0$.

(iiia) If the congruence $X^p \equiv a \pmod{P^{pe+1}}$ has a solution in $\mathcal{O}_F$, then P splits completely in K/F.

(iiib) If the congruence $X^p \equiv a \pmod{P^{pe+1}}$ has no solution in $\mathcal{O}_F$ but the congruence $X^p \equiv a \pmod{P^{pe}}$ has a solution in $\mathcal{O}_F$, then P inert in K/F.

(iiic) If the congruence $X^p \equiv a \pmod{P^{pe}}$ has no solution in $\mathcal{O}_F$, then P ramified in K/F.

Next, we will apply this theorem with case $p = 2$.

สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

Theorem 3.3.2. *Let F be a quadratic field, $K = F[\sqrt{a}]$ where a is a squarefree integer which is not a square of an element of F. Let P be any nonzero prime ideal of $\mathcal{O}_F$.*

(i) If $a\mathcal{O}_F = P^eJ$, where J is an ideal of $\mathcal{O}_F$ not a multiple of P and $e > 0$ is odd, then P is ramified in K/F.

(ii) Assume that P divides neither $a\mathcal{O}_F$ nor $2\mathcal{O}_F$.

(iia) If the congruence $X^2 \equiv a \pmod{P}$ has a solution in $\mathcal{O}_F$, then P splits completely in K/F.

(iib) If the congruence $X^2 \equiv a \pmod{P}$ has no solution in $\mathcal{O}_F$, then P is inert in K/F.

(iii) Assume that P does not divide $a\mathcal{O}_F$ but $2\mathcal{O}_F = P^eJ$ where J is an ideal of $\mathcal{O}_F$ not a multiple of P and $e > 0$.

(iiia) If the congruence $X^2 \equiv a \pmod{P^{2e+1}}$ has a solution in $\mathcal{O}_F$, then P splits completely in K/F.

(iiib) If the congruence $X^2 \equiv a \pmod{P^{2e+1}}$ has no solution in $\mathcal{O}_F$ but the congruence $X^2 \equiv a \pmod{P^{2e}}$ has a solution in $\mathcal{O}_F$, then P inert in K/F.

(iiic) If the congruence $X^2 \equiv a \pmod{P^{2e}}$ has no solution in $\mathcal{O}_F$, then P ramified in K/F.

From Theorem 3.3.2, we can find the decomposition of rational primes in biquadratic fields by choosing F to satisfy one of three conditions as above.

สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

Theorem 3.3.3. *Let $K = \mathbb{Q}[\sqrt{m}, \sqrt{n}]$ where m and n are distinct squarefree integers and $k = \dfrac{mn}{d^2}$ where $d = (m, n)$. Then*

$$2\mathcal{O}_K = \begin{cases} \mathcal{P}_1^4 & , \text{ if } \ m \equiv 3, n \equiv 2 \pmod 4 \\ \mathcal{P}_1^2\mathcal{P}_2^2 & , \text{ if } \ m \equiv 1 \pmod 8 \text{ and } n \equiv 2 \text{ or } 3 \pmod 4 \\ \mathcal{P}_1^2 & , \text{ if } \ m \equiv 5 \pmod 8 \text{ and } n \equiv 2 \text{ or } 3 \pmod 4 \\ \mathcal{P}_1\mathcal{P}_2\mathcal{P}_3\mathcal{P}_4 & , \text{ if } \ m \equiv 1 \pmod 8), n \equiv 1 \pmod 8) \\ \mathcal{P}_1\mathcal{P}_2 & , \text{ if } \ m \equiv 1 \pmod 8), n \equiv 5 \pmod 8). \end{cases}$$

Proof. **Case1** $m \equiv 3, n \equiv k \equiv 2 \pmod 4$.

Take $F = \mathbb{Q}[\sqrt{n}]$. By Theorem 2.1.20 and Theorem 2.2.27 we have $\mathcal{O}_F = \mathbb{Z} \cdot 1 + \mathbb{Z} \cdot \sqrt{n}$ and $2\mathcal{O}_F = \langle 2, \sqrt{n} \rangle^2 = P_2^2$. Since N($2\mathcal{O}_F$)=|N$_F$(2)|=4, N$(P_2)^2$ =N(P_2^2) =N($2\mathcal{O}_F$)=4, and so N(P_2)=2. Note that $K = F[\sqrt{m}]$ and N($m\mathcal{O}_F$)= $|\mathrm{N}_F(m)| = m^2$. Since $2 \nmid m$, by Corollary 2.2.13 $P_2 \nmid m\mathcal{O}_F$. This shows that P_2 satisfies Theorem 3.3.2(iii) with $e = 2$, then we have to check that the congruence $X^2 \equiv m \pmod{P_2^4}$ has a solution in $\mathcal{O}_F$ or not.

