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

Ajchara Harnchoowong and Pitchayatak Ponrod


#### Abstract

Let $K=\mathbb{Q}(\alpha)$ be a cubic field where $\alpha$ is an algebraic integer such that $\operatorname{disc}_{K}(\alpha)$ is square-free. In this paper we will classify the structure of the unit group of the quotient ring $\mathcal{O}_{K} / A$ for each non-zero ideal $A$ of $\mathcal{O}_{K}$.


## 1. Introduction

An important theorem in elementary number theory, which can be found in [2], [4] and [6], is the structure of a unit group of integers modulo $n,\left(\mathbb{Z}_{n}\right)^{\times}$, i.e., $(\mathbb{Z} / n \mathbb{Z})^{\times}$. Specifically, for an odd prime $p,\left(\mathbb{Z}_{p^{e}}\right)^{\times}$is cyclic for all natural numbers $e$, while $\left(\mathbb{Z}_{2}\right)^{\times}=\{1\},\left(\mathbb{Z}_{4}\right)^{\times}=\langle-1\rangle$ and $\left(\mathbb{Z}_{2^{e}}\right)^{\times}=\langle-1\rangle \times\langle 5\rangle$ for all natural numbers $e \geq 3$. In fact, this theorem is usually stated in terms of primitive roots. Together with the Chinese remainder theorem, we can get the structure of $\left(\mathbb{Z}_{n}\right)^{\times}$for any natural number $n$. Let $K$ be a number field, $\mathcal{O}_{K}$ be the ring of integers of $K$ and $A$ be a non-zero ideal of $\mathcal{O}_{K}$, we will study the structure of $\left(\mathcal{O}_{K} / A\right)^{\times}$. In 1910, A. Ranum [7] studied this problem in all number fields of degree 2. Later, J. T. Cross [3] in 1983 and A. A. Allan et al. [1] in 2008, apparently unaware of Ranum's work, studied this problem in the field of Gaussian numbers, which is a number field of degree 2.

In this paper we will study this problem when $K=\mathbb{Q}(\alpha)$ where $\alpha$ is a root of some monic polynomial of degree 3 in $\mathbb{Z}[x]$ which is irreducible over $\mathbb{Q}$ and $\operatorname{disc}_{K}(\alpha)$ is square-free. This implies that $\mathcal{O}_{K}=\mathbb{Z}[\alpha]$. In general, the ring of integers of a number field does not always has a nice simple form like $\mathbb{Z}[\alpha]$. One of the famous examples is $L=\mathbb{Q}(\beta)$ where $\beta$ is a root of $x^{3}-x^{2}-2 x-8$. Its ring of integers is not $\mathbb{Z}[\gamma]$ for any $\gamma \in \mathcal{O}_{L}$. In fact, its ring of integers is $\mathbb{Z}+\beta \mathbb{Z}+\left(\frac{\beta+\beta^{2}}{2}\right) \mathbb{Z}$.

[^0]Notations and properties in algebraic number theory can be found in [5] and [8].

When $\mathcal{O}_{K}=\mathbb{Z}[\alpha]$ for a number field $K$, we can use the following theorem to find all prime ideals of $\mathcal{O}_{K}$.

Theorem 1.1 ([8]). 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 $\bar{f}(x)$ be the polynomial obtained from $f$ by reducing all coefficients of $f$ modulo $p$.

Suppose that $\bar{f}(x)=\bar{f}_{1}^{e_{1}}(x) \cdots \bar{f}_{g}^{e_{g}}(x)$ is the factorization of $\bar{f}(x)$ in $\mathbb{Z}_{p}[x]$. Then

$$
\langle p\rangle=P_{1}^{e_{1}} \cdots P_{g}^{e_{g}}
$$

is the prime factorization such that $P_{i}=\left\langle p, f_{i}(\alpha)\right\rangle$ where $f_{i}(x)$ is a monic polynomial in $\mathbb{Z}[x]$ whose reduction modulo $p$ is $\bar{f}_{i}(x), \operatorname{deg} f_{i}(x)=\operatorname{deg} \bar{f}_{i}(x)$, and $\mathrm{N}\left(P_{i}\right)=p^{\operatorname{deg} f_{i}}$.

We can use some properties of the discriminant of polynomials to prove the following theorem:

Theorem 1.2. Let $x^{3}+a x^{2}+b x+c \in \mathbb{Q}[x]$ be an irreducible polynomial. Then

$$
\operatorname{disc}\left(x^{3}+a x^{2}+b x+c\right)=a^{2} b^{2}-4 b^{3}-4 a^{3} c-27 c^{2}+18 a b c
$$

## 2. Notations and lemmas

To simplify proofs, we use a square $\square$ to denote a non-specific element of $\mathcal{O}_{K}$. For example

$$
\left(1+2 p+3 p^{2}\right)(2+5 p \alpha)=2+p\left(4+5 \alpha+6 p+10 p \alpha+15 p^{2} \alpha\right)=2+p \square .
$$

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

Definition. For subgroups $H_{1}$ and $H_{2}$ of an abelian group $G$, if the product $H_{1} H_{2}$ is an (internal) direct product, i.e., $H_{1} \cap H_{2}=\{1\}$, then we will write $H_{1} \odot H_{2}$ for the direct product of $H_{1}$ and $H_{2}$.

We have two results about a direct product.
Lemma 2.1. Let $G$ be an abelian group, $H$ a subgroup of $G$ and $g \in G$ an element of order $p$ for some prime number $p$. If $g \notin H$, then $H \odot\langle g\rangle$.

Lemma 2.2. Let $G$ be a finite abelian group, $H$ a subgroup of $G$ and $g \in G$ of order $p^{e}$ for some prime number $p$ and natural number $e \geq 2$. If $H \odot\left\langle g^{p}\right\rangle$, then $H \odot\langle g\rangle$.

The following two lemmas will be used very often. The first is a generalization of Euler's $\phi$ function to number fields.

Lemma 2.3. Let $K$ be a number field, $P$ be a prime ideal of $\mathcal{O}_{K}$ and $e \in \mathbb{N}$. Then

$$
\left|\left(\mathcal{O}_{K} / P^{e}\right)^{\times}\right|=(\mathrm{N}(P)-1) \mathrm{N}(P)^{e-1}
$$

Proof. We have that $\mathcal{O}_{K} / P^{e}$ is a local ring with the unique maximal ideal $P / P^{e}$. Since in a local ring, an element is a unit if and only if it is not in the maximal ideal, we have that

$$
\left(\mathcal{O}_{K} / P^{e}\right)^{\times}=\mathcal{O}_{K} / P^{e} \backslash P / P^{e} .
$$

By the third isomorphism theorem for rings, $\frac{\mathcal{O}_{K} / P^{e}}{P / P^{e}} \cong \mathcal{O}_{K} / P$, so $\left|P / P^{e}\right|=$ $\mathrm{N}(P)^{e-1}$. Thus

$$
\left|\left(\mathcal{O}_{K} / P^{e}\right)^{\times}\right|=\left|\mathcal{O}_{K} / P^{e}\right|-\left|P / P^{e}\right|=\mathrm{N}(P)^{e}-\mathrm{N}(P)^{e-1}=(\mathrm{N}(P)-1) \mathrm{N}(P)^{e-1}
$$

Lemma 2.4. Let $K$ be a number field, $\beta \in \mathcal{O}_{K}, a \in \mathbb{N}, r, s \in \mathbb{Z}$ and $p$ be $a$ prime number. If $p \geq 3$, then

