โครงสร้างของยูนิตกรุปของริงผลหารของจำนวนเต็มในฟีลด์กำลังสามบางฟีลด์

นายพิชญทักษ์ ผลรอด

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต

สาขาวิชาคณิตศาสตร์ ภาควิชาคณิตศาสตร์และวิทยาการคอมพิวเตอร์

คณะวิทยาศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

ปีการศึกษา 2559

STRUCTURE OF UNIT GROUPS OF QUOTIENT RINGS OF INTEGERS IN SOME CUBIC FIELDS

Mr. Pitchayatak Ponrod

A Thesis Submitted in Partial Fulfillment of the Requirements

for the Degree of Master of Science Program in Mathematics

Department of Mathematics and Computer Science

Faculty of Science

Chulalongkorn University

Academic Year 2016

Thesis Title	STRUCTURE OF UNIT GROUPS OF QUOTIENT RINGS OF INTEGERS IN SOME CUBIC FIELDS
By	Mr. Pitchayatak Ponrod
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

(Associate Professor Polkit Sangvanich, Ph.D.)

THESIS COMMITTEE

.... Chairman

(Associate Professor Tuangrat Chaichana, Ph.D.)

.... Thesis Advisor

(Associate Professor Ajchara Harnchoowong, Ph.D.)

.... Examiner

(Assistant Professor Ouamporn Phuksuwan, Ph.D.)

.... External Examiner

(Assistant Professor Prapanpong Pongsriiam, Ph.D.)

พิชญทักษ์ ผลรอด: โครงสร้างของยูนิตกรุปของริงผลหารของจำนวนเต็มในฟีลด์กำลังสามบางฟีลด์ (Structure of Unit Groups of Quotient Rings of Integers in some Cubic fields) อ.ที่ปรึกษาวิทยานิพนธ์หลัก: รศ.ดร.อัจฉรา หาญชูวงศ์, 38 หน้า.

ในริงของจำนวนเต็ม $\mathbb{Z}$ โครงสร้างของยูนิตกรุปของริงผลหาร ซึ่งแทนด้วยสัญลักษณ์ $(\mathbb{Z}_n)^\times$ นั้นเป็นที่รู้จักกันโดยทั่วไป และ โดยทฤษฎีบทเศษเหลือของจีน การศึกษาโครงสร้างของ $(\mathbb{Z}_n)^\times$ ถูกลดลงเหลือการศึกษาโครงสร้างของ $(\mathbb{Z}_{p^e})^\times$ สำหรับทุกจำนวนเฉพาะ p และจำนวนนับ e เป็นที่รู้กันว่าสำหรับจำนวนเฉพาะคี่ p นั้น $(\mathbb{Z}_{p^e})^\times$ จะเป็นกรุปวัฏจักรที่มีลำดับเป็น $\phi(p^e)$ สำหรับทุกจำนวนนับ e ในขณะที่ $(\mathbb{Z}_2)^\times = \{1\}$, $(\mathbb{Z}_4)^\times = \langle -1 \rangle$ และ $(\mathbb{Z}_{2^e})^\times = \langle -1 \rangle \times \langle 5 \rangle$ สำหรับทุกจำนวนนับ $e \geq 3$

สำหรับฟีลด์จำนวน K แทนริงของจำนวนเต็มใน K ด้วย $\mathcal{O}_K$ ในวิทยานิพนธ์นี้ เราจะศึกษาโครงสร้างของยูนิตกรุปของริงผลหาร ซึ่งแทนด้วยสัญลักษณ์ $(\mathcal{O}_K/A)^\times$ สำหรับไอดีล A ใดๆของ $\mathcal{O}_K$ สำหรับฟีลด์กำลังสาม K โดยที่ดิสคริมิแนนต์ของ K นั้นปลอดกำลังสอง

ภาควิชา คณิตศาสตร์และวิทยาการคอมพิวเตอร์ ลายมือชื่อนิสิต ....

สาขาวิชา คณิตศาสตร์ ลายมือชื่อ อ.ที่ปรึกษาหลัก ....

ปีการศึกษา 2559

5772076623 : MAJOR MATHEMATICS
KEYWORDS: CUBIC FIELD/ RING OF INTEGERS/ QUOTIENT RING OF RING OF INTEGER

PITCHAYATAK PONROD: STRUCTURE OF UNIT GROUPS OF QUOTIENT RINGS OF INTEGERS IN SOME CUBIC FIELDS.
ADVISOR: ASSOC. PROF. AJCHARA HARNCHOOWONG, Ph.D., 38 pp.

In the ring of integer $\mathbb{Z}$, the structure of unit groups of quotient rings, denoted by $(\mathbb{Z}_n)^\times$, is known. By the Chinese remainder theorem, the study of structure of $(\mathbb{Z}_n)^\times$ is reduced to study the structure of $(\mathbb{Z}_{p^e})^\times$ for all primes p and natural numbers e. It is well known that for an odd prime p, $(\mathbb{Z}_{p^e})^\times$ is a cyclic group of order $\phi(p^e)$ for all natural number e, while $(\mathbb{Z}_2)^\times = \{1\}, (\mathbb{Z}_4)^\times = \langle -1 \rangle$ and $(\mathbb{Z}_{2^e})^\times = \langle -1 \rangle \times \langle 5 \rangle$ for all natural numbers $e \geq 3$.

For a number field K, denote the ring of integers in K by $\mathcal{O}_K$. In this thesis we will study the structure of unit groups of quotient rings, denoted by $(\mathcal{O}_K/A)^\times$, for any ideal A of $\mathcal{O}_K$ for cubic fields K with square-free discriminant.

Department: Mathematics and Computer Science   Student's Signature ....

Advisor's Signature ....

Field of Study: Mathematics

Academic Year: 2016

Acknowledgements

I would like to acknowledge my gratitude to my advisor, Associate Professor Dr. Ajchara Harnchoowong for her valuable advice and motivation that encourage me to accomplish this thesis. Moreover, I would like to thank Associate Professor Dr. Tuangrat Chaichana, Assistant Professor Dr. Ouamporn Phuksuwan and Assistant Professor Dr. Prapanpong Pongsriiam for being the thesis committee, Assistant Professor Wacharin Wichiramala for his valuable advice about Mathematica and most especially to my family and friends who have rendered their whole hearted support at all times. This thesis is supported by the Scholarship from the Graduate School, Chulalongkorn University to commemorate the 72nd anniversary of his Majesty King Bhumibala Aduladeja.

Table of Contents

Page

Page

CHAPTER I

INTRODUCTION

1.1 Introduction

An important theorem in elementary number theory is the following.

Theorem 1.1. *For an odd prime p, $(\mathbb{Z}_{p^e})^\times$ is cyclic for all natural numbers e, while $(\mathbb{Z}_2)^\times = \{1\}$, $(\mathbb{Z}_4)^\times = \langle -1 \rangle$ and $(\mathbb{Z}_{2^e})^\times = \langle -1 \rangle \times \langle 5 \rangle$ for all natural numbers $e \geq 3$.*

Together with the Chinese remainder theorem, we can get the structure of $(\mathbb{Z}_n)^\times$, i.e., $(\mathbb{Z}/n\mathbb{Z})^\times$, for any natural number n.

Theorem 1.2. *Let n be a natural number which can be factored into $p_1^{e_1} p_2^{e_2} \dots p_m^{e_m}$ for some prime numbers $p_1, p_2, \dots, p_m$ and natural numbers $e_1, e_2, \dots, e_m$. Then*

$$(\mathbb{Z}_n)^\times \cong (\mathbb{Z}_{p_1^{e_1}})^\times \times (\mathbb{Z}_{p_2^{e_2}})^\times \times \cdots \times (\mathbb{Z}_{p_m^{e_m}})^\times.$$

We are interested in the expanding of this result to some number fields. Using a language in algebraic number theory, we have that $\mathbb{Z}$ is the ring of integers of the field of rational numbers $\mathbb{Q}$ which is a number field of degree 1. This leads us to study an analogue of the above theorem for number fields of other degrees. For a number field K, let $\mathcal{O}_K$ be the ring of integers of K and A be a non-zero ideal of $\mathcal{O}_K$, we will study the structure of $(\mathcal{O}_K/A)^\times$. In 1910, A. Ranum [5] studied this problem in all number fields of degree 2. Later, J.T. Cross [2] in 1983 and A.A.

Allan [1] in 2005, apparently unawared of Ranum's work, studied this problem in the field of Gaussian numbers, which is a number fields of degree 2.

In this thesis we consider this problem when K is a number field of degree 3 such that the discriminant of K, $\mathrm{disc}(K)$, is square-free.

1.2 Preliminaries

In this section, we give notations, definitions and theorems used throughout the thesis. Details and proofs can be found in [3] and [6].

1.2.1 The Ring of Integers

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

Example 1.2.1. 1. A **quadratic field** is a number field of degree 2 over $\mathbb{Q}$.

2. A **cubic field** is a number field of degree 3 over $\mathbb{Q}$.

Definition. $\alpha \in \mathbb{C}$ is an **algebraic integer** if it is a root of some monic polynomial with coefficients in $\mathbb{Z}$.

In algebraic number theory, an algebraic integer usually comes up much more often than an integer in $\mathbb{Z}$. So it is convenient to use the word **integer** for an algebraic integer and use the word **rational integer** for a regular integer in $\mathbb{Z}$.

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

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

From now one, let K a number field of degree n over $\mathbb{Q}$.

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

Then there exist n embeddings of K over $\mathbb{Q}$ in $\mathbb{C}$, say $\sigma_1 = id_K, \sigma_2, \ldots, \sigma_n$.

Definition. For $\alpha \in K$, the **norm** of α is defined to be

$$N_K(\alpha) := \sigma_1(\alpha)\sigma_2(\alpha)\ldots\sigma_n(\alpha).$$

Definition. Let $\alpha_1, \alpha_2, \ldots, \alpha_n \in K$. The **discriminant** of $\alpha_1, \alpha_2, \ldots, \alpha_n$ in K is defined to be

$$\operatorname{disc}_K(\alpha_1, \alpha_2, \ldots, \alpha_n) := \det[\sigma_i(\alpha_j)]^2.$$

For $\alpha \in K$, the discriminant of α is defined to be

$$\operatorname{disc}_K(\alpha) = \operatorname{disc}_K(1, \alpha, \alpha^2, \ldots, \alpha^{n-1})$$

Theorem 1.3. *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. 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 1.4. *Let $\{\alpha_1, \ldots, \alpha_n\}$ and $\{\beta_1, \ldots, \beta_n\}$ be any integral bases of K. Then* $\operatorname{disc}_K(\alpha_1, \ldots, \alpha_n) = \operatorname{disc}_K(\beta_1, \ldots, \beta_n)$.

