Commun. Korean Math. Soc. **0** (0), No. 0, pp. 1–0
https://doi.org/10.4134/CKMS.c160254
pISSN: 1225-1763 / eISSN: 2234-3024

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 α is an algebraic integer such that $\mathrm{disc}_K(\alpha)$ 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, $(\mathbb{Z}_n)^\times$, i.e., $(\mathbb{Z}/n\mathbb{Z})^\times$. Specifically, 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 $e \geq 3$. In fact, this theorem is usually stated in terms of primitive roots. Together with the Chinese remainder theorem, we can get the structure of $(\mathbb{Z}_n)^\times$ 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 $(\mathcal{O}_K/A)^\times$. 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 α is a root of some monic polynomial of degree 3 in $\mathbb{Z}[x]$ which is irreducible over $\mathbb{Q}$ and $\mathrm{disc}_K(\alpha)$ 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 β is a root of $x^3 - x^2 - 2x - 8$. Its ring of integers is not $\mathbb{Z}[\gamma]$ for any $\gamma \in \mathcal{O}_L$. In fact, its ring of integers is $\mathbb{Z} + \beta\mathbb{Z} + (\frac{\beta+\beta^2}{2})\mathbb{Z}$.

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 72nd anniversary of his Majesty King Bhumibala Aduladeja is gratefully acknowledged.

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 $\overline{f}(x)$ 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

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

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 $\overline{f}_i(x)$, $\deg f_i(x) = \deg \overline{f}_i(x)$, and $\mathrm{N}(P_i) = p^{\deg f_i}$.

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

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

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

2. Notations and lemmas

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

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

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_1H_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 $H \odot \langle g^p \rangle$, then $H \odot \langle g \rangle$.*

The following two lemmas will be used very often. The first is a generalization of Euler's ϕ 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*

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

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

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

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

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

□

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*

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

and if also r is odd, then

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

We will see that $(\mathcal{O}_K/A)^\times$ contains an isomorphic image of $(\mathbb{Z}_n)^\times$ for some $n \in \mathbb{N}$, so we can use the structure of $(\mathbb{Z}_n)^\times$ to find the structure of $(\mathcal{O}_K/A)^\times$.

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*

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

Proof. Consider the natural homomorphism $\mathbb{Z} \to \mathcal{O}_K/A$ 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, $(\mathbb{Z}_n)^\times = (\mathbb{Z}/n\mathbb{Z})^\times \hookrightarrow (\mathcal{O}_K/A)^\times$. □

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 $(\mathcal{O}_K/\langle p\rangle)^\times$ with $p \nmid k$, then $[h^{p^e}]$ is of order k in $(\mathcal{O}_K/\langle p^e\rangle)^\times$.*

Proof. Assume $[h]$ is of order k in $(\mathcal{O}_K/\langle p\rangle)^\times$ and $[h^{p^e}]$ is of order l in $(\mathcal{O}_K/\langle p^e\rangle)^\times$. 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 $\text{disc}_K(\alpha)$ is square-free. Let $f(x) \in \mathbb{Z}[x]$ be the minimal polynomial of α. We will apply Theorem 1.1 to consider all possible factorizations of $f(x) \pmod p$. 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 polynomial $x^2 + a_1x + a_0 \in \mathbb{Z}[x]$ which is irreducible mod p 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 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) $\langle p \rangle = S_1S_2S_3$,
(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 category are distinct. Ideals denoted by S with or without a suffix are of norm p, $\text{N}(R) = p$ and $\text{N}(Q) = p^2$.

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 $|\mathcal{O}_K/S^e| = p^e$ so it suffices to show that $p^{e-1} \notin S^e$. Suppose that $p^{e-1} \in S^e$, i.e., $S^e \mid \langle p^{e-1} \rangle$. From the categorization above, the largest power of S dividing $\langle p^{e-1} \rangle$ is $e-1$ which is a contradiction. So we have proved the following theorem.