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

and if also $r$ is odd, then

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

We will see that $\left(\mathcal{O}_{K} / A\right)^{\times}$contains an isomorphic image of $\left(\mathbb{Z}_{n}\right)^{\times}$for some $n \in \mathbb{N}$, so we can use the structure of $\left(\mathbb{Z}_{n}\right)^{\times}$to find the structure of $\left(\mathcal{O}_{K} / A\right)^{\times}$.
Lemma 2.5. Let $K$ be a number field and $A$ be an non-zero ideal of $\mathcal{O}_{K}$. If $n$ is the least natural number in $A$, then there is the natural embedding

$$
\left(\mathbb{Z}_{n}\right)^{\times} \hookrightarrow\left(\mathcal{O}_{K} / A\right)^{\times} .
$$

Proof. Consider the natural homomorphism $\mathbb{Z} \rightarrow \mathcal{O}_{K} / A$ sending $a \mapsto[a]$ where [a] denotes the coset $a+A$ in $\mathcal{O}_{K} / A$. The kernel of this homomorphism is $\mathbb{Z} \cap A$ which is an ideal of $\mathbb{Z}$. Thus $\mathbb{Z} \cap A=n \mathbb{Z}$ where $n$ is the least natural number in $A$. Then by the first isomorphism theorem, $\mathbb{Z}_{n}=\mathbb{Z} / n \mathbb{Z} \hookrightarrow \mathcal{O}_{K} / A$. Consequently, $\left(\mathbb{Z}_{n}\right)^{\times}=(\mathbb{Z} / n \mathbb{Z})^{\times} \hookrightarrow\left(\mathcal{O}_{K} / A\right)^{\times}$.

One more thing that we will use throughout this paper is the following lemma:

Lemma 2.6. Let $K$ be a number field. If $[h]$ is of order $k$ in $\left(\mathcal{O}_{K} /\langle p\rangle\right)^{\times}$with $p \nmid k$, then $\left[h^{p^{e}}\right]$ is of order $k$ in $\left(\mathcal{O}_{K} /\left\langle p^{e}\right\rangle\right)^{\times}$.

Proof. Assume [ $h$ ] is of order $k$ in $\left(\mathcal{O}_{K} /\langle p\rangle\right)^{\times}$and $\left[h^{p^{e}}\right]$ is of order $l$ in $\left(\mathcal{O}_{K} /\left\langle p^{e}\right\rangle\right)^{\times}$. Then $h^{k}=1+p \square$ which implies that $h^{p^{e} k}=1+p^{e} \square$, so $l \mid k$. Also from $h^{p^{e} l}=1+p^{e} \square=1+p \square$, we have that $k \mid p^{e} l$. But $p$ is a prime number and $p \nmid k$, so $k \mid l$. Hence $k=l$.

From now on, let $K=\mathbb{Q}(\alpha)$ be a cubic field where $\alpha \in \mathcal{O}_{K}$ and $\operatorname{disc}_{K}(\alpha)$ is square-free. Let $f(x) \in \mathbb{Z}[x]$ be the minimal polynomial of $\alpha$. We will apply Theorem 1.1 to consider all possible factorizations of $f(x)(\bmod p)$. There are 5 possibilities:
(1) $f(x) \equiv(x+a)(x+b)(x+c)(\bmod p)$ for some $a, b, c \in \mathbb{Z}$ that are non-congruent modulo $p$.
(2) $f(x) \equiv\left(x^{2}+a_{1} x+a_{0}\right)(x+b)(\bmod p)$ for some polynomial $x^{2}+a_{1} x+$ $a_{0} \in \mathbb{Z}[x]$ which is irreducible $\bmod p$ and $b \in \mathbb{Z}$.
(3) $f(x) \equiv(x+a)^{2}(x+b)(\bmod p)$ for some $a, b \in \mathbb{Z}$ that are non-congruent modulo $p$.
(4) $f(x) \equiv(x+a)^{3}(\bmod p)$ for some $a \in \mathbb{Z}$.
(5) $f(x)(\bmod p)$ is irreducible.

By Theorem 1.1, each factorization of $f(x)$ corresponds respectively to the following 5 categories of factorizations of $\langle p\rangle$ in $\mathcal{O}_{K}$.
(1) $\langle p\rangle=S_{1} S_{2} S_{3}$,
(2) $\langle p\rangle=Q S$,
(3) $\langle p\rangle=R^{2} S$,
(4) $\langle p\rangle=R^{3}$,
(5) $\langle p\rangle$ stays prime,
where prime ideals in the factorization in each category are distinct. Ideals denoted by $S$ with or without a suffix are of norm $p, \mathrm{~N}(R)=p$ and $\mathrm{N}(Q)=p^{2}$.

## 3. $S_{1}, S_{2}, S_{3}$ and $S$ in the first, second, and third categories

This is the easiest case of ideals. Since $S_{1}, S_{2}$ and $S_{3}$ have the same properties as $S$, i.e., each has norm $p$ and ramification index one, we will also call them $S$. We will show that $\mathcal{O}_{K} / S^{e} \cong \mathbb{Z}_{p^{e}}$. We know that $\left|\mathcal{O}_{K} / S^{e}\right|=p^{e}$ so it suffices to show that $p^{e-1} \notin S^{e}$. Suppose that $p^{e-1} \in S^{e}$, i.e., $S^{e} \mid\left\langle p^{e-1}\right\rangle$. From the categorization above, the largest power of $S$ dividing $\left\langle p^{e-1}\right\rangle$ is $e-1$ which is a contradiction. So we have proved the following theorem.

Theorem 3.1. If $\mathrm{N}(S)=p$ and $S^{2} \nmid\langle p\rangle$, then $\left(\mathcal{O}_{K} / S^{e}\right)^{\times} \cong\left(\mathbb{Z}_{p^{e}}\right)^{\times}$.

## 4. $Q$ in the second category: $\langle p\rangle=Q S$

## 4.1. $p=2$

In this category $f(x)$ modulo 2 has to be factored into a product of two irreducible polynomials modulo 2, a linear and an irreducible quadratic polynomial modulo 2 . Since there is only one irreducible quadratic polynomial modulo 2 ,

$$
f(x) \equiv\left(x+a_{0}\right)\left(x^{2}+x+1\right) \quad(\bmod 2)
$$

for some $a_{0} \in \mathbb{Z}$. We can simplify the proof by shifting the value of $\alpha$ so that $\alpha$ is a root of a monic irreducible polynomial $f(x)$ such that

$$
f(x) \equiv x\left(\left(x-a_{0}\right)^{2}+\left(x-a_{0}\right)+1\right) \equiv x\left(x^{2}+x+1\right) \quad(\bmod 2)
$$

So $f(x)=x^{3}+c_{2} x^{2}+c_{1} x+2 c_{0}$ for some integer $c_{0}$ and odd integers $c_{1}$ and $c_{2}$. Now from $f(x) \equiv x\left(x^{2}+x+1\right)(\bmod 2)$, the principle ideal $\langle 2\rangle$ can be factorized into prime ideals as follows:

$$
\langle 2\rangle=\langle 2, \alpha\rangle\left\langle 2, \alpha^{2}+\alpha+1\right\rangle .
$$