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

Definition. Let $f(x) \in \mathbb{Q}[x]$ be a monic irreducible polynomial of degree n having $\alpha \in \mathbb{C}$ as a root. The discriminant of f, denoted by $\operatorname{disc}(f)$, is defined by

$$\operatorname{disc}(f) := \operatorname{disc}_{\mathbb{Q}(\alpha)}(\alpha).$$

Theorem 1.5. *Let $K = \mathbb{Q}(\alpha)$ for some $\alpha \in \mathcal{O}_K$ be of degree n. If $\mathrm{disc}_K(\alpha)$ is square-free, then $\delta_K = \mathrm{disc}_K(\alpha)$ and $\mathcal{O}_K = \mathbb{Z}[\alpha]$.*

1.2.2 Factorization in the Ring of Integers

Even $\mathbb{Z}$ which is the ring of integers of $\mathbb{Q}$ is a unique factorization domain, this is not true in general for the ring of integers of number fields. For example $\mathbb{Z}[\sqrt{-5}]$ which is the ring of integers of the number field $\mathbb{Q}(\sqrt{-5})$ is not a unique factorization domain. But for ideals in $\mathcal{O}_K$ we have:

Theorem 1.6. *Every non-zero proper ideal in $\mathcal{O}_K$ can be written uniquely as a product of prime ideals.*

Theorem 1.7. *If A is a non-zero ideal of $\mathcal{O}_K$, then $\mathcal{O}_K/A$ is finite.*

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

Theorem 1.8.
1. *For any $\alpha \neq 0$ in $\mathcal{O}_K$, $N(\langle\alpha\rangle) = |N_K(\alpha)|$.*
2. *For any non-zero ideal A and B in $\mathcal{O}_K$, $N(AB) = N(A)N(B)$.*
3. *For a non-zero ideal A in $\mathcal{O}_K$, $N(A) \in A$.*

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

Let K be a number field and p be a prime number in $\mathbb{Z}$. Then $p\mathcal{O}_K$ is a non-zero ideal in $\mathcal{O}_K$. We will consider the prime factorization of $p\mathcal{O}_K$ in $\mathcal{O}_K$. From now on, the term **prime ideal** means **non-zero prime ideal**.

Theorem 1.9. *Let p be a prime number and P be a prime ideal in $\mathcal{O}_K$. Then the following are equivalent.*

1. $P \mid p\mathcal{O}_K$.

2. $P \supset p\mathcal{O}_K$.

3. $P \supset p\mathbb{Z}$.

4. $P \cap \mathbb{Z} = p\mathbb{Z}$.

5. $P \cap \mathbb{Q} = p\mathbb{Z}$.

Definition. For $p\mathbb{Z}$ and P satisfying any of the above theorem, we say that P lies over (above) $p\mathbb{Z}$, or $p\mathbb{Z}$ lies under P.

Theorem 1.10. *1. Every prime P in $\mathcal{O}_K$ lies over a unique prime $p\mathbb{Z}$ of $\mathbb{Z}$.*

2. Every prime $p\mathbb{Z}$ in $\mathbb{Z}$ lies under at least one prime P in $\mathcal{O}_K$.

The following theorem gives us all prime ideals of $\mathcal{O}_K$.

Theorem 1.11. *Let K be a number field of degree n over $\mathbb{Q}$ such that $\mathcal{O}_K = \mathbb{Z}[\alpha]$ for some $\alpha \in \mathcal{O}_K$ with the minimal polynomial $f(x) \in \mathbb{Z}[x]$. Let p be a prime number and $\overline{f}(x)$ be the polynomial obtained from f by reducing all coefficients of f modulo p.*

Suppose that $\overline{f}(x) = \overline{f}_1^{e_1}(x) \cdots \overline{f}_g^{e_g}(x)$ is the factorization of $\overline{f}(x)$ in $\mathbb{Z}_p[x]$. Then

$$p\mathcal{O}_K = \langle p \rangle = P_1^{e_1} \cdots P_g^{e_g}$$

is the prime factorization such that $P_i = \langle p, f_i(\alpha) \rangle$ where $f_i(x)$ is a monic polynomial in $\mathbb{Z}[x]$ whose reduction modulo p is $\overline{f}_i(x)$ and $\deg f_i(x) = \deg \overline{f}_i(x)$ and $N(P_i) = p^{\deg f_i}$.

Using the previous theorem, we can find all prime ideals of $\mathcal{O}_K$ by factorizing $\langle p \rangle$ for all prime numbers p.

CHAPTER II

SOME LEMMAS

Throughout the thesis, we sometimes have to deal with a long summation of elements in $\mathcal{O}_K$ which we just want to say that the summation is in $\mathcal{O}_K$. For example consider

$$(1+2p+3p^2)(2+5p\alpha) = 2 + p(4+5\alpha+6p+10p\alpha+15p^2\alpha).$$

Sometime we don't care what exactly is the multiple of p, we just want to know that it is p multiplies some element of $\mathcal{O}_K$. That is why we will use a square, $\square$, as a placeholder for a non-specific element of $\mathcal{O}_K$. That is we may write

$$(1+2p+3p^2)(2+5p\alpha) = 2 + p\square.$$

Note that $\square$ is a placeholder and is not a variable. That is, each $\square$ may not be equal. We may write $2\square + 4\square = 2\square$.

Notation. For subgroups H and K of an abelian group G, if the product HK is an (internal) direct product, i.e., $H \cap K = \{1\}$, then we will write $H \odot K$ for the product HK.

Note. As $\odot$ is associative, we can write a direct product of more than 2 subgroups consecutively without parentheses. For example, for subgroups H, K and L of an abelian group G, we can write

$$H \odot K \odot L.$$

Theorem 2.1. *Let G be an abelian group and H be a subgroup of G. Let $g \in G$ be an element of order p. If $g \notin H$ then $H \odot \langle g \rangle$.*

Proof. Assume $\notin H$. Suppose the product $H\langle g \rangle$ is not direct. Then $h = g^k$ for some $h \in H \setminus \{1\}$ and $1 \leq k < p$. It can be seen that k is relatively prime to p, so there is $l \in \mathbb{N}$ such that $kl \equiv 1 \pmod{p}$. Since g is of order p, $g = g^{kl} = h^l \in H$ which is a contradiction. $\square$

Theorem 2.2. *Let G be a finite abelian group, H be a subgroup of G and g be an element of G such that the order of g is p^e for some prime number p and natural number $e \geq 2$. If $H \odot \langle g^p \rangle$, then $H \odot \langle g \rangle$.*

Proof. Suppose that $H \odot \langle g^p \rangle$ and the product $H\langle g \rangle$ is not direct. Then $g^k = h$ for some $k \in \mathbb{N}$ and $h \in H \setminus \{1\}$. So $h^p = g^{pk} \in \langle g^p \rangle$ which also implies $h^p \in H \cap \langle g^p \rangle$. Since $H \odot \langle g^p \rangle$, $g^{pk} = h^p = 1$. Since the order of g is a p^e, $p^{e-1} \mid k$. As $e \geq 2$, then $p \mid k$. Together with the fact that $g^k = h$, we get that $h \in \langle g^p \rangle$ and $H \cap \langle g^p \rangle \neq \{1\}$. Thus $H\langle g^p \rangle$ is not direct, which is a contradiction. $\square$

Next theorem is a generalization of Euler's ϕ function to a number field. We will concern only the case where the ideal is a power of a prime ideal. We can use the Chinese remainder theorem to get a general formula.

Definition. A **local ring** is a commutative ring which has a unique maximal ideal.

Theorem 2.3. *Let R be a local ring with the maximal ideal P. Then*

$$R^{\times} = R \setminus P.$$

Theorem 2.4. *For any number field K, prime ideal P of $\mathcal{O}_K$ and natural number e, $\mathcal{O}_K/P^e$ is a local ring with the maximal ideal P/P^e.*

Theorem 2.5. *Let P be a prime ideal of $\mathcal{O}_K$ and $e \in \mathbb{N}$. Then*

$$|(\mathcal{O}_K/P^e)^\times| = (N(P) - 1)N(P)^{e-1}.$$

Proof. By Theorem 2.3 and Theorem 2.4, it follows that

$$(\mathcal{O}_K/P^e)^\times = \mathcal{O}_K/P^e \setminus P/P^e.$$

By the third isomorphism theorem for rings, $\frac{\mathcal{O}_K/P^e}{P/P^e} \cong \mathcal{O}_K/P$, so by Theorem 1.8(i) $|P/P^e| = N(P)^{e-1}$. Thus

$$|(\mathcal{O}_K/P^e)^\times| = |\mathcal{O}_K/P^e| - |P/P^e| = N(P)^e - N(P)^{e-1} = (N(P) - 1)N(P)^{e-1}.$$

□

Definition. Let p be a prime number and $n \in \mathbb{N}$. Denote the highest power m of p such that $p^m \mid n$ by $\nu_p(n)$.

To find the structure of $(\mathcal{O}_K/P^e)^\times$, we need to find the order of some elements of $(\mathcal{O}_K/P^e)^\times$ by the application of the following lemmas and theorems.

Lemma 2.6. *Let p be a prime and $m \in \mathbb{N}$. If either*

1. *$p \geq 3$ and $m \geq 2$, or*

2. *$p = 2$ and $m \geq 3$,*

then
$$m - \nu_p(m) \geq 2.$$

Proof. We first consider the case where $p \geq 3$ and $m = 2$. Since $p \geq 3$, $\nu_p(2) = 0$, so

$$m - \nu_p(m) = 2 - \nu_p(2) = 2 \geq 2.$$

Next for the case of any prime p, suppose for a contradiction that there exists $m \geq 3$ such that $m - \nu_p(m) < 2$. Let l be the least of such m. So

$$l - \nu_p(l) < 2. \tag{1}$$

If $p \nmid l$, then $l - \nu_p(l) = l - 0 \geq 2$, which contradicts (1). So $p \mid l$.

Let $l = pl'$. Since $l' < l$, by the minimality of l, either $l' = 1$, $l' = 2$ or $l' - \nu_p(l') \geq 2$. If $l' = 1$, then $l = p$. So

$$l - \nu_p(l) = p - \nu_p(p) = p - 1 \geq 2,$$

which contradicts (1). If $l' = 2$, then

$$l - \nu_p(l) = 2p - \nu_p(2p) \geq 2p - 2 \geq 2$$

which also contradicts (1). Thus

$$l' - \nu_p(l') \geq 2. \tag{2}$$

Substitute $l = pl'$ in (1), we get $2 > pl' - \nu_p(pl') = pl' - \nu_p(l') - 1$, so

$3 > pl' - \nu_p(l') = (p-1)l' + (l' - \nu_p(l')) \geq (p-1)l' + 2,$ which implies that

$1 > (p-1)l'$. This is impossible since both $p - 1$ and l' are natural numbers. $\square$

Lemma 2.7. *Let p be a prime number and a, m natural numbers such that $0 < m \leq p^a$. Then*

$$\nu_p(\binom{p^a}{m}) = a - \nu_p(m)$$

Proof. For any $i \in \mathbb{N}$ such that $0 < i < p^a$, we see that $\nu_p(i) = \nu_p(p^a - i)$. Consider

$$\binom{p^a}{m} = \frac{p^a(p^a-1)\cdots(p^a-m+1)}{1(2)\cdots(m-1)m}.$$

Since $\nu_p(i) = \nu_p(p^a - i)$ for any $0 < i < p^a$, $\nu_p(p^a - 1) = \nu_p(1), \nu(p^a - 2) = \nu_p(2), \ldots, \nu_p(p^a - m + 1) = \nu_p(m-1)$. Thus $\nu_p(\binom{p^a}{m}) = \nu_p(\frac{p^a}{m}) = a - \nu_p(m)$. $\square$

Theorem 2.8. *Let $a \in \mathbb{N}$ and $r, s \in \mathbb{Z}$. If $p \geq 3$ is a prime number, then*

$$(r + ps\alpha)^{p^a} = r^{p^a} + p^{a+1}r^{p^a-1}s\alpha + p^{a+2}\square.$$

If r and s are odd numbers, then

$$(r + 2s\alpha)^{2^a} = r^{2^a} + 2^{a+1}\alpha + 2^{a+1}\alpha^2 + 2^{a+2}\square.$$

Proof. Let $p \geq 3$ be a prime number. Then

$$(r + ps\alpha)^{p^a} = \sum_{m=0}^{p^a} \binom{p^a}{m} r^{p^a-m}(ps\alpha)^m.$$

By the previous lemma, $\nu_p(\binom{p^a}{m}) = a - \nu_p(m)$ for $m \geq 2$, it follows by Lemma 2.6,

$$\nu_p(\binom{p^a}{m}p^m) = a - \nu_p(m) + m \geq a + 2.$$

for $m \geq 2$. That is every terms from the third term onward ($m \geq 2$) can be combined into $p^{a+2}\square$. The first and second terms are clearly r^{p^a} and $p^{a+1}r^{p^a-1}s\alpha$, respectively.

