สามสิงอันดับพีทาโกรัสเหนือฟีลด์จำนวน

นางสาวชีรนุช สมบูรณ์กุลวุฒิ

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรดุษฎีบัณฑิต
สาขาวิชาคณิตศาสตร์ ภาควิชาคณิตศาสตร์และวิทยาการคอมพิวเตอร์
คณะวิทยาศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2554

PYTHAGOREAN TRIPLES OVER NUMBER FIELDS

Miss Cheranoot Somboonkulavudi

A Dissertation Submitted in Partial Fulfillment of the Requirements
for the Degree of Doctor of Philosophy Program in Mathematics
Department of Mathematics and Computer Science
Faculty of Science
Chulalongkorn University
Academic Year 2011

Thesis Title	PYTHAGOREAN TRIPLES OVER NUMBER FIELDS
By	Miss Cheranoot Somboonkulavudi
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 Doctoral Degree

....Dean of the Faculty of Science
(Professor Supot Hannongbua, Dr.rer.nat.)

THESIS COMMITTEE

....Chairman
(Associate Professor Patanee Udomkavanich, Ph.D.)

....Thesis Advisor
(Associate Professor Ajchara Harnchoowong, Ph.D.)

....Examiner
(Assistant Professor Yotsanan Meemark, Ph.D.)

....Examiner
(Assistant Professor Tuangrat Chaichana, Ph.D.)

....External Examiner
(Associate Professor Utsanee Leerawat, Ph.D.)

ชีรนุช สมบูรณ์กุลวุฒิ : สามสิ่งอันดับพีทาโกรัสเหนือฟีลด์จำนวน. (PYTHAGOREAN TRIPLES OVER NUMBER FIELDS) อ. ที่ปรึกษาวิทยานิพนธ์หลัก : รศ. ดร. อัจฉรา หาญชูวงศ์, 40 หน้า.

เป็นที่รู้กันว่าสามสิ่งอันดับพีทาโกรัสปฐมฐานของจำนวนนับแต่ละตัวจะถูกสร้างได้จากจำนวนนับสองตัวซึ่งเป็นจำนวนเฉพาะสัมพัทธ์กันและมีภาวะคู่หรือคี่ต่างกัน นอกจากนี้สามสิ่งอันดับพีทาโกรัสยังถูกจำแนกบนโดเมนที่แยกตัวประกอบได้อย่างเดียว

เซตของสามสิ่งอันดับพีทาโกรัสของจำนวนเต็มเคยถูกศึกษาในแง่ของโครงสร้างของมัน การดำเนินการทวิภาคถูกกำหนดทำให้เซตนี้เป็นกึ่งกรุป กรุป หรือริง ในวิทยานิพนธ์ฉบับนี้เราขยายแนวคิดดังกล่าว และศึกษาคุณสมบัติและโครงสร้างของกึ่งกรุปของสามสิ่งอันดับพีทาโกรัสเหนือจำนวนเต็มเกาส์เซียน ริงของสามสิ่งอันดับพีทาโกรัสเหนือฟีลด์กำลังสองและฟีลด์กำลังสี่ และกรุปของสามสิ่งอันดับพีทาโกรัสเหนือฟีลด์จำนวน และเรายังได้หารูปแบบของสามสิ่งอันดับพีทาโกรัสทั้งหมดในริงของจำนวนเต็มของฟีลด์จำนวนทั้งหมด

ภาควิชา.........คณิตศาสตร์และ......... ลายมือชื่อนิสิต...

.........วิทยาการคอมพิวเตอร์......... ลายมือชื่อ อ.ที่ปรึกษาวิทยานิพนธ์หลัก...........................

สาขาวิชา.........คณิตศาสตร์.........

ปีการศึกษา.........2554.........

5073818523 : MAJOR MATHEMATICS
KEYWORDS : NUMBER FIELDS / PYTHAGOREAN TRIPLES

CHERANOOT SOMBOONKULAVUDI : PYTHAGOREAN TRIPLES OVER NUMBER FIELDS. ADVISOR : ASSOC. PROF. AJCHARA HARNCHOOWONG, Ph.D., 40 pp.

It is well-known that each primitive Pythagorean triple of natural numbers is uniquely determined by a pair of natural numbers which are relatively prime and have different parities. In addition, Pythagorean triples were also characterized in an arbitrary unique factorization domain.

The set of Pythagorean triples of integers was also studied in terms of its structure. Binary operations can be defined so that this set is a semigroup, a group or a ring. In this thesis, we extend the ideas and investigate properties and structures of the semigroup of Pythagorean triples over Gaussian integers, the ring of Pythagorean triples over quadratic fields and biquadratic fields, and the group of Pythagorean triples over any number fields. Moreover, we determine all Pythagorean triples in the ring of integers of any number field.

Department : Mathematics and Computer Science Student's Signature ....
Advisor's Signature ....
Field of Study : Mathematics
Academic Year : 2011

ACKNOWLEDGEMENTS

I would like to express my deep gratitude to Associate Professor Dr. Ajchara Harnchoowong, my thesis advisor, for her helpful comments and suggestions in my thesis. Moreover, I would like to thank Associate Professor Dr. Patanee Udomkavanich, Assistant Professor Dr. Yotsanan Meemark, Assistant Professor Dr. Tuangrat Chaichana and Associate Professor Dr. Utsanee Leerawat, my thesis commitee, for value suggestions. Next, I am grateful to all of my teachers and lecturers during my study.

In particular, my sincere appreciation goes to Chulalongkorn University for Chulalongkorn University Graduate Scholarship to Commemorate the 72^{nd} Anniversary of His Majesty King Bhumibol Adulyadej and Conference Grant for Ph.D. student.

Finally, I wish to thank my beloved parents for their encouragement throughout my study.

CONTENTS

page

CHAPTER I
INTRODUCTION

1.1 Introduction

Let K be a number field with the ring of integers R. A triple (a, b, c) of elements of R is said to be a *Pythagorean triple* if $a^2+b^2 = c^2$. For $R = \mathbb{Z}$, Bryan Dawson [4] defined operations on the set of all Pythagorean triples so that this set is a ring. E. Eckert [5] defined an operation, addition, by $(a_1, b_1, c_1) + (a_2, b_2, c_2) = (a_1a_2 - b_1b_2, a_1b_2+b_1a_2, c_1c_2)$ so that the set of Pythagorean triples of natural numbers and (1, 0, 1) with + is a free abelian group. P. Zanardo and U. Zannier [11] generalized the domain from $\mathbb{Z}$ to the ring of integers R of any field K such that $i \notin R$. R. Beauregard and E. Suryanarayan [1] considered the set of Pythagorean triples over $\mathbb{Z}$ and defined $*$ by $(a_1, b_1, c_1) * (a_2, b_2, c_2) = (a_1a_2, b_1c_2 + b_2c_1, b_1b_2 + c_1c_2)$. The well-known representation of Pythagorean triples in Number Theory resulted in properties and a unique factorization theorem of primitive Pythagorean triples. The set of equivalence classes of Pythagorean triples is a free abelian group which is isomorphic to the multiplicative group of positive rationals. In this thesis, we wish to investigate properties and structures of the set of Pythagorean triples.

N. Sexauer [10] investigated solutions of the equation $x^2 + y^2 = z^2$ on unique factorization domains satisfying some hypotheses. Later, K. Kubota [6] characterized Pythagorean triples in an arbitrary unique factorization domain. Where R is the Gaussian integers, James T. Cross [3] displayed a method for generating all Pythagorean triples. Each equivalence class of primitive Pythagorean triples is mapped from a certain pair of Gaussian integers. In this thesis, we wish to determine all Pythagorean triples in the ring of integers of any number field.

In section 1.2, we introduce definitions and prove auxiliary theorems used throughout this thesis.

In chapter 2, we describe the unique factorization of primitive Pythagorean triples when R is the Gaussian integers.

In chapter 3, we consider a quadractic field and a biquadratic field such that its ring of integers R is a UFD. The set P of all Pythagorean triples in R is partitioned into P_η, sets of triples (α, β, γ) in P where $\eta = \gamma - \beta$. We show ring structures of each P_η and P from the ring structure of R.

In chapter 4, for any number field K with the ring of integers R, we characterize all Pythagorean triples in R and demonstrate an isomorphism between the multiplicative group of K and the group of Pythagorean triples of R. Moreover, we describe that the group of Pythagorean triples in R whose first components are non-zero with operation $*$ is isomorphic to the group of Pythagorean triples in R whose third components are non-zero with the operation $+$ defined above.

1.2 Preliminaries

In this section, we give notation, definitions and theorems used throughout the thesis. Details and proofs can be found in [7], [8] and [9] unless otherwise stated.

1.2.1 The Ring of Integers

Definition 1.2.1. A *number field* is a finite extension of $\mathbb{Q}$ (in $\mathbb{C}$).

Definition 1.2.2. Let K be an integral domain with identity 1. $\alpha \in K$ 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 1.2.3. $\alpha \in \mathbb{Q}$ is an algebraic integer if and only if $\alpha \in \mathbb{Z}$.

Definition 1.2.4. The ring of all algebraic integers in a number field K is called the *ring of integers* in K and denoted by $\mathcal{O}_K$.

Definition 1.2.5. An *embedding* of L over K in $\mathbb{C}$ is a one to one homomorphism $\sigma : L \to \mathbb{C}$ fixing K pointwise. An *embedding* of L in $\mathbb{C}$ is an embedding of L over $\mathbb{Q}$ in $\mathbb{C}$.

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 $\mathbb{C}$ denoted by $\sigma_1 = id_L, \sigma_2, \ldots, \sigma_n$.

Definition 1.2.6. For $\alpha \in L$, define the *relative trace* of α $=\mathrm{Tr}_{L/K}(\alpha) = \sigma_1(\alpha) + \sigma_2(\alpha) + \ldots + \sigma_n(\alpha)$ 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 denote $\mathrm{Tr}_{L/\mathbb{Q}}$ by Tr_L and $\mathrm{N}_{L/\mathbb{Q}}$ by N_L and call the *absolute trace* and *absolute norm*, respectively.

Definition 1.2.7. 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 $\mathrm{disc}_{L/K}(\alpha_1, \alpha_2, \ldots, \alpha_n) := det[\sigma_i(\alpha_j)]^2$.

Theorem 1.2.8. *Let K be a number field of degree n over $\mathbb{Q}$. Then $\mathcal{O}_K$ 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 $\mathbb{Z}$.*

Definition 1.2.9. 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 1.2.10. *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 1.2.11. 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.

1.2.2 Factorization of Elements in the Ring of Integers

The factorization of elements in the ring of integers will appear in chapters 2 and 3, especially chapter 2 where we show the unique factorization of a Pythagorean triple which comes from the prime factorization of its first component.

Definition 1.2.12. Let D be an integral domain with identity 1.
(1) Let $x, y \in D$ such that $x \neq 0$. x *divides* y (or y is divisible by x), in notation $x|y$, if and only if there exists $z \in D$ such that $y = xz$.
(2) $u \in D$ is a *unit* if and only if $u|1$.

(3) $x, y \in D$ are *associates* or y is an *associate* of x, in notation $x \sim y$, if and only if there exists a unit $u \in D$ such that $x = yu$.

(4) A nonzero nonunit $x \in D$ is *irreducible* if and only if for all $m \in D$, if $m|x$ then m is a unit or m and x are associates.

(5) A nonzero nonunit $x \in D$ is *prime* if and only if for all $m, n \in D$, if $x|mn$ then $x|m$ or $x|n$.

(6) Let $x, y \in D$ such that $x \neq 0$ or $y \neq 0$. A nonzero $d \in D$ is a *greatest common divisor* of x and y, in notation $d =$gcd(x, y), if and only if $d|x$ and $d|y$ and for all $z \in D$, if $z|x$ and $z|y$ then $z|d$.

Note.

(1) x and y are associates if and only if $x|y$ and $y|x$.

(2) If x is irreducible, then for every associate y of x, y is irreducible.

(3) If x is prime, then for every associate y of x, y is prime.

(4) If x and y are associates and $x = yz$ for some $z \in D$, then z is a unit.

Proposition 1.2.13. *Let D be an integral domain with identity 1 and $x, y \in D \smallsetminus \{0\}$. Then*

(i) x and y are associates if and only $< x >=< y >$.

(ii) x is prime if and only $< x >$ is a prime ideal.

Proposition 1.2.14. *Let $x, y \in \mathcal{O}_K$. Then*

(i) if $x|y$ in $\mathcal{O}_K$, then $\mathrm{N}_K(x)|\mathrm{N}_K(y)$ in $\mathbb{Z}$.

(ii) if x and y are associates, then $\mathrm{N}_K(x) = \pm\mathrm{N}_K(y)$.

Theorem 1.2.15. *Let D be a UFD. Then $x \in D$ is irreducible if and only if x is prime.*

1.2.3 Decomposition of Ideals

This subsection will be used for theorems about quadratic and biquadratic fields in the next subsection.

Theorem 1.2.16. *Every nonzero proper ideal in $\mathcal{O}_K$ can be written uniquely as a product of prime ideals.*

Definition 1.2.17. The *norm* of a nonzero ideal A in $\mathcal{O}_K$, denoted by $\mathrm{N}(A)$, is defined to be $|\mathcal{O}_K/A|$.

Theorem 1.2.18. *For any $\alpha \neq 0$ in $\mathcal{O}_K$, $\mathrm{N}(\langle\alpha\rangle)= |\mathrm{N}_K(\alpha)|$.*

Remark 1.2.19. If P is a nonzero ideal such that $\mathrm{N}(P) = p$ a prime number, then P is a prime ideal in $\mathcal{O}_K$.

Let $L \supseteq K$ be a finite extension of number fields. Let P be a nonzero prime ideal in $\mathcal{O}_K$. Then $P\mathcal{O}_L$ is a nonzero ideal in $\mathcal{O}_L$. We will consider the prime factorization of $P\mathcal{O}_L$ in $\mathcal{O}_L$. From now on, the term *prime ideals* means *nonzero prime ideals.*

Theorem 1.2.20. *Let P be a prime ideal in $\mathcal{O}_K$ and $\mathcal{P}$ be a prime ideal in $\mathcal{O}_L$. Then the following are equivalent.*
(i) $\mathcal{P}|P\mathcal{O}_L$.
(ii) $\mathcal{P} \supset P\mathcal{O}_L$.
(iii) $\mathcal{P} \supset P$.
(iv) $\mathcal{P} \cap \mathcal{O}_K = P$.
(v) $\mathcal{P} \cap K = P$.