That is $Q=\left\langle 2, \alpha^{2}+\alpha+1\right\rangle$. Thus $2^{e}$ and $\left(\alpha^{2}+\alpha+1\right)^{e}$ are in $Q^{e}$. Using the facts that $\alpha^{3}+c_{2} \alpha^{2}+c_{1} \alpha+2 c_{0}=0$ and $c_{1}, c_{2}$ being odd, it can be shown by induction that $\left(\alpha^{2}+\alpha+1\right)^{e}=r \alpha^{2}+s \alpha+t$ such that $2 \nmid r, s, t$. Also $2^{e} \in Q^{e}$, thus we have that $\alpha^{2}-d_{1} \alpha-d_{0} \in Q^{e}$ for some odd integers $d_{0}$ and $d_{1}$. This means that in $\mathcal{O}_{K} / Q^{e},\left[\alpha^{2}\right]=\left[d_{1} \alpha+d_{0}\right]$. Together with the fact that $\left|\mathcal{O}_{K} / Q^{e}\right|=2^{2 e}$, we have that elements in $\mathcal{O}_{K} / Q^{e}$ can be represented uniquely in the form $[r+s \alpha]$ where $0 \leq r, s<2^{e}$, i.e.,

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

Now we consider the structure of $\left(\mathcal{O}_{K} / Q^{e}\right)^{\times}$. By Lemma 2.3, the order of $\left(\mathcal{O}_{K} / Q^{e}\right)^{\times}$is $3\left(2^{2 e-2}\right)$, so it has an element of order 3, denoted by [h]. For $e \geq 3,(1+2 \alpha)^{2^{e-1}}=1+2^{e} \square$, while

$$
\begin{aligned}
(1+2 \alpha)^{2^{e-2}} & =1+2^{e-1} \alpha+2^{e-1} \alpha^{2}+2^{e} \square \\
& =1+2^{e-1}\left(\alpha+d_{1} \alpha+d_{0}\right)+2^{e} \square=1+2^{e-1}+2^{e} \square .
\end{aligned}
$$

Thus the order of $[1+2 \alpha]$ is $2^{e-1}$ and $\left[(1+2 \alpha)^{2^{e-2}}\right]=\left[1+2^{e-1}\right]$ 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 for $e \geq 3$, since

$$
(1+4 \alpha)^{2^{e-2}}=1+2^{e-2}(4 \alpha)+\binom{2^{e-2}}{2}(4 \alpha)^{2}+2^{e} \square=1+2^{e} \square
$$

while

$$
(1+4 \alpha)^{2^{e-3}}=1+2^{e-3}(4 \alpha)+2^{e} \square=1+2^{e-1} \alpha+2^{e} \square,
$$

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

$$
\left(\mathcal{O}_{K} / Q\right)^{\times}=\langle[h]\rangle \cong \mathbb{Z}_{3} \cong\left(\mathbb{Z}_{2}\right)^{\times} \times \mathbb{Z}_{3} .
$$

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

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

Since $[1+2 \alpha] \notin\langle[-1]\rangle,\langle[-1]\rangle \odot\langle[1+2 \alpha]\rangle$. Since the order of $\left(\mathcal{O}_{K} / Q^{2}\right)^{\times}$is $3\left(2^{2}\right)$, then together with $[h]$, an element of order 3, we then have that

$$
\left(\mathcal{O}_{K} / Q^{2}\right)^{\times}=\langle[-1]\rangle \odot\langle[1+2 \alpha]\rangle \odot\langle[h]\rangle \cong \mathbb{Z}_{2} \times \mathbb{Z}_{2} \times \mathbb{Z}_{3} \cong\left(\mathbb{Z}_{2^{2}}\right)^{\times} \times \mathbb{Z}_{2} \times \mathbb{Z}_{3}
$$

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

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

Since $e \geq 3,\left[1+2^{e-1}\right] \notin\langle[-1]\rangle$, so by Lemma 2.1, we have that $\langle[-1]\rangle \odot$ $\left\langle\left[1+2^{e-1}\right]\right\rangle$. The previous direct product contains only cosets representable by integers, so $\left[1+2^{e-1} \alpha\right] \notin\langle[-1]\rangle \odot\left\langle\left[1+2^{e-1}\right]\right\rangle$. Thus

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

Since $\left[(1+2 \alpha)^{2^{e-2}}\right]=\left[1+2^{e-1}\right]$ and $\left[(1+4 \alpha)^{2^{e-3}}\right]=\left[1+2^{e-1} \alpha\right]$,

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

By Lemma 2.2, we then have that

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

It is a direct product of order $(2)\left(2^{e-1}\right)\left(2^{e-2}\right)=2^{2 e-2}$. Since the order of $\left(\mathcal{O}_{K} / Q^{e}\right)^{\times}$is $3\left(2^{2 e-2}\right)$, together with the element $[h]$ of order 3 , we have that

$$
\begin{aligned}
\left(\mathcal{O}_{K} / Q^{e}\right)^{\times} & =\langle[-1]\rangle \odot\langle[1+4 \alpha]\rangle \odot\langle[1+2 \alpha]\rangle \odot\langle[h]\rangle \\
& \cong \mathbb{Z}_{2} \times \mathbb{Z}_{2^{e-2}} \times \mathbb{Z}_{2^{e-1}} \times \mathbb{Z}_{3} \\
& \cong\left(\mathbb{Z}_{2^{e}}\right)^{\times} \times \mathbb{Z}_{2^{e-1}} \times \mathbb{Z}_{3} .
\end{aligned}
$$

To summarize:
Theorem 4.1. If $Q$ is a prime ideal lying over 2 of norm 4, then

$$
\left(\mathcal{O}_{K} / Q^{e}\right)^{\times} \cong\left(\mathbb{Z}_{2^{e}}\right)^{\times} \times \mathbb{Z}_{2^{e-1}} \times \mathbb{Z}_{3}
$$

## 4.2. $p \geq 3$

We find that it is easier to consider $\left(\mathcal{O}_{K} / S^{e} Q^{e}\right)^{\times}=\left(\mathcal{O}_{K} /\left\langle p^{e}\right\rangle\right)^{\times}$instead of just $\left(\mathcal{O}_{K} / Q^{e}\right)^{\times}$and use the isomorphism $\left(\mathcal{O}_{K} / S^{e} Q^{e}\right)^{\times} \cong\left(\mathcal{O}_{K} / S^{e}\right)^{\times} \times$ $\left(\mathcal{O}_{K} / Q^{e}\right)^{\times}$to get the structure of $\left(\mathcal{O}_{K} / Q^{e}\right)^{\times}$. We have that elements of $\mathcal{O}_{K} /\left\langle p^{e}\right\rangle$ can be uniquely represented by $\left[r+s \alpha+t \alpha^{2}\right]$ where $0 \leq r, s, t<p^{e}$, i.e.,

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

Since $\left(\mathcal{O}_{K} / Q\right)^{\times}$is the unit group of the field $\mathcal{O}_{K} / Q$, it is a cyclic group of order $p^{2}-1$. Since $\left(\mathcal{O}_{K} / Q\right)^{\times}$can be embedded into $\left(\mathcal{O}_{K} /\langle p\rangle\right)^{\times},\left(\mathcal{O}_{K} /\langle p\rangle\right)^{\times}$ has an element $[h]$ of order $p^{2}-1$. By Lemma 2.6, $\left[h^{p^{e}}\right]$ is of order $p^{2}-$ 1 in $\left(\mathcal{O}_{K} /\left\langle p^{e}\right\rangle\right)^{\times}$. 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 $\left(1+p \alpha^{2}\right)^{p^{e-1}}=1+p^{e} \square$, while $\left(1+p \alpha^{2}\right)^{p^{e-2}}=1+p^{e-1} \alpha^{2}+p^{e} \square$. Hence the orders of $[1+p \alpha]$ and $\left[1+p \alpha^{2}\right]$ are both $p^{e-1}$. Also $\left[(1+p \alpha)^{p^{e-2}}\right]=\left[1+p^{e-1}\right]$ and $\left[\left(1+p \alpha^{2}\right)^{p^{e-2}}\right]=\left[1+p^{e-1} \alpha^{2}\right]$.