Again using the previous theorem, from the fourth term onward ($m \geq 3$) of the expansion of $(r + 2s\alpha)^{2^a}$ can be combine to $2^{a+2}\square$, that is,

$$(r + 2s\alpha)^{2^a} = r^{2^a} + 2^{a+1}r^{2^a-1}s\alpha + 2^{a+1}(2^a - 1)r^{2^a-2}s^2\alpha^2 + 2^{a+2}\square.$$

Since r and s are odd, so does $r^{2^a-1}s$. So we can write

$$2^{a+1}r^{2^a-1}s\alpha = 2^{a+1}(1 + 2\square)\alpha = 2^{a+1}\alpha + 2^{a+2}\square.$$

Similarly

$$2^{a+1}(2^a - 1)r^{2^a-2}s^2\alpha^2 = 2^{a+1}(1 + 2\square)\alpha^2 = 2^{a+1}\alpha^2 + 2^{a+2}\square.$$

That is

$$\begin{aligned}(r + 2s\alpha)^{2^a} &= r^{2^a} + (2^{a+1}\alpha + 2^{a+2}\square) + (2^{a+1}\alpha^2 + 2^{a+2}\square) + 2^{a+2}\square. \\ &= r^{2^a} + 2^{a+1}\alpha + 2^{a+1}\alpha^2 + 2^{a+2}\square.\end{aligned}$$

$\square$

Many literatures give only a formula for finding the discriminant of an irreducible polynomial of the form $x^3 + ax + b \in \mathbb{Q}[x]$.

Theorem 2.9. *Let $x^3 + ax + b \in \mathbb{Q}[x]$ be an irreducible polynomial. Then*

$$\operatorname{disc}(x^3 + ax + b) = -4a^3 - 27b^2.$$

We can use the following theorem to obtain a formula for finding discriminant of general monic irreducible cubic polynomials.

Theorem 2.10. *Let $f(x) \in \mathbb{Q}[x]$. Then for all $a \in \mathbb{Q}$,*

$$\operatorname{disc}(f(x+a)) = \operatorname{disc}(f(x)).$$

Theorem 2.11. *If $x_a^3x^2 + bx + c \in \mathbb{Q}[x]$ is an irreducible polynomial, then*

$$\operatorname{disc}(x^3 + ax^2 + bx + c) = a^2b^2 - 4b^3 - 4a^3c - 27c^2 + 18abc.$$

Proof. To make the coefficient of x^2 vanishes, we substitute $x - \frac{a}{3}$ to x. Then

$$\begin{aligned}
&(x-\frac{a}{3})^3 + a(x-\frac{a}{3})^2 + b(x-\frac{a}{3}) + c \\
&\quad = (x^3 - 3x^2(\frac{a}{3}) + 3x(\frac{a^2}{9}) - \frac{a^3}{2}7) + a(x^2 - 2x(\frac{a}{3}) + \frac{a^2}{9}) + b(x - \frac{a}{3}) + c \\
&\quad = x^3 + (-a+a)x^2 + (\frac{a^2}{3} - \frac{2a^2}{3} + b)x + (-\frac{a^3}{27} + \frac{a^3}{9} - \frac{ab}{3} + c) \\
&\quad = x^3 + (-\frac{a^2}{3} + b)x + (\frac{2a^3}{27} - \frac{ab}{3} + c).
\end{aligned}$$

Thus

$$\begin{aligned}
\operatorname{disc}(x^3 + ax^2 + bx + c) &= \operatorname{disc}((x-\frac{a}{3})^3 + a(x-\frac{a}{3})^2 + b(x-\frac{a}{3}) + c) \\
&= -4(-\frac{a^2}{3} + b)^3 - 27(\frac{2a^3}{27} - \frac{ab}{3} + c)^2 \\
&= -4(-\frac{a^6}{27} + \frac{a^4}{3}b - a^2b^2 + b^3) \\
&\quad - 27(\frac{4a^6}{729} + \frac{a^2b^2}{9} + c^2 - \frac{4a^4b}{81} + \frac{4a^3c}{27} - \frac{2abc}{3}) \\
&= a^2b^2 - 4b^3 - 4a^3c - 27c^2 + 18abc.
\end{aligned}$$

$\square$

Sometimes we can use the structure of $(\mathbb{Z}_m)^\times$ for some natural number m to find the structure of $(\mathcal{O}_K/A)^\times$ for some ideal A.

Theorem 2.12. *Let A be an non-zero ideal of $\mathcal{O}_K$. If n is the least natural number in A, then there is the natural embedding*

$$(\mathbb{Z}_n)^\times \hookrightarrow (\mathcal{O}_K/A)^\times.$$

Proof. Consider the natural homomorphism

$$\mathbb{Z} \to \mathcal{O}_K/A$$
$$a \mapsto [a].$$

The kernel of this homomorphism is $\mathbb{Z} \cap A$ which is an ideal of $\mathbb{Z}$. Since A is a non-zero ideal, $0 < N(A) \in A$ and $N(A) \in \mathbb{Z}$, then $\mathbb{Z} \cap A$ is not a zero ideal. Thus

$$\mathbb{Z} \cap A = n\mathbb{Z}$$

for some $n \in \mathbb{N}$. Then by the first isomorphism theorem,

$$\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} \hookrightarrow \mathcal{O}_K/A.$$

Consequently,

$$(\mathbb{Z}_n)^\times = (\mathbb{Z}/n\mathbb{Z})^\times \hookrightarrow (\mathcal{O}_K/A)^\times$$

as desired. Moreover since $\mathbb{Z} \cap A = n\mathbb{Z}$, n is actually the least natural number in A. $\square$

We will concern when the ideal A in the above theorem is P^e or $\langle p^e \rangle$ where P is a prime ideal lying over $p\mathbb{Z}$ and $e \in \mathbb{N}$. Consider the least natural number n in P^e. Since $p \in P$, $p^e \in P^e$, so $\gcd(n, p^e) \in P^e$. Since n is the least natural number in P^e, $n = \gcd(n, p^e)$. Since P^e is a proper ideal, $n \neq 1$, thus $n = p^m$ for some $m \geq 1$. Hence

$$(\mathbb{Z}_{p^m})^\times \hookrightarrow (\mathcal{O}_K/P^e)^\times.$$

For $\langle p^e \rangle$, we proceed similarly. Since $p^e \in \langle p^e \rangle$, then $\gcd(n, p^e) \in \langle p^e \rangle$. Since n is the least natural number in $\langle p^e \rangle$, $n = \gcd(n, p^e)$, thus $n = p^m$ for some $m \geq 1$. Also since $p^m \in \langle p^e \rangle$, $\langle p^e \rangle \mid \langle p^m \rangle$, thus $e \leq m$. This forces $m = e$. Hence

$$(\mathbb{Z}_{p^e})^\times \hookrightarrow (\mathcal{O}_K / \langle p^e \rangle)^\times.$$

CHAPTER III

MAIN THEOREMS

Throughout this chapter, let K be a cubic field such that $\mathcal{O}_K = \mathbb{Z}[\alpha]$ for some $\alpha \in \mathcal{O}_K$ and $\operatorname{disc}(K) = \operatorname{disc}_K(\alpha)$ is square-free. This α will be a root of some monic irreducible polynomial of degree 3, say $f(x)$, in $\mathbb{Z}[x]$. Thus in essence, we study the structure of $(\mathbb{Z}[\alpha]/A)^\times$ for all non-zero ideals A of $\mathbb{Z}[\alpha]$. Applying the Chinese remainder theorem, we only need to consider the structure of $(\mathbb{Z}[\alpha]/P^e)^\times$ for all prime ideals P of $\mathbb{Z}[\alpha]$ and natural numbers e.

3.1 Categories of prime factorizations

We will apply Theorem 1.11 to consider possible factorizations of a monic cubic polynomial $f(x) \pmod{p}$. There are 5 possibilities:

1. $f(x) \equiv (x+a)(x+b)(x+c) \pmod{p}$ for some $a, b, c \in \mathbb{Z}$ that are non-congruent modulo p.

2. $f(x) \equiv (x^2 + a_1x + a_0)(x+b) \pmod{p}$ for some irreducible polynomial $x^2 + a_1x + a_0 \in \mathbb{Z}[x]$ and $b \in \mathbb{Z}$.

3. $f(x) \equiv (x+a)^2(x+b) \pmod{p}$ for some $a, b \in \mathbb{Z}$ that are non-congruent modulo p.

4. $f(x) \equiv (x+a)^3 \pmod{p}$ for some $a \in \mathbb{Z}$.

5. $f(x) \pmod{p}$ is irreducible.

By using Theorem 1.11, each factorization of $f(x)$ corresponds respectively to the following 5 categories:

1. $\langle p\rangle = S_1S_2S_3$
2. $\langle p\rangle = QS$
3. $\langle p\rangle = R^2S$
4. $\langle p\rangle = R^3$
5. $\langle p\rangle$ stays prime

where prime ideals in the factorization in each categories are distinct. Ideals denoted by S with or without a suffix are of norm p, $N(R) = p$ and $N(Q) = p^2$.

3.2 S in the first, second and third categories

This is the easiest case of ideals. Since S_1, S_2 or S_3 does not make any different from S, we will also call them S. We will show that $\mathcal{O}_K/S^e \cong \mathbb{Z}_{p^e}$. We know that $|\mathcal{O}_K/S^e|N(S^e) = p^e$ so it suffices to show that $[0], [1], \ldots, [p^e - 1]$ are distinct in $\mathcal{O}_K/S^e$. Suppose not, then $[a] = [b]$ for some $0 \leq a < b < p^e$ i.e. $b - a \in S^e$. We know that $p^e \in S^e$ so the g.c.d of p^e and $b-a$ which is p^l for some $0 \leq l < e$ is also in S^e and so $\langle p^l\rangle \subseteq S^e$. By the property of ideals in $\mathcal{O}_K$, S^e divides $\langle p^l\rangle$. From the categorization above, the largest power of S dividing $\langle p\rangle$ is 1, so the largest power of S dividing $\langle p^l\rangle$ is l. Since $l < e$ so $S^e \nmid \langle p^l\rangle$ which is a contradiction. So we have the following theorem.

Theorem 3.1. $(\mathcal{O}_K/S^e)^\times \cong (\mathbb{Z}_{p^e})^\times$.