Since $\mathcal{O}_F = \mathbb{Z} \cdot 1 + \mathbb{Z} \cdot \sqrt{n}$, we have

$$\begin{aligned} P_2^4 &= (P_2^2)^2 \\ &= (2\mathcal{O}_F)^2 \\ &= 4\mathcal{O}_F \\ &= 4(\mathbb{Z} \cdot 1 + \mathbb{Z} \cdot \sqrt{n}) \\ &= \mathbb{Z} \cdot 4 + \mathbb{Z} \cdot 4\sqrt{n}. \end{aligned}$$

Claim that $X^2 \equiv m \pmod{P_2^4}$ has no solution in $\mathcal{O}_F$. Suppose not, i.e. there exists an $X = u + v\sqrt{n}$ for some $u, v \in \mathbb{Z}$ which is a solution of $X^2 \equiv m \pmod{P_2^4}$. Then $X^2 - m \in \mathbb{Z} \cdot 4 + \mathbb{Z} \cdot 4\sqrt{n}$. Since $X^2 - m = (u^2 + v^2n - m) + (2uv)\sqrt{n}$, we have $4 \mid u^2 + v^2n - m$ and $4 \mid 2uv$, and so $2 \mid uv$. If $2 \mid u$, from $4 \mid u^2 + v^2n - m$ we obtain that $4 \mid v^2n - m$ which contradicts the fact that $v^2n - m$ is odd. If $2 \mid v$, from $4 \mid u^2 + v^2n - m$ we obtain that $4 \mid u^2 - m$ which contradicts the fact that

สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

$x^2 \equiv 3 \pmod 4$ has no solution in $\mathbb{Z}$. Hence we have the claim. This shows that P_2 satisfies Theorem 3.3.2(iiic). Hence P_2 is ramified, i.e. $P_2\mathcal{O}_K = \mathcal{P}_1^2$ where $\mathcal{P}_1$ is a prime ideal of $\mathcal{O}_K$. Thus $2\mathcal{O}_K = \mathcal{P}_1^4$.

Case2 $m \equiv 1, n \equiv k \equiv 2$ or $3 \pmod 4$.

Case2.1 $m \equiv 1 \pmod 8$ and $n \equiv k \equiv 2$ or $3 \pmod 4$.

Take $F = \mathbb{Q}[\sqrt{n}]$. By Theorem 2.1.20 and Theorem 2.2.27 we have $\mathcal{O}_F = \mathbb{Z}\cdot 1+\mathbb{Z}\cdot\sqrt{n}$ and $2\mathcal{O}_F = \langle 2, \sqrt{n}\rangle^2 = P_2^2$. Since N($2\mathcal{O}_F$)=$|\mathrm{N}_F(2)|$=4, N$(P_2)^2$=N$(P_2^2)$ =N($2\mathcal{O}_F$)=4, and so N(P_2)=2. Note that $K = F[\sqrt{m}]$ and N($m\mathcal{O}_F$)=$|\mathrm{N}_F(m)| = m^2$. Since $2 \nmid m$, by Corollary 2.2.13 $P_2 \nmid m\mathcal{O}_F$. This shows that P_2 satisfies Theorem 3.3.2(iii) with $e = 2$, then we have to check that the congruence $X^2 \equiv m$ (mod P_2^5) has a solution in $\mathcal{O}_F$ or not.

Since $\mathcal{O}_F = \mathbb{Z}\cdot 1 + \mathbb{Z}\cdot\sqrt{n}$, we have

$$\begin{aligned} P_2^5 &= (P_2^4)(P_2) \\ &= \langle 4\rangle \left\langle 2, \sqrt{n}\right\rangle \\ &= \left\langle 8, 4\sqrt{n}\right\rangle \\ &= 8\mathcal{O}_F + 4\sqrt{n}\mathcal{O}_F \\ &= \mathbb{Z}\cdot 8 + \mathbb{Z}\cdot 8\sqrt{n} + \mathbb{Z}\cdot 4\sqrt{n} + \mathbb{Z}\cdot 4n \\ &= \mathbb{Z}\cdot 8 + \mathbb{Z}\cdot 4\sqrt{n}. \end{aligned}$$

Choose $X = 1$ as a solution of $X^2 \equiv m$ (mod P_2^5). Since $m \equiv 1 \pmod 8$, then $1 - m \in \mathbb{Z}\cdot 8 \subseteq \mathbb{Z}\cdot 8 + \mathbb{Z}\cdot 4\sqrt{n}$. This shows that P_2 satisfies Theorem 3.3.2(iiia), Hence P_2 splits completely, i.e. $P_2\mathcal{O}_K = \mathcal{P}_1\mathcal{P}_2$ where $\mathcal{P}_1, \mathcal{P}_2$ are distinct prime ideals of $\mathcal{O}_K$. Thus $2\mathcal{O}_K = \mathcal{P}_1^2\mathcal{P}_2^2$.

สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

Case2.2 $m \equiv 5 \pmod 8$ and $n \equiv k \equiv 2 \pmod 4$.