Let $[g]$ be a generator of $\left(\mathbb{Z}_{p^{e}}\right)^{\times}$embedded naturally in $\left(\mathcal{O}_{K} /\left\langle p^{e}\right\rangle\right)^{\times}$. Consider the product

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

Since the first subgroup contains only cosets representable by natural numbers, $\left[1+p^{e-1} \alpha\right] \notin\langle[g]\rangle$, so the product of the first two subgroups is direct. Since $\left(1+p^{e-1} \alpha\right)^{l}=1+l p^{e-1} \alpha+p^{e} \square$ for any natural number $l$, the product of
the first two subgroups contains only cosets representable by an element of the form $r+s \alpha$. Hence $\left[1+p^{e-1} \alpha^{2}\right] \notin\langle[g]\rangle\left\langle\left[1+p^{e-1} \alpha\right]\right.$ and from this we have

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

Since $\left[(1+p \alpha)^{p^{e-2}}\right]=\left[1+p^{e-1} \alpha\right]$ and $\left[\left(1+p \alpha^{2}\right)^{p^{e-2}}\right]=\left[1+p^{e-1} \alpha^{2}\right]$, we have that the above product is equal to

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

By Lemma 2.2, we have that

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

and the order is $(p-1) p^{e-1} p^{e-1} p^{e-1}=(p-1) p^{3 e-3}$. Since the order of $\left(\mathcal{O}_{K} /\left\langle p^{e}\right\rangle\right)^{\times}$is $(p-1)\left(p^{2}-1\right) p^{3 e-3}$, then together with the fact that the order of $\left[h^{p^{e}}\right]$ in $\left(\mathcal{O}_{K} /\left\langle p^{e}\right\rangle\right)^{\times}$is $p^{2}-1$, we have that

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

Since $\left(\mathcal{O}_{K} /\left\langle p^{e}\right\rangle\right)^{\times} \cong\left(\mathcal{O}_{K} / S^{e}\right)^{\times} \times\left(\mathcal{O}_{K} / Q^{e}\right)^{\times} \cong \mathbb{Z}_{p-1} \times \mathbb{Z}_{p^{e-1}} \times\left(\mathcal{O}_{K} / Q^{e}\right)^{\times}$,

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

To summarize:
Theorem 4.2. Let $Q$ be a prime ideal lying over $p \geq 3$ of norm $p^{2}$. Then

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

## 5. $R$ in the third category: $\langle p\rangle=R^{2} S$

To fall in this category, the minimal polynomial $f(x)$ of $\alpha$ will be congruent to $\left(x+a_{0}\right)\left(x+a_{1}\right)^{2}(\bmod p)$ for some $a_{0}, a_{1} \in \mathbb{N}$ such that $a_{0} \not \equiv a_{1}(\bmod p)$. We can shift the value of $\alpha$ to make $f(x) \equiv\left(x+b_{0}\right) x^{2}(\bmod p)$ for some $b_{0} \in \mathbb{N}$ such that $p \nmid b_{0}$ and so

$$
\langle p\rangle=\left\langle p, \alpha+b_{0}\right\rangle\langle p, \alpha\rangle^{2} .
$$

Since $f(x) \equiv x^{3}+b_{0} x^{2}(\bmod p), f(x)=x^{3}+a_{2} x^{2}+p a_{1} x+p a_{0}$ for some $a_{0}, a_{1}, a_{2} \in \mathbb{Z}$ such that $p \nmid a_{2}$ and $a_{2} \equiv b_{0}(\bmod p)$. By Theorem 1.2

$$
\operatorname{disc}(f)=-4 a_{1}^{3} p^{3}+\left(-27 a_{0}^{2}+18 a_{1} a_{2} a_{0}+a_{1}^{2} a_{2}^{2}\right) p^{2}-4 a_{0} a_{2}^{3} p
$$

which is not square-free if $p \mid a_{0}$ or $p=2$. Thus $p \neq 2$ and $p \nmid a_{0}$. Next we consider a representation set of $\mathcal{O}_{K} / R^{e}$. The following lemma can be easily proved by induction.

Lemma 5.1. For all $e \geq 1$, there exist $c_{0}, c_{1} \in \mathbb{Z}$ such that $\alpha^{2}+p c_{1} \alpha+p c_{0} \in R^{e}$ and $p \nmid c_{0}$.

Now we can choose representations of cosets in $\left(\mathcal{O}_{K} / R^{e}\right)^{\times}$. 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 $\left(\mathcal{O}_{K} / R^{e}\right)^{\times}$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 $2 e$ for some $e \geq 1$. Since $\left\langle p^{e}\right\rangle=$ $R^{2 e} S^{e} \subseteq R^{2 e}, p^{e}, p^{e} \alpha \in R^{2 e}$. Since $\left|\mathcal{O}_{K} / R^{2 e}\right|=\mathrm{N}\left(R^{2 e}\right)=p^{2 e}$, each element of $\mathcal{O}_{K} / R^{2 e}$ can be represented uniquely by $[r+s \alpha]$ where $0 \leq r, s<p^{e}$, i.e.,

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

Similarly for an odd exponent, say it is $2 e+1$ for some $e \geq 0$. Since $R^{2 e+1} \supseteq$ $R^{2 e+1} S^{e}=\left\langle p^{e}\right\rangle\langle p, \alpha\rangle=\left\langle p^{e+1}, p^{e} \alpha\right\rangle, p^{e+1}, p^{e} \alpha \in R^{2 e+1}$. Since $\left|\mathcal{O}_{K} / R^{2 e+1}\right|=$ $\mathrm{N}\left(R^{2 e+1}\right)=p^{2 e+1}$, each element of $\mathcal{O}_{K} / R^{2 e+1}$ can be represented uniquely by $[r+s \alpha]$ where $0 \leq r<p^{e+1}$ and $0 \leq s<p^{e}$, i.e.,

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

Next we consider structures of $\left(\mathcal{O}_{K} / R^{2 e}\right)^{\times}$and $\left(\mathcal{O}_{K} / R^{2 e+1}\right)^{\times}$. First, $\left(\mathcal{O}_{K} / R\right)^{\times}$ is a cyclic group of order $p-1$. Since $\mathcal{O}_{K} / R^{2}=\{[r+s \alpha] \mid 0 \leq r, s<p\}$ has a subgroup isomorphic to $\mathbb{Z}_{p},\left(\mathcal{O}_{K} / R^{2}\right)^{\times}$has a subgroup isomorphic to $\mathbb{Z}_{p-1}$. By Lemma 2.3, $\left|\left(\mathcal{O}_{K} / R^{2}\right)^{\times}\right|=(p-1) p$, so

$$
\left(\mathcal{O}_{K} / R^{2}\right)^{\times} \cong \mathbb{Z}_{p-1} \times \mathbb{Z}_{p}
$$

Similarly $\mathcal{O}_{K} / R^{3}=\left\{[r+s \alpha] \mid 0 \leq r<p^{2}, 0 \leq s<p\right\}$, which has a subgroup isomorphic to $\mathbb{Z}_{p^{2}}$. Since $\left(\mathbb{Z}_{p^{2}}\right)^{\times} \cong \mathbb{Z}_{p(p-1)},\left(\mathcal{O}_{K} / R^{3}\right)^{\times}$has a subgroup isomorphic to $\mathbb{Z}_{p(p-1)}$. By Lemma 5.1, $\left[\alpha^{2}\right]=\left[-p a_{1} \alpha-p a_{0}\right]=[p \square]$. Thus for $p \geq 3$, $\left[\alpha^{p}\right]=\left[\alpha^{2}(\alpha) \alpha^{p-3}\right]=[p \alpha \square]$. Thus for any $[r+s \alpha] \in\left(\mathcal{O}_{K} / R^{3}\right)^{\times}$,

$$
[r+s \alpha]^{p}=\left[r^{p}+p r^{p-1} s \alpha+\cdots+\operatorname{pr}(s \alpha)^{p-1}+\alpha^{p}\right]=\left[r^{p}+p \alpha \square\right]=\left[r^{p}\right]
$$