3.3 Q in the second category: $\langle p\rangle = QS$.

Case: $p = 2$

In order for $\langle 2\rangle$ to fall in the second category, by mean of Theorem 1.11, under modulo 2, $f(x)$ has to be factored into a product of two irreducible polynomials, a linear and an irreducible quadratic polynomial modulo 2. Since there is only one irreducible polynomial modulo 2, so

$$f(x) \equiv (x + a_0)(x^2 + x + 1) \pmod 2$$

for some $a_0 \in \mathbb{Z}$. We can simplify the proof by shifting the value of α. Since $\mathbb{Z}[\alpha] = \mathbb{Z}[\alpha + n]$ and $\mathrm{disc}(\alpha) = \mathrm{disc}(\alpha + n)$ for any $n \in \mathbb{Z}$, we can choose a new α such that α is a root of a monic irreducible polynomial $f(x)$ such that

$$f(x) \equiv x((x - a_0)^2 + (x - a_0) + 1) \equiv x(x^2 + x + 1) \pmod 2$$

without changing the structure of $(\mathcal{O}_K/Q^e)^\times$. So $f(x) = x^3 + c_2x^2 + c_1x + 2c_0$ for some natural number c_0 and odd numbers c_1 and c_2. Now from $f(x) \equiv x(x^2+x+1) \pmod 2$, the principle ideal $\langle 2\rangle$ can be factorized to prime ideals as follows:

$$\langle 2\rangle = \langle 2, \alpha\rangle\langle 2, \alpha^2 + \alpha + 1\rangle.$$

That is $Q = \langle 2, \alpha^2 + \alpha + 1\rangle$. Thus 2^e and $(\alpha^2 + \alpha + 1)^e$ are in Q^e. Using the fact that $\alpha^3 + c_2\alpha^2 + c_1\alpha + 2c_0 = 0$, we will show that $(\alpha^2 + \alpha + 1)^e = r\alpha^2 + s\alpha + t$ such that $2 \nmid r, s, t$ by induction. For $e = 1$ it is obvious. Now let $e \geq 1$ and assume that $(\alpha^2 + \alpha + 1)^e = r_e\alpha^2 + s_e\alpha + t_e$ such that $2 \nmid r_e, s_e, t_e$. So

$$(\alpha^2+\alpha+1)^{e+1} = (r_e\alpha^2+s_e\alpha+t_e)(\alpha^2+\alpha+1) = r_e\alpha^4+(r_e+s_e)\alpha^3+(r_e+s_e+t_e)\alpha^2+(s_e+t_e)\alpha+t_e.$$

Using the fact that $\alpha^3 = -c_2\alpha^2 - c_1\alpha - 2c_0$, we have

$$\begin{aligned}(\alpha^2 + \alpha + 1)^{e+1} &= (r_e + s_e + t_e - r_ec_1 - r_ec_2 - s_ec_2 + r_ec_2^2)\alpha^2 \\ &\quad +(s_e + t_e - 2r_ec_0 - r_ec_1 - s_ec_1 + r_ec_1c_2)\alpha + (t_e - 2r_ec_0 - 2s_ec_0 + 2r_ec_0c_2).\end{aligned}$$

Except c_0, we know that every constant is odd, so coefficients of α^2, α and α^0 in the above expression are all odd. So we get the claim that there exists odd numbers r, s, t such that $r\alpha^2 + s\alpha + t \in Q^e$. Also $2^e \in Q^e$ so multiply the previous polynomial by an inverse of r modulo 2^e, we have that $\alpha^2 - d_1\alpha - d_0 \in Q^e$ for some odd numbers d_0 and d_1. This means that in Q^e, $[\alpha^2] = [d_1\alpha + d_0]$. Together with the fact that $|\mathcal{O}_K/Q^e| = 2^{2e}$, we have that elements in $\mathcal{O}_K/Q^e$ can be represented uniquely as follows:

$$\mathcal{O}_K/Q^e = \{[r + s\alpha] \mid 0 \leq r, s < 2^e\}.$$

Now we consider a generating set of $(\mathcal{O}_K/Q^e)^\times$. By Theorem 2.5, the order of $(\mathcal{O}_K/Q^e)^\times$ is $3(2^{2e-2})$ and thus has an element of order 3, denoted by $[h]$. Now we consider the part of elements of order power of 2. For $e \geq 3$, by Theorem 2.8

$$[(1 + 2\alpha)^{2^{e-1}}] = [1 + 2^e\square] = [1],$$

while

$$\begin{aligned}
[(1 + 2\alpha)^{2^{e-2}}] &= [1 + 2^{e-1}\alpha + 2^{e-1}\alpha^2 + 2^e\square] \\
&= [1 + 2^{e-1}\alpha + 2^{e-1}(d_1 + d_0\alpha) + 2^e\square] \\
&= [1 + 2^{e-1}\alpha + 2^{e-1}(1 + \alpha) + 2^e\square] \\
&= [1 + 2^{e-1} + 2^e\square] \\
&= [1 + 2^{e-1}] \\
&\neq [1].
\end{aligned}$$

Thus the order of $[1 + 2\alpha]$ is 2^{e-1} for all $e \geq 3$. For $e = 1, 2$, we can see that the order of $[1 + 2\alpha]$ is also 2^{e-1}. And

$$\begin{aligned}
(1 + 4\alpha)^{2^{e-2}} &= 1 + 2^{e-2}(4\alpha) + \binom{2^{e-2}}{2}(4\alpha)^2 + 2^e\square \\
&= 1 + 2^e\square,
\end{aligned}$$

while

$$\begin{aligned}(1+4\alpha)^{2^{e-3}} &= 1+2^{e-3}(4\alpha)+2^e\Box \\ &= 1+2^{e-1}\alpha+2^e\Box.\end{aligned}$$

Thus the order of $[1+4\alpha]$ is 2^{e-2} for $e \geq 3$ and the order is 1 for $e = 1, 2$. When $e = 1$, $(\mathcal{O}_K/Q)^\times$ is just a cyclic group of order 3.

$$(\mathcal{O}_K/Q)^\times = \langle [h] \rangle \cong \mathbb{Z}_3 \cong (\mathbb{Z}_2)^\times \times \mathbb{Z}_3.$$

When $e = 2$, consider the product of two subgroups generated by elements of order 2:

$$\langle [1+2\alpha] \rangle \langle [-1] \rangle.$$

Since $[1+2\alpha] \notin \langle [-1] \rangle$, so by Theorem 2.1, the product is direct. Since the order of $(\mathcal{O}_K/Q^2)^\times$ is $3(2^2)$, then together with $[h]$, an element of order 3, we get that

$$(\mathcal{O}_K/Q^2)^\times = \langle [1+2\alpha] \rangle \odot \langle [-1] \rangle \odot \langle [h] \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \cong (\mathbb{Z}_{2^2})^\times \times \mathbb{Z}_2 \times \mathbb{Z}_3.$$

Now for $e \geq 3$, consider the product of three subgroups generated by elements of order 2:

$$\langle [1+2^{e-1}] \rangle \langle [1+2^{e-1}\alpha] \rangle \langle [-1] \rangle.$$

Since $e \geq 3$, $[1+2^{e-1}] \neq [-1]$ and so $\langle [1+2^{e-1}] \rangle \odot \langle [-1] \rangle$. The previous direct product contains only cosets representable by natural numbers so $[1+2^{e-1}\alpha] \notin \langle [1+2^{e-1}] \rangle \odot \langle [-1] \rangle$. By Theorem 2.1, we have

$$\langle [1+2^{e-1}] \rangle \odot \langle [1+2^{e-1}\alpha] \rangle \odot \langle [-1] \rangle.$$

By computations above, the product can be written as

$$\langle [(1+4\alpha)^{2^{e-3}}] \rangle \odot \langle [(1+2\alpha)^{2^{e-2}}] \rangle \odot \langle [-1] \rangle.$$

By Theorem 2.2,

$$\langle[1+4\alpha]\rangle \odot \langle[1+2\alpha]\rangle \odot \langle[-1]\rangle.$$

It is a direct product of order $(2^{e-2})(2^{e-1})(2) = 2^{2e-2}$. Since the order of $(\mathcal{O}_K/Q^e)^\times$ is $3(2^{2e-2})$, thus together with an element $[h]$ of order 3, We have

$$\begin{aligned}(\mathcal{O}_K/Q^e)^\times &= \langle[1+4\alpha]\rangle \odot \langle[1+2\alpha]\rangle \odot \langle[-1]\rangle \odot \langle[h]\rangle \\ &\cong \mathbb{Z}_{2^{e-2}} \times \mathbb{Z}_{2^{e-1}} \times \mathbb{Z}_2 \times \mathbb{Z}_3 \\ &\cong (\mathbb{Z}_{2^e})^\times \times \mathbb{Z}_{2^{e-1}} \times \mathbb{Z}_3.\end{aligned}$$

To summarize,

Theorem 3.2. *Let Q be a prime ideal lying over 2 of norm 4. Then*

$$(\mathcal{O}_K/Q^e)^\times \cong (\mathbb{Z}_{2^e})^\times \times \mathbb{Z}_{2^{e-1}} \times \mathbb{Z}_3.$$

Case: $p \geq 3$

We find that it is easier to consider instead $(\mathcal{O}_K/S^eQ^e)^\times = (\mathcal{O}_K/\langle p^e\rangle)^\times$ and use the isomorphism $(\mathcal{O}_K/S^eQ^e)^\times \cong (\mathcal{O}_K/S^e)^\times \times (\mathcal{O}_K/Q^e)^\times$ to get the structure of $(\mathcal{O}_K/Q^e)^\times$. Elements of $\mathcal{O}_K/\langle p^e\rangle$ can be represented uniquely by

$$\mathcal{O}_K/\langle p^e\rangle = \{[r+s\alpha+t\alpha^2] \mid 0 \leq r,s,t < p^e\}.$$

Since $(\mathcal{O}_K/Q)^\times$ is the unit group of the field $\mathcal{O}_K/Q$, it is a cyclic group of order p^2-1. $(\mathcal{O}_K/Q)^\times$ can be embedded into $(\mathcal{O}_K/\langle p\rangle)^\times$, thus $(\mathcal{O}_K/\langle p\rangle)^\times$ has an element $[h]$ of order p^2-1. So

$$h^{p^2-1} = 1 + p\square.$$

Then

$$h^{p^e(p^2-1)} = 1 + p^e\square.$$

Let m be the order of $[h^{p^e}]$ in $(\mathcal{O}_K/\langle p^e\rangle)^\times$. Then $m \mid p^2-1$ and $h^{p^e m} = 1 + p^e\square = 1 + p\square$, so the order of $[h]$ in $(\mathcal{O}_K/Q)^\times$ divides $p^e m$, i.e., $p^2-1 \mid p^e m$. Since

$\gcd(p^2-1, p^e) = 1$, $p^2 - 1 \mid m$, so $m = p^2 - 1$, i.e., $[h^{p^e}]$ is of order $p^2 - 1$ in $(\mathcal{O}_K/\langle p^e\rangle)^\times$. When $e = 1$, $(\mathcal{O}_K/Q)^\times$ is the group of units of the field $\mathcal{O}_K/Q$ thus is cyclic of order $p^2 - 1$, so

$$(\mathcal{O}_K/Q)^\times \cong \mathbb{Z}_{p^2-1}.$$

Now for $e \geq 2$, we have

$$(1 + p\alpha)^{p^{e-1}} = 1 + p^e\square$$

while

$$(1 + p\alpha)^{p^{e-2}} = 1 + p^{e-1}\alpha + p^e\square.$$

Similarly

$$(1 + p\alpha^2)^{p^{e-1}} = 1 + p^e\square$$

while

$$(1 + p\alpha^2)^{p^{e-2}} = 1 + p^{e-1}\alpha^2 + p^e\square.$$

Let $[g]$ be a generator of $(\mathbb{Z}_{p^e})^\times$ embedded naturally in $(\mathcal{O}_K/\langle p^e\rangle)^\times$ thus $[g^{p-1}]$ is of order p^{e-1}. Consider the product

$$\langle [g^{(p-1)p^{e-2}}]\rangle\langle[1 + p^{e-1}\alpha]\rangle\langle[1 + p^{e-1}\alpha^2]\rangle.$$