Definition 1.2.21. For P and $\mathcal{P}$ satisfying any of the above theorem, we say that $\mathcal{P}$ *lies over/above* P or P *lies under* $\mathcal{P}$.

Definition 1.2.22. Let $P\mathcal{O}_L = \displaystyle\prod_{i=1}^{g} \mathcal{P}_i^{e_i}$ be the prime factorization 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.

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 1.2.23. 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 1.2.24. $\mathrm{N}(\mathcal{P}_i) = \mathrm{N}(P)^f$ where $f = f(\mathcal{P}_i/P)$.

Theorem 1.2.25. *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 $n = \sum\limits_{i=1}^{g} e_i f_i$.*

Definition 1.2.26. 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 $f_1 = 1$ and $P\mathcal{O}_L = \mathcal{P}_1^n$.

(2) P *splits completely* in L if $g = n$, so $e_i = 1$, $f_1 = 1$ for all i and $P\mathcal{O}_L = \mathcal{P}_1\mathcal{P}_2 \ldots \mathcal{P}_n$.

Theorem 1.2.27. *Let $L \supseteq K$ be a Galois extension 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., $P\mathcal{O}_L = (\mathcal{P}_1 \ldots \mathcal{P}_g)^e$, hence $n = efg$ where $e = e(\mathcal{P}_i/P)$ and $f = f(\mathcal{P}_i/P)$.*

1.2.4 Quadratic and Biquadratic Fields

We collect necessary results of quadratic and biquadratic fields here. These properties will be used in chapter 3.

Definition 1.2.28. A *quadratic extension* is a field extension E over F of degree two, 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. The integral basis of K can be found as follows [7].

Theorem 1.2.29. *Let $K = \mathbb{Q}[\sqrt{d}]$ where d is a squarefree integer.*
(i) If $d \equiv 1 \pmod 4$, then

$$\mathcal{O}_K = \left\{ \frac{u + v\sqrt{d}}{2} | u, v \in \mathbb{Z} \text{ and } u \equiv v \pmod 2 \right\} = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right].$$

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 $3 \pmod 4$, then

$$\mathcal{O}_K = \left\{ u + v\sqrt{d} | u, v \in \mathbb{Z} \right\} = \mathbb{Z}[\sqrt{d}].$$

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

Next, the decomposition of principal ideals generated by 2 in quadratic fields can be determined in the following theorem [7].

Theorem 1.2.30. *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 $d \equiv 2$ or $3 \pmod 4$.

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

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

Moreover, if $2\mathbb{Z}$ is totally ramified in $\mathcal{O}_K$, there is a prime $\delta \in \mathcal{O}_K$ such that $2 \sim \delta^2$ and $|\mathcal{O}_K / <\delta>| = 2$. If $2\mathbb{Z}$ splits completely in $\mathcal{O}_K$, there are non-associate prime $\delta, \overline{\delta} \in \mathcal{O}_K$ such that $2 \sim \delta\overline{\delta}$ and $|\mathcal{O}_K / <\delta>| = \left|\mathcal{O}_K / <\overline{\delta}>\right| = 2$. If $2\mathbb{Z}$ is inert in $\mathcal{O}_K$, 2 is a prime in $\mathcal{O}_K$.

Definition 1.2.31. A *biquadratic field* is an extension of degree four over $\mathbb{Q}$ of the form $\mathbb{Q}[\sqrt{m}, \sqrt{n}]$ where m, n are distinct squarefree integers.

The study of the decomposition of principal ideals generated by 2 in biquadratic fields can be found in [2].

Theorem 1.2.32. *Let $K = \mathbb{Q}[\sqrt{d_1}, \sqrt{d_2}] \supset k_i = \mathbb{Q}[\sqrt{d_i}]$ where, for $i = 1, 2, 3$, d_i are discriminant of k_i, $d_3 = d_1 d_2 / t^2$ and $t \in \mathbb{Z}$. Then*

(i) $2 = \delta^4$ if $d_1 \equiv d_2 \equiv 8 \pmod{16}$ and $d_3 \equiv 12 \pmod 8$.

(ii) $2 = \delta^2$ if $d_1 \equiv d_2 \equiv 8$ or $12 \pmod{16}$ and $d_3 \equiv 5 \pmod 8$.

(iii) $2 = \delta_1^2 \delta_2^2$ if $d_1 \equiv d_2 \equiv 8$ or $12 \pmod{16}$ and $d_3 \equiv 1 \pmod 8$.

(iv) $2 = \delta_1\delta_2\delta_3\delta_4$ *if* $d_1 \equiv d_2 \equiv d_3 \equiv 1 \pmod 8$.

(v) $2 = \delta_1\delta_2$ *if* $d_1 \equiv d_2 \equiv 5 \pmod 8$ *and* $d_3 \equiv 1 \pmod 8$.

CHAPTER II
THE SEMIGROUP OF PYTHAGOREAN TRIPLES OVER GAUSSIAN INTEGERS

Inspired by R. Beauregard and E. Suryanarayan's work [1], this chapter investigates the unique factorization of primitive Pythagorean triples over the Gaussian integers.

2.1 The Semigroup

Let PT be the set of all Pythagorean triples in the ring of Gaussian integers where their first components are non-zero; i.e.,

$$PT = \{(a, b, c) \mid a, b, c \in \mathbb{Z}[i] \text{ with } a \neq 0 \text{ and } a^2 + b^2 = c^2\}.$$

Define the operation $*$ on PT by

$$(a_1, b_1, c_1) * (a_2, b_2, c_2) = (a_1a_2, b_1c_2 + b_2c_1, b_1b_2 + c_1c_2). \tag{2.1}$$

Proposition 2.1.1. *The set PT under the operation $*$ is a commutative monoid with the identity element $(1, 0, 1)$.*

Proof. Let $(a_1, b_1, c_1), (a_2, b_2, c_2), (a_3, b_3, c_3) \in PT$. It is easy to see that $(a_1a_2)^2 + (b_1c_2+b_2c_1)^2 = (b_1b_2+c_1c_2)^2$ and $[(a_1, b_1, c_1)*(a_2, b_2, c_2)]*(a_3, b_3, c_3) = (a_1, b_1, c_1)* [(a_2, b_2, c_2)*(a_3, b_3, c_3)]$. Clearly, $(PT, *)$ is commutative. Since $(a, b, c)*(1, 0, 1) = (a, b, c)$, we have that $(1, 0, 1)$ is the identity element in PT. Therefore, $(PT, *)$ is a commutative monoid. □

K. Kubota [6] determined the representation of Pythagorean triples in a unique factorization domain. We applied the theorem to the ring of the Gaussian integers.

Proposition 2.1.2. *If $(a, b, c) \in PT$, then there exist $f, u, v, d \in \mathbb{Z}[i]$ where d is a factor of 2 relatively prime to f and $d \mid u^2 \pm v^2$ such that*

$$a = \frac{2fuv}{d}, \qquad b = \frac{f(u^2 - v^2)}{d}, \qquad \text{and } c = \frac{f(u^2 + v^2)}{d}. \tag{2.2}$$

Definition 2.1.3. A Pythagorean triple (a, b, c) is said to be *primitive* if the components a, b, c have no common divisor.

Corollary 2.1.4. *If $(a, b, c) \in PT$ is primitive, then there exist $u, v, d \in \mathbb{Z}[i]$ where d is a factor of 2 and $d \mid u^2 \pm v^2$ such that*

$$a = \frac{2uv}{d}, \qquad b = \frac{u^2 - v^2}{d}, \qquad \text{and } c = \frac{u^2 + v^2}{d}. \tag{2.3}$$

Proof. From Proposition 2.1.2, if f is not a unit, then (a, b, c) is not primitive. □

Parity makes things much easier in $\mathbb{Z}$. James T. Cross [3] use $\delta := 1 + i$ to define "even" and "odd" Gaussian integers and gave a proof of the following lemma.

Lemma 2.1.5. $\mathbb{Z}[i] / < \delta > = \{[0], [1]\}$.

Here $[0]$ and $[1]$ are the residue classes of 0 and 1 in $\mathbb{Z}[i] / < \delta >$, respectively.

Definition 2.1.6. Let a be a Gaussian integer. We say that a is *even* or *odd* according as a is in the residue class determined by 0 or 1, respectively.

It follows that the sum of two even or two odd Gaussian integers gives an even one, the sum of an even Gaussian integer and an odd one gives an odd one, the product of two odd ones gives an odd one, and the product of an even one and any Gaussian integer gives an even one.

Lemma 2.1.7. *If $(a, b, c) \in PT$ is primitive, then only one of a, b, c is even and the others are odd.*

Proof. Suppose that two of a, b, c are even. Since $a^2 + b^2 = c^2$, all a, b, c are even. This contradicts the fact that (a, b, c) is primitive. □

A significant difference between the set of integers and the set of Gaussian integers is i. This number is the key to the next lemma which plays important role in several following theorems. The proof is straightforward.

Lemma 2.1.8. *$(a, b, c) \in PT$ if and only if $(c, bi, a) \in PT$.*

Recall that the notation $a \sim b$ will be used when a and b are associates, i.e., $b = \pm a$ or $\pm ai$. For example, if $d \mid 2$, then $d \sim 1$, δ or δ^2.

Proposition 2.1.9. *For each primitive triple (a, b, c) in PT, either a, b or c is a multiple of δ^3.*

Proof. By Lemma 2.1.7, only one of a, b, c is even and the others are odd. If a is an even Gaussian integer, by Corollary 2.1.4, there exist Gaussian integers u, v, d where $d \mid 2$ and $d \mid u^2 \pm v^2$ such that

$$a = \frac{2uv}{d}, \qquad b = \frac{u^2 - v^2}{d}, \qquad \text{and } c = \frac{u^2 + v^2}{d}.$$

Case 1 : u is even and v is odd. Then $u^2 - v^2$ is odd. Since b is odd, we have $d \sim 1$. Hence $a \sim 2uv$ and thus a is divisible by δ^3.
Case 2 : u is odd and v is even. This is similar to the above case.
Case 3 : u and v are odd. Both $u - v$ and $u + v$ are divisible by δ. Therefore, $u^2 - v^2$ is divisible by δ^2. Since b is odd, it follows that $d \sim \delta^2 \sim 2$ and $a \sim uv$. Hence a is odd, a contradiction.
Case 4 : u and v are even. If $\delta^2 \mid u$ or $\delta^2 \mid v$, then a is divisible by δ^3 and we are done. Suppose that $\delta^2 \nmid u$ and $\delta^2 \nmid v$. Thus $u = \delta u_1$ and $v = \delta v_1$ where u_1, v_1 are odd Gaussian integers. Since $b = (u^2 - v^2)/d = \delta^2(u_1^2 - v_1^2)/d$ and $u_1^2 - v_1^2$ is even, b is even. This is a contradiction.

For the case that b is even, we can prove in a similar way.

When c is even by Lemma 2.1.8, $(c, bi, a) \in PT$ and the above proof shows that c is divisible by δ^3. □

From Proposition 2.1.9 and Lemma 2.1.7, there are no Gaussian integers b_1, b_2, c_1, c_2 such that (δ, b_1, c_1) and $(2, b_2, c_2)$ are primitive. However, every odd prime appears in specific forms of primitive Pythagorean triples.

Proposition 2.1.10. *Let p be an odd prime in the Gaussian integers (i.e., $p \nsim \delta$). If p occurs as a component of a primitive Pythagorean triple in PT, then it must be one of the following forms:*

(i) $(p, \pm\frac{p^2-1}{2}, \pm\frac{p^2+1}{2})$ *and* $(p, \pm\frac{p^2+1}{2}i, \pm\frac{p^2-1}{2}i)$

(ii) $(\pm\frac{p^2-1}{2}, p, \pm\frac{p^2+1}{2})$ *and* $(\pm\frac{p^2+1}{2}i, p, \pm\frac{p^2-1}{2}i)$

(iii) $(\pm\frac{p^2+1}{2}, \pm\frac{p^2-1}{2}i, p)$ *and* $(\pm\frac{p^2-1}{2}i, \pm\frac{p^2+1}{2}, p)$.

Proof. First we will show that $(p, \pm\frac{p^2-1}{2}, \pm\frac{p^2+1}{2})$ and $(p, \pm\frac{p^2+1}{2}i, \pm\frac{p^2-1}{2}i)$ are elements in PT. If p is a prime in $\mathbb{Z}$, then $p \equiv 3 \pmod 4$ and it is obvious that $\frac{p^2 \pm 1}{2} \in \mathbb{Z}$. If $p \notin \mathbb{Z}$, then $p \sim a + bi$ where $a, b \in \mathbb{Z}$, $a > 0$, $b \neq 0$ and $a^2 + b^2 \equiv 1 \pmod 4$. Hence $a^2 - b^2 \equiv 1 \pmod 2$ and

$$\frac{p^2 \pm 1}{2} = \frac{\pm(a+bi)^2 \pm 1}{2} = \frac{\pm(a^2 - b^2 + 2abi) \pm 1}{2} = \frac{\pm(a^2 - b^2 \pm 1) \pm 2abi}{2}$$

are Gaussian integers.

Now we will show that case (i) is the only way in which p can occur as the first component of a primitive Pythagorean triple. Let $(p, b, c) \in PT$. By Corollary 2.1.4, there exist Gaussian integers u, v, d where $d \mid 2$ and $d \mid u^2 \pm v^2$ such that

$$p = \frac{2uv}{d}, \qquad b = \frac{u^2 - v^2}{d}, \qquad \text{and } c = \frac{u^2 + v^2}{d}.$$

Since p is odd, $p \nsim 2/d$. Therefore, $p \sim u$ or $p \sim v$. If $p \sim u$, then $v \sim 1$ and d follows from $p = 2uv/d$. It can be seen that there exist exactly sixteen combinations that satisfy the conditions that $p \sim u$ (i.e., $p = u, -u, ui, -ui$) and $v \sim 1$ (i.e., $v = 1, -1, i, -i$). Upon substituting each of these combinations into the formulas for b and c, we obtain four possible forms as follows: $(p, (p^2 - 1)/2, (p^2 + 1)/2)$, $(p, -(p^2 - 1)/2, -(p^2 + 1)/2)$, $(p, (p^2 + 1)i/2, (p^2 - 1)i/2)$ and $(p, -(p^2 + 1)i/2, -(p^2 - 1)i/2)$. If $p \sim v$, then $u \sim 1$. Substituting the sixteen combinations that satisfy the condition into the formulas given in Corollary 2.1.4, we obtain four formulas where each of the middle components has the different sign from the four previous formulas as follows: $(p, -(p^2 - 1)/2, (p^2 + 1)/2)$, $(p, (p^2 - 1)/2, -(p^2 + 1)/2)$, $(p, -(p^2 + 1)i/2, (p^2 - 1)i/2)$ and $(p, (p^2 + 1)i/2, -(p^2 - 1)i/2)$.