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

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

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,

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

for some $a_0 \in \mathbb{Z}$. We can simplify the proof by shifting the value of α so that α is a root of a monic irreducible polynomial $f(x)$ such that

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

So $f(x) = x^3 + c_2x^2 + c_1x + 2c_0$ for some integer c_0 and odd integers 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 into 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 facts that $\alpha^3 + c_2\alpha^2 + c_1\alpha + 2c_0 = 0$ and c_1, c_2 being odd, it can be shown by induction that $(\alpha^2 + \alpha + 1)^e = r\alpha^2 + s\alpha + t$ 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 $\mathcal{O}_K/Q^e$, $[\alpha^2] = [d_1\alpha + d_0]$. 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 in the form $[r + s\alpha]$ where $0 \le r, s < 2^e$, i.e.,

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

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

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

Thus the order of $[1+2\alpha]$ is 2^{e-1} and $[(1+2\alpha)^{2^{e-2}}] = [1+2^{e-1}]$ for all $e \ge 3$. For $e = 1, 2$, we can see that the order of $[1 + 2\alpha]$ is also 2^{e-1}. And for $e \ge 3$, 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 $[(1 + 4\alpha)^{2^{e-3}}] = [1 + 2^{e-1}\alpha]$ for $e \ge 3$. For $e = 1, 2$, the order of $[1 + 4\alpha]$ is 1. When $e = 1$, $(\mathcal{O}_K/Q)^\times$ is a cyclic group of order 3, i.e.,

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

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

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

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

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

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

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

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

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

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

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

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 $(2)(2^{e-1})(2^{e-2}) = 2^{2e-2}$. Since the order of $(\mathcal{O}_K/Q^e)^\times$ is $3(2^{2e-2})$, together with the element $[h]$ of order 3, we have that

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

To summarize:

Theorem 4.1. *If Q is a prime ideal lying over 2 of norm 4, then*

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

4.2. $p \geq 3$

We find that it is easier to consider $(\mathcal{O}_K/S^eQ^e)^\times = (\mathcal{O}_K/\langle p^e \rangle)^\times$ instead of just $(\mathcal{O}_K/Q^e)^\times$ 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 $(\mathcal{O}_K/Q^e)^\times$. We have that elements of $\mathcal{O}_K/\langle p^e \rangle$ can be uniquely represented by $[r+s\alpha+t\alpha^2]$ where $0 \leq r,s,t < p^e$, i.e.,

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

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

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

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

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

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

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

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

By Lemma 2.2, we have that

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

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

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

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

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

To summarize:

Theorem 4.2. *Let Q be a prime ideal lying over $p \geq 3$ of norm p^2. Then*

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

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

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 1.2

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

which is not square-free if $p \mid a_0$ or $p = 2$. Thus $p \neq 2$ 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 $\alpha^2 + pc_1\alpha + pc_0 \in R^e$ and $p \nmid c_0$.*

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 $\langle p^e\rangle = R^{2e}S^e \subseteq R^{2e}$, $p^e, p^e\alpha \in R^{2e}$. Since $|\mathcal{O}_K/R^{2e}| = \mathrm{N}(R^{2e}) = p^{2e}$, each element of $\mathcal{O}_K/R^{2e}$ can be represented uniquely by $[r+s\alpha]$ where $0 \leq r, s < p^e$, i.e.,

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

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

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

Next we consider structures of $(\mathcal{O}_K/R^{2e})^\times$ and $(\mathcal{O}_K/R^{2e+1})^\times$. First, $(\mathcal{O}_K/R)^\times$ 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 $\mathbb{Z}_p$, $(\mathcal{O}_K/R^2)^\times$ has a subgroup isomorphic to $\mathbb{Z}_{p-1}$. By Lemma 2.3, $|(\mathcal{O}_K/R^2)^\times| = (p-1)p$, 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 $\mathbb{Z}_{p^2}$. Since $(\mathbb{Z}_{p^2})^\times \cong \mathbb{Z}_{p(p-1)}$, $(\mathcal{O}_K/R^3)^\times$ has a subgroup isomorphic to $\mathbb{Z}_{p(p-1)}$. By Lemma 5.1, $[\alpha^2] = [-pa_1\alpha - pa_0] = [p\square]$. Thus for $p \geq 3$, $[\alpha^p] = [\alpha^2(\alpha)\alpha^{p-3}] = [p\alpha\square]$. Thus for any $[r+s\alpha] \in (\mathcal{O}_K/R^3)^\times$,