As always we will use Theorem 2.1 to show that the above product is direct. The first subgroup only contains cosets representable by natural numbers, thus $[1 + p^{e-1}\alpha] \notin \langle[g^{(p-1)p^{e-2}}]\rangle$, so the product of the first two subgroups is direct. Since $(1 + p^{e-1}\alpha)^l = 1 + lp^{e-1} + p^e\square$ so the product of the first two subgroup only contains cosets representable by an element in the form $r+s\alpha$. Hence $[1+p^{e-1}\alpha^2] \notin \langle[g^{p^{e-2}}]\rangle\langle[1 + p^{e-1}\alpha]$ and we have

$$\langle[g^{(p-1)p^{e-2}}]\rangle \odot \langle[1 + p^{e-1}\alpha]\rangle \odot \langle[1 + p^{e-1}\alpha^2]\rangle.$$

By Theorem 2.2,

$$\langle [g^{p-1}] \rangle \odot \langle [1+p\alpha] \rangle \odot \langle [1+p\alpha^2] \rangle$$

of order $p^{e-1}p^{e-1}p^{e-1} = p^{3e-3}$. Since the order of $(\mathcal{O}_K/\langle p^e \rangle)^\times$ is $(p-1)(p^2-1)p^{3e-3}$. Together with the fact that the element $[g^{p^{e-1}}]$ is of order $p-1$ and $[h^{p^e}]$ is of order p^2-1, we have that

$$\begin{aligned}(\mathcal{O}_K/\langle p^e \rangle)^\times &= \langle [g^{p^{e-1}}] \rangle \odot \langle [g^{p-1}] \rangle \odot \langle [1+p\alpha] \rangle \odot \langle [1+p\alpha^2] \rangle \odot \langle [h^{p^e}] \rangle \\ &\cong \mathbb{Z}_{p-1} \times \mathbb{Z}_{p^{e-1}} \times \mathbb{Z}_{p^{e-1}} \times \mathbb{Z}_{p^{e-1}} \times \mathbb{Z}_{p^2-1}.\end{aligned}$$

Now $(\mathcal{O}_K/\langle p^e \rangle)^\times \cong (\mathcal{O}_K/S^e)^\times \times (\mathcal{O}_K/Q^e)^\times \cong \mathbb{Z}_{p^{e-1}(p-1)} \times (\mathcal{O}_K/Q^e)^\times$. Hence

$$(\mathcal{O}_K/Q^e)^\times \cong \mathbb{Z}_{p^{e-1}} \times \mathbb{Z}_{p^{e-1}} \times \mathbb{Z}_{p^2-1}.$$

To summarize,

Theorem 3.3. *Let Q be a prime ideal lying over $p \geq 3$ of norm p^2. Then*

$$(\mathcal{O}_K/Q^e)^\times \cong \mathbb{Z}_{p^{e-1}} \times \mathbb{Z}_{p^{e-1}} \times \mathbb{Z}_{p^2-1}.$$

3.4 R in the third category: $\langle p \rangle = R^2S$

We will see that under our assumption that the discriminant of K is square-free prevents the case $p = 2$. To fall in this category, the minimal polynomial $f(x)$ of α will be congruent to $(x+a_0)(x+a_1)^2 \pmod{p}$ for some $a_0, a_1 \in \mathbb{N}$ such that $a_0 \not\equiv a_1 \pmod{p}$. We can shift the value of α to make $f(x) \equiv (x+b_0)x^2 \pmod{p}$ for some $b_0 \in \mathbb{N}$ such that $p \nmid b_0$ and so

$$\langle p \rangle = \langle p, \alpha + b_0 \rangle \langle p, \alpha \rangle^2.$$

Since $f(x) \equiv x^3 + b_0x^2 \pmod{p}$, $f(x) = x^3 + a_2x^2 + pa_1x + pa_0$ for some $a_0, a_1, a_2 \in \mathbb{Z}$ such that $p \nmid a_2$ and $a_2 \equiv b_0 \pmod{p}$. By Theorem 2.11

$$\operatorname{disc}(f) = -4a_1^3p^3 + \left(-27a_0^2 + 18a_1a_2a_0 + a_1^2a_2^2\right)p^2 - 4a_0a_2^3p$$

which is not square-free if $p \mid a_0$ or $p = 2$. Thus in this section $p \neq 2$ and $p \nmid a_0$. Next we consider a representation set of $\mathcal{O}_K/R^e$. First we need this lemma:

Lemma 3.4. *For all $e \geq 1$, there exist $c_0, c_1 \in \mathbb{Z}$ such that $\alpha^2 + pc_1\alpha + pc_0 \in R^e$ and $p \nmid c_0$.*

Proof. We prove by induction. First $R = \langle p, \alpha \rangle$ so $\alpha^2 \in R$. Let $e \geq 1$ and assume there exists c_0, c_1 such that $\alpha^2 + pc_1\alpha + pc_0 \in R^e$ and $p \nmid c_0$. Since $\alpha \in R$, $\alpha(\alpha^2 + pc_1\alpha + pc_0) \in R^{e+1}$. Using $\alpha^3 = -a_2\alpha^2 - pa_1\alpha - pa_0$, we have

$$\alpha(\alpha^2 + pc_1\alpha + pc_0) = (pc_1 - a_2)\alpha^2 + (pc_0 - pa_1)\alpha - pa_0.$$

Since $p \nmid a_2$, $p \nmid pc_1 - a_2$, thus $pc_1 - a_2$ have an inverse modulo $p^{e+1} \in R^{e+1}$. Multiply by the inverse, we have

$$(pc_1 - a_2)^{-1}\Big((pc_1 - a_2)\alpha^2 + (pc_0 - pa_1)\alpha - pa_0\Big) \in R^{e+1}.$$

So

$$\alpha^2 + (pc_1 - a_2)^{-1}(pc_0 - pa_1)\alpha - (pc_1 - a_2)^{-1}pa_0 \in R^{e+1}.$$

We see that $p \mid (pc_1 - a_2)^{-1}(pc_0 - pa_1)$ and $p \mid (pc_1 - a_2)^{-1}pa_0$. Moreover, $p \nmid a_0(pc_1 - a_2)^{-1}$, so we get the lemma. $\square$

Now we can choose representations of cosets in $(\mathcal{O}_K/R^e)^\times$. Since $\alpha^2 + c_1\alpha + c_0 \in R^e$ for some $c_0, c_1 \in \mathbb{Z}$, a representation of any coset in $(\mathcal{O}_K/R^e)^\times$ can be chosen in a form $r + s\alpha$. We divide into two cases: an exponent of R is even or odd.

When an exponent of R is even, say it is $2e$ for some $e \geq 1$. Since $\langle p^e \rangle = R^{2e}S^e \subseteq R^{2e}$, $p^e, p^e\alpha \in R^{2e}$. Also $|\mathcal{O}_K/R^{2e}| = N(R^{2e}) = p^{2e}$, thus $\mathcal{O}_K/R^{2e}$ can be represented uniquely as

$$\mathcal{O}_K/R^{2e} = \{[r + s\alpha] \mid 0 \leq r, s < p^e\}.$$

Similarly for an odd exponent, say it is $2e+1$ for some $e \geq 0$. Since $R^{2e+1} \supseteq R^{2e+1}S^e = \langle p^e \rangle \langle p, \alpha \rangle = \langle p^{e+1}, p^e\alpha \rangle$, $p^{e+1}, p^e\alpha \in R^{2e+1}$. Also $|\mathcal{O}_K/R^{2e+1}| = N(R^{2e+1}) = p^{2e+1}$, thus $\mathcal{O}_K/R^{2e+1}$ can be represented uniquely as

$$\mathcal{O}_K/R^{2e+1} = \{[r + s\alpha] \mid 0 \leq r < p^{e+1}, 0 \leq s < p^e\}.$$

Now we consider a generating set. First, some basic cases. $(\mathcal{O}_K/R)^\times$ is the unit group of the field $\mathcal{O}_K/R$, so is a cyclic group of order $p-1$, i.e.,

$$(\mathcal{O}_K/R)^\times \cong \mathbb{Z}_{p-1}.$$

Since $\mathcal{O}_K/R^2 = \{[r + s\alpha] \mid 0 \leq r, s < p\}$ has a subgroup isomorphic to $\mathbb{Z}_p$, $(\mathcal{O}_K/R^2)^\times$ has a subgroup isomorphic to $\mathbb{Z}_{p-1}$. By Theorem 2.5, $|(\mathcal{O}_K/R^2)^\times| = (p-1)p$, so

$$(\mathcal{O}_K/R^2)^\times \cong \mathbb{Z}_{p-1} \times \mathbb{Z}_p.$$

Similarly $\mathcal{O}_K/R^3 = \{[r + s\alpha] \mid 0 \leq r < p^2, 0 \leq s < p\}$, which has a subgroup isomorphic to $\mathbb{Z}_{p^2}$. Thus $(\mathcal{O}_K/R^3)^\times$ has a subgroup isomorphic to $\mathbb{Z}_{p(p-1)}$. By Lemma 3.4, $[\alpha^2] = [-pa_1\alpha - pa_0]$, so $[\alpha^2] = [p\Box]$. Thus for $p \geq 3$, $[\alpha^p] = [\alpha^2(\alpha)\alpha^{p-3}] = [p\alpha\Box]$. Thus for any $[r + s\alpha] \in (\mathcal{O}_K/R^3)^\times$,

$$[r + s\alpha]^p = [r^p + pr^{p-1}s\alpha + \cdots + pr(s\alpha)^{p-1} + \alpha^p] = [r^p + p\alpha\Box] = [r^p].$$

And the order of $[r^p]$ in $\mathcal{O}_K/R^3$ is at most $p-1$. So the order of any element of $(\mathcal{O}_K/R^3)^\times$ is at most $p(p-1)$, thus

$$(\mathcal{O}_K/R^3)^\times \cong \mathbb{Z}_{p-1} \times \mathbb{Z}_p \times \mathbb{Z}_p.$$

Next we consider $(\mathcal{O}_K/R^{2e})^\times$ and $(\mathcal{O}_K/R^{2e+1})^\times$ for $e \geq 2$. For $p \geq 5$,

$$[(1 + \alpha)^p] = [1 + p\alpha + p(p-1)\alpha^2 + \cdots + p\alpha^{p-1} + \alpha^p].$$

From Lemma 3.4, we know that $[\alpha^2] = [pa_1\alpha + pa_0] = [p\square]$ and for any $k \geq 2$, $[p\alpha^k] = [p^2\alpha^{k-2}\square] = [p^2\square]$.