Case (ii) can be proved similarly and case (iii) follows from Lemma 2.1.8. □

Since each Gaussian integer has the unique factorization up to units, this fact effects the unique factorization of each Pythagorean triple. We then introduce units and irreducible elements in PT.

Definition 2.1.11. $(a,b,c) \in PT$ is called a *unit* if there exists $(d,e,f) \in PT$ such that $(a,b,c) * (d,e,f) = (1,0,1)$.

Lemma 2.1.12. *All units in PT are $(\pm 1, 0, \pm 1)$, $(\pm 1, \pm i, 0)$, $(\pm i, 0, \pm i)$ and $(\pm i, \pm 1, 0)$.*

Proof. If $(1,b,c) \in PT$, then there exist $u, v, d \in \mathbb{Z}[i]$ where $d \mid 2$ and $d \mid u^2 \pm v^2$ such that

$$1 = \frac{2uv}{d}, \qquad b = \frac{u^2 - v^2}{d}, \qquad \text{and } c = \frac{u^2 + v^2}{d}$$

by Corollary 2.1.4. This implies that $d \sim 2$, $u \sim 1$, $v \sim 1$ and all triples satisfying these conditions are $(1,0,\pm 1)$ and $(1, \pm i, 0)$. Since the first component of a unit in PT must associate 1, we are done. □

Definition 2.1.13. Let $(a,b,c), (d,e,f) \in PT$. If there exists a unit $(x,y,z) \in PT$ such that $(a,b,c) = (d,e,f) * (x,y,z)$, we say that (a,b,c) *associates* (d,e,f) denoted by $(a,b,c) \approx (d,e,f)$.

For example, $(3,4,5) \approx (3, 5i, 4i)$ since $(3,5i,4i) = (3,4,5) * (1,i,0)$.

Definition 2.1.14. A non-unit $(a,b,c) \in PT$ is said to be *irreducible* provided that: whenever $(a,b,c) = (u,v,w) * (x,y,z)$ we will have (u,v,w) or (x,y,z) is a unit.

For example, $(1+2i, -2+2i, -1+2i)$ is irreducible but $(12,5,13) = (3,4,5) * (4,-3,5)$ is not. Furthermore, every triple in case (i) of Proposition 2.1.10 is irreducible because the prime p cannot be factored.

Proposition 2.1.15. *For each positive integer $k \geq 3$, δ^k occurs as the first component of a primitive Pythagorean triple in PT as follows and in no other way: $(\delta^k, \pm(\delta^{2k-4}+1), \pm(\delta^{2k-4}-1))$ and $(\delta^k, \pm(\delta^{2k-4}-1)i, \pm(\delta^{2k-4}+1)i)$. Moreover, these triples are irreducible.*

Proof. Let $(\delta^k, b, c) \in PT$ be primitive. By Lemma 2.1.7, b and c must be odd. Then

$$\delta^k = \frac{2uv}{d}, \qquad b = \frac{u^2 - v^2}{d}, \qquad \text{and } c = \frac{u^2 + v^2}{d}$$

for some Gaussian integers u, v, d where $d \mid 2$ and $d \mid u^2 \pm v^2$ by Corollary 2.1.4.

Case 1 : u is even and v is odd. Then $u^2 - v^2$ is odd. Since b is odd, $d \sim 1$ and $\delta^k \sim 2uv$. Hence $v \sim 1$ and $u \sim \delta^{k-2}$. These conditions give rise to four possible forms, namely, $(\delta^k, \delta^{2k-4} + 1,\ \delta^{2k-4} - 1)$, $(\delta^k, -(\delta^{2k-4} + 1),\ -(\delta^{2k-4} - 1))$, $(\delta^k, (\delta^{2k-4} - 1)i, (\delta^{2k-4} + 1)i)$ and $(\delta^k, -(\delta^{2k-4} - 1)i, -(\delta^{2k-4} + 1)i)$.

Case 2 : u is odd and v is even. Similarly, $d \sim 1$, $u \sim 1$ and $v \sim \delta^{k-2}$. We obtain another four possible forms where the middle components have different signs from the previous case: $(\delta^k, -(\delta^{2k-4} + 1), \delta^{2k-4} - 1)$, $(\delta^k, \delta^{2k-4} + 1, -(\delta^{2k-4} - 1))$, $(\delta^k, -(\delta^{2k-4} - 1)i, (\delta^{2k-4} + 1)i)$ and $(\delta^k, (\delta^{2k-4} - 1)i, -(\delta^{2k-4} + 1)i)$.

Case 3 : u and v are odd. Since $\delta^k = 2uv/d$ and $k \geq 3$, this is a contradiction.

Case 4 : u and v are even. Since $b = (u^2 - v^2)/d$ is odd, $d \sim 2$ and u, v cannot be both divisible by δ^2. If $u \sim \delta$, then $v \sim \delta^{k-1}$ and the result is the same as in case 2. For $v \sim \delta$, we have $u \sim \delta^{k-1}$ and the result is the same as in case 1.

Now suppose that $(\delta^k, b, c) = (\delta^i, b_1, c_1) * (\delta^j, b_2, c_2)$ where $b_1, b_2, c_1, c_2 \in \mathbb{Z}[i]$ and $i, j \in \mathbb{N}$. Since (δ^k, b, c) is primitive, (δ^i, b_1, c_1) and (δ^j, b_2, c_2) are primitive. By Lemma 2.1.7, b_1, b_2, c_1, c_2 are odd. Then $c = b_1 b_2 + c_1 c_2$ is even, a contradiction. Hence (δ^k, b, c) is irreducible. □

2.2 Unique Factorization Theorem

The unique factorization of any primitive Pythagorean triple (a, b, c) is reflected by the unique factorization of a, its first component. The following theorem shows how a primitive Pythagorean triple can be factored into a product of irreducible triples. We use the usual integer-exponent notation. For example, $A^0 = (1, 0, 1)$, $A^1 = A$, $A^2 = A * A$ for $A \in PT$.

Theorem 2.2.1. *(Unique factorization theorem)*

Let $A = (a, b, c) \in PT$ be primitive and $a = \mu \delta^{s_0} p_1^{s_1} ... p_k^{s_k}$, where μ is a unit, p_i

are non-associate odd primes, s_i are non-negative integers and $s_0 \neq 1, 2$. Then A has the unique (up to order of factors and the multiplication of factors by units) factorization

$$A = P_0 * P_1^{s_1} * \ldots * P_k^{s_k}$$

where

$$P_0 \approx \begin{cases} (1, 0, 1) & \textit{if } a \textit{ is odd,} \\ (\delta^{s_0}, \pm(\delta^{2s_0-4}+1), \delta^{2s_0-4}-1) & \textit{if } a \textit{ is even} \end{cases}$$

and

$$P_i \approx (p_i, \pm\frac{p_i^2-1}{2}, \frac{p_i^2+1}{2})$$

for $i \geq 1$. The choice of $\pm$ depending on (a, b, c).

Proof. There exist Gaussian integers u, v, d where $d \mid 2$ and $d \mid u^2 \pm v^2$ such that

$$a = \frac{2uv}{d}, \qquad b = \frac{u^2-v^2}{d}, \qquad \text{and } c = \frac{u^2+v^2}{d}.$$

If a is odd, then $d \sim 2$. We obtain

$$\begin{aligned}(a, b, c) &\approx (uv, \frac{u^2-v^2}{2}, \frac{u^2+v^2}{2}) \\ &= (u, \frac{u^2-1}{2}, \frac{u^2+1}{2}) * (v, \frac{1-v^2}{2}, \frac{1+v^2}{2})\end{aligned}$$

where the two triples on the right-hand side are elements in PT. Mathematical induction implies the factorization in this case.

In case that a is even, b and c are odd by Lemma 2.1.7. The parity of u and v can be divided into four cases as follows:

Case 1 : u is even and v is odd. Since $b = (u^2 - v^2)/d$ is odd, $d \sim 1$. Let $2u = \delta^k n$ where n is an odd Gaussian integer and $k \in \mathbb{N}$. Then

$$\begin{aligned}(a, b, c) &\approx (2uv, u^2 - v^2, u^2 + v^2) \\ &= (\delta^k nv, -\delta^{2k-4}n^2 - v^2, -\delta^{2k-4}n^2 + v^2) \\ &= (\delta^k, -(\delta^{2k-4}+1), -(\delta^{2k-4}-1)) * (nv, (n^2-v^2)/2, (n^2+v^2)/2).\end{aligned}$$

Since n and v are odd, $(nv, (n^2 - v^2)/2, (n^2 + v^2)/2) \in PT$ is primitive. We then factor $(nv, (n^2 - v^2)/2, (n^2 + v^2)/2)$ as in the odd case.

Case 2 : u is odd and v is even. This is similar to the above case.

Case 3 : u and v are odd. Then δ^3 does not divide a. This is a contradiction.

Case 4 : u and v are even. Thus $u = \delta m$ and $v = \delta n$ for some $m, n \in \mathbb{Z}[i]$. Since $b = (u^2 - v^2)/d = (\delta^2 m^2 - \delta^2 n^2)/d$ is odd, we have $d \sim 2$ and $b \sim m^2 - n^2$. This means that m and n must have the different parity. Then $(a, b, c) \approx (2mn, m^2 - n^2, m^2 + n^2)$ which can be factored as in case 1 or case 2.

From the property that $(x, y, z) * (x, -y, z) = (x^2, 0, x^2)$ for all $(x, y, z) \in PT$, the choice ± of the term $P_i^{s_i}$ of A cannot vary, otherwise A would not be primitive. Since a determines the first components of all factors of A, we assume that

$$A = P_0 * P_1^{s_1} * ... * P_k^{s_k} = Q_0 * Q_1^{s_1} * ... * Q_k^{s_k}$$

where for each i, P_i and Q_i are irreducible triples with identical first components. Now if $P = (x, y, z)$, we define $P' = (x, -y, z)$. If $P_j \approx Q_j$ for some j, it can be cancelled by multiplying P'_j on both sides of the equation. Repeating this process until we have

$$P_{x_0} * P_{x_1} * ... * P_{x_m} = Q_{x_0} * Q_{x_1} * ... * Q_{x_m}$$

which is a factor of A and P_{x_i} does not associate Q_{x_i}. Propositions 2.1.10 and 2.1.15 and Lemma 2.1.12 show that $P_{x_i} \approx Q'_{x_i}$. Then, by multiplying the above equation by each of the Q'_{x_i}, we have

$$(P_{x_0} * P_{x_1} * ... * P_{x_m})^2 = (r^2, 0, r^2)$$

where the Gaussian integer r is the product of the first components of P_{x_i}. It follows that $P_{x_0} * P_{x_1} * ... * P_{x_m} \approx (r, 0, r)$ which contradicts primitivity. This completes the proof. □

Observe that $(l, 0, l) * (a, b, c) = (la, lb, lc)$. We will use the notation $l(a, b, c)$ for $(l, 0, l) * (a, b, c)$ in the next proposition which indicates how $(\delta^k, \pm(\delta^{2k-4} + 1), \delta^{2k-4} - 1)$ can be generated from $(\delta^3, \pm(\delta^2 + 1), \delta^2 - 1)$.

Proposition 2.2.2. *If $k \geq 3$ is an integer, then $\delta^{2k-6}(\delta^k, \delta^{2k-4}+1, \delta^{2k-4}-1) \approx (\delta^3, \delta^2+1, \delta^2-1)^{k-2}$ and $\delta^{2k-6}(\delta^k, -(\delta^{2k-4}+1), \delta^{2k-4}-1) \approx (\delta^3, -(\delta^2+1), \delta^2-1)^{k-2}$.*

Proof. It is trivial when $k = 3$. For $k > 3$,

$$\begin{aligned}
\delta^2(\delta^k, \delta^{2k-4}+1, \delta^{2k-4}-1) &= (\delta^{k+2}, \delta^{2k-2}+\delta^2, \delta^{2k-2}-\delta^2)\\
&\approx (\delta^{k+2}, -(\delta^{2k-2}-\delta^2)i, -(\delta^{2k-2}+\delta^2)i)\\
&= (\delta^{k+2}, 2\delta^{2k-4}-2, 2\delta^{2k-4}+2)\\
&= ((\delta^3)(\delta^{k-1}), (\delta^2+1)(\delta^{2k-6}-1)+(\delta^2-1)(\delta^{2k-6}+1),\\
&\quad (\delta^2+1)(\delta^{2k-6}+1)+(\delta^2-1)(\delta^{2k-6}-1))\\
&= (\delta^3, \delta^2+1, \delta^2-1) * (\delta^{k-1}, \delta^{2k-6}+1, \delta^{2k-6}-1).
\end{aligned}$$

Mathematical induction gives the desired result. When middle components have different signs the proof is similar. □

Example 2.2.3. For the primitive triple $(96+72i, -24+151i, 24+137i)$ and $96+72i = \delta^6 \cdot 3 \cdot (1+2i)^2$, Proposition 2.2.1 provides $(96+72i, -24+151i, 24+137i)$ $= (\delta^6, \delta^8+1, \delta^8-1) * (3, 5i, 4i) * (1+2i, 2-2i, -1+2i)^2$. By Proposition 2.2.2, $\delta^6(96+72i, -24+151i, 24+137i)$ can be written as $(1, -i, 0) * (\delta^3, \delta^2+1, \delta^2-1)^4 * (3, 5i, 4i) * (1+2i, 2-2i, -1+2i)^2$.

CHAPTER III
THE RING OF PYTHAGOREAN TRIPLES OVER QUADRATIC FIELDS AND BIQUADRATIC FIELDS

Let K be a number field such that the ring of integers R of K is a UFD. Let P be the set of all Pythagorean triples in R; i.e.,

$$P = \{(\alpha, \beta, \gamma) \in R^3 \mid \alpha^2 + \beta^2 = \gamma^2\}.$$

The set P is partitioned into sets

$$P_\eta = \{(\alpha, \beta, \gamma) \in P \mid \gamma - \beta = \eta\}$$

for all $\eta \in R$. Bryan Dawson [4] gave a construction in such a way as to give P and P_η ring structures when $R = \mathbb{Z}$. We apply his ideas on quadratic fields and biquadratic fields.