Since the order of $\left[r^{p}\right]$ in $\left(\mathcal{O}_{K} / R^{3}\right)^{\times}$is at most $p-1$, the order of any element of $\left(\mathcal{O}_{K} / R^{3}\right)^{\times}$is at most $p(p-1)$, so

$$
\left(\mathcal{O}_{K} / R^{3}\right)^{\times} \cong \mathbb{Z}_{p-1} \times \mathbb{Z}_{p} \times \mathbb{Z}_{p}
$$

Now we consider structures of $\left(\mathcal{O}_{K} / R^{2 e}\right)^{\times}$and $\left(\mathcal{O}_{K} / R^{2 e+1}\right)^{\times}$for $e \geq 2$. For $p \geq 5$,

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

From Lemma 5.1, we know that $\left[\alpha^{2}\right]=\left[p a_{1} \alpha+p a_{0}\right]=[p \square]$ and for any $k \geq 2$, $\left[p \alpha^{k}\right]=\left[p^{2} \alpha^{k-2} \square\right]=\left[p^{2} \square\right]$. Hence $\left[\alpha^{p}\right]=\left[\alpha^{2}\right]\left[\alpha^{2}\right]\left[\alpha^{p-4}\right]=[p \square][p \square][\square]=$ $\left[p^{2} \square\right]$. Thus from the expansion of $\left[(1+\alpha)^{p}\right]$, the third term onward can be combined into $p^{2} \square$, i.e.,

$$
\left[(1+\alpha)^{p}\right]=\left[1+p \alpha+p^{2} \square\right]
$$

We will see later that if $p=3$, then $[1+\alpha]^{3}$ may not always be $\left[1+3 \alpha+3^{2} \square\right]$. From Lemma 5.1, $\alpha^{2}+3 m \alpha+3 n \in R^{e}$ for some $m, n \in \mathbb{Z}$ where $3 \nmid n$, i.e., $\left[\alpha^{2}\right]=[-3 m \alpha-3 n]$. Thus $\left[\alpha^{3}\right]=\left[-3 m \alpha^{2}-3 n \alpha\right]=[-3 m(-3 m \alpha-3 n)-3 n \alpha]=$ $\left[\left(9 m^{2}-3 n\right) \alpha+9 m n\right]=[-3 n \alpha+9 \square]$, and so

$$
\left[(r+s \alpha)^{3}\right]=\left[r^{3}+3 r^{2} s \alpha+3 r s^{2} \alpha^{2}+s^{3} \alpha^{3}\right]
$$

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

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

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

while

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

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

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

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

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

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

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

is a subgroup of $\left(\mathcal{O}_{K} / R^{2 e}\right)^{\times}$of order $p^{2 e-1}(p-1)$ which is equal to the order of $\left(\mathcal{O}_{K} / R^{2 e}\right)^{\times}$. For $\left(\mathcal{O}_{K} / R^{2 e+1}\right)^{\times}$, let $[g]$ be a generator of $\left(\mathbb{Z}_{p^{e+1}}\right)^{\times}$embedded in $\left(\mathcal{O}_{K} / R^{2 e+1}\right)^{\times}$. We can prove similarly that $\left(\mathcal{O}_{K} / R^{2 e+1}\right)^{\times}=\langle[g]\rangle \odot\langle[r+s \alpha]\rangle$.

Thus for $p=3$,

$$
\begin{gathered}
\left(\mathcal{O}_{K} / R^{2 e}\right)^{\times}=\langle[g]\rangle \odot\langle[1+2 \alpha]\rangle \\
\left(\mathcal{O}_{K} / R^{2 e+1}\right)^{\times}=\langle[g]\rangle \odot\langle[1+2 \alpha]\rangle
\end{gathered}
$$

and for $p \geq 5$,

$$
\begin{gathered}
\left(\mathcal{O}_{K} / R^{2 e}\right)^{\times}=\langle[g]\rangle \odot\langle[1+\alpha]\rangle \\
\left(\mathcal{O}_{K} / R^{2 e+1}\right)^{\times}=\langle[g]\rangle \odot\langle[1+\alpha]\rangle .
\end{gathered}
$$

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

$$
\left[(r+s \alpha)^{3}\right]=\left[r^{3}+3\left(r^{2} s-n s^{3}\right) \alpha+9 \square\right]
$$

(1) If $3 \mid r$, then

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

Since $3^{e} \in R^{e},[3 \square]$ is a zero-divisor in $\mathcal{O}_{K} / R^{e}$, then $[r+s \alpha]$ is also a zero-divisor $\mathcal{O}_{K} / R^{e}$, i.e., $[r+s \alpha] \notin\left(\mathcal{O}_{K} / R^{e}\right)^{\times}$, so we do not have to consider this case.
(2) If $3 \nmid r$ and $3 \mid s$, then

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

(3) If $3 \nmid r$ and $3 \nmid s$, then

$$
r^{2} s-n s^{3} \equiv r^{2} s-s^{3} \equiv r^{2} s-s \equiv s\left(r^{2}-1\right) \equiv s(1-1) \equiv 0 \quad(\bmod 3)
$$

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

$$
\left[(r+s \alpha)^{3}\right]=\left[r^{3}+3\left(r^{2} s-n s^{3}\right) \alpha+9 \square\right]=\left[r^{3}+9 \square\right]
$$

By Lemma 2.3 and the fact that $\mathrm{N}(R)=3$, we have that

$$
\left|\left(\mathcal{O}_{K} / R^{2 e}\right)^{\times}\right|=(3-1) 3^{2 e-1}=2\left(3^{2 e-1}\right)
$$

and

$$
\left|\left(\mathcal{O}_{K} / R^{2 e+1}\right)^{\times}\right|=(3-1) 3^{2 e}=2\left(3^{2 e}\right)
$$

Since $(1+3 \alpha)^{3^{e-1}}=1+3^{e} \square$, while $(1+3 \alpha)^{3^{e-2}}=1+3^{e-1} \alpha+3^{e} \square$, the order of $1+3 \alpha$ in $\left(\mathcal{O}_{K} / R^{2 e}\right)^{\times}$is $3^{e-1}$ and $\left[(1+3 \alpha)^{3^{e-2}}\right]=\left[1+3^{e-1} \alpha\right]$. Let $[g]$ be a generator of $\left(\mathbb{Z}_{3^{e}}\right)^{\times}$embedded naturally in $\left(\mathcal{O}_{K} / R^{2 e}\right)^{\times}$, so $[g]$ is of order $2\left(3^{e-1}\right)$. Since $\left[1+3^{e-1} \alpha\right] \notin\langle[g]\rangle$, by Lemma 2.1,

$$
\langle[g]\rangle \odot\left\langle\left[1+3^{e-1} \alpha\right]\right\rangle .
$$

Since $\left[1+3^{e-1} \alpha\right]=\left[(1+3 \alpha)^{3^{e-2}}\right]$ in $\left(\mathcal{O}_{K} / R^{2 e}\right)^{\times}$, by Lemma 2.2 we have