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

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

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

Now we consider structures of $(\mathcal{O}_K/R^{2e})^\times$ 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 5.1, we know that $[\alpha^2] = [pa_1\alpha + pa_0] = [p\square]$ and for any $k \geq 2$, $[p\alpha^k] = [p^2\alpha^{k-2}\square] = [p^2\square]$. Hence $[\alpha^p] = [\alpha^2][\alpha^2][\alpha^{p-4}] = [p\square][p\square][\square] = [p^2\square]$. Thus from the expansion of $[(1+\alpha)^p]$, the third term onward can be combined into $p^2\square$, i.e.,

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

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

$$[(r+s\alpha)^3] = [r^3 + 3r^2s\alpha + 3rs^2\alpha^2 + s^3\alpha^3]$$

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

Since $3 \nmid n$, $n \equiv 1$ 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 $n \equiv 2 \pmod 3$ together with the case $p \geq 5$ because in both cases, there are $r, s \in \mathbb{Z}$ such that $[r + s\alpha]^p = [1 + p\alpha + p^2\square]$. For $e \geq 2$,

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

while

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

Thus 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 $p \geq 5$, $[1 + \alpha]^p = [1 + p\alpha + p^2\square]$ 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 $(\mathbb{Z}_{p^e})^\times$ naturally embedded in $(\mathcal{O}_K/R^{2e})^\times$. Consider the product

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

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

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

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 Lemma 2.2 that,

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

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

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 $\alpha^2 + 3m\alpha + 3n \in R^e$ where $n \equiv 1 \pmod 3$. Recall that

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

(1) If $3 \mid r$, then
$$[(r+s\alpha)^3] = [r^3 + 3(r^2 s - ns^3)\alpha + 9\square] = [3\square].$$
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., $[r+s\alpha] \notin (\mathcal{O}_K/R^e)^\times$, so we do not have to consider this case.

(2) If $3 \nmid r$ and $3 \mid s$, then
$$[(r+s\alpha)^3] = [r^3 + 3(r^2 s - ns^3)\alpha + 9\square] = [r^3 + 9\square].$$

(3) If $3 \nmid r$ and $3 \nmid s$, then
$$r^2 s - ns^3 \equiv r^2 s - s^3 \equiv r^2 s - s \equiv s(r^2-1) \equiv s(1-1) \equiv 0 \pmod 3.$$

Thus for any $[r+s\alpha] \in (\mathcal{O}_K/R^e)^\times$,
$$[(r+s\alpha)^3] = [r^3 + 3(r^2 s - ns^3)\alpha + 9\square] = [r^3 + 9\square].$$