Throughout this chapter, all variables will be assumed to represent algebraic integers unless otherwise stated. The notation $\lceil r \rceil$ will be used for the smallest rational integer greater than or equal to the real number r.

3.1 Pythagorean Triples Over Quadratic Fields

This section shows how to find all elements of each P_η with all elements of P as the byproducts when $K = \mathbb{Q}[\sqrt{d}]$ where d is a squarefree integer.

The parity is significant in many theorems about Pythagorean triples. Lemma 2.1.5 shows that $1 + i$ plays a role in the ring of Gaussian integers like that played by 2 in $\mathbb{Z}$. We employ this concept by using Theorem 1.2.30.

We will separate each case of R into three subsections. If 2 is ramified in R, there is a prime $\delta \in R$ such that $2 \sim \delta^2$ and $|R/ < \delta >| = 2$. For $\alpha \in R$, we may say that α is *even* if α is divisible by δ and α is *odd* otherwise. It follows that all elementary properties of evenness and oddness hold. For example, the sum of an even algebraic integer and an odd one is odd. Moreover, since $\delta|2$, 2 and all integers that are divisible by 2 are even algebraic integers. All units in R are odd. In case that 2 splits completely in R, there are non-associate primes $\delta, \overline{\delta} \in R$ such that $2 \sim \delta\overline{\delta}$ and $|R/<\delta>| = \left|R/<\overline{\delta}>\right| = 2$. If 2 is inert in R, 2 is a prime in R.

Let π be a prime in R. The set $R \setminus \pi R$ contains all elements of R which are not divisible by π. We use the countability property of R to show a connection between $R \setminus \pi R$ and R which leads to a one-to-one correspondence between P_η and R.

Definition 3.1.1. Let π be a prime in R. All non-associate primes in R can be put into order, say π, π_1, π_2, π_3,... Define $\Psi_\pi : (R \setminus \pi R) \to R$ by

$$\Psi_\pi(u\pi_1^{a_1}\pi_2^{a_2}\pi_3^{a_3}...) = u\pi^{a_1}\pi_1^{a_2}\pi_2^{a_3}...$$

where $\{a_1, a_2, ...\} \subset \mathbb{Z}_0^+$ and u is a unit in R. It is not difficult to see that the mapping Ψ_π is a one-to-one correspondence.

First, we consider the case that $\eta = 0$.

Theorem 3.1.2. $P_0 = \{(0, \beta, \beta) \mid \beta \in R\}$ *and the mapping* $\varphi : P_0 \to R$ *defined by*

$$\varphi((0, \beta, \beta)) = \beta$$

is a one-to-one correspondence.

3.1.1 2 is Ramified in R

In this subsection, there is a prime $\delta \in R$ such that $2 \sim \delta^2$ and $|R/<\delta>| = 2$. To show a ring structure of P_η and P, we characterize P_η and define bijections by considering three cases of η where η is odd, $\delta||\eta$, and $\delta^2|\eta$ in the following theorems.

Theorem 3.1.3. *Let η be an odd algebraic integer and $\eta = u\pi_1^{a_1}\pi_2^{a_2}...\pi_m^{a_m}$ where $a_k \in \mathbb{Z}_0^+$, u is a unit and $\pi_k \in R$ are non-associate odd primes. Set $\rho = \pi_1^{b_1}\pi_2^{b_2}...\pi_m^{b_m}$ where $b_k = \lceil \frac{a_k}{2} \rceil$. Then P_η is*

$$\left\{ \left(\alpha, \frac{\alpha^2 - \eta^2}{2\eta}, \frac{\alpha^2 + \eta^2}{2\eta} \right) \mid \alpha = \tau\rho \text{ for some odd } \tau \in R \right\}.$$

Moreover, the mapping $\varphi : P_\eta \longrightarrow R$ defined by

$$\varphi((\alpha, \beta, \gamma)) = \Psi_\delta(\frac{\alpha}{\rho})$$

is a one-to-one correspondence.

Proof. Suppose $(\alpha, \beta, \gamma) \in P_\eta$. Since $\eta = \gamma - \beta$, we have

$$(\alpha, \beta, \gamma) = (\alpha, \frac{\alpha^2 - \eta^2}{2\eta}, \frac{\alpha^2 + \eta^2}{2\eta}).$$

Therefore, $2\eta|\alpha^2 + \eta^2$. Thus $\alpha^2 + \eta^2$ is even. Since η^2 is odd, α^2 is odd and so is α. We also have $\eta|\alpha^2 + \eta^2$. Hence $\eta|\alpha^2$. This means that $\pi_1^{a_1}\pi_2^{a_2}...\pi_m^{a_m}|\alpha^2$. Since for each $k = 1, ..., m$, $b_k = \lceil \frac{a_k}{2} \rceil$, we have $\pi_1^{b_1}\pi_2^{b_2}...\pi_m^{b_m}|\alpha$. Then $\alpha = \tau\rho$ for some odd $\tau \in R$.

Conversely, suppose $\alpha = \tau\rho$ where τ is odd. Then α is odd and $\alpha^2 = \tau^2\pi_1^{2b_1}\pi_2^{2b_2}...\pi_m^{2b_m}$. Since $2b_k = 2\lceil \frac{a_k}{2} \rceil \geq a_k$, we have $\pi_1^{a_1}\pi_2^{a_2}...\pi_m^{a_m}|\alpha^2$. Hence $\eta|\alpha^2 - \eta^2$. Since α and η are odd, $\alpha + \eta$ and $\alpha - \eta$ are divisible by δ. Then $2|\alpha^2 - \eta^2$. Since $\gcd(\eta, 2) = 1$, we have $2\eta|\alpha^2 - \eta^2$ and thus $2\eta|\alpha^2 + \eta^2$.

If $(\alpha, \beta, \gamma) \in P_\eta$, then α/ρ is an odd algebraic integer and $\Psi_\delta(\alpha/\rho)$ makes the mapping φ injective and surjective. □

Example 3.1.4. Let $R = \mathbb{Z}[i]$. For $\eta = i$, we have $\rho = 1$ and

τ odd	$\alpha = \tau$	$\beta = \frac{\alpha^2+1}{2i}$	$\gamma = \frac{\alpha^2-1}{2i}$
± 1	± 1	$-i$	0
$\pm i$	$\pm i$	0	i
$\pm(1+2i)$	$\pm(1+2i)$	$2+i$	$2+2i$
$\pm(1-2i)$	$\pm(1-2i)$	$-2+i$	$-2+2i$
$\pm(2+i)$	$\pm(2+i)$	$2-2i$	$2-i$
$\pm(2-i)$	$\pm(2-i)$	$-2-2i$	$-2-i$

Theorem 3.1.5. *Let η be an even algebraic integer and $\eta = u\delta\pi_1^{a_1}\pi_2^{a_2}...\pi_m^{a_m}$ where $a_k \in \mathbb{Z}_0^+$, u is a unit and $\pi_k \in R$ are non-associate odd primes. Set $\rho = \delta\pi_1^{b_1}\pi_2^{b_2}...\pi_m^{b_m}$ where $b_k = \lceil \frac{a_k}{2} \rceil$. Then P_η is*

$$\left\{ \left(\alpha, \frac{\alpha^2 - \eta^2}{2\eta}, \frac{\alpha^2 + \eta^2}{2\eta} \right) \mid \alpha = \tau\rho \textit{ for some odd } \tau \in R \right\}.$$

Moreover, the mapping $\varphi : P_\eta \to R$ defined by

$$\varphi((\alpha, \beta, \gamma)) = \Psi_\delta(\frac{\alpha}{\rho})$$

is a one-to-one correspondence.

Proof. Suppose $(\alpha, (\alpha^2 - \eta^2)/2\eta, (\alpha^2 + \eta^2)/2\eta) \in P_\eta$. Then $2\eta | \alpha^2 + \eta^2$. We have $\delta^3\pi_1^{a_1}\pi_2^{a_2}...\pi_m^{a_m} | \alpha^2 + u^2\delta^2\pi_1^{2a_1}\pi_2^{2a_2}...\pi_m^{2a_m}$. Hence $\delta^2\pi_1^{a_1}\pi_2^{a_2}...\pi_m^{a_m} | \alpha^2$ and thus $\delta\pi_1^{b_1}\pi_2^{b_2}...\pi_m^{b_m} | \alpha$ where $b_1, ..., b_m$ are defined as in theorem. Therefore, there exist an algebraic integer τ such that $\alpha = \tau\rho$. If τ is even, then $\delta^3 | \alpha^2$ and thus $\delta^3 | \delta^2\pi_1^{2a_1}\pi_2^{2a_2}...\pi_m^{2a_m}$. This is a contradiction, so τ is odd.

Conversely, suppose $\alpha = \tau\rho$ where τ is odd. We have $\alpha^2 + \eta^2 = \tau^2\delta^2\pi_1^{2b_1}\pi_2^{2b_2}...\pi_m^{2b_m} + u^2\delta^2\pi_1^{2a_1}\pi_2^{2a_2}...\pi_m^{2a_m} = \delta^2(\tau^2\pi_1^{2b_1}\pi_2^{2b_2}...\pi_m^{2b_m} + u^2\pi_1^{2a_1}\pi_2^{2a_2}...\pi_m^{2a_m})$. Since $\tau^2\pi_1^{2b_1}\pi_2^{2b_2}...\pi_m^{2b_m}$ and $u^2\pi_1^{2a_1}\pi_2^{2a_2}...\pi_m^{2a_m}$ are odd and the summation of these two numbers is even, $\delta^3 | \alpha^2 + \eta^2$. Since $2b_k \geq a_k$, we have $\pi_1^{a_1}\pi_2^{a_2}...\pi_m^{a_m} | \alpha^2 + \eta^2$. Hence $\alpha^2 + \eta^2$ is divisible by $\delta^3\pi_1^{a_1}\pi_2^{a_2}...\pi_m^{a_m}$. Consequently, $2\eta | \alpha^2 + \eta^2$.

It is not difficult to see that the mapping φ is a one-to-one correspondence. □

Example 3.1.6. Let $R = \mathbb{Z}[i]$. For $\eta = 9 + 9i = \delta \times 3^2$, we have $\rho = \delta \times 3$ and

τ odd	$\alpha = \tau\rho$	$\beta = \frac{\alpha^2 - 162i}{18+18i}$	$\gamma = \frac{\alpha^2 + 162i}{18+18i}$
± 1	$\pm(3 + 3i)$	$-4 - 4i$	$5 + 5i$
$\pm i$	$\pm(-3 + 3i)$	$-5 - 5i$	$4 + 4i$
$\pm(1 + 2i)$	$\pm(-3 + 9i)$	$-8 - 4i$	$1 + 5i$
$\pm(1 - 2i)$	$\pm(9 - 3i)$	$-4 - 8i$	$5 + i$
$\pm(2 + i)$	$\pm(3 + 9i)$	$-5 - i$	$4 + 8i$
$\pm(2 - i)$	$\pm(9 + 3i)$	$-1 - 5i$	$8 + 4i$

Theorem 3.1.7. *Let η be an even algebraic integer and $\eta = u\delta^{a_0}\pi_1^{a_1}\pi_2^{a_2}...\pi_m^{a_m}$ where $a_0 \geq 2$ and for $k \geq 1$, $a_k \in \mathbb{Z}_0^+$, u is a unit and $\pi_k \in R$ are non-associate odd primes. Set $\rho = \delta^{b_0}\pi_1^{b_1}\pi_2^{b_2}...\pi_m^{b_m}$ where $b_0 = \lceil\frac{a_0+2}{2}\rceil$ and $b_k = \lceil\frac{a_k}{2}\rceil$. Then P_η is*

$$\left\{\left(\alpha, \frac{\alpha^2-\eta^2}{2\eta}, \frac{\alpha^2+\eta^2}{2\eta}\right) \mid \alpha = \tau\rho \text{ for some } \tau \in R\right\}.$$

Moreover, the mapping $\varphi : P_\eta \to R$ defined by

$$\varphi((\alpha, \beta, \gamma)) = \frac{\alpha}{\rho}$$

is a one-to-one correspondence.

Proof. Suppose $(\alpha, (\alpha^2-\eta^2)/2\eta, (\alpha^2+\eta^2)/2\eta) \in P_\eta$. Then $\delta^{a_0+2}\pi_1^{a_1}\pi_2^{a_2}...\pi_m^{a_m}|\alpha^2 + u^2\delta^{2a_0}\pi_1^{2a_1}\pi_2^{2a_2}...\pi_m^{2a_m}$. Therefore, $\delta^{a_0+2}\pi_1^{a_1}\pi_2^{a_2}...\pi_m^{a_m}|\alpha^2$. Hence $\delta^{b_0}\pi_1^{b_1}\pi_2^{b_2}...\pi_m^{b_m}|\alpha$. Thus $\alpha = \tau\rho$ for some $\tau \in R$.

Conversely, suppose $\alpha = \tau\rho$ where $\tau \in R$. We have $\alpha^2 = \tau^2\delta^{2b_0}\pi_1^{2b_1}\pi_2^{2b_2}...\pi_m^{2b_m}$ which is divisible by 2η. Moreover, η^2 is divisible by 2η because $2|\eta$. Hence $2\eta|\alpha^2+\eta^2$.

Since any algebraic integer can be written in the form α/ρ, the mapping φ is bijective. □

Example 3.1.8. Let $R = \mathbb{Z}[i]$. For $\eta = -2+2i = \delta^3$, we have $\rho = \delta^3$ and

$\tau \in \mathbb{Z}[i]$	$\alpha = \tau\rho$	$\beta = \frac{\alpha^2+8i}{-4+4i}$	$\gamma = \frac{\alpha^2-8i}{-4+4i}$
0	0	$1-i$	$-1+i$
± 1	$\pm(-2+2i)$	0	$-2+2i$
$\pm i$	$\pm(-2-2i)$	$2-2i$	0
$\pm(1+i)$	∓ 4	$-1-3i$	$-3-i$
$\pm(1-i)$	$\pm 4i$	$3+i$	$1+3i$

3.1.2 2 Splits Completely in R

There are non-associate primes $\delta, \overline{\delta} \in R$ such that $2 \sim \delta\overline{\delta}$ and $|R/<\delta>| = |R/<\overline{\delta}>| = 2$. Notice that the ideas of even and odd we used in the proofs of the previous theorems are also practical in this subsection where we consider four cases of η depending on the divisibility by δ and $\overline{\delta}$.