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

and its order is $2\left(3^{2 e-2}\right)$. This means that $\langle[g]\rangle \odot\langle[1+3 \alpha]\rangle$ is a subgroup of index 3 in $\left(\mathcal{O}_{K} / R^{2 e}\right)^{\times}$. 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 $\left(\mathcal{O}_{K} / R^{2 e}\right)^{\times}$is either

$$
\mathbb{Z}_{2} \times \mathbb{Z}_{3^{e}} \times \mathbb{Z}_{3^{e-1}} \quad \text { or } \quad \mathbb{Z}_{2} \times \mathbb{Z}_{3^{e-1}} \times \mathbb{Z}_{3^{e-1}} \times \mathbb{Z}_{3}
$$

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

$$
\left(\mathcal{O}_{K} / R^{2 e}\right)^{\times} \cong \mathbb{Z}_{2} \times \mathbb{Z}_{3^{e-1}} \times \mathbb{Z}_{3^{e-1}} \times \mathbb{Z}_{3}
$$

Next consider $\left(\mathcal{O}_{K} / R^{2 e+1}\right)^{\times}$, which is of order $(p-1) p^{2 e}$. Let $[g]$ be a generator of $\left(\mathbb{Z}_{3^{e+1}}\right)^{\times}$embedded naturally in $\left(\mathcal{O}_{K} / R^{2 e+1}\right)^{\times}$. Then the subgroup $\langle[g]\rangle \odot$ $\langle[1+3 \alpha]\rangle$ which is of order $2\left(3^{e}\right)\left(3^{e-1}\right)=2\left(3^{2 e-1}\right)$ 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 $\left(\mathcal{O}_{K} / R^{2 e+1}\right)^{\times}$is either

$$
\mathbb{Z}_{2} \times \mathbb{Z}_{3^{e+1}} \times \mathbb{Z}_{3^{e-1}}, \quad \mathbb{Z}_{2} \times \mathbb{Z}_{3^{e}} \times \mathbb{Z}_{3^{e}} \quad \text { or } \quad \mathbb{Z}_{2} \times \mathbb{Z}_{3^{e}} \times \mathbb{Z}_{3^{e-1}} \times \mathbb{Z}_{3}
$$

Similar to the above, any element in $\left(\mathcal{O}_{K} / R^{2 e+1}\right)^{\times}$is of order at most $2\left(3^{e}\right)$ so the first form is impossible. To show that the second form is also impossible, we use the following lemma:
Lemma 5.2. 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

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

Suppose for a contradiction that $\left(\mathcal{O}_{K} / R^{2 e+1}\right)^{\times} \cong \mathbb{Z}_{2} \times \mathbb{Z}_{3^{e}} \times \mathbb{Z}_{3^{e}}$. Let [g] be a generator of $\left(\mathbb{Z}_{3^{e+1}}\right)^{\times}$naturally embedded in $\left(\mathcal{O}_{K} / R^{2 e+1}\right)^{\times}$, then the order of $\left[g^{2}\right]$ is $3^{e}$. By Lemma 5.2, we can find $[r+s \alpha]$ of order $3^{e}$ such that $\left\langle\left[g^{2}\right]\right\rangle \odot\langle[r+s \alpha]\rangle$. Since $[r+s \alpha]^{3}=\left[r^{3}+9 \square\right],[r+s \alpha]^{3^{e-1}}=\left[r^{3}+9 \square\right]^{3^{e-2}}=$ $\left[r^{3^{e-1}}\right] .[r+s \alpha]$ is of order $3^{e}$, so $\left[r^{3^{e-1}}\right]$ is of order 3. Since $[g]$ is a generator of $\left(\mathbb{Z}_{3^{e+1}}\right)^{\times}$embedded naturally in $\left(\mathcal{O}_{K} / R^{2 e+1}\right)^{\times},\left\langle\left[g^{2}\right]\right\rangle$ will contains all coset of order 3 generated by natural numbers, specifically $\left[r^{3^{e-1}}\right]$. Thus the product $\left\langle\left[g^{2}\right]\right\rangle\langle[r+s \alpha]\rangle$ is not direct, which is a contradiction. Hence the structure of $\left(\mathcal{O}_{K} / R^{2 e+1}\right)^{\times}$is not $\mathbb{Z}_{2} \times \mathbb{Z}_{3^{e}} \times \mathbb{Z}_{3^{e}}$ either. This leaves only one possibility that is

$$
\left(\mathcal{O}_{K} / R^{2 e+1}\right)^{\times} \cong \mathbb{Z}_{2} \times \mathbb{Z}_{3^{e}} \times \mathbb{Z}_{3^{e-1}} \times \mathbb{Z}_{3}
$$

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 $\alpha^{2}+3 m \alpha+3 n \in R^{e}$ and $n \equiv 1(\bmod 3)$. Let $f(x)=x^{3}+a x^{2}+3 b x+3 c$, that is $\alpha^{3}=-a \alpha^{2}-3 b \alpha-3 c$. For $e=1,2$ or 3 the structure of $\left(\mathcal{O}_{K} / R^{e}\right)^{\times}$are the same whether $n \equiv 1$ or $2(\bmod 3)$. Thus we consider $e \geq 4$. We will use the following lemma:
Lemma 5.3. Let $e \geq 4$ and $\alpha^{2}+3 m \alpha+3 n \in R^{e}$. 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 $n \equiv \frac{l}{3}(\bmod 3)$.
Proof. Since $\alpha^{2}+3 m \alpha+3 n, \alpha^{2}+k \alpha+l \in R^{e},(3 m-k) \alpha+(3 n-l) \in R^{e}$. If $e$ is even, then $e=2 i$ for some $i \geq 2$. We have already shown that $3^{i}, 3^{i} \alpha \in R^{2 i}$. Write $(3 m-k)=3^{i} q_{1}+r_{1}$ and $(3 n-l)=3^{i} q_{2}+r_{2}$ where $q_{1}, q_{2}, r_{1}, r_{2} \in \mathbb{Z}$ and $0 \leq r_{1}, r_{2}<3^{i}$. So $r_{1} \alpha+r_{2} \in R^{2 i}$ which implies that $\left[r_{1} \alpha+r_{2}\right]=[0]$ in $\mathcal{O}_{K} / R^{2 i}$. Since we have that the cosets $[r+s \alpha]$ where $0 \leq r, s<3^{i}$ are all distinct, we have $r_{1}=r_{2}=0$. Thus $3^{i} \mid(3 n-l)$. Since $i \geq 2,3 \mid l$ and $9 \mid 3 n-l$, and so $n \equiv \frac{l}{3}(\bmod 3)$. If $e$ is odd, then $e=2 i+1$ for some $i \geq 2$. We have that $3^{i+1}, 3^{i} \alpha \in R^{2 i+1}$. We can show similarly to the above that $3 \mid l$ and $n \equiv \frac{l}{3}(\bmod 3)$.