Take $F = \mathbb{Q}[\sqrt{m}]$. By Theorem 2.1.20 and Theorem 2.2.27 we have $\mathcal{O}_F = \mathbb{Z} \cdot 1 + \mathbb{Z} \cdot \frac{1+\sqrt{m}}{2}$ and $2\mathcal{O}_F = P_2$ is inert. Since $n = 4a+2 = 2(2a+1)$ for some $a \in \mathbb{Z}$, then $n\mathcal{O}_F = 2\mathcal{O}_F(2a+1)\mathcal{O}_F = P_2 J$. This shows that P_2 satisfies Theorem 3.3.2(i) with $e = 1$ which is odd, so P_2 is ramified, i.e. $P_2\mathcal{O}_K = \mathcal{P}_1^2$ where $\mathcal{P}_1$ is a prime ideal of $\mathcal{O}_K$. Hence $2\mathcal{O}_K = \mathcal{P}_1^2$

Case2.3 $m \equiv 5 \pmod 8$ and $n \equiv k \equiv 3 \pmod 4$.

Take $F = \mathbb{Q}[\sqrt{m}]$. By Theorem 2.1.20 and Theorem 2.2.27 we have $\mathcal{O}_F = \mathbb{Z} \cdot 1 + \mathbb{Z} \cdot \frac{1+\sqrt{m}}{2}$ and $2\mathcal{O}_F = P_2$ is inert. Since $\mathrm{N}(2\mathcal{O}_F)$=$|\mathrm{N}_F(2)|$=4, $\mathrm{N}(P_2)$=4. Note that $K = F[\sqrt{n}]$ and $\mathrm{N}(n\mathcal{O}_F)$=$|\mathrm{N}_F(n)| = n^2$. Since $4 \nmid n$, by Corollary 2.2.13 $P_2 \nmid n\mathcal{O}_F$. This shows that P_2 satisfies Theorem 3.3.2(iii) with $e = 1$, then we have to check that the congruence $X^2 \equiv n \pmod{P_2^2}$ has a solution in $\mathcal{O}_F$ or not.

Since $\mathcal{O}_F = \mathbb{Z} \cdot 1 + \mathbb{Z} \cdot \frac{1+\sqrt{m}}{2}$, we have

$$\begin{aligned} P_2^2 &= (2\mathcal{O}_F)^2 \\ &= 4\mathcal{O}_F \\ &= 4(\mathbb{Z} \cdot 1 + \mathbb{Z} \cdot \frac{1+\sqrt{m}}{2}) \\ &= \mathbb{Z} \cdot 4 + \mathbb{Z} \cdot 4(\frac{1+\sqrt{m}}{2}). \end{aligned}$$

Claim that $X^2 \equiv n \pmod{P_2^2}$ has no solution in $\mathcal{O}_F$. Suppose not, i.e. there exists an $X = u + v(\frac{1+\sqrt{m}}{2})$ for some $u, v \in \mathbb{Z}$ which is a solution of $X^2 \equiv n \pmod{P_2^2}$. Then $X^2 - n \in \mathbb{Z} \cdot 4 + \mathbb{Z} \cdot 4(\frac{1+\sqrt{m}}{2})$.

$$\begin{aligned} \text{Consider } X^2 - n &= u^2 + 2uv(\tfrac{1+\sqrt{m}}{2}) + v^2(\tfrac{1+m+2\sqrt{m}}{4}) - n \\ &= u^2 + v^2(\tfrac{1+m}{4}) - \tfrac{v^2}{2} - n + (2uv + v^2)(\tfrac{1+\sqrt{m}}{2}) \\ &= u^2 + v^2(\tfrac{m-1}{4}) - n + v(2u+v)(\tfrac{1+\sqrt{m}}{2}) \in \mathbb{Z} \cdot 4 + \mathbb{Z} \cdot 4(\tfrac{1+\sqrt{m}}{2}), \end{aligned}$$

we have $4 \mid u^2 + v^2(\dfrac{m-1}{4}) - n$ and $4 \mid v(2u+v)$. Then v is even, and so we have $4 \mid u^2 - n$ which contradicts the fact that $x^2 \equiv 3 \pmod 4$ has no solution in $\mathbb{Z}$. This shows that P_2 satisfies Theorem 3.3.2(iiic), then P_2 is ramified, i.e. $P_2\mathcal{O}_K = \mathcal{P}_1^2$ where $\mathcal{P}_1$ is a prime ideal of $\mathcal{O}_K$. Hence $2\mathcal{O}_K = \mathcal{P}_1^2$.

สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

Case3 $m \equiv n \equiv k \equiv 1 \pmod 4$. We have only 2 subcases as follows:
(1) $m \equiv n \equiv k \equiv 1 \pmod 8$,
(2) $m \equiv 1, n \equiv k \equiv 5 \pmod 8$.
Take $F = \mathbb{Q}[\sqrt{m}]$. By Theorem 2.1.20 and Theorem 2.2.27 we have $\mathcal{O}_F = \mathbb{Z}\cdot 1 + \mathbb{Z}\cdot \frac{1+\sqrt{m}}{2}$ and $2\mathcal{O}_F = \langle 2, \frac{1+\sqrt{m}}{2}\rangle\langle 2, \frac{1-\sqrt{m}}{2}\rangle = P_2\bar{P}_2$. Since N($2\mathcal{O}_F$)=$|\mathrm{N}_F(2)|$=4 and N($P_2$)=N($\bar{P}_2$), N($P_2$)=2 and N$(\bar{P}_2) = 2$. Note that $K = F[\sqrt{n}]$ and N($n\mathcal{O}_F$)= $|\mathrm{N}_F(n)| = n^2$. Since $2 \nmid n$, by Corollary 2.2.13 $P_2 \nmid n\mathcal{O}_F$ and $\bar{P}_2 \nmid n\mathcal{O}_F$. This shows that P_2 and $\bar{P}_2$ satisfy Theorem 3.3.2(iii) with $e = 1$, then we have to check that the congruence $X^2 \equiv n \pmod{P_2^2}$ has a solution in $\mathcal{O}_F$ or not.
Since $\mathcal{O}_F = \mathbb{Z}\cdot 1 + \mathbb{Z}\cdot \frac{1+\sqrt{m}}{2}$, we have