Theorem 3.1.9. *Let $\eta \in R$ and $\eta = u\overline{\delta}^{\overline{a}_0}\pi_1^{a_1}...\pi_m^{a_m}$ where $\overline{a}_0 \geq 1$, and for $k \geq 1$, $a_k \in \mathbb{Z}_0^+$, u is a unit and $\pi_k \in R$ are non-associate primes where $\pi_k \nsim \delta, \overline{\delta}$. Set $\rho = \overline{\delta}^{\overline{b}_0}\pi_1^{b_1}...\pi_m^{b_m}$ where $\overline{b}_0 = \lceil\frac{\overline{a}_0+1}{2}\rceil$ and $b_k = \lceil\frac{a_k}{2}\rceil$. Then P_η is*

$$\left\{\left(\alpha, \frac{\alpha^2 - \eta^2}{2\eta}, \frac{\alpha^2 + \eta^2}{2\eta}\right) \mid \alpha = \tau\rho \text{ for some } \tau \in R \text{ where } \delta \nmid \tau\right\}.$$

Moreover, the mapping $\varphi : P_\eta \longrightarrow R$ defined by

$$\varphi((\alpha, \beta, \gamma)) = \Psi_\delta(\frac{\alpha}{\rho})$$

is a one-to-one correspondence.

Proof. Suppose $(\alpha, (\alpha^2 - \eta^2)/2\eta, (\alpha^2 + \eta^2)/2\eta) \in P_\eta$. Then $2\eta|\alpha^2 + \eta^2$ and thus $\delta\overline{\delta}^{\overline{a}_0+1}\pi_1^{a_1}\pi_2^{a_2}...\pi_m^{a_m}|\alpha^2 + u^2\overline{\delta}^{2\overline{a}_0}\pi_1^{2a_1}\pi_2^{2a_2}...\pi_m^{2a_m}$. Therefore, $\overline{\delta}^{\overline{a}_0+1}\pi_1^{a_1}\pi_2^{a_2}...\pi_m^{a_m}|\alpha^2$. Hence $\overline{\delta}^{\overline{b}_0}\pi_1^{b_1}\pi_2^{b_2}...\pi_m^{b_m}|\alpha$. Thus $\alpha = \tau\rho$ for some $\tau \in R$. If $\delta|\tau$, then $\delta|\alpha^2$ and $\delta|u^2\overline{\delta}^{2\overline{a}_0}\pi_1^{2a_1}\pi_2^{2a_2}...\pi_m^{2a_m}$, a contradiction. This means that $\delta \nmid \tau$.

Conversely, suppose $\alpha = \tau\rho$ where $\tau \in R$ and $\delta \nmid \tau$. We have $\overline{\delta}\eta|\alpha^2 + \eta^2$. Since $\delta \nmid \alpha^2$ (odd wrt δ) and $\delta \nmid \eta^2$, we have $\delta|\alpha^2 + \eta^2$ (even wrt δ). Since $2 \sim \delta\overline{\delta}$, $2\eta|\alpha^2 + \eta^2$.

It is easy to check that the mapping φ is a one-to-one correspondence. □

The next three theorems can be proved similarly.

Theorem 3.1.10. *Let $\eta \in R$ and $\eta = u\delta^{a_0}\pi_1^{a_1}...\pi_m^{a_m}$ where $a_0 \geq 1$, and for $k \geq 1$, $a_k \in \mathbb{Z}_0^+$, u is a unit and $\pi_k \in R$ are non-associate primes where $\pi_k \nsim \delta, \overline{\delta}$. Set $\rho = \delta^{b_0}\pi_1^{b_1}...\pi_m^{b_m}$ where $b_0 = \lceil\frac{a_0+1}{2}\rceil$, and $b_k = \lceil\frac{a_k}{2}\rceil$. Then P_η is*

$$\left\{\left(\alpha, \frac{\alpha^2 - \eta^2}{2\eta}, \frac{\alpha^2 + \eta^2}{2\eta}\right) \mid \alpha = \tau\rho \text{ for some } \tau \in R \text{ where } \overline{\delta} \nmid \tau\right\}.$$

Moreover, the mapping $\varphi : P_\eta \longrightarrow R$ defined by

$$\varphi((\alpha, \beta, \gamma)) = \Psi_{\overline{\delta}}(\frac{\alpha}{\rho})$$

is a one-to-one correspondence.

Theorem 3.1.11. *Let $\eta \in R$ and $\eta = u\delta^{a_0}\overline{\delta}^{\overline{a}_0}\pi_1^{a_1}...\pi_m^{a_m}$ where $a_0 \geq 1$, $\overline{a}_0 \geq 1$, and for $k \geq 1$, $a_k \in \mathbb{Z}_0^+$, u is a unit and $\pi_k \in R$ are non-associate primes where*

$\pi_k \nsim \delta, \overline{\delta}$. Set $\rho = \delta^{b_0}\overline{\delta}^{\overline{b}_0}\pi_1^{b_1}...\pi_m^{b_m}$ where $b_0 = \lceil\frac{a_0+1}{2}\rceil$, $\overline{b}_0 = \lceil\frac{\overline{a}_0+1}{2}\rceil$ and $b_k = \lceil\frac{a_k}{2}\rceil$. Then P_η is

$$\left\{\left(\alpha, \frac{\alpha^2-\eta^2}{2\eta}, \frac{\alpha^2+\eta^2}{2\eta}\right) \mid \alpha = \tau\rho \textit{ for some } \tau \in R\right\}.$$

Moreover, the mapping $\varphi : P_\eta \to R$ defined by

$$\varphi((\alpha,\beta,\gamma)) = \frac{\alpha}{\rho}$$

is a one-to-one correspondence.

The following theorem use the idea that all non-associate primes in R can be put into order, say δ, $\overline{\delta}$, π_1, π_2,...

Theorem 3.1.12. *Let $\eta \in R$ and $\eta = u\pi_1^{a_1}...\pi_m^{a_m}$ where $a_k \in \mathbb{Z}_0^+$, u is a unit and $\pi_k \in R$ are non-associate primes where $\pi_k \nsim \delta, \overline{\delta}$. Set $\rho = \pi_1^{b_1}...\pi_m^{b_m}$ where $b_k = \lceil\frac{a_k}{2}\rceil$. Then P_η is*

$$\left\{\left(\alpha, \frac{\alpha^2-\eta^2}{2\eta}, \frac{\alpha^2+\eta^2}{2\eta}\right) \mid \alpha = \tau\rho \textit{ for some } \tau \in R \textit{ where } \delta \nmid \tau, \overline{\delta} \nmid \tau\right\}.$$

Moreover, the mapping $\varphi : P_\eta \to R$ defined by

$$\varphi((\alpha,\beta,\gamma)) = \Psi_\delta(\Psi_{\overline{\delta}}(\frac{\alpha}{\rho}))$$

is a one-to-one correspondence.

3.1.3 2 is Inert in R

By Theorems 1.2.29 and 1.2.30, $R = \left\{\frac{u+v\sqrt{d}}{2} \mid u, v \in \mathbb{Z} \text{ and } u \equiv v \pmod 2\right\}$ and 2 is a prime in R. Notice that the norm of 2 in $\mathbb{Q}[\sqrt{d}]$ is 4, this means that the parity is not as useful as in the previous subsections.

Theorem 3.1.13. *Let $\eta \in R$ and $\eta = u\pi_1^{a_1}\pi_2^{a_2}...\pi_m^{a_m}$ where $a_k \in \mathbb{Z}_0^+$, u is a unit and $\pi_k \in R$ are non-associate primes such that $2 \nmid \pi_k$. Set $\rho = \pi_1^{b_1}\pi_2^{b_2}...\pi_m^{b_m}$ where $b_k = \lceil\frac{a_k}{2}\rceil$. Then P_η is*

$$\left\{\left(\alpha, \frac{\alpha^2-\eta^2}{2\eta}, \frac{\alpha^2+\eta^2}{2\eta}\right) \mid \alpha = \tau\rho \textit{ for some } \tau \in R \textit{ where } 2 \nmid \tau\right\}.$$

Moreover, the mapping $\varphi : P_\eta \to R$ defined by

$$\varphi((\alpha, \beta, \gamma)) = \Psi_2(\frac{\alpha}{\rho})$$

is a one-to-one correspondence.

Proof. Suppose $(\alpha, (\alpha^2 - \eta^2)/2\eta, (\alpha^2 + \eta^2)/2\eta) \in P_\eta$. Then $2\eta | \alpha^2 + \eta^2$ and thus $2\pi_1^{a_1}\pi_2^{a_2}...\pi_m^{a_m} | \alpha^2 + u^2\pi_1^{2a_1}\pi_2^{2a_2}...\pi_m^{2a_m}$. Therefore, $\pi_1^{a_1}\pi_2^{a_2}...\pi_m^{a_m} | \alpha^2$. Hence $\rho | \alpha$, say $\alpha = \tau\rho$ for some $\tau \in R$. If $2|\tau$, then $2|\alpha^2$ and $2|u^2\pi_1^{2a_1}\pi_2^{2a_2}...\pi_m^{2a_m}$, a contradiction. This means that $2 \nmid \tau$.

Conversely, suppose $\alpha = \tau\rho$ where $\tau \in R$ and $2 \nmid \tau$. We have $\eta | \alpha^2 - \eta^2$. Let $\alpha = (x + y\sqrt{d})/2$ and $\eta = (u + v\sqrt{d})/2$ where $x, y, u, v \in \mathbb{Z}$ and $x \equiv y, u \equiv v \pmod 2$. Since $2 \nmid \alpha$ and $2 \nmid \eta$, $x \equiv y \equiv u \equiv v \equiv 1 \pmod 2$. Hence $2|\alpha - \eta$ and thus $2|\alpha^2 - \eta^2$. Since $\gcd(\eta, 2) = 1$, $2\eta|\alpha^2 + \eta^2$.

Clearly, the mapping φ is a one-to-one correspondence. □

Theorem 3.1.14. *Let $\eta \in R$ and $\eta = u2^{a_0}\pi_1^{a_1}\pi_2^{a_2}...\pi_m^{a_m}$ where $a_0 \geq 1$ and for $k \geq 1$, $a_k \in \mathbb{Z}_0^+$, u is a unit and $\pi_k \in R$ are non-associate primes such that $2 \nmid \pi_k$. Set $\rho = 2^{b_0}\pi_1^{b_1}\pi_2^{b_2}...\pi_m^{b_m}$ where $b_0 = \lceil \frac{a_0+1}{2} \rceil$ and $b_k = \lceil \frac{a_k}{2} \rceil$. Then P_η is*

$$\left\{ \left(\alpha, \frac{\alpha^2 - \eta^2}{2\eta}, \frac{\alpha^2 + \eta^2}{2\eta} \right) \mid \alpha = \tau\rho \text{ for some } \tau \in R \right\}.$$

Moreover, the mapping $\varphi : P_\eta \to R$ defined by

$$\varphi((\alpha, \beta, \gamma)) = \frac{\alpha}{\rho}$$

is a one-to-one correspondence.

Proof. The proof is similar to the proof of Theorem 3.1.7. □

3.2 Pythagorean Triples Over Biquadratic Fields

In this section, let K be a biquadratic field such that the ring of integers R of K is a UFD. We extend ideas in the previous section and show how to find all elements of the set P and P_η.

By Theorem 1.2.32, R is separated into five cases depending on factorization of 2 which are $2 = \delta^4$, $2 = \delta^2$, $2 = \delta_1^2\delta_2^2$, $2 = \delta_1\delta_2\delta_3\delta_4$ and $2 = \delta_1\delta_2$. We need the following lemmas to show features of elements of P_η.

Lemma 3.2.1. *Let $\delta, \alpha, \beta \in R$. If δ is a prime such that $\delta|2$ and $\delta|\alpha^2 - \beta^2$, then $\delta|\alpha - \beta$ and $\delta|\alpha + \beta$.*

Proof. Assume $\delta|\alpha^2 - \beta^2$. Then $\delta|\alpha - \beta$ or $\delta|\alpha + \beta$. Since $\alpha - \beta = (\alpha + \beta) - 2\beta$, we are done. □

Lemma 3.2.2. *Let $\delta, \alpha, \beta \in R$. If δ is a prime such that $2 = \delta^4$ and $\delta^3|\alpha^2 - \beta^2$, then $\delta^2|\alpha - \beta$.*

Proof. Assume $\delta^3|\alpha^2 - \beta^2$. By Lemma 3.2.1, $\delta|\alpha - \beta$, i.e., $\alpha - \beta = \delta\gamma$ for some $\gamma \in R$. It follows that $\alpha^2 - \beta^2 = (\alpha - \beta)(\alpha - \beta + 2\beta) = (\delta\gamma)(\delta\gamma + \delta^4\beta)$ is divisible by δ^3. Hence $\delta|(\gamma)(\gamma + \delta^3\beta)$. This means that $\delta|\gamma$ and $\delta^2|\alpha - \beta$. □

The case that $\eta = 0$ is similar to the case for quadratic fields. However, we state it here for completeness.

Theorem 3.2.3. *$P_0 = \{(0, \beta, \beta) \mid \beta \in R\}$ and the mapping $\varphi : P_0 \to R$ defined by*

$$\varphi((0, \beta, \beta)) = \beta$$

is a one-to-one correspondence.

3.2.1 $2 = \delta^4$

In this subsection, there is a prime $\delta \in R$ such that $2 = \delta^4$. We consider two cases of η as follows.