By Lemma 2.3 and the fact that $\mathrm{N}(R) = 3$, we have that
$$|(\mathcal{O}_K/R^{2e})^\times| = (3-1)3^{2e-1} = 2(3^{2e-1})$$
and
$$|(\mathcal{O}_K/R^{2e+1})^\times| = (3-1)3^{2e} = 2(3^{2e}).$$
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 $(\mathcal{O}_K/R^{2e})^\times$ is 3^{e-1} and $[(1+3\alpha)^{3^{e-2}}] = [1+3^{e-1}\alpha]$. Let $[g]$ be a generator of $(\mathbb{Z}_{3^e})^\times$ embedded naturally in $(\mathcal{O}_K/R^{2e})^\times$, so $[g]$ is of order $2(3^{e-1})$. Since $[1+3^{e-1}\alpha] \notin \langle [g] \rangle$, by Lemma 2.1,
$$\langle [g] \rangle \odot \langle [1+3^{e-1}\alpha] \rangle.$$
Since $[1+3^{e-1}\alpha] = [(1+3\alpha)^{3^{e-2}}]$ in $(\mathcal{O}_K/R^{2e})^\times$, by Lemma 2.2 we have
$$\langle [g] \rangle \odot \langle [1+3\alpha] \rangle$$
and its order is $2(3^{2e-2})$. 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
$$\mathbb{Z}_2 \times \mathbb{Z}_{3^e} \times \mathbb{Z}_{3^{e-1}} \quad \text{or} \quad \mathbb{Z}_2 \times \mathbb{Z}_{3^{e-1}} \times \mathbb{Z}_{3^{e-1}} \times \mathbb{Z}_3.$$
From the earlier, for any $[r+s\alpha] \in (\mathcal{O}_K/R^{2e})^\times$, $[r+s\alpha]^3 = [r^3+9\square]$, 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
$$(\mathcal{O}_K/R^{2e})^\times \cong \mathbb{Z}_2 \times \mathbb{Z}_{3^{e-1}} \times \mathbb{Z}_{3^{e-1}} \times \mathbb{Z}_3.$$
Next 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
$$\mathbb{Z}_2 \times \mathbb{Z}_{3^{e+1}} \times \mathbb{Z}_{3^{e-1}}, \quad \mathbb{Z}_2 \times \mathbb{Z}_{3^e} \times \mathbb{Z}_{3^e} \quad \text{or} \quad \mathbb{Z}_2 \times \mathbb{Z}_{3^e} \times \mathbb{Z}_{3^{e-1}} \times \mathbb{Z}_3.$$

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 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 $(\mathcal{O}_K/R^{2e+1})^\times \cong \mathbb{Z}_2 \times \mathbb{Z}_{3^e} \times \mathbb{Z}_{3^e}$. 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 3^e. By Lemma 5.2, we can find $[r + s\alpha]$ of order 3^e such that $\langle [g^2] \rangle \odot \langle [r + s\alpha] \rangle$. Since $[r + s\alpha]^3 = [r^3 + 9\square]$, $[r + s\alpha]^{3^{e-1}} = [r^3 + 9\square]^{3^{e-2}} = [r^{3^{e-1}}]$. $[r + s\alpha]$ is of order 3^e, so $[r^{3^{e-1}}]$ is of order 3. Since $[g]$ is a generator 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 whether $n \equiv 1$ or $2 \pmod 3$. Thus we consider $e \geq 4$. We will use the following lemma:

Lemma 5.3. *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 $\alpha^2 + 3m\alpha + 3n, \alpha^2 + k\alpha + l \in R^e$, $(3m - k)\alpha + (3n - l) \in R^e$. If e is even, then $e = 2i$ for some $i \geq 2$. We have already shown that $3^i, 3^i\alpha \in R^{2i}$. Write $(3m - k) = 3^i q_1 + r_1$ and $(3n - l) = 3^i q_2 + r_2$ where $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ and $0 \leq r_1, r_2 < 3^i$. So $r_1\alpha + r_2 \in R^{2i}$ which implies that $[r_1\alpha + r_2] = [0]$ in $\mathcal{O}_K/R^{2i}$. 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 $3^i \mid (3n - l)$. Since $i \geq 2$, $3 \mid l$ and $9 \mid 3n - l$, and so $n \equiv \frac{l}{3} \pmod 3$. If e is odd, then $e = 2i + 1$ for some $i \geq 2$. We have that $3^{i+1}, 3^i\alpha \in R^{2i+1}$. We can show similarly to the above that $3 \mid l$ and $n \equiv \frac{l}{3} \pmod 3$. □

From the lemma we have that if we can 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 $n' \equiv n \equiv 2 \pmod 3$. Thus to show that there is no $m, n \in \mathbb{Z}$ such that $\alpha^2 + 3m\alpha + 3n \in R^e$ and $n \equiv 1 \pmod 3$, we only need to show that there are $m, n \in \mathbb{Z}$ such that $\alpha^2 + 3m\alpha + 3n \in R^e$ and $n \equiv 2 \pmod 3$.