$$\begin{aligned} P_2^2 &= \langle 2, \frac{1+\sqrt{m}}{2}\rangle\langle 2, \frac{1+\sqrt{m}}{2}\rangle \\ &= \langle 4, 1+\sqrt{m}, \frac{1+m+2\sqrt{m}}{4}\rangle. \end{aligned}$$

Since $m \equiv 1 \pmod 8$, $\frac{m-1}{8} \in \mathbb{Z}$ and so $1+\sqrt{m} = (\frac{1-m}{8})(4) + (2)(\frac{1+m+2\sqrt{m}}{4})$, we obtain that

$$\begin{aligned} P_2^2 &= \langle 4, \frac{1+m+2\sqrt{m}}{4}\rangle \\ &= 4\mathcal{O}_K + \frac{1+m+2\sqrt{m}}{4}\mathcal{O}_K \\ &= \mathbb{Z}\cdot 4 + \mathbb{Z}\cdot 4(\frac{1+\sqrt{m}}{2}) + \mathbb{Z}\cdot \frac{1+m+2\sqrt{m}}{4} + \mathbb{Z}\cdot(\frac{1+m+2\sqrt{m}}{4})(\frac{1+\sqrt{m}}{2}) \\ &= \mathbb{Z}\cdot 4 + \mathbb{Z}\cdot(2+2\sqrt{m}) + \mathbb{Z}\cdot \frac{1+m+2\sqrt{m}}{4} + \mathbb{Z}\cdot(\frac{3m+1+(m+3)\sqrt{m}}{8}). \end{aligned}$$

Since $m \equiv 1 \pmod 8$, $\frac{m-1}{8} \in \mathbb{Z}$ and so we have $2+2\sqrt{m} = (\frac{1-m}{4})(4) + 4(\frac{1+m+2\sqrt{m}}{4})$ and $(\frac{3m+1+(m+3)\sqrt{m}}{8}) = -(\frac{m-1}{8})^2(4) + (\frac{m+3}{4})(\frac{1+m+2\sqrt{m}}{4})$, this shows that

$$P_2^2 = \mathbb{Z}\cdot 4 + \mathbb{Z}\cdot \frac{1+m+2\sqrt{m}}{4}.$$

Choose $X = 1$ as a solution of $X^2 \equiv n \pmod{P_2^2}$. Since $n \equiv 1 \pmod 4$, then $1 - n \in \mathbb{Z}\cdot 4 \subseteq \mathbb{Z}\cdot 4 + \mathbb{Z}\cdot(\frac{1+m+2\sqrt{m}}{4})$. This shows that P_2 does not satisfy Theorem 3.3.2(iiic). Hence we have to check that the congruence $X^2 \equiv n \pmod{P_2^3}$ has a

สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

solution in $\mathcal{O}_F$ or not. Since $\mathcal{O}_F = \mathbb{Z}\cdot 1 + \mathbb{Z}\cdot \frac{1+\sqrt{m}}{2}$, we have

$$\begin{aligned}
P_2^3 &= \langle 4, \frac{1+m+2\sqrt{m}}{4}\rangle\langle 2, \frac{1+\sqrt{m}}{2}\rangle \\
&= \langle 8, 2+2\sqrt{m}, \frac{m+1+2\sqrt{m}}{2}, \frac{(3m+1)+(m+3)\sqrt{m}}{8}\rangle.
\end{aligned}$$

Since $m \equiv 1 \pmod 8$, $\frac{m-1}{8} \in \mathbb{Z}$ and so $2+2\sqrt{m} = (\frac{1-m}{8})(8) + (2)(\frac{1+m+2\sqrt{m}}{2})$, we obtain that

$$\begin{aligned}
P_2^3 &= \langle 8, \frac{m+1+2\sqrt{m}}{2}, \frac{(3m+1)+(m+3)\sqrt{m}}{8}\rangle \\
&= \langle 8, \frac{m+1+2\sqrt{m}}{2}, \frac{(3m+1)+(m+3)\sqrt{m}}{8} - (\frac{m-1}{8})(\frac{m+1+2\sqrt{m}}{2})\rangle \\
&= \langle 8, \frac{m+1+2\sqrt{m}}{2}, \frac{(-m^2+6m+3)+8\sqrt{m}}{16}\rangle.
\end{aligned}$$