Theorem 3.2.4. *Let $\eta \in R$ and $\eta = u\delta^{a_0}\pi_1^{a_1}...\pi_m^{a_m}$ where $a_0 = 0, 1, 2, 3$ and for $k \geq 1$, $a_k \in \mathbb{Z}_0^+$, u is a unit and $\pi_k \in R$ are non-associate primes where $\pi_k \nsim \delta$. Set $\rho = \delta^{a_0}\pi_1^{b_1}...\pi_m^{b_m}$ where $b_k = \lceil \frac{a_k}{2} \rceil$. Then P_η is*

$$\left\{ \left(\alpha, \frac{\alpha^2 - \eta^2}{2\eta}, \frac{\alpha^2 + \eta^2}{2\eta} \right) \mid \alpha = \tau\rho \text{ where } \tau = \delta^{\lceil \frac{4-a_0}{2} \rceil}\mu + u\pi_1^{a_1-b_1}...\pi_m^{a_m-b_m} \text{ and } \mu \in R \right\}.$$

Moreover, the mapping $\varphi : P_\eta \longrightarrow R$ defined by

$$\varphi((\alpha, \beta, \gamma)) = \frac{\frac{\alpha}{\rho} - u\pi_1^{a_1-b_1}...\pi_m^{a_m-b_m}}{\delta^{\lceil \frac{4-a_0}{2} \rceil}}$$

is a one-to-one correspondence.

Proof. Suppose $(\alpha, (\alpha^2 - \eta^2)/2\eta, (\alpha^2 + \eta^2)/2\eta) \in P_\eta$. Therefore, $2\eta | \alpha^2 - \eta^2$. Thus $\delta^{a_0+4}\pi_1^{a_1}...\pi_m^{a_m} | \alpha^2 - u^2\delta^{2a_0}\pi_1^{2a_1}...\pi_m^{2a_m}$. We obtain $\delta^{2a_0}\pi_1^{a_1}...\pi_m^{a_m} | \alpha^2$. This means that $\delta^{a_0}\pi_1^{b_1}...\pi_m^{b_m} | \alpha$. Then $\alpha = \tau\rho$ for some $\tau \in R$ and
$\delta^{a_0+4}\pi_1^{a_1}...\pi_m^{a_m} | \tau^2\delta^{2a_0}\pi_1^{2b_1}...\pi_m^{2b_m} - u^2\delta^{2a_0}\pi_1^{2a_1}...\pi_m^{2a_m}$.
Thus $\delta^{4-a_0}\pi_1^{a_1}...\pi_m^{a_m} | \tau^2\pi_1^{2b_1}...\pi_m^{2b_m} - u^2\pi_1^{2a_1}...\pi_m^{2a_m}$. Since $\gcd(\delta^{4-a_0}, \pi_1^{2b_1}...\pi_m^{2b_m}) = 1$, we have $\delta^{4-a_0} | \tau^2 - u^2\pi_1^{2a_1-2b_1}...\pi_m^{2a_m-2b_m}$. From Lemmas 3.2.1 and 3.2.2, $\delta^{\lceil \frac{4-a_0}{2} \rceil} | \tau - u\pi_1^{a_1-b_1}...\pi_m^{a_m-b_m}$. Hence $\tau = \delta^{\lceil \frac{4-a_0}{2} \rceil}\mu + u\pi_1^{a_1-b_1}...\pi_m^{a_m-b_m}$ for some $\mu \in R$.

Conversely, suppose $\alpha = \tau\rho$ where $\tau = \delta^{\lceil \frac{4-a_0}{2} \rceil}\mu + u\pi_1^{a_1-b_1}...\pi_m^{a_m-b_m}$ and $\mu \in R$. We have

$$\begin{aligned} \alpha^2 - \eta^2 &= (\delta^{\lceil \frac{4-a_0}{2} \rceil}\mu + u\pi_1^{a_1-b_1}...\pi_m^{a_m-b_m})^2\delta^{2a_0}\pi_1^{2b_1}...\pi_m^{2b_m} - u^2\delta^{2a_0}\pi_1^{2a_1}...\pi_m^{2a_m} \\ &= \delta^{2\lceil \frac{4-a_0}{2} \rceil + 2a_0}\mu^2\pi_1^{2b_1}...\pi_m^{2b_m} + 2\delta^{\lceil \frac{4-a_0}{2} \rceil + 2a_0}\mu u\pi_1^{a_1+b_1}...\pi_m^{a_m+b_m} \end{aligned}$$

which is divisible by 2η. It follows that $2\eta | \alpha^2 - \eta^2$.

If $(\alpha, \beta, \gamma) \in P_\eta$, then $\varphi((\alpha, \beta, \gamma)) = \mu$ for some $\mu \in R$. Indeed, the mapping φ is injective and surjective. □

Theorem 3.2.5. *Let $\eta \in R$ and $\eta = u\delta^{a_0}\pi_1^{a_1}...\pi_m^{a_m}$ where $a_0 \geq 4$ and for $k \geq 1$, $a_k \in \mathbb{Z}_0^+$, u is a unit and $\pi_k \in R$ are non-associate primes where $\pi_k \nsim \delta$. Set $\rho = \delta^{b_0}\pi_1^{b_1}...\pi_m^{b_m}$ where $b_0 = \lceil \frac{a_0+4}{2} \rceil$ and $b_k = \lceil \frac{a_k}{2} \rceil$. Then P_η is*

$$\left\{ \left(\alpha, \frac{\alpha^2 - \eta^2}{2\eta}, \frac{\alpha^2 + \eta^2}{2\eta} \right) \mid \alpha = \mu\rho \text{ where } \mu \in R \right\}.$$

Moreover, the mapping $\varphi : P_\eta \to R$ defined by

$$\varphi((\alpha,\beta,\gamma)) = \frac{\alpha}{\rho}$$

is a one-to-one correspondence.

Proof. Suppose $(\alpha, (\alpha^2-\eta^2)/2\eta, (\alpha^2+\eta^2)/2\eta) \in P_\eta$. Then $2\eta|\alpha^2-\eta^2$. We have $\delta^{a_0+4}\pi_1^{a_1}...\pi_m^{a_m}|\alpha^2 - u^2\delta^{2a_0}\pi_1^{2a_1}...\pi_m^{2a_m}$. Hence $\delta^{a_0+4}\pi_1^{a_1}...\pi_m^{a_m}|\alpha^2$ and thus $\delta^{b_0}\pi_1^{b_1}...\pi_m^{b_m}|\alpha$. Therefore, there exist an algebraic integer μ such that $\alpha = \mu\rho$.

Conversely, suppose $\alpha = \mu\rho$ where $\mu \in R$. We have $\alpha^2-\eta^2 = \mu^2\delta^{2b_0}\pi_1^{2b_1}...\pi_m^{2b_m} - u^2\delta^{2a_0}\pi_1^{2a_1}...\pi_m^{2a_m}$. Hence $2\eta|\alpha^2-\eta^2$.

Clearly, the mapping φ is a one-to-one correspondence. □

3.2.2 $2 = \delta^2$

There is a prime $\delta \in R$ such that $2 = \delta^2$. We consider 2 cases of η depending on the divisibility by δ.

Theorem 3.2.6. *Let $\eta \in R$ and $\eta = u\delta^{a_0}\pi_1^{a_1}...\pi_m^{a_m}$ where $a_0 = 0, 1$ and for $k \geq 1$, $a_k \in \mathbb{Z}_0^+$, u is a unit and $\pi_k \in R$ are non-associate primes where $\pi_k \nsim \delta$. Set $\rho = \delta^{a_0}\pi_1^{b_1}...\pi_m^{b_m}$ where $b_k = \lceil \frac{a_k}{2} \rceil$. Then P_η is*

$$\left\{ \left(\alpha, \frac{\alpha^2-\eta^2}{2\eta}, \frac{\alpha^2+\eta^2}{2\eta}\right) \mid \alpha = \tau\rho \text{ where } \tau = \delta\mu + u\pi_1^{a_1-b_1}...\pi_m^{a_m-b_m} \text{ and } \mu \in R \right\}.$$

Moreover, the mapping $\varphi : P_\eta \to R$ defined by

$$\varphi((\alpha,\beta,\gamma)) = \frac{\frac{\alpha}{\rho} - u\pi_1^{a_1-b_1}...\pi_m^{a_m-b_m}}{\delta}$$

is a one-to-one correspondence.

Proof. Suppose $(\alpha, (\alpha^2-\eta^2)/2\eta, (\alpha^2+\eta^2)/2\eta) \in P_\eta$. We obtain $2\eta|\alpha^2-\eta^2$, i.e., $\delta^{a_0+2}\pi_1^{a_1}...\pi_m^{a_m}|\alpha^2 - u^2\delta^{2a_0}\pi_1^{2a_1}...\pi_m^{2a_m}$. Thus $\delta^{2a_0}\pi_1^{a_1}...\pi_m^{a_m}|\alpha^2$. Hence $\delta^{a_0}\pi_1^{b_1}...\pi_m^{b_m}|\alpha$. Then $\alpha = \tau\rho$ for some $\tau \in R$ and $\delta^{a_0+2}\pi_1^{a_1}...\pi_m^{a_m}|\tau^2\delta^{2a_0}\pi_1^{2b_1}...\pi_m^{2b_m} - u^2\delta^{2a_0}\pi_1^{2a_1}...\pi_m^{2a_m}$. Thus $\delta^{2-a_0}|\tau^2 - u^2\pi_1^{2a_1-2b_1}...\pi_m^{2a_m-2b_m}$. From Lemma 3.2.1, $\delta|\tau - u\pi_1^{a_1-b_1}...\pi_m^{a_m-b_m}$. Therefore, $\tau = \delta\mu + u\pi_1^{a_1-b_1}...\pi_m^{a_m-b_m}$ for some $\mu \in R$.

Conversely, suppose $\alpha = \tau\rho$ where $\tau = \delta\mu + u\pi_1^{a_1-b_1}...\pi_m^{a_m-b_m}$ and $\mu \in R$. We have

$$\begin{aligned}\alpha^2 - \eta^2 &= (\delta\mu + u\pi_1^{a_1-b_1}...\pi_m^{a_m-b_m})^2\delta^{2a_0}\pi_1^{2b_1}...\pi_m^{2b_m} - u^2\delta^{2a_0}\pi_1^{2a_1}...\pi_m^{2a_m} \\ &= \delta^{2+2a_0}\mu^2\pi_1^{2b_1}...\pi_m^{2b_m} + 2\delta^{1+2a_0}\mu u\pi_1^{a_1+b_1}...\pi_m^{a_m+b_m}\end{aligned}$$

which is divisible by 2η. Hence $2\eta|\alpha^2 - \eta^2$.

Moreover, for $(\alpha, \beta, \gamma) \in P_\eta$, $\varphi((\alpha, \beta, \gamma)) = \mu$ for some $\mu \in R$ and the mapping φ is a one-to-one correspondence. □

Theorem 3.2.7. *Let $\eta \in R$ and $\eta = u\delta^{a_0}\pi_1^{a_1}...\pi_m^{a_m}$ where $a_0 \geq 2$ and for $k \geq 1$, $a_k \in \mathbb{Z}_0^+$, u is a unit and $\pi_k \in R$ are non-associate primes where $\pi_k \nsim \delta$. Set $\rho = \delta^{b_0}\pi_1^{b_1}...\pi_m^{b_m}$ where $b_0 = \lceil\frac{a_0+2}{2}\rceil$ and $b_k = \lceil\frac{a_k}{2}\rceil$. Then P_η is*

$$\left\{\left(\alpha, \frac{\alpha^2-\eta^2}{2\eta}, \frac{\alpha^2+\eta^2}{2\eta}\right) \mid \alpha = \mu\rho \text{ where } \mu \in R\right\}.$$

Moreover, the mapping $\varphi : P_\eta \longrightarrow R$ defined by

$$\varphi((\alpha, \beta, \gamma)) = \frac{\alpha}{\rho}$$

is a one-to-one correspondence.

Proof. The proof is similar to the proof of Theorem 3.2.5. □

3.2.3 $2 = \delta_1^2\delta_2^2$

There are non-associate primes $\delta_1, \delta_2 \in R$ such that $2 = \delta_1^2\delta_2^2$.

Theorem 3.2.8. *Let $\eta \in R$ and $\eta = u\delta_1^{c_1}\delta_2^{c_2}\pi_1^{a_1}...\pi_m^{a_m}$ where $c_j, a_k \in \mathbb{Z}_0^+$, u is a unit and $\pi_k \in R$ are non-associate primes where $\pi_k \nsim \delta_1, \delta_2$. Set $\rho = \delta_1^{d_1}\delta_2^{d_2}\pi_1^{b_1}...\pi_m^{b_m}$ where*

$$d_j = \begin{cases} c_j & \text{if } c_j = 0, 1 \\ \lceil\frac{c_j+2}{2}\rceil & \text{if } c_j \geq 2 \end{cases}$$

and $b_k = \lceil\frac{a_k}{2}\rceil$. Set

$$e_j = \begin{cases} 1 & \text{if } c_j = 0, 1 \\ 0 & \text{if } c_j \geq 2. \end{cases}$$

Then P_η *is* $\Big\{\Big(\alpha, \frac{\alpha^2-\eta^2}{2\eta}, \frac{\alpha^2+\eta^2}{2\eta}\Big) \mid \alpha = \tau\rho$ *where* $\tau = \delta_1^{e_1}\delta_2^{e_2}\mu$ $+u\delta_1^{c_1-d_1}\delta_2^{c_2-d_2}\pi_1^{a_1-b_1}...\pi_m^{a_m-b_m}$ *and* $\mu \in R\Big\}$.

Moreover, the mapping $\varphi : P_\eta \to R$ *defined by*

$$\varphi((\alpha,\beta,\gamma)) = \frac{\frac{\alpha}{\rho} - u\delta_1^{c_1-d_1}\delta_2^{c_2-d_2}\pi_1^{a_1-b_1}...\pi_m^{a_m-b_m}}{\delta_1^{e_1}\delta_2^{e_2}}$$

is a one-to-one correspondence.