Since $p \geq 5$, $[\alpha^p] = [\alpha^2][\alpha^2][\alpha^{p-4}] = [p\square][p\square][\square] = [p^2\square]$. Thus from the third term of the expansion of $[(1+\alpha)^p]$ onward can be combined into $p^2\square$, that is,

$$[(1+\alpha)^p] = [1 + p\alpha + p^2\square].$$

We will see later that if $p = 3$, $[1+\alpha]^3$ may not always be $[1 + 3\alpha + 3^2\square]$. From Lemma 3.4, $\alpha^2 + 3m\alpha + 3n \in Q^e$ for some $m, n \in \mathbb{Z}$, that is, $[\alpha^2] = [-3m\alpha - 3n]$. So $[\alpha^3] = [-3m\alpha^2 - 3n\alpha] = [-3m(-3m\alpha - 3n) - 3n\alpha] = [(9m^2 - 3n)\alpha + 9mn] = [-3n\alpha + 9\square]$. Thus

$$\begin{aligned}
[(r+s\alpha)^3] &= [r^3 + 3r^2 s\alpha + 3rs^2\alpha^2 + s^3\alpha^3] \\
&= [r^3 + 3r^2 s\alpha + 3rs^2(-3m\alpha - 3n) + (-3ns^3\alpha + 9\square)] \\
&= [r^3 + 3r^2 s\alpha + 9\square + (-3ns^3\alpha + 9\square)] \\
&= [r^3 + 3(r^2 s - ns^3)\alpha + 9\square + 9\square] \\
&= [r^3 + 3(r^2 s - ns^3)\alpha + 9\square].
\end{aligned}$$

Since we get m, n from Lemma 3.4, $3 \nmid n$, so $n \equiv 1$ or $2 \pmod 3$. We will consider first the case $n \equiv 2 \pmod 3$, we choose $r = 1$ and $s = 2$ so that the above coset will be $[(r+s\alpha)^3] = [1+3(2-2(8))\alpha+9\square] = [1+3\alpha+9\square]$. We will consider the case $p = 3$ when $n \geq 1 \pmod 3$ together with the case $p \geq 5$ because both of the cases has $r, s \in \mathbb{Z}$ such that $[r+s\alpha]^p = [1 + p\alpha + p^2\square]$. For $e \geq 2$,

$$(1 + p\alpha + p^2\square)^{p^{e-1}} = 1 + p^e\alpha + p^{e+1}\square,$$

while

$$\begin{aligned}(1+p\alpha+p^2\square)^{p^{e-2}} &= (1+p(\alpha+p\square))^{p^{e-2}} \\ &= 1+p^{e-1}(\alpha+p\square)+p^e\square \\ &= 1+p^{e-1}+p^e\square\end{aligned}$$

Since $p^e, p^e\alpha \in R^{2e}, p^{e+1}, p^e\alpha \in R^{2e+1}$,

$$\mathcal{O}_K/R^{2e} = \{[r+s\alpha] \mid 0 \le r < p^e \text{ and } 0 \le s < p^e\},$$

and

$$\mathcal{O}_K/R^{2e+1} = \{[r+s\alpha] \mid 0 \le r < p^{e+1} \text{ and } 0 \le s < p^e\},$$

then in both $(\mathcal{O}_K/R^{2e})^\times$ and $(\mathcal{O}_K/R^{2e+1})^\times$, the order of $[1+p\alpha+p^2\square]$ is p^{e-1}. Since for $p \ge 5$, $[1+\alpha]^p = [1+p\alpha+p^2\square]$ and for $p=3$, $[1+2\alpha]^3 = [1+3\alpha+9\square]$, then for $p \ge 5$, the order of $[1+\alpha]$ is p^e and for $p=3$, the order of $[1+2\alpha]$ is p^e. Now let $[g]$, be a generator of $(\mathbb{Z}_{p^e})^\times$ naturally embedded in $(\mathcal{O}_K/R^{2e})^\times$, so the order of $[g]$ in $(\mathcal{O}_K/R^{2e})^\times$ is $(p-1)p^{e-1}$. Consider the product

$$\langle [g^{(p-1)p^{e-2}}] \rangle \langle [1+p^{e-1}\alpha] \rangle.$$

Since $\langle [g^{(p-1)p^{e-2}}] \rangle$ only contains cosets representable by natural numbers, $[1+p^{e-1}\alpha] \notin \langle [g^{(p-1)p^{e-2}}] \rangle$ so by Theorem 2.1,

$$\langle [g^{(p-1)p^{e-2}}] \rangle \odot \langle [1+p^{e-1}\alpha] \rangle.$$

Since $[r+s\alpha]^p = [1+p\alpha+p^2\square]$ and $[1+p\alpha+p^2\square]^{p^{e-2}} = [1+p^{e-1}\alpha]$, we then have by Theorem 2.2 that,

$$\langle [g^{p-1}] \rangle \odot \langle [r+s\alpha] \rangle$$

is a direct product of order $p^{e-1}p^e = p^{2e-1}$. Thus

$$\langle [g] \rangle \odot \langle [r+s\alpha] \rangle$$

is a subgroup of $(\mathcal{O}_K/R^{2e})^\times$ of order $p^{2e-1}(p-1)$ which is the same as the order of $(\mathcal{O}_K/R^{2e})^\times$. Similarly, let $[g]$ be a generator of $(\mathbb{Z}_{p^{e+1}})^\times$ embedded in $(\mathcal{O}_K/R^{2e+1})^\times$. Consider the product

$$\langle [g^{(p-1)p^{e-1}}] \rangle \langle [1+p^{e-1}\alpha] \rangle.$$

Since $\langle [g^{(p-1)p^{e-1}}] \rangle$ only contains cosets representable by natural numbers, then $[1+p^{e-1}\alpha] \notin \langle [g^{(p-1)p^{e-1}}] \rangle$. Thus by Theorem 2.1,

$$\langle [g^{(p-1)p^{e-1}}] \rangle \odot \langle [1+p^{e-1}\alpha] \rangle$$

Similarly as in the above, we have by Theorem 2.2 that

$$\langle [g^{p-1}] \rangle \odot \langle [r+s\alpha] \rangle$$

is a direct product of order $p^e p^e = p^{2e}$. Thus

$$\langle [g] \rangle \odot \langle [r+s\alpha] \rangle$$

is a subgroup of $(\mathcal{O}_K/R^{2e+1})^\times$ of order $p^{2e}(p-1)$ which is the same as the order of $(\mathcal{O}_K/R^{2e+1})^\times$. Thus for $p=3$,

$$(\mathcal{O}_K/R^{2e})^\times = \langle [g] \rangle \odot \langle [1+2\alpha] \rangle,$$

$$(\mathcal{O}_K/R^{2e+1})^\times = \langle [g] \rangle \odot \langle [1+2\alpha] \rangle,$$

and for $p \geq 5$,

$$(\mathcal{O}_K/R^{2e})^\times = \langle [g] \rangle \odot \langle [1+\alpha] \rangle,$$

$$(\mathcal{O}_K/R^{2e+1})^\times = \langle [g] \rangle \odot \langle [1+\alpha] \rangle.$$

Now for the special case we left out earlier which is the case when $p=3$ and $\alpha^2+3m\alpha+3n \in R^e$ such that $n \equiv 1 \pmod 3$. Recall that

$$[(r+s\alpha)^3] = [r^3 + 3(r^2 s - n s^3)\alpha + 9\square].$$

1. If $3 \mid r$, then

$$[(r+s\alpha)^3] = [r^3 + 3(r^2s - ns^3)\alpha + 9\square] = [3\square].$$

Since $3^k \in R^e$ for some k, $[3\square]$ is a zero-divisor in $\mathcal{O}_K/R^e$, then $[r+s\alpha]$ is also a zero-divisor, that is, $[r+s\alpha] \notin (\mathcal{O}_K/R^e)^\times$, so we do not need to consider this case.

2. If $3 \nmid r$ and $3 \mid s$, then

$$[(r+s\alpha)^3] = [r^3 + 3(r^2s - ns^3)\alpha + 9\square] = [r^3 + 9\square].$$

3. If $3 \nmid r$ and $3 \nmid s$, then

$$r^2s - ns^3 \equiv r^2s - s^3 \equiv r^2s - s \equiv s(r^2-1) \equiv s(1-1) \equiv 0 \pmod 3.$$

Thus for any $[r+s\alpha] \in (\mathcal{O}_K/R^e)^\times$,

$$[(r+s\alpha)^3] = [r^3 + 3(r^2s - ns^3)\alpha + 9\square] = [r^3 + 9\square].$$

By Theorem 2.5,

$$|(\mathcal{O}_K/R^{2e})^\times| = (3-1)3^{2e-1} = 2(3^{2e-1})$$

and

$$|(\mathcal{O}_K/R^{2e+1})^\times| = (3-1)3^{2e} = 2(3^{2e}).$$

Now we consider the structures of $(\mathcal{O}_K/R^{2e})^\times$ for $e \geq 2$. From the earlier $|(\mathcal{O}_K/R^{2e})^\times| = 2(3^{2e-1})$. Consider

$$(1+3\alpha)^{3^{e-1}} = 1 + 3^e\square,$$

while

$$(1+3\alpha)^{3^{e-2}} = 1 + 3^{e-1}\alpha + 3^e\square.$$

Let $[g]$ be a generator of $(\mathbb{Z}_{3^e})^\times$ embedded naturally in $(\mathcal{O}_K/R^{2e})^\times$. Since $[1+3^{e-1}\alpha] \notin \langle [g^{2(3^{e-2})}] \rangle$, by Theorem 2.1,

$$\langle [g^{2(3^{e-2})}] \rangle \odot \langle [1+3^{e-1}\alpha] \rangle.$$

By Theorem 2.2, we have

$$\langle [g^2] \rangle \odot \langle [1+3\alpha] \rangle$$

is a direct product of subgroups of order $3^{e-1}3^{e-1} = 3^{2e-2}$. Thus $\langle [g] \rangle \odot \langle [1+3\alpha] \rangle$ is of order $2(3^{2e-2})$. This means that $\langle [g] \rangle \odot \langle [1+3\alpha] \rangle$ is a subgroup of index 3 in $(\mathcal{O}_K/R^{2e})^\times$. Since $\langle [g] \rangle \odot \langle [1+3\alpha] \rangle$ is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_{3^{e-1}} \times \mathbb{Z}_{3^{e-1}}$, then the structure of $(\mathcal{O}_K/R^{2e})^\times$ is either

$$\mathbb{Z}_2 \times \mathbb{Z}_{3^e} \times \mathbb{Z}_{3^{e-1}} \qquad \text{or} \qquad \mathbb{Z}_2 \times \mathbb{Z}_{3^{e-1}} \times \mathbb{Z}_{3^{e-1}} \times \mathbb{Z}_3.$$

From the earlier, for any $[r+s\alpha] \in (\mathcal{O}_K/R^{2e})^\times$, $[r+s\alpha]^3 = [r^3+9\square]$, so $[r+s\alpha]^{2(3^{e-1})} = [r^3+9\square]^{2(3^{e-2})} = [r^{3^{e-1}}+3^e\square]^2 = [r^{2(3^{e-1})}] = [1]$. Thus the order of any element in $(\mathcal{O}_K/R^{2e})^\times$ is not greater than $2(3^{e-1})$. This means that

$$(\mathcal{O}_K/R^{2e})^\times \cong \mathbb{Z}_2 \times \mathbb{Z}_{3^{e-1}} \times \mathbb{Z}_{3^{e-1}} \times \mathbb{Z}_3.$$

Now consider $(\mathcal{O}_K/R^{2e+1})^\times$, which is of order $(p-1)p^{2e}$. Let $[g]$ be a generator of $(\mathbb{Z}_{3^{e+1}})^\times$ embedded naturally in $(\mathcal{O}_K/R^{2e+1})^\times$. Then the subgroup $\langle [g] \rangle \odot \langle [1+3\alpha] \rangle$ which is of order $2(3^e)(3^{e-1}) = 2(3^{2e-1})$ is of index 3 and isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_{3^e} \times \mathbb{Z}_{3^{e-1}}$. Hence the structure of $(\mathcal{O}_K/R^{2e+1})^\times$ is either

$$\mathbb{Z}_2 \times \mathbb{Z}_{3^{e+1}} \times \mathbb{Z}_{3^{e-1}} \quad , \quad \mathbb{Z}_2 \times \mathbb{Z}_{3^e} \times \mathbb{Z}_{3^e} \quad \text{or} \quad \mathbb{Z}_2 \times \mathbb{Z}_{3^e} \times \mathbb{Z}_{3^{e-1}} \times \mathbb{Z}_3.$$