Since $m \equiv 1 \pmod 8$, $\frac{m-1}{8} \in \mathbb{Z}$ and so $\frac{m+1+2\sqrt{m}}{2} = (\frac{m-1}{8})^2(8) + (2)(\frac{-m^2+6m+3+8\sqrt{m}}{16})$, we obtain that

$$\begin{aligned}
P_2^3 &= \langle 8, \frac{m+1+2\sqrt{m}}{2}, \frac{(-m^2+6m+3)+8\sqrt{m}}{16}\rangle \\
&= \langle 8, \frac{(-m^2+6m+3)+8\sqrt{m}}{16}\rangle \\
&= 8\mathcal{O}_K + \frac{(-m^2+6m+3)+8\sqrt{m}}{16}\mathcal{O}_K \\
&= \mathbb{Z}\cdot 8 + \mathbb{Z}\cdot 8(\frac{1+\sqrt{m}}{2}) + \mathbb{Z}\cdot(\frac{(-m^2+6m+3)+8\sqrt{m}}{2}) \\
&\quad + \mathbb{Z}\cdot(\frac{(-m^2+6m+3)+8\sqrt{m}}{16})(\frac{1+\sqrt{m}}{2}) \\
&= \mathbb{Z}\cdot 8 + \mathbb{Z}\cdot(4+4\sqrt{m}) + \mathbb{Z}\cdot(\frac{-m^2+6m-5}{16} + \frac{1+\sqrt{m}}{2}) \\
&\quad + \mathbb{Z}\cdot(\frac{-m^2+14m+3}{32} + \frac{(-m^2+6m+11)\sqrt{m}}{32}) \\
&= \mathbb{Z}\cdot 8 + \mathbb{Z}\cdot(4+4\sqrt{m}) + \mathbb{Z}\cdot(\frac{-m^2+6m-5}{16} + \frac{1+\sqrt{m}}{2}) \\
&\quad + \mathbb{Z}\cdot(\frac{m-1}{4} - (\frac{(m^2-6m-11)}{16})(\frac{1+\sqrt{m}}{2})).
\end{aligned}$$

สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

Since $m \equiv 1 \pmod 8$, $\frac{m-1}{8} \in \mathbb{Z}$ and so we have $4+4\sqrt{m} = (\frac{-(m-1)(m-5)}{16})(8) + 8(\frac{-m^2+6m-5}{16} + \frac{1+\sqrt{m}}{2})$ and $(\frac{m-1}{4} - (\frac{(m^2-6m-11)}{16})(\frac{1+\sqrt{m}}{2})) = (\frac{-(m-1)^4+8(m-1)^3}{2048})(8) - (\frac{m^2-6m-11}{16})(\frac{-m^2+6m-5}{16} + \frac{1+\sqrt{m}}{2})$, this shows that

$$\begin{aligned} P_2^3 &= \mathbb{Z}\cdot 8 + \mathbb{Z}\cdot(\frac{-m^2+6m-5}{16} + \frac{1+\sqrt{m}}{2}) \\ &= \mathbb{Z}\cdot 8 + \mathbb{Z}\cdot(\frac{4(m-1)-(m-1)^2+8+8\sqrt{m}}{16}). \end{aligned}$$

Suppose $X = u + v(\frac{1+\sqrt{m}}{2})$ where $u, v \in \mathbb{Z}$ is a solution of $X^2 \equiv n \pmod{P_2^3}$ in $\mathcal{O}_F$. Then $X^2 - n \in \mathbb{Z}\cdot 8 + \mathbb{Z}\cdot(\frac{4(m-1)-(m-1)^2+8+8\sqrt{m}}{16})$.

$$\begin{aligned} \text{Since } X^2 - n &= u^2 + 2uv(\tfrac{1+\sqrt{m}}{2}) + v^2(\tfrac{1+m+2\sqrt{m}}{4}) - n \\ &= u^2 + uv + v^2(\tfrac{1+m}{4}) - n + (2uv+v^2)(\tfrac{\sqrt{m}}{2}) \\ &= u^2 + uv + v^2(\tfrac{1+m}{4}) - n + (2uv+v^2)(\tfrac{8\sqrt{m}}{16}) \\ &= u^2 + uv + v^2(\tfrac{1+m}{4}) - n - (2uv+v^2)(\tfrac{4(m-1)-(m-1)^2+8}{16}) \\ &\quad +(2uv+v^2)(\tfrac{4(m-1)-(m-1)^2+8+8\sqrt{8}}{16}) \\ &= u^2 - uv(\tfrac{(m-1)(m+3)}{8}) + v^2\tfrac{(m-1)^2}{16} - n \\ &\quad +(2uv+v^2)(\tfrac{4(m-1)-(m-1)^2+8+8\sqrt{8}}{16}) \\ &\quad \in \mathbb{Z}\cdot 8 + \mathbb{Z}\cdot(\tfrac{4(m-1)-(m-1)^2+8+8\sqrt{m}}{16}), \end{aligned}$$

we have

$$\begin{aligned} &8 \mid u^2 - uv(\frac{(m-1)(m+3)}{8}) + v^2\frac{(m-1)^2}{16} - n \\ &8 \mid u^2 - 2uv\frac{m-1}{4} + v^2\frac{(m-1)^2}{16} + 2uv\frac{m-1}{4} - uv(\frac{(m-1)(m+3)}{8}) - n \\ &8 \mid (u - v(\frac{m-1}{4}))^2 - uv\frac{(m-1)^2}{8} - n. \end{aligned}$$

Since $m \equiv 1 \pmod 8$,$8 \mid \frac{uv(m-1)^2}{8}$ so we have $8 \mid (u - v(\frac{m-1}{4}))^2 - n$.