Proof. Suppose $(\alpha, (\alpha^2-\eta^2)/2\eta, (\alpha^2+\eta^2)/2\eta) \in P_\eta$. Therefore, $2\eta|\alpha^2-\eta^2$ and so $\delta_1^{c_1+2}\delta_2^{c_2+2}\pi_1^{a_1}...\pi_m^{a_m}|\alpha^2 - u^2\delta_1^{2c_1}\delta_2^{2c_2}\pi_1^{2a_1}...\pi_m^{2a_m}$. Hence

$$\delta_1^{\min\{c_1+2,2c_1\}}\delta_2^{\min\{c_2+2,2c_2\}}\pi_1^{a_1}...\pi_m^{a_m}|\alpha^2.$$

This means that $\delta_1^{d_1}\delta_2^{d_2}\pi_1^{b_1}...\pi_m^{b_m}|\alpha$. Thus $\alpha = \tau\rho$ for some $\tau \in R$ and $\delta_1^{c_1+2}\delta_2^{c_2+2}\pi_1^{a_1}...\pi_m^{a_m}|\tau^2\delta_1^{2d_1}\delta_2^{2d_2}\pi_1^{2b_1}...\pi_m^{2b_m} - u^2\delta_1^{2c_1}\delta_2^{2c_2}\pi_1^{2a_1}...\pi_m^{2a_m}$. We obtain $\delta_1^{e_1}\delta_2^{e_2}|\tau^2 - u^2\delta_1^{c_1-2d_1}\delta_2^{2c_2-2d_2}\pi_1^{2a_1-2b_1}...\pi_m^{2a_m-2b_m}$. By Lemma 3.2.1, $\delta_1^{e_1}\delta_2^{e_2}|\tau - u\delta_1^{c_1-d_1}\delta_2^{c_2-d_2}\pi_1^{a_1-b_1}...\pi_m^{a_m-b_m}$. Hence $\tau = \delta_1^{e_1}\delta_2^{e_2}\mu + u\delta_1^{c_1-d_1}\delta_2^{c_2-d_2}\pi_1^{a_1-b_1}...\pi_m^{a_m-b_m}$ for some $\mu \in R$.

Conversely, suppose $\alpha = \tau\rho$ where $\tau = \delta_1^{e_1}\delta_2^{e_2}\mu + u\delta_1^{c_1-d_1}\delta_2^{c_2-d_2}\pi_1^{a_1-b_1}...\pi_m^{a_m-b_m}$ and $\mu \in R$. We have

$$\begin{aligned}\alpha^2 - \eta^2 &= (\delta_1^{e_1}\delta_2^{e_2}\mu + u\delta_1^{c_1-d_1}\delta_2^{c_2-d_2}\pi_1^{a_1-b_1}...\pi_m^{a_m-b_m})^2\delta_1^{2d_1}\delta_2^{2d_2}\pi_1^{2b_1}...\pi_m^{2b_m}\\ &\quad - u^2\delta_1^{c_1}\delta_2^{2c_2}\pi_1^{2a_1}...\pi_m^{2a_m}\\ &= \delta_1^{2e_1+2d_1}\delta_2^{2e_2+2d_2}\mu^2\pi_1^{2b_1}...\pi_m^{2b_m} + 2\delta_1^{e_1+c_1+d_1}\delta_2^{e_2+c_2+d_2}\mu u\pi_1^{a_1+b_1}...\pi_m^{a_m+b_m}\end{aligned}$$

which is divisible by 2η. Therefore, $(\alpha, (\alpha^2-\eta^2)/2\eta, (\alpha^2+\eta^2)/2\eta) \in P_\eta$.

It is straightforward to check that φ is a one-to-one correspondence. □

3.2.4 $2 = \delta_1\delta_2\delta_3\delta_4$

There are non-associate primes $\delta_1, \delta_2, \delta_3, \delta_4 \in R$ such that $2 = \delta_1\delta_2\delta_3\delta_4$.

Theorem 3.2.9. *Let* $\eta \in R$ *and* $\eta = u\delta_1^{c_1}\delta_2^{c_2}\delta_3^{c_3}\delta_4^{c_4}\pi_1^{a_1}...\pi_m^{a_m}$ *where* $c_j, a_k \in \mathbb{Z}_0^+$, u *is a unit and* $\pi_k \in R$ *are non-associate primes where* $\pi_k \nsim \delta_1, \delta_2, \delta_3, \delta_4$. *Set*

$\rho = \delta_1^{d_1}\delta_2^{d_2}\delta_3^{d_3}\delta_4^{d_4}\pi_1^{b_1}...\pi_m^{b_m}$ *where*

$$d_j = \begin{cases} 0 & \textit{if } c_j = 0 \\ \lceil \frac{c_j+1}{2} \rceil & \textit{if } c_j \geq 1 \end{cases}$$

and $b_k = \lceil \frac{a_k}{2} \rceil$. *Set*

$$e_j = \begin{cases} 1 & \textit{if } c_j = 0 \\ 0 & \textit{if } c_j \geq 1. \end{cases}$$

Then P_η *is* $\Big\{ \Big(\alpha, \frac{\alpha^2-\eta^2}{2\eta}, \frac{\alpha^2+\eta^2}{2\eta}\Big) \mid \alpha = \tau\rho$ *where* $\tau = \delta_1^{e_1}\delta_2^{e_2}\delta_3^{e_3}\delta_4^{e_4}\mu$ $+u\delta_1^{c_1-d_1}\delta_2^{c_2-d_2}\delta_3^{c_3-d_3}\delta_4^{c_4-d_4}\pi_1^{a_1-b_1}...\pi_m^{a_m-b_m}$ *and* $\mu \in R\Big\}$.

Moreover, the mapping $\varphi : P_\eta \to R$ *defined by*

$$\varphi((\alpha,\beta,\gamma)) = \frac{\frac{\alpha}{\rho} - u\delta_1^{c_1-d_1}\delta_2^{c_2-d_2}\delta_3^{c_3-d_3}\delta_4^{c_4-d_4}\pi_1^{a_1-b_1}...\pi_m^{a_m-b_m}}{\delta_1^{e_1}\delta_2^{e_2}\delta_3^{e_3}\delta_4^{e_4}}$$

is a one-to-one correspondence.

Proof. Suppose $(\alpha, (\alpha^2-\eta^2)/2\eta, (\alpha^2+\eta^2)/2\eta) \in P_\eta$. Therefore, $2\eta|\alpha^2-\eta^2$ and so $\delta_1^{c_1+1}\delta_2^{c_2+1}\delta_3^{c_3+1}\delta_4^{c_4+1}\pi_1^{a_1}...\pi_m^{a_m}|\alpha^2 - u^2\delta_1^{2c_1}\delta_2^{2c_2}\delta_3^{2c_3}\delta_4^{2c_4}\pi_1^{2a_1}...\pi_m^{2a_m}$. Hence

$$\delta_1^{\min\{c_1+1,2c_1\}}\delta_2^{\min\{c_2+1,2c_2\}}\delta_3^{\min\{c_3+1,2c_3\}}\delta_4^{\min\{c_4+1,2c_4\}}\pi_1^{a_1}...\pi_m^{a_m}|\alpha^2.$$

This means that $\delta_1^{d_1}\delta_2^{d_2}\delta_3^{d_3}\delta_4^{d_4}\pi_1^{b_1}...\pi_m^{b_m}|\alpha$. Thus $\alpha = \tau\rho$ for some $\tau \in R$ and $\delta_1^{c_1+1}\delta_2^{c_2+1}\delta_3^{c_3+1}\delta_4^{c_4+1}\pi_1^{a_1}...\pi_m^{a_m}|\tau^2\delta_1^{2d_1}\delta_2^{2d_2}\delta_3^{2d_3}\delta_4^{2d_4}\pi_1^{2b_1}...\pi_m^{2b_m} - u^2\delta_1^{2c_1}\delta_2^{2c_2}\delta_3^{2c_3}\delta_4^{2c_4}\pi_1^{2a_1}...\pi_m^{2a_m}$. We obtain $\delta_1^{e_1}\delta_2^{e_2}\delta_3^{e_3}\delta_4^{e_4}|\tau^2 - u^2\delta_1^{c_1-2d_1}\delta_2^{2c_2-2d_2}\delta_3^{2c_3-2d_3}\delta_4^{2c_4-2d_4}\pi_1^{2a_1-2b_1}...\pi_m^{2a_m-2b_m}$. By Lemma 3.2.1, $\delta_1^{e_1}\delta_2^{e_2}\delta_3^{e_3}\delta_4^{e_4}|\tau - u\delta_1^{c_1-d_1}\delta_2^{c_2-d_2}\delta_3^{c_3-d_3}\delta_4^{c_4-d_4}\pi_1^{a_1-b_1}...\pi_m^{a_m-b_m}$. Hence $\tau = \delta_1^{e_1}\delta_2^{e_2}\delta_3^{e_3}\delta_4^{e_4}\mu + u\delta_1^{c_1-d_1}\delta_2^{c_2-d_2}\delta_3^{c_3-d_3}\delta_4^{c_4-d_4}\pi_1^{a_1-b_1}...\pi_m^{a_m-b_m}$ for some $\mu \in R$.

Conversely, suppose $\alpha = \tau\rho$. We have

$$\begin{aligned}
&\alpha^2 - \eta^2 \\
&= (\delta_1^{e_1}\delta_2^{e_2}\delta_3^{e_3}\delta_4^{e_4}\mu + u\delta_1^{c_1-d_1}\delta_2^{c_2-d_2}\delta_3^{c_3-d_3}\delta_4^{c_4-d_4}\pi_1^{a_1-b_1}...\pi_m^{a_m-b_m})^2\delta_1^{2d_1}\delta_2^{2d_2}\delta_3^{2d_3}\delta_4^{2d_4}\pi_1^{2b_1}...\pi_m^{2b_m} \\
&\quad - u^2\delta_1^{c_1}\delta_2^{2c_2}\delta_3^{2c_3}\delta_4^{2c_4}\pi_1^{2a_1}...\pi_m^{2a_m} \\
&= \delta_1^{2e_1+2d_1}\delta_2^{2e_2+2d_2}\delta_3^{2e_3+2d_3}\delta_4^{2e_4+2d_4}\mu^2\pi_1^{2b_1}...\pi_m^{2b_m} \\
&\quad + 2\delta_1^{e_1+c_1+d_1}\delta_2^{e_2+c_2+d_2}\delta_3^{e_3+c_3+d_3}\delta_4^{e_4+c_4+d_4}\mu u\pi_1^{a_1+b_1}...\pi_m^{a_m+b_m} \text{ which is divisible by } 2\eta.
\end{aligned}$$

Therefore, $2\eta|\alpha^2 - \eta^2$.

It is not difficult to check that the mapping φ is injective and surjective. □

3.2.5 $2 = \delta_1\delta_2$

There are non-associate primes δ_1, δ_2 such that $2 = \delta_1\delta_2$.

Theorem 3.2.10. *Let $\eta \in R$ and $\eta = u\delta_1^{c_1}\delta_2^{c_2}\pi_1^{a_1}...\pi_m^{a_m}$ where $c_j, a_k \in \mathbb{Z}_0^+$, u is a unit and $\pi_k \in R$ are non-associate primes where $\pi_k \nsim \delta_1, \delta_2$. Set $\rho = \delta_1^{d_1}\delta_2^{d_2}\pi_1^{b_1}...\pi_m^{b_m}$ where*

$$d_j = \begin{cases} 0 & \text{if } c_j = 0 \\ \lceil \frac{c_j+1}{2} \rceil & \text{if } c_j \geq 1 \end{cases}$$

and $b_k = \lceil \frac{a_k}{2} \rceil$. Set

$$e_j = \begin{cases} 1 & \text{if } c_j = 0 \\ 0 & \text{if } c_j \geq 1. \end{cases}$$

Then P_η is $\Big\{ \Big(\alpha, \frac{\alpha^2-\eta^2}{2\eta}, \frac{\alpha^2+\eta^2}{2\eta}\Big) \mid \alpha = \tau\rho$ where $\tau = \delta_1^{e_1}\delta_2^{e_2}\mu$ $+u\delta_1^{c_1-d_1}\delta_2^{c_2-d_2}\pi_1^{a_1-b_1}...\pi_m^{a_m-b_m}$ and $\mu \in R\Big\}$.

Moreover, the mapping $\varphi : P_\eta \to R$ defined by

$$\varphi((\alpha, \beta, \gamma)) = \frac{\frac{\alpha}{\rho} - u\delta_1^{c_1-d_1}\delta_2^{c_2-d_2}\pi_1^{a_1-b_1}...\pi_m^{a_m-b_m}}{\delta_1^{e_1}\delta_2^{e_2}}$$

is a one-to-one correspondence.

Proof. Through the proof of Theorem 3.2.9, this theorem can be proved in a similar way. □

3.3 The Ring Structure

Let K be a quadratic/biquadratic field such that the ring of integers R of K is a UFD. We define bijections between P_η and R, which construct a one-to-one correspondence between P and $R \times R$.

Corollary 3.3.1. *Let η be a algebraic integer. $(P_\eta, \oplus, \odot)$ is a commutative ring with identity where $\oplus$ and $\odot$ are operations on P_η defined by*

$$(\alpha, \beta, \gamma) \oplus (\mu, \nu, \lambda) = \varphi^{-1}(\varphi((\alpha, \beta, \gamma)) + \varphi((\mu, \nu, \lambda)))$$

and

$$(\alpha,\beta,\gamma)\odot(\mu,\nu,\lambda)=\varphi^{-1}(\varphi((\alpha,\beta,\gamma))\cdot\varphi((\mu,\nu,\lambda))).$$

Proof. The ring structures of P_η are constructed from the ring structure of R by using mappings in Theroems 3.1.2, 3.1.3, 3.1.5, 3.1.7, 3.1.9, 3.1.10, 3.1.11, 3.1.12, 3.1.13, 3.1.14, 3.2.3, 3.2.4, 3.2.5, 3.2.6, 3.2.7, 3.2.8, 3.2.9 and 3.2.10. □

Corollary 3.3.2. *The mapping* $\Phi : P \to R \times R$ *given by*

$$\Phi((\alpha,\beta,\gamma))=(\gamma-\beta,\varphi((\alpha,\beta,\gamma)))$$

is a bijection. Consequently, $(P,\boxplus,\boxdot)$ *is a commutative ring with identity where* $\boxplus$ *and* $\boxdot$ *are operations on* P *defined by*

$$(\alpha,\beta,\gamma)\boxplus(\mu,\nu,\lambda)=\Phi^{-1}(\Phi((\alpha,\beta,\gamma))+\Phi((\mu,\nu,\lambda)))$$

and

$$(\alpha,\beta,\gamma)\boxdot(\mu,\nu,\lambda)=\Phi^{-1}(\Phi((\alpha,\beta,\gamma))\cdot\Phi((\mu,\nu,\lambda))).$$

CHAPTER IV
THE GROUP OF PYTHAGOREAN TRIPLES OVER NUMBER FIELDS

Let K be a number field and R be the ring of integers in K. In this chapter, we determine all Pythagorean triples in R and study the set of Pythagorean triples in terms of its structure.

4.1 The Representation of Pythagorean Triples

K. K. Kubota [6] characterized Pythagorean triples in a UFD. We extend his work to the ring of integers of any number field.