Let $e \geq 3$. Assume $\alpha^2+3m\alpha+3n \in R^e$. Since $R = \langle 3, \alpha\rangle$, $\alpha^3+3m\alpha^2+3n\alpha \in R^{e+1}$ and

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

Let k be a positive integer such that $3^k \in R^{e+1}$ and $(3m-a)^{-1}$ be an inverse of $3m-a$ modulo 3^k, i.e., $(3m-a)^{-1}(3m-a)-1 \in R^{e+1}$. We have

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

so $-c(3m-a)^{-1} \equiv -c(-a)^{-1} \equiv ca^{-1} \pmod 3$. That is R^{e+1} will be in the special case if and only if $a \equiv c \pmod 3$. To summarize:

Theorem 5.4. *Let $e \geq 2$. If either $p \geq 5$, or $p = 3$ 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

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

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

Under our assumption that the discriminant of the minimal polynomial of α 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 $f(x) \equiv (x+a)^3 \pmod p$ for some $a \in \mathbb{N}$. We can shift the value of α to $\alpha - a$ without the change of $\operatorname{disc}(f)$ 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 $a_0, a_1, a_2 \in \mathbb{Z}$. Hence by Theorem 1.2, the discriminant of f is

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

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

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 α 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 $f(x) = x^3 - a_2x^2 - a_1x - a_0$ 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 we will have that $\alpha^3 = a_2\alpha^2 + a_1\alpha + a_0$). Then

$$\alpha^4 = \alpha(a_2\alpha^2 + a_1\alpha + a_0) = a_2(a_2\alpha^2 + a_1\alpha + a_0) + a_1\alpha^2 + a_0\alpha$$

$$= (a_1 + a_2^2)\alpha^2 + (a_0 + a_1a_2)\alpha + a_0a_2.$$

Now we consider the structure of $(\mathcal{O}_K/\langle 2^e\rangle)^\times$. First, since $|(\mathcal{O}_K/\langle 2^e\rangle)^\times| = (\mathrm{N}(\langle 2\rangle) - 1)\mathrm{N}(\langle 2\rangle)^{e-1} = 7(8^{e-1})$, $(\mathcal{O}_K/\langle 2^e\rangle)^\times$ 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 $(\mathcal{O}_K/\langle 2^e\rangle)^\times$ is 2^{e-1}. Also

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

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

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

Thus the order of $[1 + 2\alpha^2]$ in $(\mathcal{O}_K/\langle 2^e\rangle)^\times$ is 2^{e-1}. 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. 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 $[1+2\alpha^2] \notin \langle[-1]\rangle\langle[1+2\alpha]\rangle$. 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

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

As usual we will use Lemma 2.1 to show that the previous product is direct. Since $(\mathbb{Z}_{2^e})^\times$ is embedded naturally in $(\mathcal{O}_K/\langle 2^e\rangle)^\times$, $\langle[5]\rangle \odot \langle[-1]\rangle$ 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 $[1 + 2^{e-1}a_0a_2 + 2^{e-1}\alpha]$. 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

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

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

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

$$\cong \mathbb{Z}_7 \times \mathbb{Z}_{2^{e-2}} \times \mathbb{Z}_2 \times \mathbb{Z}_{2^{e-1}} \times \mathbb{Z}_{2^{e-1}}.$$

To summarize:

Theorem 7.1. *If the ideal $\langle 2 \rangle$ stays prime, then*

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

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

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

One difference is that since $\langle p \rangle$ is a prime ideal, $(\mathcal{O}_K/\langle p \rangle)^\times$ is a cyclic group of order $p^3 - 1$, say generated by $[h]$ for some $h \in \mathcal{O}_K$. By Lemma 2.6 $[h^{p^{e-1}}]$ 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 7.2. *Let $p \geq 3$. If the ideal $\langle p \rangle$ stays prime, then*

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

8. Examples

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

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

which is square-free, $\mathcal{O}_K = \mathbb{Z}[\alpha]$. We select some prime numbers to show factorizations of $\langle p \rangle$ by using Theorem 1.1

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

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

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

$$\langle 3 \rangle = \langle 3, \alpha + 2 \rangle \langle 3, \alpha^2 + \alpha + 2 \rangle.$$

(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 a prime ideal.

Using previous results, we have that

(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 §**3**, thus

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

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 an 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 an ideal in the third category which is 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] 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 ϕ-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