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

Let $e \geq 3$. Assume $\alpha^{2}+3 m \alpha+3 n \in R^{e}$. Since $R=\langle 3, \alpha\rangle, \alpha^{3}+3 m \alpha^{2}+3 n \alpha \in$ $R^{e+1}$ and
$\alpha^{3}+3 m \alpha^{2}+3 n \alpha=\left(-a \alpha^{2}-3 b \alpha-3 c\right)+3 m \alpha^{2}+3 n \alpha=(3 m-a) \alpha^{2}+(3 n-3 b) \alpha-3 c$.
Let $k$ be a positive integer such that $3^{k} \in R^{e+1}$ and $(3 m-a)^{-1}$ be an inverse of $3 m-a$ modulo $3^{k}$, i.e., $(3 m-a)^{-1}(3 m-a)-1 \in R^{e+1}$. We have

$$
\alpha^{2}+(3 m-a)^{-1}(3 n-3 b) \alpha-3 c(3 m-a)^{-1} \in R^{e+1}
$$

so $-c(3 m-a)^{-1} \equiv-c(-a)^{-1} \equiv c a^{-1}(\bmod 3)$. That is $R^{e+1}$ will be in the special case if and only if $a \equiv c(\bmod 3)$. To summarize:
Theorem 5.4. Let $e \geq 2$. If either $p \geq 5$, or $p=3$ and $f(x)=x^{3}+a x^{2}+$ $3 b x+3 c$ such that $a \not \equiv c(\bmod 3)$, then

$$
\begin{aligned}
\left(\mathcal{O}_{K} / R\right)^{\times} & =\mathbb{Z}_{p-1} \\
\left(\mathcal{O}_{K} / R^{e}\right)^{\times} & =\mathbb{Z}_{p-1} \times \mathbb{Z}_{p^{\left\lfloor\frac{e-1}{2}\right\rfloor}} \times \mathbb{Z}_{p^{\left\lfloor\frac{e}{2}\right\rfloor}}
\end{aligned}
$$

If $p=3$ and $f(x)=x^{3}+a x^{2}+3 b x+3 c$ such that $a \equiv c(\bmod 3)$, then

$$
\begin{aligned}
\left(\mathcal{O}_{K} / R\right)^{\times} & =\mathbb{Z}_{2} \\
\left(\mathcal{O}_{K} / R^{e}\right)^{\times} & =\mathbb{Z}_{2} \times \mathbb{Z}_{3^{\left\lfloor\frac{e-1}{2}\right\rfloor}} \times \mathbb{Z}_{3^{\left\lfloor\frac{e-2}{2}\right\rfloor}} \times \mathbb{Z}_{3}
\end{aligned}
$$

## 6. $R$ in the fourth category: $\langle p\rangle=R^{3}$

Under our assumption that the discriminant of the minimal polynomial of $\alpha$ is square-free, 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 $f(x) \equiv(x+a)^{3}(\bmod p)$ for some $a \in \mathbb{N}$. We can shift the value of $\alpha$ to $\alpha-a$ without the change of $\operatorname{disc}(f)$ so that $f(x) \equiv x^{3}(\bmod p)$. This makes $f(x)$ to be in the form $f(x)=x^{3}+p a_{2} x^{2}+p a_{1} x+p a_{0}$ for some $a_{0}, a_{1}, a_{2} \in \mathbb{Z}$. Hence by Theorem 1.2, the discriminant of $f$ is

$$
\operatorname{disc}(f)=-27 p^{2} a_{0}^{2}-4 p^{3} a_{1}^{3}+18 p^{3} a_{0} a_{1} a_{2}+p^{4} a_{1}^{2} a_{2}^{2}-4 p^{4} a_{0} a_{2}^{3}
$$

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

## 7. $\langle p\rangle$ stays prime

## 7.1. $p=2$

In order to have $\langle 2\rangle$ stays prime, the minimal polynomial $f(x)$ of $\alpha$ has to remain irreducible modulo 2 . Since there are only two irreducible cubic polynomials modulo 2 , namely, $x^{3}+x+1$ and $x^{3}+x^{2}+1$, thus $f(x)$ is congruent modulo 2 to one of these two polynomials. That is $f(x)=x^{3}-a_{2} x^{2}-a_{1} x-a_{0}$ 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 we will have that $\alpha^{3}=a_{2} \alpha^{2}+a_{1} \alpha+a_{0}$ ). Then

$$
\alpha^{4}=\alpha\left(a_{2} \alpha^{2}+a_{1} \alpha+a_{0}\right)=a_{2}\left(a_{2} \alpha^{2}+a_{1} \alpha+a_{0}\right)+a_{1} \alpha^{2}+a_{0} \alpha
$$

$$
=\left(a_{1}+a_{2}^{2}\right) \alpha^{2}+\left(a_{0}+a_{1} a_{2}\right) \alpha+a_{0} a_{2}
$$

Now we consider the structure of $\left(\mathcal{O}_{K} /\left\langle 2^{e}\right\rangle\right)^{\times}$. First, since $\left|\left(\mathcal{O}_{K} /\left\langle 2^{e}\right\rangle\right)^{\times}\right|=$ $(\mathrm{N}(\langle 2\rangle)-1) \mathrm{N}(\langle 2\rangle)^{e-1}=7\left(8^{e-1}\right),\left(\mathcal{O}_{K} /\left\langle 2^{e}\right\rangle\right)^{\times}$has an element $[h]$ of order 7. Next we consider the part with elements of order powers of 2 . For $e \geq 3$, we have

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

while

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

Hence the order of $1+2 \alpha$ in $\left(\mathcal{O}_{K} /\left\langle 2^{e}\right\rangle\right)^{\times}$is $2^{e-1}$. Also

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

while

$$
\begin{aligned}
\left(1+2 \alpha^{2}\right)^{2^{e-2}} & =1+2^{e-1} \alpha^{2}+2^{e-1} \alpha^{4}+2^{e} \square \\
& =1+2^{e-1} \alpha^{2}+2^{e-1}\left(\left(a_{1}+a_{2}^{2}\right) \alpha^{2}+\left(a_{0}+a_{1} a_{2}\right) \alpha+a_{0} a_{2}\right)+2^{e} \square .
\end{aligned}
$$

Since $a_{0}$ is odd and either $a_{1}$ or $a_{2}$ is odd, $a_{1}+a_{2}^{2}$ and $a_{0}+a_{1} a_{2}$ are both odd, so the above expression can be reduced to

$$
\left(1+2 \alpha^{2}\right)^{2^{e-2}}=1+2^{e-1} a_{0} a_{2}+2^{e-1} \alpha+2^{e} \square .
$$

Thus the order of $\left[1+2 \alpha^{2}\right]$ in $\left(\mathcal{O}_{K} /\left\langle 2^{e}\right\rangle\right)^{\times}$is $2^{e-1}$. Now we are ready to find the structure of $\left(\mathcal{O}_{K} /\left\langle 2^{e}\right\rangle\right)^{\times}$. If $e=1$, it is just a cyclic group. For $e=2$, consider $\langle[-1]\rangle\langle[1+2 \alpha]\rangle\left\langle\left[1+2 \alpha^{2}\right]\right\rangle$ which is the product of three subgroups, each generated by an element of order 2 . Since $[1+2 \alpha] \notin\langle[-1]\rangle$, the product of the first two subgroups is direct. Also the product of the first two subgroups contains only coset representable by an element $r+s \alpha$ for some $r, s \in \mathbb{Z}$. This implies that $\left[1+2 \alpha^{2}\right] \notin\langle[-1]\rangle\langle[1+2 \alpha]\rangle$. Together with $[h]$, an element of order 7 in $\left(\mathcal{O}_{K} /\left\langle 2^{2}\right\rangle\right)^{\times}$,

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

Now for $e \geq 3$, consider

$$
\langle[5]\rangle\langle[-1]\rangle\left\langle\left[1+2^{e-1} a_{0} a_{2}+2^{e-1} \alpha\right]\right\rangle\left\langle\left[1+2^{e-1} \alpha+2^{e-1} \alpha^{2}\right]\right\rangle .
$$