Similar to the above, any element in $(\mathcal{O}_K/R^{2e+1})^\times$ is of order at most $2(3^e)$ so the first form is impossible. To show that the second form is also impossible, we need the following lemma:

Lemma 3.5. *Let p be a prime number and $e \in \mathbb{N}$. For any element (a, b) of order p^e in the additive group $\mathbb{Z}_{p^e} \times \mathbb{Z}_{p^e}$, we can find an element (c, d), also of order p^e, such that*

$$\mathbb{Z}_{p^e} \times \mathbb{Z}_{p^e} = \langle (a, b) \rangle \oplus \langle (c, d) \rangle.$$

Proof. Since (a, b) is of order p^e, $(p^{e-1}a, p^{e-1}b) \neq (0, 0)$. That is $p^{e-1}a \neq 0$ or $p^{e-1}b \neq 0$. If $p^{e-1}a \neq 0$, then we choose $(c, d) = (0, 1)$. Similarly, if $p^{e-1}b \neq 0$, we choose $(c, d) = (1, 0)$. □

Suppose for a contradiction that $(\mathcal{O}_K/R^{2e+1})^\times \cong \mathbb{Z}_2 \times \mathbb{Z}_{3^e} \times \mathbb{Z}_{3^e}$. Let $[g]$ be a generator of $(\mathbb{Z}_{3^{e+1}})^\times$ naturally embedded in $(\mathcal{O}_K/R^{2e+1})^\times$, then the order of $[g^2]$ is p^e. By the Lemma 3.5 above, we can find $[r+s\alpha]$ of order 3^e such that $\langle [g^2] \rangle \odot \langle [r+s\alpha] \rangle$. Since $[r+s\alpha]^3 = [r^3+9\square]$, $[r+s\alpha]^{3^{e-1}} = [r^3+9\square]^{3^{e-2}} = [r^{3^{e-1}}]$. Since $[r+s\alpha]$ is of order 3^e, $[r^{3^{e-1}}]$ is of order 3. Since $[g]$ is a generators of $(\mathbb{Z}_{3^{e+1}})^\times$ embedded naturally in $(\mathcal{O}_K/R^{2e+1})^\times$, $\langle [g^2] \rangle$ will contains all coset of order 3 generated by natural numbers, specifically $[r^{3^{e-1}}]$. Thus the product $\langle [g^2] \rangle \langle [r+s\alpha] \rangle$ is not direct, which is a contradiction. Hence the structure of $(\mathcal{O}_K/R^{2e+1})^\times$ is not $\mathbb{Z}_2 \times \mathbb{Z}_{3^e} \times \mathbb{Z}_{3^e}$ either. This leaves only one possibility that is

$$(\mathcal{O}_K/R^{2e+1})^\times \cong \mathbb{Z}_2 \times \mathbb{Z}_{3^e} \times \mathbb{Z}_{3^{e-1}} \times \mathbb{Z}_3.$$

Now that we established the structure of this special case, we will find out which minimal polynomial $f(x)$ that will make this special case occurs. We already have that this special case occurs when there are $m, n \in \mathbb{Z}$ such that $\alpha^2+3m\alpha+3n \in R^e$ and $n \equiv 1 \pmod 3$. Let $f(x) = x^3 + ax^2 + 3bx + 3c$, that is $\alpha^3 = -a\alpha^2 - 3b\alpha - 3c$. For $e = 1, 2$ or 3 the structure of $(\mathcal{O}_K/R^e)^\times$ are the same as $n \equiv 1$ or $2 \pmod 3$. Thus we consider $e \geq 4$. We will use the following lemma:

Lemma 3.6. *Let $e \geq 4$ and $\alpha^2 + 3m\alpha + 3n \in R^e$. Then for any $k, l \in \mathbb{Z}$, such that $\alpha^2 + k\alpha + l \in R^e$, we have that $3 \mid l$ and $n \equiv \frac{l}{3} \pmod 3$.*

Proof. Since $\alpha^2 + 3m\alpha + 3n, \alpha^2 + k\alpha + l \in R^e$, $(3m - l)\alpha + (3n - l) \in R^e$. If e is even, $e = 2i$ for some $i \geq 2$, then from Page 23, last paragraph, $3^i, 3^i\alpha \in R^{2i}$. Suppose for contradiction that $3m - k \not\equiv 0 \pmod{3^i}$. Then $(3m - l)\alpha + (3n - l)$ can be reduced by $3^i \in R^e$ to $r\alpha + (3n - l) \in R^{2i}$ for some $0 < r < 3^i$. This makes $[r\alpha + (3n - l)] = [0]$ in $\mathcal{O}_K/R^{2i}$, which is a contradiction since we have that every coset in $\{[r + s\alpha] \mid 0 \leq r, s < 3^i\}$ are distinct. That is $r = 0$ and $3n - l \in R^{2i}$. Using the same argument we have $3^i \mid 3n - l$. Since $i \geq 2$, $9 \mid 3n - l$, then $3 \mid n - \frac{l}{3}$. If e is odd, $e = 2i+1$ for some $i \geq 2$. Also from Page 24, first paragraph, $3^{i+1}, 3^i\alpha \in R^{2i+1}$. We can show similarly to above that $n \equiv \frac{l}{3} \pmod 3$. $\square$

From the lemma we have that if we find one element $\alpha^2 + 3m\alpha + 3n \in R^e$ such that $n \equiv 2 \pmod 3$, other elements of the form $\alpha^2 + 3m'\alpha + 3n' \in R^e$ will also be such that $n' \equiv 2 \pmod 3$. Thus to show that there is no $m, n \in \mathbb{Z}$ such that $\alpha^2 + 3m\alpha + 3n \in R^e$ and $n \equiv 1$, we only need to show that there is $m, n \in \mathbb{Z}$ such that $\alpha^2 + 3m\alpha + 3n \in R^e$ and $n \equiv 2 \pmod 3$.

Let $e \geq 4$, assume $\alpha^2 + 3m\alpha + 3n \in R^e$. Then $\alpha^3 + 3m\alpha^2 + 3n\alpha \in R^{e+1}$.

$$\alpha^3 + 3m\alpha^2 + 3n\alpha = (-a\alpha^2 - 3b\alpha - 3c) + 3m\alpha^2 + 3n\alpha = (3m - a)\alpha^2 + (3n - 3b)\alpha - 3c.$$

Under inverse modulo $3^k \in R^{e+1}$, $\alpha^2 + (3m - a)^{-1}(3n - 3b)\alpha - 3c(3m - a)^{-1} \in R^{e+1}$. Under modulo 3, $-c(3m - a)^{-1} \equiv -c(-a)^{-1} \equiv ca^{-1} \pmod 3$. That is R^{e+1} will fall in the special case if and only if $a \equiv c \pmod 3$. To summarize

Theorem 3.7. *Let $e \geq 2$. If either*

1. *$p \geq 5$, or*

2. *$p = 3$ and $f(x) = x^3 + ax^2 + 3bx + 3c$ such that $a \not\equiv c \pmod 3$, then*

$$(\mathcal{O}_K/R)^\times = \mathbb{Z}_{p-1},$$

$$(\mathcal{O}_K/R^e)^\times = \mathbb{Z}_{p-1} \times \mathbb{Z}_{p^{\lfloor \frac{e-1}{2} \rfloor}} \times \mathbb{Z}_{p^{\lfloor \frac{e}{2} \rfloor}}$$

If $p = 3$ *and* $f(x) = x^3 + ax^2 + 3bx + 3c$ *such that* $a \equiv c \pmod 3$*, then*

$$(\mathcal{O}_K/R)^\times = \mathbb{Z}_2,$$

$$(\mathcal{O}_K/R^e)^\times = \mathbb{Z}_2 \times \mathbb{Z}_{3^{\lfloor \frac{e-1}{2} \rfloor}} \times \mathbb{Z}_{3^{\lfloor \frac{e-2}{2} \rfloor}} \times \mathbb{Z}_3.$$

3.5 R in the fourth category: $\langle p \rangle = R^3$

Under our assumption that the discriminant of the minimal polynomial of α is a square-free rational integer, this case does not actually occur because for $\langle p \rangle$ to be factorized to R^3, the minimal polynomial $f(x)$ has to satisfy $f(x) \equiv (x + a)^3 \pmod p$ for some $a \in \mathbb{N}$. We can shift the value of α to $\alpha - a$ without change $\mathrm{disc}(f)$ so that $f(x) \equiv x^3 \pmod p$. This makes $f(x)$ to be in the form $f(x) = x^3 + pa_2x^2 + pa_1x + pa_0$ for some $a_0, a_1, a_2 \in \mathbb{Z}$. Input in Theorem 2.11, the discriminant of f is

$$\mathrm{disc}(f) = -27p^2a_0^2 - 4p^3a_1^3 + 18p^3a_0a_1a_2 + p^4a_1^2a_2^2 - 4p^4a_0a_2^3,$$

which is divisible by p^2, thus is not square-free.

3.6 $\langle p \rangle$ stays prime

Case: $p = 2$

In order for $\langle 2 \rangle$ to stay prime, the minimal polynomial $f(x)$ of α has to remain irreducible under modulo 2. There are only two irreducible cubic polynomials modulo 2, $x^3 + x + 1$ and $x^3 + x^2 + 1$. Thus $f(x)$ is congruent modulo 2 to one of the two polynomials. That is $f(x) = x^3 - a_2x^2 - a_1x - a_0$ for some $a_0, a_1, a_2 \in \mathbb{Z}$ such that a_0 is odd and either a_1 or a_2 is odd (we turn those signs to minus to make some latter calculations less confusing, specifically because it makes $\alpha^3 =$

$a_2\alpha^2 + a_1\alpha + a_0$). We get that

$$\begin{aligned}\alpha^4 &= \alpha(a_2\alpha^2 + a_1\alpha + a_0) = a_2(a_2\alpha^2 + a_1\alpha + a_0\alpha) + a_1\alpha^2 + a_0 \\ &= (a_1 + a_2^2)\alpha^2 + (a_0 + a_1a_2)\alpha + a_0a_2.\end{aligned}$$

Now we consider a generating set of $(\mathcal{O}_K/\langle 2^e\rangle)^\times$. First, since $|(\mathcal{O}_K/\langle 2^e\rangle)^\times| = 7(8^{e-1})$, $(\mathcal{O}_K/\langle 2^e\rangle)^\times$ has an element $[h]$ of order 7. Now we consider the part with elements of order power of 2. First one, $1+2\alpha$, is the same as the second category Q when $p = 2$. We repeat the result here. For $e \geq 3$

$$(1+2\alpha)^{2^{e-1}} = 1 + 2^e\square$$

while

$$(1+2\alpha)^{2^{e-2}} = 1 + 2^{e-1}\alpha + 2^{e-1}\alpha^2 + 2^e\square.$$

Next

$$(1+2\alpha^2)^{2^{e-1}} = 1 + 2^e\square$$

while

$$\begin{aligned}(1+2\alpha^2)^{2^{e-2}} &= 1 + 2^{e-1}\alpha^2 + 2^{e-1}\alpha^4 + 2^e\square \\ &= 1 + 2^{e-1}\alpha^2 + 2^{e-1}\left((a_1 + a_2^2)\alpha^2 + (a_0 + a_1a_2)\alpha + a_0a_2\right) + 2^e\square\end{aligned}$$

Since a_0 is odd and either a_1 or a_2 is odd, $a_1 + a_2^2$ and $a_0 + a_1a_2$ are both odd, so the above expression can be reduced to

$$= 1 + 2^{e-1}a_0a_2 + 2^{e-1}\alpha + 2^e\square.$$

Now we are ready to find the structure of $(\mathcal{O}_K/\langle 2^e\rangle)^\times$. If $e = 1$, it is just a cyclic group. For $e = 2$, consider $\langle[-1]\rangle\langle[1+2\alpha]\rangle\langle[1+2\alpha^2]\rangle$ which is the product of three subgroups, each generated by an element of order 2. $[1+2\alpha] \notin \langle[-1]\rangle$ so the product of the first two subgroup is direct. Also the product of the first two subgroups only contains coset representable by an element $r + s\alpha$ for some $r, s \in \mathbb{Z}$.