Theorem 4.1.1. *Let R be the ring of integers of a number field K. If (a, b, c) is a Pythagorean triple in R, then there exist $f, u, v, d \in R$ where $d \mid u^2 \pm v^2$ and $d \mid 2uv$ such that*

$$a = \frac{2fuv}{d}, \qquad b = \frac{f(u^2 - v^2)}{d}, \qquad \text{and } c = \frac{f(u^2 + v^2)}{d}. \tag{4.1}$$

Proof. Let (a, b, c) be a Pythagorean triple in R. If $b + c = 0$, then $a = 0$ and we choose $f = b, u = 0, v = 1, d = -1$ which satisfy equation (4.1).

Suppose $b + c \neq 0$. Let f be a common divisor of a, b, c. Let $a_1 = a/f$, $b_1 = b/f$, $c_1 = c/f \in R$. Define $u = b_1 + c_1$, $v = a_1$, $d = 2(b_1 + c_1)$. Then

$$\frac{2fuv}{d} = \frac{2f(b_1 + c_1)a_1}{2(b_1 + c_1)} = fa_1 = a,$$

$$\frac{f(u^2 - v^2)}{d} = \frac{f(b_1^2 + c_1^2 + 2b_1c_1 - a_1^2)}{2(b_1 + c_1)} = \frac{f(2b_1^2 + 2b_1c_1)}{2(b_1 + c_1)} = fb_1 = b,$$

$$\frac{f(u^2 + v^2)}{d} = \frac{f(b_1^2 + c_1^2 + 2b_1c_1 + a_1^2)}{2(b_1 + c_1)} = \frac{f(2c_1^2 + 2b_1c_1)}{2(b_1 + c_1)} = fc_1 = c.$$

Since $(2uv)/d = a_1$, $(u^2 - v^2)/d = b_1$ and $(u^2 + v^2)/d = c_1$, it follows that $d \mid 2uv$ and $d \mid u^2 \pm v^2$ and the proof is complete. □

4.2 The Group of Equivalence Classes

In this section, we show the isomorphisms between the multiplicative group of K and the groups of Pythagorean triples with different operations.

Definition 4.2.1. Let $(a, b, c), (d, e, f)$ be Pythagorean triples in R. We say that (a, b, c) is *equivalent* to (d, e, f) if there exists a nonzero element $k \in K$ such that $(a, b, c) = (kd, ke, kf)$. Denote the equivalence class of (a, b, c) by $[a, b, c]$.

In a UFD, the set of all equivalence classes of Pythagorean triples may be considered as the set of all primitive Pythagorean triples. For this reason, let

$$PPT_R = \{[a, b, c] \mid a, b, c \in R \text{ with } a \neq 0 \text{ and } a^2 + b^2 = c^2\}$$

be the set of all equivalence classes of Pythagorean triples in R where first components are not zero. Define the operation $*$ as in (2.1) as follows:

$$[a_1, b_1, c_1] * [a_2, b_2, c_2] = [a_1a_2, b_1c_2 + b_2c_1, b_1b_2 + c_1c_2].$$

It is not hard to see that PPT_R with $*$ is an abelian group.

Proposition 4.2.2. *(PPT_R,$*$) is an abelian group. The identity element in PPT_R is $[1, 0, 1]$, and the inverse of $[a, b, c]$ is $[a, -b, c]$.*

Corollary 4.2.3. *($PPT_{\mathbb{Z}[i]}$,$*$) is an abelian group.*

Next we investigate a free abelian group, making use of the subgroup

$$H := \{[1, 0, 1], [1, 0, -1], [1, i, 0], [1, -i, 0]\}$$

of $PPT_{\mathbb{Z}[i]}$. Propositions 2.2.1, 2.2.2 and 4.2.3 give the following corollary.

Corollary 4.2.4. *($PPT_{\mathbb{Z}[i]}/H$,$*$) is a free abelian group which is generated by the set of $[a, b, c]H$ with $a = \delta^3$ or a is an odd prime.*

We establishs an isomorphism between the group of Pythagorean triples of R and the multiplicative group of its quotient field K.

Proposition 4.2.5. *(PPT_R,$*$) is isomorphic to $(K^\times, \cdot)$.*

Proof. Note that if $[a,b,c] \in PPT_R$, then $b{+}c \neq 0$. Define $\varphi : (PPT_R,*) \to (K^\times, \cdot)$ by $\varphi([a,b,c]) = (b+c)/a$. It is clear that φ is well-defined. Let $[a,b,c],[d,e,f] \in PPT_R$. Then

$$\begin{aligned}\varphi([a,b,c]*[d,e,f]) &= \varphi([ad, bf+ec, be+cf]) \\ &= \frac{be+cf+bf+ec}{ad} \\ &= \frac{b+c}{a}\cdot\frac{e+f}{d} \\ &= \varphi([a,b,c])\cdot\varphi([d,e,f]).\end{aligned}$$

To show that φ is injective, let $[a,b,c] \in PPT_R$ be such that $\varphi([a,b,c]) = 1$. Hence $(b+c)/a = 1$, i.e., $a = b+c$. Since $a^2+b^2=c^2$, we obtain $2b(b+c)=0$. Then $b=0$ or $b+c=0$. But $b+c=a$ which is not 0, then $b=0$ and $a=c$. Therefore, $[a,b,c]=[a,0,a]=[1,0,1]$ as desired.

Now let $u/v \in K^\times$ where $u,v \in R \smallsetminus \{0\}$. Choose $a = 2uv, b = u^2-v^2, c = u^2+v^2 \in R$. Then $\varphi([a,b,c]) = (b+c)/a = (u^2+v^2+u^2-v^2)/2uv = u/v$. This implies that φ is an isomorphism. □

Corollary 4.2.6. *($PPT_{\mathbb{Z}[i]}$,$*$) is isomorphic to* $(\mathbb{Q}[i]^\times, \cdot)$.

In order to make PPT_R a field, we add [0, 1, 1] into PPT_R and define the operation addition $\oplus$ by using the isomorphism φ between (PPT_R,$*$) and $(K^\times,\cdot)$. The mapping $\phi : PPT_R \cup \{[0,1,1]\} \to K$ given by

$$\phi([a,b,c]) = \begin{cases} \varphi([a,b,c]) & \text{if } [a,b,c] \in PPT_R, \\ 0 & \text{if } [a,b,c] = [0,1,1] \end{cases}$$

is both injective and surjective. Define the operation $\oplus$ on $PPT_R \cup \{[0,1,1]\}$ by

$$[a,b,c] \oplus [d,e,f] = \phi^{-1}(\phi([a,b,c]) + \phi([d,e,f])).$$

Proposition 4.2.7. *($PPT_R \cup \{[0,1,1]\}$, $\oplus$, $*$) is a field.*

Proof. First, we show that ($PPT_R \cup \{[0,1,1]\}$, $\oplus$) is an abelian group. Clearly, ($PPT_R \cup \{[0,1,1]\}$, $\oplus$) is closed and commutative. Let $[a,b,c],[d,e,f],[x,y,z] \in$

$PPT_R \cup \{[0,1,1]\}$. We have

$$\begin{aligned}
([a,b,c] \oplus [d,e,f]) \oplus [x,y,z] &= \phi^{-1}(\phi([a,b,c]) + \phi([d,e,f])) \oplus [x,y,z] \\
&= \phi^{-1}((\phi([a,b,c]) + \phi([d,e,f])) + \phi([x,y,z])) \\
&= \phi^{-1}(\phi([a,b,c]) + (\phi([d,e,f]) + \phi([x,y,z]))) \\
&= \phi^{-1}(\phi([a,b,c]) + \phi(\phi^{-1}(\phi([d,e,f]) + \phi([x,y,z])))) \\
\text{(by definition of } \oplus) &= [a,b,c] \oplus \phi^{-1}(\phi([d,e,f]) + \phi([x,y,z])) \\
&= [a,b,c] \oplus ([d,e,f] \oplus [x,y,z]).
\end{aligned}$$

Let $[a,b,c] \in PPT_R \cup \{[0,1,1]\}$ and $a \neq 0$. Then

$$\begin{aligned}
[a,b,c] \oplus [0,1,1] &= \phi^{-1}(\phi([a,b,c]) + \phi([0,1,1])) \\
&= \phi^{-1}\left(\frac{b+c}{a} + 0\right) \\
&= [a,b,c]
\end{aligned}$$

and

$$\begin{aligned}
[a,b,c] \oplus [-a,b,c] &= \phi^{-1}(\phi([a,b,c]) + \phi([-a,b,c])) \\
&= \phi^{-1}\left(\frac{b+c}{a} + \frac{b+c}{-a}\right) \\
&= \phi^{-1}(0) \\
&= [0,1,1].
\end{aligned}$$

Moreover, $[0,1,1] \oplus [0,1,1] = [0,1,1]$. Hence $[0,1,1]$ is the identity element in $(PPT_R \cup \{[0,1,1]\}, \oplus)$ and the inverse element to $[a,b,c]$ is $[-a,b,c]$.

Next, it is easy to see that $[0,1,1] * [a,b,c] = [0, b+c, b+c] = [0,1,1]$ for all $[a,b,c] \in PPT_R \cup \{[0,1,1]\}$.

It remains to prove the distributive law. Let $[a,b,c], [d,e,f], [x,y,z] \in PPT_R \cup \{[0,1,1]\}$. Notice that the distributive law holds if $a, d,$ or $x = 0$, so we consider the case where $a, d,$ and x are non-zero. We have

$$\begin{aligned}
&([a,b,c] \oplus [d,e,f]) * [x,y,z] \\
&= \varphi^{-1}(\varphi([a,b,c]) + \varphi([d,e,f])) * [x,y,z] \\
&= \varphi^{-1}(\varphi([a,b,c]) + \varphi([d,e,f])) * \varphi^{-1}(\varphi([x,y,z]))
\end{aligned}$$

$= \varphi^{-1}((\varphi([a,b,c]) + \varphi([d,e,f])) \cdot \varphi([x,y,z]))$ (since φ^{-1} is a homomorphism)

$= \varphi^{-1}((\varphi([a,b,c]) \cdot \varphi([x,y,z])) + (\varphi([d,e,f]) \cdot \varphi([x,y,z])))$ (by distributive law of K)

$= \varphi^{-1}(\varphi([a,b,c]) \cdot \varphi([x,y,z])) \oplus \varphi^{-1}(\varphi([d,e,f]) \cdot \varphi([x,y,z]))$ (by definition of $\oplus$)

$= ([a,b,c] * [x,y,z]) \oplus ([d,e,f] * [x,y,z])$ (since φ^{-1} is a homomorphism). □

The set of Pythagorean triples with operation $+$ defined by

$$[a,b,c] + [d,e,f] = [ad - be, ae + bd, cf] \tag{4.2}$$

was also studied in terms of its structure. In [11], P. Zanardo and U. Zannier described on a ring of integers R such that $i = \sqrt{-1} \notin R$. In case of a ring of integers R where $i \in R$, let

$$\mathcal{PPT}_R = \{[a,b,c] \mid a,b,c \in R \text{ with } c \neq 0; a^2 + b^2 = c^2\}.$$

With operation $+$ in (4.2), $\mathcal{PPT}_R$ is a group. Note that i comes in handy when we show the relation between two operations.

Lemma 4.2.8. *Assume that $i \in R$. $[a,b,c] \in PPT_R$ if and only if $[c, bi, a] \in \mathcal{PPT}_R$.*

The next proposition will show that $(PPT_R,*)$ and $(\mathcal{PPT}_R, +)$ are isomorphic. Hence $(\mathcal{PPT}_R, +)$ is isomorphic to $(K^\times, \cdot)$ as well.

Proposition 4.2.9. *Assume that $i \in R$. $(PPT_R,*)$ is isomorphic to $(\mathcal{PPT}_R, +)$.*

Proof. Define $\lambda : (PPT_R,*) \to (\mathcal{PPT}_R, +)$ by $\lambda([a,b,c]) = [c, bi, a]$.
Let $[a,b,c], [d,e,f] \in PPT_R$. Then

$$\begin{aligned}
\lambda([a,b,c] * [d,e,f]) &= \lambda([ad, bf + ec, be + cf]) \\
&= [be + cf, (bf + ec)i, ad] \\
&= [cf - biei, cei + fbi, ad] \\
&= [c, bi, a] + [f, ei, d] \\
&= \lambda([a,b,c]) + \lambda([d,e,f]).
\end{aligned}$$

The rest of the proof comes from the above lemma. □

REFERENCES

[1] Beauregard, R.A., Suryanarayan, E.R.: Pythagorean Triples: The Hyperbolic View, *The College Mathematics Journal* **27**, 170-181 (1996).

[2] Cohn, H.: *A Classical Invitation to Algebraic Numbers and Class Fields*, Springer-Verlag, New York, 1978.

[3] Cross, J.T.: Primitive Pythagorean Triples of Gaussian Integers, *Mathematics Magazine* **59**, 106-110 (1986).

[4] Dawson, B.: A Ring of Pythagorean Triples, *Missouri Journal of Mathematical Sciences* **6**, 72-77 (1994).

[5] Eckert, E.J.: The Group of Primitive Pythagorean Triangles, *Mathematics Magazine* **57**, 22-27 (1984).

[6] Kubota, K.K.: Pythagorean Triples in Unique Factorization Domains, *The American Mathematical Monthly* **79**, 503-505 (1972).

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

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

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

[10] Sexauer, N.E.: Pythagorean triples over gaussian domains, *The American Mathematical Monthly* **73**, 829-834 (1966).

[11] Zanardo, P., Zannier, U.: The group of pythagorean triples in number fields, *Annali di Matematica pura ed applicata (IV)* **CLIX**, 81-88 (1991).

VITA

Name	Miss Cheranoot Somboonkulavudi
Education	B.Sc. Mathematics (First Class Honor, Gold Medal)
	Chulalongkorn University, 2002
	Full Scholarship Granted by Chulalongkorn University
	M.Sc. Mathematics & Finance
	Imperial College London, 2003
	Full Graduate Scholarship Granted by Royal Thai government
Reward	Gold Medal from IMSO Thailand Camp 1997
	Winner of High School Mathematical Competition (team)
	by Mathematical Association of Thailand 1998
	Runner-up of High School Mathematical Competition (individual)
	by Mathematical Association of Thailand 1998
	Bronze Award in the Asian Pacific Mathematics Olympiad 1998