As usual we will use Lemma 2.1 to show that the previous product is direct. Since $\left(\mathbb{Z}_{2^{e}}\right)^{\times}$is embedded naturally in $\left(\mathcal{O}_{K} /\left\langle 2^{e}\right\rangle\right)^{\times},\langle[5]\rangle \odot\langle[-1]\rangle$ is direct. $\langle[5]\rangle\langle[-1]\rangle$ only contains cosets representable by $r$ for some $r \in \mathbb{Z}$ thus the product of the first two subgroups does not contain $\left[1+2^{e-1} a_{0} a_{2}+2^{e-1} \alpha\right]$. Thus the product of the first three subgroups is direct. Again the product of the first three subgroups contains only cosets representable by $r+s \alpha$ for some $r, s \in \mathbb{Z}$, so the product of all four subgroups is direct. By Lemma 2.2, the product

$$
\langle[5]\rangle\langle[-1]\rangle\left\langle\left[1+2 \alpha^{2}\right]\right\rangle\langle[1+2 \alpha]\rangle
$$

is direct of order $2^{3 e-3}$. Combine with $[h]$, an element of order 7 , we have that

$$
\left(\mathcal{O}_{K} /\left\langle 2^{e}\right\rangle\right)^{\times}=\langle[h]\rangle \odot\langle[5]\rangle \odot\langle[-1]\rangle \odot\langle[1+2 \alpha]\rangle \odot\left\langle\left[1+2 \alpha^{2}\right]\right\rangle
$$

$$
\cong \mathbb{Z}_{7} \times \mathbb{Z}_{2^{e-2}} \times \mathbb{Z}_{2} \times \mathbb{Z}_{2^{e-1}} \times \mathbb{Z}_{2^{e-1}}
$$

To summarize:
Theorem 7.1. If the ideal $\langle 2\rangle$ stays prime, then

$$
\left(\mathcal{O}_{K} /\left\langle 2^{e}\right\rangle\right)^{\times} \cong \mathbb{Z}_{7} \times\left(\mathbb{Z}_{2^{e}}\right)^{\times} \times \mathbb{Z}_{2^{e-1}} \times \mathbb{Z}_{2^{e-1}} .
$$

## 7.2. $p \geq 3$

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

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

One difference is that since $\langle p\rangle$ is a prime ideal, $\left(\mathcal{O}_{K} /\langle p\rangle\right)^{\times}$is a cyclic group of order $p^{3}-1$, say generated by $[h]$ for some $h \in \mathcal{O}_{K}$. By Lemma $2.6\left[h^{p^{e-1}}\right]$ is of order $p^{3}-1$ in $\left(\mathcal{O}_{K} /\left\langle p^{e}\right\rangle\right)^{\times}$. Thus

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

To summarize:
Theorem 7.2. Let $p \geq 3$. If the ideal $\langle p\rangle$ stays prime, then

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

## 8. Examples

Consider the irreducible polynomial $f(x)=x^{3}+x+1$ over $\mathbb{Q}$. Let $\alpha$ be a root of $f(x)$ in $\mathbb{C}$ and $K=\mathbb{Q}[\alpha]$. Since

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

which is square-free, $\mathcal{O}_{K}=\mathbb{Z}[\alpha]$. We select some prime numbers to show factorizations of $\langle p\rangle$ by using Theorem 1.1.
(1) Let $p=47$. Since $x^{3}+x+1 \equiv(x+12)(x+13)(x+22)(\bmod 47)$,

$$
\langle 47\rangle=\langle 47, \alpha+12\rangle\langle 47, \alpha+13\rangle\langle 47, \alpha+22\rangle .
$$

(2) Let $p=3$. Since $x^{3}+x+1(\bmod 3) \equiv(x+2)\left(x^{2}+x+2\right)(\bmod 3)$,

$$
\langle 3\rangle=\langle 3, \alpha+2\rangle\left\langle 3, \alpha^{2}+\alpha+2\right\rangle .
$$

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

$$
\langle 31\rangle=\langle 31, \alpha+17\rangle^{2}\langle 31, \alpha+28\rangle .
$$

(4) Let $p=2$. Since $x^{3}+x+1(\bmod 2)$ is irreducible, $\langle 2\rangle$ is a prime ideal.

Using previous results, we have that

UNIT GROUPS OF QUOTIENT RINGS OF INTEGERS IN SOME CUBIC FIELDS 803
(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 denoted by $S$ in $\S \mathbf{3}$, thus

$$
\begin{aligned}
\left(\mathcal{O}_{K} /\langle 47, \alpha+12\rangle^{e}\right)^{\times} & \cong\left(\mathcal{O}_{K} /\langle 47, \alpha+13\rangle^{e}\right)^{\times} \\
& \cong\left(\mathcal{O}_{K} /\langle 47, \alpha+22\rangle^{e}\right)^{\times} \cong\left(\mathbb{Z}_{47^{e}}\right)^{\times} \\
\left(\mathcal{O}_{K} /\langle 3, \alpha+2\rangle^{e}\right)^{\times} & \cong\left(\mathbb{Z}_{3^{e}}\right)^{\times}
\end{aligned}
$$

and

$$
\left(\mathcal{O}_{K} /\langle 31, \alpha+28\rangle^{e}\right)^{\times} \cong\left(\mathbb{Z}_{31^{e}}\right)^{\times}
$$

(2) $\left\langle 3, \alpha^{2}+\alpha+2\right\rangle$ is an ideal in the second category which is denoted by $Q$. Thus

$$
\left(\mathcal{O}_{K} /\left\langle 3, \alpha^{2}+\alpha+2\right\rangle^{e}\right)^{\times} \cong \mathbb{Z}_{3^{e-1}} \times \mathbb{Z}_{3^{e-1}} \times \mathbb{Z}_{8}
$$

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

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

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

$$
\left(\mathcal{O}_{K} /\langle 2\rangle^{e}\right)^{\times} \cong \mathbb{Z}_{7} \times\left(\mathbb{Z}_{2^{e}}\right)^{\times} \times \mathbb{Z}_{2^{e-1}} \times \mathbb{Z}_{2^{e-1}}
$$

## References

[1] A. A. Allan, M. J. Dunne, J. R. Jack, J. C. Lynd, and H. W. Ellingsen Jr., Classification of the group of units in the Gaussian integers modulo n, Pi Mu Epsilon J. 12 (2008), no. 9, 513-519.
[2] D. M. Burton, Elementary Number Theory, Allyn and Bacon, Inc., Massachusetts, 1980.
[3] J. T. Cross, The Euler $\phi$-function in the Gaussian integers, Amer. Math. Monthly 90 (1983), no. 8, 518-528.
[4] K. Ireland and M. Rosen, A Classical Introduction to Modern Number Theory, 2nd ed., Springer-Verlag, New York, 1990.
[5] D. A. Marcus, Number Fields, Springer-Verlag, New York, 1977.
[6] I. Niven, H. S. Zuckerman, and H. L. Montgomery, An Introduction to the Theory of Numbers, 5th ed., John Wiley \& Sons, Inc., New York, 1993.
[7] A. Ranum, The group of classes of congruent quadratic integers with respect to a composite ideal modulus, Trans. Amer. Math. Soc. 11 (1910), no. 2, 172-198.
[8] P. Ribenboim, Classic Theory of Algebraic Numbers, Springer-Verlag, New York, 2001.
Ajchara Harnchoowong
Department of Mathematics and Computer Science
Chulalongkorn University
Bangkok 10330, Thailand
E-mail address: ajchara.h@chula.ac.th
Pitchayatak Ponrod
Department of Mathematics and Computer Science
Chulalongkorn University
Bangkok 10330, Thailand
E-mail address: pitchayatak.po@student.chula.ac.th


[^0]:    Received December 4, 2016; Revised May 15, 2017; Accepted June 28, 2017.
    2010 Mathematics Subject Classification. Primary 11R16.
    Key words and phrases. unit group, quotient ring of integers, cubic field, square-free discriminant.

    The Scholarship from the Graduate School, Chulalongkorn University to commemorate the 72 nd anniversary of his Majesty King Bhumibala Aduladeja is gratefully acknowledged.