Case1 $n \equiv 1 \pmod 8$. We choose $u = 1, v = 0$. Then the congruence $X^2 \equiv n \pmod{P_2^3}$ has a solution in $\mathcal{O}_F$ and so P_2 satisfies Theorem 3.3.2(iiia). Hence P_2 splits completely. Similarly we can prove that $\bar{P}_2$ also splits completely. Thus $P_2\mathcal{O}_K = \mathcal{P}_1\mathcal{P}_2$ and $\bar{P}_2\mathcal{O}_K = \mathcal{P}_3\mathcal{P}_4$ where $\mathcal{P}_1, \mathcal{P}_2, \mathcal{P}_3$ and $\mathcal{P}_4$ are distinct prime ideals of $\mathcal{O}_K$. Hence $2\mathcal{O}_K = \mathcal{P}_1\mathcal{P}_2\mathcal{P}_3\mathcal{P}_4$.

สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

Case2 $n \equiv 5 \pmod 8$. Since $x^2 \equiv 5 \pmod 8$ has no solution in $\mathbb{Z}$, we obtain that the congruence $X^2 \equiv n \pmod{P_2^3}$ has no solution in $\mathcal{O}_F$ and so then P_2 satisfies Theorem 3.3.2(iiib). Hence P_2 is inert. Similarly we can prove that $\bar{P}_2$ is also inert. Then $2\mathcal{O}_K = \mathcal{P}_1\mathcal{P}_2$ where $\mathcal{P}_1$ and $\mathcal{P}_2$ are distinct prime ideals of $\mathcal{O}_K$.
That completes the proof. $\square$

Lemma 3.3.4. *Let p be an odd prime number, m, n be squarefree integers not a multiple of p and $k = \dfrac{mn}{d^2}$ where $d = (m, n)$. Then $(m/p)(n/p) = (k/p)$.*

Proof. Recall the fact that $(a/p)(b/p) = (ab/p)$, then apply this fact by $a = d^2$, $b = \frac{mn}{d^2}$. Since $(d^2/p) = 1$, $(m/p)(n/p) = (mn/p) = (\frac{mn}{d^2}/p)(d^2/p) = (k/p)$, so we complete the proof. $\square$

Next, we will use Theorem 3.3.2 and Lemma 3.3.4 to compute explicitly factors of p in each case.

Theorem 3.3.5. *Let $K = \mathbb{Q}[\sqrt{m}, \sqrt{n}]$ where m and n are distinct squarefree integers and $k = \dfrac{mn}{d^2}$ where $d = (m, n)$. Then*

$$p\mathcal{O}_K = \begin{cases} \mathcal{P}_1^2\mathcal{P}_2^2 & , \textit{ if } p \mid m, p \mid n, p \nmid k \textit{ and } (k/p) = 1 \\ \mathcal{P}_1^2 & , \textit{ if } p \mid m, p \mid n, p \nmid k \textit{ and } (k/p) = -1 \\ \mathcal{P}_1\mathcal{P}_2\mathcal{P}_3\mathcal{P}_4 & , \textit{ if } p \nmid mnk, (m/p) = 1, \textit{ and } (n/p) = 1 \\ \mathcal{P}_1\mathcal{P}_2 & , \textit{ if } p \nmid mnk, (m/p) = -1 \textit{ and } (n/p) = -1 \end{cases}.$$

Proof. Since m, n are squarefree integers, we have only 2 cases as follows:
Case1 p divides at least one of m, n or k.
Without loss of generality, we say $p \mid m$. Claim that p divides exactly one of n or k. Suppose that $p \nmid n$. Then $p \nmid d$. Since $p \mid m$, $p \mid d^2k$ so $p \mid k$.
Next, suppose that $p \mid n$. Since m and n are squarefree, $m = px$ and $n = py$ for some $x, y \in \mathbb{Z}$ such that $p \nmid x$ and $p \nmid y$. Hence $p \mid d$ and $kd^2/p^2 = xy$. Since $p \nmid x$ and $p \nmid y$, $p \nmid k$.

สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

In this case we assume that $p \mid m$ and $p \mid n$ so we have $p \nmid k$.