This makes $[1+2\alpha^2] \notin \langle[-1]\rangle\langle[1+2\alpha]\rangle$. Together with $[h]$, an element of order 7 in $(\mathcal{O}_K/\langle 2^2\rangle)^\times$,

$$(\mathcal{O}_K/\langle 2^2\rangle)^\times = \langle[h]\rangle \odot \langle[-1]\rangle \odot \langle[1+2\alpha]\rangle \odot \langle[1+2\alpha^2]\rangle.$$

Now for $e \geq 3$, consider

$$\langle[5^{2^{e-3}}]\rangle\langle[-1]\rangle\langle[1+2^{e-1}a_0a_2+2^{e-1}\alpha]\rangle\langle[1+2^{e-1}\alpha+2^{e-1}\alpha^2]\rangle.$$

As usual we will use Theorem 2.1 to help showing that the previous product is direct. $(\mathbb{Z}_{2^e})^\times$ is embedded naturally in $(\mathcal{O}_K/\langle 2^e\rangle)^\times$. Thus since $[5]$ and $[-1]$ form a generating set of $(\mathbb{Z}_{2^e})^\times$, then $\langle[5^{2^{e-3}}]\rangle \odot \langle[-1]\rangle$ is direct. $\langle[5^{2^{e-3}}]\rangle \times \langle[-1]\rangle$ only contains cosets representable by r for some $r \in \mathbb{Z}$ thus the product of the first two subgroups does not contain $[1+2^{e-1}a_0a_2+2^{e-1}\alpha]$. This makes the product of the first three subgroups direct. Again the product of the first three subgroups only contains cosets representable by $r+s\alpha$ for some $r,s \in \mathbb{Z}$ so the full product is direct. By Theorem 2.2, the product

$$\langle[5]\rangle\langle[-1]\rangle\langle[1+2\alpha^2]\rangle\langle[1+2\alpha]\rangle$$

is also direct. It is a product of order $(2^{e-2})2(2^{e-1})2^{e-1} = 2^{3e-3}$. Combine with $[h]$, an element of order 7, we get

$$\begin{aligned}(\mathcal{O}_K/\langle 2^e\rangle)^\times &= \langle[h]\rangle \odot \langle[5]\rangle \odot \langle[-1]\rangle \odot \langle[1+2\alpha]\rangle \odot \langle[1+2\alpha^2]\rangle \\ &= \mathbb{Z}_7 \times \mathbb{Z}_{2^{e-2}} \times \mathbb{Z}_2 \times \mathbb{Z}_{2^{e-1}} \times \mathbb{Z}_{2^{e-1}}.\end{aligned}$$

To summarize

Theorem 3.8. *If the ideal $\langle 2\rangle$ stays prime, then*

$$(\mathcal{O}_K/\langle 2^e\rangle)^\times \cong \mathbb{Z}_7 \times (\mathbb{Z}_{2^e})^\times \times \mathbb{Z}_{2^{e-1}} \times \mathbb{Z}_{2^{e-1}}.$$

Case: $p \geq 3$

This category use almost the same set of generators as the case Q when $p \geq 3$ and also use the same explanation that

$$\langle [g^{p-1}] \rangle \odot \langle [1 + p\alpha] \rangle \odot \langle [1 + p\alpha^2] \rangle.$$

One different is that since $\langle p \rangle$ is a prime ideal, $(\mathcal{O}_K/\langle p \rangle)^\times$ is a cyclic group of order $p^3 - 1$ generated by $[h]$ for some $h \in \mathcal{O}_K$. It follows that $h^{p^3-1} = 1 + p\square$. Thus for $e \geq 2$,

$$h^{(p^3-1)p^{e-1}} = (1 + p\square)^{p^{e-1}} = 1 + p^e\square.$$

Since the order of h in $(\mathcal{O}_K/\langle p \rangle)^\times$ is $p^3 - 1$, $p^3 - 1$ divides the order of h in $(\mathcal{O}_K/\langle p^e \rangle)^\times$. Hence $[h^{p^{e-1}}]$ is of order $p^3 - 1$ in $(\mathcal{O}_K/\langle p^e \rangle)^\times$. Thus

$$\begin{aligned}(\mathcal{O}_K/\langle p^e \rangle)^\times &= \langle [h^{p^{e-1}}] \rangle \odot \langle [g^{p-1}] \rangle \odot \langle [1 + p\alpha] \rangle \odot \langle [1 + p\alpha^2] \rangle \\ &\cong \mathbb{Z}_{p^3-1} \times \mathbb{Z}_{p^{e-1}} \times \mathbb{Z}_{p^{e-1}} \times \mathbb{Z}_{p^{e-1}}.\end{aligned}$$

To summarize,

Theorem 3.9. *Let $p \geq 3$. If the ideal $\langle p \rangle$ stays prime, then*

$$(\mathcal{O}_K/\langle p^e \rangle)^\times \cong \mathbb{Z}_{p^3-1} \times \mathbb{Z}_{p^{e-1}} \times \mathbb{Z}_{p^{e-1}} \times \mathbb{Z}_{p^{e-1}}.$$

3.7 Examples

Consider $f(x) = x^3 + x + 1$. Since it is a monic polynomial of order 3, if $f(x)$ is not irreducible, then it has a root in $\mathbb{Z}$ dividing 1. Substituting 1 and -1 in $f(x)$ does not give 0, so $x^3 + x + 1$ is irreducible. Let α be a root of $f(x)$ and $K = \mathbb{Q}[\alpha]$. Since

$$\operatorname{disc}(x^3 + x + 1) = -4 - 27 = -31$$

which is square-free, $\mathcal{O}_K = \mathbb{Z}[\alpha]$ and $\mathrm{disc}(K)$ is also square-free. We select some prime numbers to show some factorizations of $\langle p \rangle$ by using Theorem 1.11

1. Let $p = 47$. Since $x^3 + x + 1 \equiv (x + 12)(x + 13)(x + 22) \pmod{47}$,
$$\langle 47 \rangle = \langle 47, \alpha + 12 \rangle \langle 47, \alpha + 13 \rangle \langle 47, \alpha + 22 \rangle.$$

2. Let $p = 3$. Since $x^3+x+1 \pmod 3 \equiv (x-1)(x^2+x+2) \equiv (x+2)(x^2+x+2) \pmod 3$,
$$\langle 3 \rangle = \langle 3, \alpha + 2 \rangle \langle 3, \alpha^2 + \alpha + 2 \rangle.$$

3. Let $p = 31$. Since $x^3 + x + 1 \equiv (x + 17)^2(x + 28) \pmod{31}$,
$$\langle 31 \rangle = \langle 31, \alpha + 17 \rangle^2 \langle 31, \alpha + 28 \rangle.$$

4. Let $p = 2$. Since $x^3 + x + 1 \pmod 2$ is irreducible, $\langle 2 \rangle$ is already a prime ideal.

Using previous results, we have

1. $\langle 47, \alpha + 12 \rangle, \langle 47, \alpha + 13 \rangle, \langle 47, \alpha + 22 \rangle, \langle 3, \alpha + 2 \rangle$ and $\langle 31, \alpha + 28 \rangle$ are ideals we denoted by S in Section 3.1, thus
$$(\mathcal{O}_K/\langle 47, \alpha + 12 \rangle^e)^\times \cong (\mathcal{O}_K/\langle 47, \alpha + 13 \rangle^e)^\times \cong (\mathcal{O}_K/\langle 47, \alpha + 22 \rangle^e)^\times \cong (\mathbb{Z}_{47^e})^\times,$$
$$(\mathcal{O}_K/\langle 3, \alpha + 2 \rangle^e)^\times \cong (\mathbb{Z}_{3^e})^\times,$$
and
$$(\mathcal{O}_K/\langle 31, \alpha + 28 \rangle^e)^\times \cong (\mathbb{Z}_{31^e})^\times.$$

2. $\langle 3, \alpha^2 + \alpha + 2 \rangle$ is a ideal in the second category which is denoted by Q. Thus
$$(\mathcal{O}_K/\langle 3, \alpha^2 + \alpha + 2 \rangle^e)^\times \cong \mathbb{Z}_{3^{e-1}} \times \mathbb{Z}_{3^{e-1}} \times \mathbb{Z}_8.$$

3. $\langle 31, \alpha + 17 \rangle$ is a ideal in the third category which is we denoted by R. Thus

$$(\mathcal{O}_K/\langle 31, \alpha + 17\rangle^e)^\times \cong \mathbb{Z}_{30} \times \mathbb{Z}_{31^{\lfloor \frac{e-1}{2} \rfloor}} \times \mathbb{Z}_{31^{\lfloor \frac{e}{2} \rfloor}}.$$

4. $\langle 2 \rangle$ stays prime, so it is in the fifth category. Thus

$$(\mathcal{O}_K/\langle 2\rangle^e)^\times \cong \mathbb{Z}_7 \times (\mathbb{Z}_{2^e})^\times \times \mathbb{Z}_{2^{e-1}} \times \mathbb{Z}_{2^{e-1}}.$$

REFERENCES

[1] Allan, A.A., Dunne, M.J., Jack, J.R.: Classification of the group of units in the Gaussian integers modulo n, *Pi Mu Epsilon J.*, **12**(9), 513-519 (2008).

[2] Cross, J.T.: The Euler ϕ-function in the Gaussian integers, *Amer. Math. Monthly*, **90**(8), 518-528 (Oct., 1983).

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

[4] Niven, I., Zuckerman, H.S., Montgomery, H.L.: *An Introduction to the Theory of Numbers*, 5th ed., John Wiley & Sons, Inc., New York, 1993.

[5] Ranum, A.: The Group of Classes of Congruent Quadratic Integers with Respect to a Composite Ideal Modulus, *Trans. Amer. Math. Soc.* **11**(2), 172-198 (Apr., 1910).

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

VITA

Name	Mr. Pitchayatak Ponrod
Date of Birth	31 July 1992
Place of Birth	Ratchaburi, Thailand
Education	B.Sc. (Mathematics), Chulalongkorn University, 2014
Scholarship	Scholarship from the Graduate School, Chulalongkorn University to commemorate the 72nd anniversary of his Majesty King Bhumibala Aduladeja
Conference	**Presentation** • *Primitive root in some quadratic fields* at Annual Pure and Applied Mathematics Conference : AMM&APAM 2016, 23–25 May 2016 at Chulalongkorn University