Case1.1 $(k/p) = 1$. Take $F = \mathbb{Q}[\sqrt{k}]$. By Theorem 2.2.28 $p\mathcal{O}_F = \langle p, a+\sqrt{k}\rangle\langle p, a-\sqrt{k}\rangle = P\bar{P}$ where $a \in \mathbb{Z}$ such that $k \equiv a^2 \pmod{p}$. Since $p \mid m$ and m is a squarefree integer, $m = px$ for some $x \in \mathbb{Z}$ such that $p \nmid x$. Then $m\mathcal{O}_F = p\mathcal{O}_F x\mathcal{O}_F = P\bar{P}x\mathcal{O}_F$. So we have $m\mathcal{O}_F = PJ$ where $J = \bar{P}x\mathcal{O}_F$ and $P \nmid \bar{P}x\mathcal{O}_F$. Similarly we have $m\mathcal{O}_F = \bar{P}J'$ where $J' = Px\mathcal{O}_F$ and $\bar{P} \nmid Px\mathcal{O}_F$. Hence P and $\bar{P}$ satisfy Theorem 3.3.2(i) with $e = 1$ which is odd, so P and $\bar{P}$ are ramified, i.e. $P\mathcal{O}_K = \mathcal{P}_1^2$ and $\bar{P}\mathcal{O}_K = \mathcal{P}_2^2$ where $\mathcal{P}_1$ and $\mathcal{P}_2$ are distinct prime ideals of $\mathcal{O}_K$. Hence $p\mathcal{O}_K = \mathcal{P}_1^2\mathcal{P}_2^2$.

Case1.2 $(k/p) = -1$. By Theorem 2.2.28 $p\mathcal{O}_F = P$ is inert. Since $p \mid m$ and m is a squarefree integer, $m = px$ for some $x \in \mathbb{Z}$ such that $p \nmid x$. Then $m\mathcal{O}_F = p\mathcal{O}_F x\mathcal{O}_F = Px\mathcal{O}_F$ and $P \nmid x\mathcal{O}_F$. Hence P satisfies Theorem 3.3.2(i) with $e = 1$ which is odd, so P is ramified, i.e. $P\mathcal{O}_K = \mathcal{P}_1^2$ where $\mathcal{P}_1$ is a prime ideal of $\mathcal{O}_K$. Hence $p\mathcal{O}_K = \mathcal{P}_1^2$.

Case2 p does not divide m, n and k.

By Lemma 3.3.4 we have only 2 cases as follows:

(1) $(m/p) = (n/p) = (k/p) = 1$,

(2) exactly one of $(m/p), (n/p)$ and (k/p) equals 1.

Case2.1 $(m/p) = (n/p) = (k/p) = 1$.

Take $F = \mathbb{Q}[\sqrt{m}]$, by Theorem 2.2.28 $p\mathcal{O}_F = \langle p, a+\sqrt{m}\rangle\langle p, a-\sqrt{m}\rangle = P\bar{P}$ where $a \in \mathbb{Z}$ such that $m \equiv a^2 \pmod{p}$. Since $\mathrm{N}(p\mathcal{O}_F)$=$|\mathrm{N}_F(p)| = p^2$ and $\mathrm{N}(P)$=$\mathrm{N}(\bar{P})$, $\mathrm{N}(P)$=$\mathrm{N}(\bar{P}) = p$. Note that $K = F[\sqrt{n}]$ and $\mathrm{N}(n\mathcal{O}_F)$=$|\mathrm{N}_F(n)| = n^2$. Since $p \nmid n$ and $p \nmid 2$, by Corollary 2.2.13 we have $P \nmid n\mathcal{O}_F$, $P \nmid 2\mathcal{O}_F$, $\bar{P} \nmid n\mathcal{O}_F$ and $\bar{P} \nmid 2\mathcal{O}_F$. Hence P and $\bar{P}$ satisfy Theorem 3.3.2(ii). Then we have to check that $X^2 \equiv n \pmod{P}$ has solution in $\mathcal{O}_F$ or not. Since $(n/p) = 1$, there exists $b \in \mathbb{Z}$ such that $b^2 \equiv n \pmod{p}$. Then we choose $X = b$, so $X \in \mathbb{Z} \subseteq \mathcal{O}_F$ and $X^2 - n \in \mathbb{Z} \cdot p \subseteq p\mathcal{O}_F \subseteq P$. This means that P satisfies Theorem 3.3.2(iia), so P splits completely. Similarly we can prove that $\bar{P}$ splits completely. Then $P\mathcal{O}_K = \mathcal{P}_1\mathcal{P}_2$ and $\bar{P}\mathcal{O}_K = \mathcal{P}_3\mathcal{P}_4$ where $\mathcal{P}_1, \mathcal{P}_2, \mathcal{P}_3$ and $\mathcal{P}_4$ are distinct prime ideals

สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

of $\mathcal{O}_K$. Hence $p\mathcal{O}_K = \mathcal{P}_1\mathcal{P}_2\mathcal{P}_3\mathcal{P}_4$.

Case2.2 Exactly one of $(m/p), (n/p)$ and (k/p) equals 1.

Without loss of generality, we say $(m/p) = 1$ and $(n/p) = -1$.

Take $F = \mathbb{Q}[\sqrt{n}]$, by Theorem 2.2.28 $p\mathcal{O}_F = P$ is inert. Since $\mathrm{N}(p\mathcal{O}_F)$= $|\mathrm{N}_F(p)| = p^2$, $\mathrm{N}(P) = p^2$. Note that $K = F[\sqrt{m}]$ and $\mathrm{N}(m\mathcal{O}_F)$=$|\mathrm{N}_F(m)| = m^2$. Since $p \nmid m$ and $p \nmid 2$, by Corollary 2.2.13 we have $P \nmid m\mathcal{O}_F$ and $P \nmid 2\mathcal{O}_F$. This shows that P satisfies Theorem 3.3.2(ii). Then we have to check that $X^2 \equiv m \pmod{P}$ has solution in $\mathcal{O}_F$ or not. Since $(m/p) = 1$, there exists $c \in \mathbb{Z}$ such that $c^2 \equiv m \pmod{p}$. Then we choose $X = c$, so $X \in \mathbb{Z} \subseteq \mathcal{O}_F$ and $X^2 - m \in \mathbb{Z}\cdot p \subseteq P$. This means that P satisfies Theorem 3.3.2(iia), so P splits completely, i.e. $P\mathcal{O}_K = \mathcal{P}_1\mathcal{P}_2$ where $\mathcal{P}_1$ and $\mathcal{P}_2$ are distinct prime ideals of $\mathcal{O}_K$. Hence $p\mathcal{O}_K = \mathcal{P}_1\mathcal{P}_2$. The proof is completed. □

Corollary 3.3.6. *Let $K = \mathbb{Q}[\sqrt{m}, \sqrt{n}]$ where m and n are distinct squarefree integers and $k = \dfrac{mn}{d^2}$ where $d = (m, n)$. Then*

(i) No prime p is inert in K,

(ii) If a prime p is ramified in each of the quadratic subfields, then p is totally ramified in K, and

(iii) If a prime p splits completely in each of the quadratic subfields, then p splits completely in K.

Proof. (i) Follows by Theorem 3.3.3 and Theorem 3.3.5.

(ii) Suppose a prime p is ramified in each of the quadratic subfields.

Case1 $p = 2$.

Since 2 is ramified in each of the quadratic subfields, $m \equiv 2$ or $3 \pmod 4$, $n \equiv 2$ or $3 \pmod 4$ and $k \equiv 2$ or $3 \pmod 4$. If $m \equiv n \equiv k \equiv 3 \pmod 4$, then d is odd, so $3 \equiv k \equiv kd^2 \equiv mn \equiv 1 \pmod 4$ which is a contradiction. Hence exactly one of m, n and $k \equiv 3 \pmod 4$ and the others $\equiv 2 \pmod 4$. By Theorem 3.3.3, 2 is totally ramified.

สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

Case2 p is odd.

Since p is ramified in each of the quadratic subfields, $p \mid m$, $p \mid n$ and $p \mid k$, which is impossible. Hence this case never occur.

(iii) Suppose a prime p splits completely in each of the quadratic subfields.

Case1 $p = 2$.

Since 2 splits completely in each of the quadratic subfields, $m \equiv n \equiv k \equiv 1 \pmod 8$. By Theorem 3.3.3, 2 splits completely.

Case2 p is odd.

Since p splits completely in each of the quadratic subfields, $p \nmid m, (m/p) = 1$, $p \nmid n, (n/p) = 1$ and $p \nmid k$, $(k/p) = 1$. Hence $p \nmid mnk, (m/p) = 1$ and $(n/p) = 1$. By Theorem 3.3.5, p splits completely. □

สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

REFERENCES

[1] Delone, B.N. and Faddeev, D.K. *The Theory of Irrationalities of The Third Degree*, Transl. Math. Monographs, vol. 10, Amer. Math. Soc., Providence, R.I., 1964.

[2] Martinet, J. and Payan, J.J. *Sur les extensions cubiques non-Galoisiennes des rationnels et leur clôture Galoisienne*, J. Reine Angew. Math. 228(1967), 15-37.

[3] Llorente, P. and Nart, E. *Effective determinantion of the decomposition of the rational primes in a cubic field*, Proc. Amer. Math. Soc., No. 4, 87(1983), 579-585.

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

[5] Mollin, R. *Algebraic Number Theory*, Chapman & Hall CRC, New York, 1999.

[6] Ribenboim, P. *Classical Theory of Algebraic Numbers*, Springer-Verlag, New York, 2001.

[7] Harnchoowong, A. *Lecture note on Algebraic Numbers Theory*, Bangkok, 2005. (Unpublished Manuscript)

สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

VITA

Name	:	Mr. Chaiya Riablershirun
Date of Birth	:	19 July 1981
Place of Birth	:	Bangkok, Thailand
Education	:	B.Eng.(Chemical), Chulalongkorn University, 2002
Reward	:	Gold Medal from IMSO Thailand Camp 1997, Winner of Secondary Level in Eastern and Middle of Thailand Mathematical Compettition 1997 (Team), Runner-up of Secondary Level in Eastern and Middle of Thailand Mathematical Compettition 1997 (individual).

สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย