Communications in Mathematics **31** (2023), no. 2, 209–250
DOI: https://doi.org/10.46298/cm.11138

Well-Rounded ideal lattices of cyclic cubic and quartic fields

Dat Tan Tran, Nam Hoai Le, Ha Thanh Nguyen Tran

Abstract. In this paper, we find criteria for when cyclic cubic and cyclic quartic fields have well-rounded ideal lattices. We show that every cyclic cubic field has at least one well-rounded ideal. We also prove that there exist families of cyclic quartic fields that have well-rounded ideals and explicitly construct their minimal bases. In addition, for a given prime number p, if a cyclic quartic field has a unique prime ideal above p, then we provide the necessary and sufficient conditions for that ideal to be well-rounded. Moreover, in cyclic quartic fields, we provide the prime decomposition of all odd prime numbers and construct an explicit integral basis for every prime ideal.

1 Introduction

A well-rounded (WR) ideal lattice or a WR ideal is an ideal of a number field for which the associated lattice is well-rounded. WR ideal lattices can be used to investigate various problems such as kissing numbers [21], sphere packing problems [18, 17], and Minkowski's conjecture [22]. They also have a variety of applications to coding theory [14, 13]. Previously, Fukshanksy et. al. proved results on WR ideals in real quadratic fields [12, 11], and Araujo and Costa obtained results on WR lattices (but not necessarily for WR ideals) of cyclic fields with degrees equal to odd primes [8]. Generalizing this work,

MSC 2020: AMS classification 11R16, 06B10, 06B99, 11Y40.
Keywords: well-rounded ideal, lattices, cyclic cubic field, cyclic quartic field
Contact information:
Dat.T. Tran:
Affiliation: University of Science, Vietnam National University Ho Chi Minh City, Vietnam.
Email: ttdat1323@gmail.com
Nam H. Le:
Affiliation: University of Science, Vietnam National University Ho Chi Minh City, Vietnam.
Email: namhoai12to2@gmail.com
Ha T.N. Tran:
Affiliation: Concordia University of Edmonton, Canada.
Email: hatran1104@gmail.com

Damir and Mantilla-Soler [7] construct a parametric family of WR sub-lattices of a tame lattice with a Lagrangian basis. Another generalization of WR lattices are WR twists of ideal lattices which are investigated for real quadratic fields in [5] and for imaginary fields in [19]. In [26], it is shown that for any lattice L there exists a diagonal real matrix D with determinant equal to one and with positive entries such that DL is WR. Further, [4] provides an analysis of some WR lattices used in wiretap channels, and [6] shows how to use WR lattices to optimize coset codes for Gaussian and fading wiretap channels.

In this paper, we investigate WR ideals of cyclic cubic and cyclic quartic fields. In the cyclic cubic case, let F be a cyclic cubic field with discriminant Δ_F and Galois group $\mathrm{Gal}(F) = \langle\sigma\rangle$. If a prime p divides Δ_F, it is ramified in F and $p\mathcal{O}_F = P^3$ for a unique prime ideal P and $\sigma^i(P) = P$ for $i \in \{0, 1, 2\}$. If x is a shortest vector in P and the set $\{\sigma^i(x) : 0 \le i \le 2\}$ is linearly independent, then P is WR (see Definition 2.1). This idea is not valid only for prime ideals: it also works for other ideals whose norms divide Δ_F (for example, ideals of the form $\prod_i P_i^{m_i}$ where P_i are ramified prime ideals and $0 < m_i \in \mathbb{Z}$). We can also do similarly for cyclic quartic fields with some modifications.

Our experiment: To implement the idea outlined above, we do the following: First, we find the defining polynomials of cyclic cubic and cyclic quartic fields. Using these polynomials together with Pari/GP [28], we generate a list of all integral ideals of norms bounded by a certain number for each field. We then test which ideals in the list are WR by listing the shortest vectors of each ideal, using the function `qfminim` in Pari/GP. We check if their conjugates form a set of rank 3 in $\mathbb{R}^3$ (for the cyclic cubic case) or rank 4 in $\mathbb{R}^4$ (for the cyclic quartic case). After identifying the WR ideals we examined their properties such as the geometry of their integral bases, the coordinates of shortest vectors with respect to a given integral basis, etc., and formulated conjectures. Finally, we proved these conjectures.

Our contributions: Our main contribution is establishing the conditions for the existence of WR ideal lattices in cyclic number fields of degrees 3 and 4. For cyclic quartic fields, we consider both the real and complex cases. The results can be seen in Theorems 1.1 – 1.6. This is the first time such results are obtained for these classes of number fields. Further, we give families of cyclic cubic and cyclic quartic fields that admit WR ideals. We explicitly construct minimal integral bases of these ideals, which have applications in coding theory [14, 13]. Our other major contribution is that we provide the type decomposition of all odd primes in cyclic quartic fields (see Theorem 4.18) and construct an explicit integral basis for every prime ideal (see Section 4.1).

The results in Theorems 1.1, 1.3, 1.4, 1.5, and the one in Theorem 1.2 where $3 \mid m$ are new and have not been studied before. The WR ideals presented in these theorems are generally not tame and are hence not mentioned in [7]. In [8], WR ideals of quartic fields (found in Theorems 1.4 and 1.5) and of cyclic cubic fields with $3 \mid m$ (found in Theorem 1.1.ii), Theorems 1.2 and 1.3) are not investigated. For the case of cyclic cubic fields where $3 \nmid m$, it has been showed that if $\frac{m}{4} \le q^2 \le 4m$ then Q is WR [8, Theorem 4.1]. For this last case, we used a different technique to prove that this condition is not only sufficient but also necessary (see Theorem 1.2). Moreover, the ideals in Theorem 1.1.i) have larger norms, m^2, which fall outside the range of $[m/4, 4m]$, and thus, they are distinct from those discussed in [8, Theorem 4.1].

We remark that in this paper, all the ideals are integral, and we only consider the well-roundedness of an ideal if it is primitive.

The following theorem regarding cyclic cubic fields can be obtained from Propositions 3.7, 3.11 and 3.18.

Theorem 1.1. *Every cyclic cubic field F has orthogonal and WR ideal lattices. In particular, denoting by m the conductor of F, we have the following.*

i) If $9 \nmid m$, then the unique ideal of norm m^2 is orthogonal and WR.

ii) If $9 \mid m$, then the unique ideal of norm $\frac{m^2}{27}$ is orthogonal and WR.

Moreover, we obtain the following theorem by combining Propositions 3.8, 3.15 and 3.20.

Theorem 1.2. *Let q be a square-free divisor of the conductor m of a cyclic cubic field F. There is a unique ideal Q of $\mathcal{O}_F$ such that $N(Q) = q$. In this case, Q is WR if and only if the following conditions are verified:*

- $\frac{m}{4} \leq q^2 \leq 4m$ *when* $3 \nmid m$, *or*
- $3 \mid q, \frac{m}{4} \leq q^2 \leq 4m$ *when* $3 \mid m$.

When the conductor of a cyclic cubic field is divisible by 9, we have the following result (see Proposition 3.25).

Theorem 1.3. *Let $m = 9p_1p_2 \cdots p_r (r \geq 2)$ and q, q' be two coprime divisors of $p_1p_2 \cdots p_r$. The unique ideal of norm $3q^2q'$ is WR if and only if $\frac{m}{36} \leq qq'^2 \leq \frac{4m}{9}$.*

Combining Theorem 4.18, Propositions 4.19, 4.20, 4.21, 4.22 and 4.23, one obtains the following theorem.

Theorem 1.4. *Let F be a cyclic quartic field defined by a, b, c, d as in (3) and $p_I \mid d$, $q_J \mid a$ such that d is a quadratic non-residue modulo q for each prime divisor q of q_J. Then there are unique ideals of norms p_I and q_J, denoted by P_I and Q_J respectively. Let*

$$\mathcal{M} = \left\{16q_J^2d,\ 8|a|d,\ 4q_I^2d + 4|a|d,\ 16p_I^2q_J^2,\ 4p_I^2q_J^2 + 4|a|d,\ 4p_I^2q_J^2 + 4q_J^2d\right\}.$$

Then the ideal P_IQ_J is WR if and only if

$$d \equiv 1 \pmod 4,\ b \equiv 1 \pmod 2,\ a + b \equiv 1 \pmod 4,$$
$$\text{and} \quad p_I^2q_J^2 + q_J^2d + 2|a|d \leq \min \mathcal{M}.$$

Theorem 1.5. *With the notation given in Theorem 1.4, the following hold.*

i) The lattice P_I is WR if and only if $d \equiv 1 \pmod 4$, $b \equiv 0 \pmod 2$, $a + b \equiv 1 \pmod 4$ and one of the following conditions is satisfied.

- $|a| = 1$ *and* $\frac{1}{5}d \leq p_I^2 \leq 5d$,
- $|a| = 3$ *and* $d \leq p_I^2 \leq 9d$,
- $|a| = 5$ *and* $\frac{7}{3}d \leq p_I^2 \leq 5d$.

ii) The lattice Q_J *is WR if and only if* $d = 5,\ b = 2,\ c = 1$ *and* $|a| \leq q_J^2 \leq 5|a|$.

Note that the proof of Theorem 1.5 is presented after the proof of Proposition 4.23.

For cyclic quartic fields F, considering any odd prime integer p, Theorem 4.18 provides a classification of classes of prime p based on the ideal factorization of $p\mathcal{O}_F$. This can be done for F because its defining polynomial (see in (3)) has the special form $(x^2 - ad)^2 - a^2b^2d$. However, this has not been done for cyclic cubic fields since we do not know how their defining polynomials (see in (2)) are factorized modulo an arbitrary prime.

Let p be any prime number. Based on the result of Theorem 4.18, we can establish necessary and sufficient conditions on p to have a unique prime ideal above p. Given this condition and by Theorem 1.5, we obtain conditions which are equivalent to the well-roundedness of these prime ideals as below.

Theorem 1.6. *Let* F *be a cyclic quartic field defined by* a, b, c, d *as in* (3) *and a prime* p. *There is a unique prime ideal of* $\mathcal{O}_F$ *above* p *if and only one of the following conditions is satisfied.*

i) The prime $p \mid d$.

ii) The prime $p \mid a$ *and* d *is a quadratic non-residue modulo* p.

iii) The prime $p \nmid abcd$ *and* d *is a quadratic non-residue modulo* p.

Moreover, let P *denote the unique prime ideal of* $\mathcal{O}_F$ *above* p. *Then* P *is WR if and only if the conditions in Theorem 1.5 are satisfied.*

Explicit minimal bases of these WR ideals can be seen in the above-mentioned propositions and Lemmas. Additionally, since Δ_F is given in (4), Theorem 1.6 also tells us that if $\mathcal{O}_F$ has only one prime ideal P above a given prime p, then P being WR implies that $p \mid \Delta_F$.

The structure of this paper is as follows. Section 2 serves to provide an initial review of WR ideal lattices and their properties, defining polynomials, integral bases, discriminants, and prime factorizations of ideals in cyclic cubic and cyclic quartic fields. We then investigate WR ideals of cyclic cubic fields in Section 3 and of cyclic quartic fields in Section 4. Finally, in Section 5 we provide some conclusions and a conjecture related to WR ideals of these fields for future research.

2 Background

In this section, we will recall some fundamental knowledge about WR ideal latices, cyclic cubic, and cyclic quartic fields.

2.1 Well-rounded ideal lattices

Let $\mathcal{B} = \{v_1, v_2, \ldots, v_m\}$ be a linearly independent set of vectors in $\mathbb{R}^n$, $1 \leq m \leq n$. The set $L = \{\sum_{i=1}^m a_i v_i | a_i \in \mathbb{Z}\}$ is called a *lattice* in $\mathbb{R}^n$ of rank m and the set $\mathcal{B}$ is said to be a *basis* of L. In case $m = n$, we say that L is a *full rank lattice*.

The value $|L| = \min_{0 \neq u \in L} \|u\|^2$ is called the *minimum norm* of the lattice $L \subset \mathbb{R}^n$, where $\|.\|$ denotes the usual Euclidean norm in $\mathbb{R}^n$, and the set of *minimum vectors* of L is defined as

$$S(L) := \{u \in L : \|u\|^2 = |L|\}.$$

Definition 2.1. Let L be a lattice in $\mathbb{R}^n$.

1. The lattice L is **WR** if $S(L)$ generates $\mathbb{R}^n$, that is, if $S(L)$ contains n linearly independent vectors.

2. The lattice L is said **strongly WR** if $S(L)$ consists of a basis of L. In this case, we call this basis a *minimal* basis of L.

For lattices in dimensions at most 3 and most lattices in dimension 4, WRness and strong WRness are equivalent by [21, Corollary 2.6.10].

We denote by B is an $n \times m$-matrix whose columns are the vectors of $\mathcal{B}$.

Definition 2.2. Let L be a lattice of rank n and its matrix basis B. The **determinant** of L, denoted by $\det(L)$, is defined $\det(L) := \sqrt{\det(B^T B)}$. In the special case that L is a full rank lattice, B is a square matrix, then we have $\det(L) = |\det(B)|$.

The determinant of a lattice is well-defined since it is independent of our choice of basis B. Indeed, B_1 and B_2 are two bases of L, if and only if $B_2 = B_1 U$ for some unimodular matrix U with integer entries. Hence,

$$\sqrt{\det(B_2^T B_2)} = \sqrt{\det(U^T B_1^T B_1 U)} = \sqrt{\det(B_1^T B_1)}.$$

We recall the following result.

Lemma 2.3. *Let L and L' be two full rank lattices in $\mathbb{R}^n$ ($n \geq 1$). Assume that $L' \subseteq L$ and $\det(L) = \det(L')$. Then $L' = L$.*

Proof. Let B, B' be bases of L, L', respectively. Suppose $B' = BA$, then

$$[L : L'] = |\det(A)| = \frac{|\det(B')|}{|\det(B)|} = \frac{\det(L')}{\det(L)} = 1.$$

Hence, $L = L'$. □

Let F be a number field of degree n and signature (r_1, r_2). Then F has $r_1 + r_2$ embeddings up to conjugation: $\sigma_1, \ldots, \sigma_{r_1+r_2}$ where the first r_1 of them are real, and the remaining r_2 are complex. We denote by $\Phi : F \hookrightarrow F \otimes \mathbb{R} \cong \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ the map defined by $\Phi(f) = (\sigma_1(f), \cdots, \sigma_{r_1+r_2}(f))$. Here $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ is a Euclidean space with the scalar product: $\langle u, v\rangle = \sum_{i=1}^{r_1} u_i v_i + 2\sum_{i=r_1+1}^{r_2} \Re(u_i\overline{v_i})$ where $\overline{v_i}$ is the complex conjugate of v_i.

Let Q be a (fractional) ideal of F. Then it is known that $\Phi(Q)$ is a lattice in $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ by [1]. By identifying Q and $\Phi(Q)$, one has that Q is an ideal of F and also a lattice in $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$. Hence, we call ideals of F ideal lattices, see [1] and also [25, Section 4] for more details. An ideal lattice Q is called WR if the lattice $\Phi(Q)$ is WR.

2.2 Cyclic cubic fields

Let F be a cyclic cubic field with conductor m. By [20, pp.6-10], one has

$$m = \frac{a^2 + 3b^2}{4} \tag{1}$$

where a and b are integers satisfying one of the following conditions,

- $a \equiv 2 \pmod 3$, $b \equiv 0 \pmod 3$ and $b > 0$ for $3 \nmid m$;
- $a \equiv 6 \pmod 9$, $b \equiv 3$ or $6 \pmod 9$ and $b > 0$ for $3|m$.

We recall that the conductor m of F has the form

$$m = q_1 q_2 \cdots q_r,$$

where $r \in \mathbb{Z}_{>0}$ and $q_1, \cdots, q_r$ are distinct integers from the set

$$\{9\} \cup \{q : q \text{ is prime and } q \equiv 1 \pmod 3\} = \{7, 9, 13, 19, 31, 37, \dots\}.$$

The discriminant of F is $\Delta_F = m^2$. See Hasse [15] for more details. From [20], the following polynomial, denoted by df, can be used to define F,

$$df(x) = \begin{cases} x^3 - x^2 + \frac{1-m}{3}x - \frac{m(a-3)+1}{27}, & \text{if } 3 \nmid m \\ x^3 - \frac{m}{3}x - \frac{am}{27}, & \text{if } 3|m \end{cases}. \tag{2}$$

Let $m = p_1 \cdots p_r$ or $m = 9 \cdot p_1 \cdots p_r$, where all the p_i are distinct prime numbers congruent to 1 modulo 3. We arrange the p_i such that $3 = p_0 < p_1 < p_2 < \cdots < p_r$.

From now on, we denote by α a root of the defining polynomial $df(x)$ in (2).

Lemma 2.4. *Let $id_3 = [\mathcal{O}_F : \mathbb{Z}[\alpha]]$. Then p_i does not divide the index id_3 for all $i \geq 0$.*

Proof. We suppose by contradiction that there exists $i \geq 0$ such that $p_i | id_3$. By (2), we can calculate the discriminant of df as

$$\Delta_{df} = \frac{m^2(4m - a^2)}{27}.$$

Since F has discriminant m^2, one must have id^2 divides $\frac{4m-a^2}{27}$ or equal to $\frac{4m-a^2}{27}$. Thus, p_i^2 divides $\frac{4m-a^2}{27}$. Moreover, $p_i|m$. It leads to $p_i^2|m$ which implies that $p_i = 3$ since 3 is the only prime of which square divides the conductor m given in (1). In other words, $3|m$ and hence 9 divides $\frac{4m-a^2}{27} = \frac{b^2}{9}$ which is a contradiction since $b \equiv 3$ or $6 \pmod 9$ in (1). Thus, $p_i \nmid id_3$ for all i. □

We prove the following.

Lemma 2.5. *Let $g \in \mathcal{O}_F \backslash \mathbb{Z}$. Then $Tr(g) \neq 0$ if and only if $\{g, \sigma(g), \sigma^2(g)\}$ is $\mathbb{R}$-linearly independent.*

Proof. It is implied from the following equality

$$\begin{vmatrix} g & \sigma(g) & \sigma^2(g) \\ \sigma(g) & \sigma^2(g) & g \\ \sigma^2(g) & g & \sigma(g) \end{vmatrix} = -\tfrac{1}{2}(g+\sigma(g)+\sigma^2(g))\big((g-\sigma(g))^2 + (\sigma(g)-\sigma^2(g))^2 + (\sigma^2(g)-g)^2\big).$$

□

2.3 Cyclic quartic fields

We first recall the facts about cyclic quartic fields and their properties. See [16] for more details. Let $F = \mathbb{Q}(\beta)$ where a, b, c, d are integers such that a is squarefree and odd, $d = b^2 + c^2$ is squarefree, $b > 0, c > 0$, $\gcd(a, d) = 1$ and $\beta = \sqrt{a(d - b\sqrt{d})}$. If $a > 0$ then F is a totally real cyclic quartic field. If $a < 0$ then F is a totally imaginary cyclic quartic field.

A defining polynomial of F, which is also the minimum polynomial of β, is

$$df(x) = x^4 - 2adx^2 + a^2c^2d. \tag{3}$$

It is easy to verify that the discriminant of $df(x)$ is $\Delta_{df} = 256a^6b^4c^2d^3$ and by [16], the discriminant of F is

$$\Delta_F = \begin{cases} 2^8a^2d^3 & \text{if } d \equiv 0 \pmod 2, \\ 2^6a^2d^3 & \text{if } d \equiv 1 \pmod 2,\ b \equiv 1 \pmod 2, \\ 2^4a^2d^3 & \text{if } d \equiv 1 \pmod 2,\ b \equiv 0 \pmod 2,\ a+b \equiv 3 \pmod 4, \\ a^2d^3 & \text{if } d \equiv 1 \pmod 2,\ b \equiv 0 \pmod 2,\ a+b \equiv 1 \pmod 4. \end{cases} \tag{4}$$

Let id_4 be the index of $\mathbb{Z}[\beta]$ in $\mathcal{O}_F$. Then, by (4), id_4^2 divides the following quantity

$$\frac{\Delta_{df}}{\Delta_F} = \begin{cases} a^2b^2c & \text{if } d \equiv 0 \pmod 2, \\ 2a^2b^2c & \text{if } d \equiv 1 \pmod 2,\ b \equiv 1 \pmod 2, \\ 2^2a^2b^2c & \text{if } d \equiv 1 \pmod 2,\ b \equiv 0 \pmod 2,\ a+b \equiv 3 \pmod 4, \\ 2^4a^2b^2c & \text{if } d \equiv 1 \pmod 2,\ b \equiv 0 \pmod 2,\ a+b \equiv 1 \pmod 4. \end{cases} \tag{5}$$

For $K = \mathbb{Q}(\sqrt{d})$, we always have the tower of field extensions

$$\mathbb{Q} \leq K \leq F. \tag{6}$$

The field F has four embeddings: $1, \sigma, \sigma^2, \sigma^3$ where

$$\sigma : \beta \longmapsto \sigma(\beta), \qquad \sigma(\beta) \longmapsto -\beta, \qquad \sqrt{d} \longmapsto -\sqrt{d}. \tag{7}$$

In case $a < 0$, the field F is totally complex and the four roots of $df(x)$ are the following: $\beta, -\beta, \sigma(\beta) = \sqrt{a(d + b\sqrt{d})}, -\sigma(\beta)$, which are all in $\mathbb{R}i$. Here one has $\overline{1} = \sigma^2$ and $\overline{\sigma} = \sigma^3$. Thus F has two embeddings 1 and σ up to conjugation. For $\delta \in F$, we embed it to $(\delta, \sigma(\delta)) \in \mathbb{C}^2$ which is then can be viewed as $(\Re(\delta), \Im(\delta), \Re(\sigma(\delta)), \Im(\sigma(\delta))) \in \mathbb{R}^4$. The four roots of $df(x)$ are totally imaginary hence, they have the form $(0, z_1, 0, z_2)$ for some $z_1, z_2 \in \mathbb{R}$ when embedded in $\mathbb{R}^4$.

In case $a > 0$, the field F is totally real and the 4 roots of $df(x)$ are the following: $\beta, -\beta, \sigma(\beta) = \sqrt{a(d + b\sqrt{d})}, -\sigma(\beta)$, which are all in $\mathbb{R}$. When we embed an element $\delta \in F$ in $\mathbb{R}^4$, we obtain the vector $(\delta, \sigma(\delta), \sigma^2(\delta), \sigma^3(\delta))$.

Although the embeddings of imaginary and the totally real fields are different, we can still verify that if $\delta = s_1 + s_2\sqrt{d} + s_3\beta + s_4\sigma(\beta) \in F$ where $s_i \in \mathbb{Q}$ for all $i \in \{1, 2, 3, 4\}$, then

$$\|\delta\|^2 = 4\left(s_1^2 + s_2^2 d + |a|ds_3^2 + |a|ds_4^2\right). \tag{8}$$

In particular,

$$\|\beta\|^2 = 4|a|d.$$

Remark 2.6. The following integral basis $\mathcal{B} = \{\gamma_1', \gamma_2', \gamma_3', \gamma_4'\}$ in this order of F is provided in [16] which we will use in the later sections.

i) $\left\{1, \sqrt{d}, \sigma(\beta), \beta\right\}$, if $d \equiv 0 \pmod 2$;

ii) $\left\{1, \frac{1}{2}(1 + \sqrt{d}), \sigma(\beta), \beta\right\}$, if $d \equiv b \equiv 1 \pmod 2$;

iii) $\left\{1, \frac{1}{2}(1 + \sqrt{d}), \frac{1}{2}(\sigma(\beta) + \beta), \frac{1}{2}(\sigma(\beta) - \beta)\right\}$, if

$$d \equiv 1 \pmod 2,\ b \equiv 0 \pmod 2,\ a + b \equiv 3 \pmod 4;$$

iv) $\left\{1, \frac{1}{2}(1 + \sqrt{d}), \frac{1}{4}(1 + \sqrt{d} + \sigma(\beta) - \beta), \frac{1}{4}(1 - \sqrt{d} + \sigma(\beta) + \beta)\right\}$, if

$$d \equiv 1 \pmod 2,\ b \equiv 0 \pmod 2,\ a + b \equiv 1 \pmod 4,\ a \equiv -c \pmod 4;$$

v) $\left\{1, \frac{1}{2}(1 + \sqrt{d}), \frac{1}{4}(1 + \sqrt{d} + \sigma(\beta) + \beta), \frac{1}{4}(1 - \sqrt{d} + \sigma(\beta) - \beta)\right\}$, if

$$d \equiv 1 \pmod 2,\ b \equiv 0 \pmod 2,\ a + b \equiv 1 \pmod 4,\ a \equiv c \pmod 4;$$

where $\beta = \sqrt{a(d - b\sqrt{d})}$ and $\sigma(\beta) = \sqrt{a(d + b\sqrt{d})}$.

Lemma 2.7. *Let $\delta \in \mathcal{O}_F \backslash \mathbb{Z}$. Then $Tr(\delta) \neq 0$ if and only if the set $\{\delta, \sigma(\delta), \sigma^2(\delta), \sigma^3(\delta)\}$ is $\mathbb{R}$-linearly independent.*

Lemma 2.8. *One has the following results.*

$$\mathbb{N}\left(\sqrt{d}\right) = d^2, \quad \mathbb{N}(\beta) = a^2c^2d, \quad \mathbb{N}\left(\frac{\beta+\sigma(\beta)}{2}\right) = \frac{a^2b^2d}{4}, \tag{9}$$

$$\beta \cdot \sqrt{d} = c\sigma(\beta) - b\beta, \quad \sigma(\beta)\cdot\sqrt{d} = c\beta + b\sigma(\beta). \tag{10}$$

Proof. It is easy to verify all equalities in (9). Hence, we only claim two equalities in (10). It is sufficient to show that $\beta\sqrt{d} = c\sigma(\beta) - b\beta$. Indeed, one has

$$\beta\sqrt{d} = \frac{acd}{\sigma(\beta)} = c\frac{\beta^2+\sigma(\beta)^2}{2\sigma(\beta)} = c\frac{(\beta+\sigma(\beta))^2 - 2\sigma(\beta)\beta}{2\sigma(\beta)} = c\frac{(\beta+\sigma(\beta))^2}{2\sigma(\beta)} - c\beta.$$

Moreover,

$$c\frac{(\beta+\sigma(\beta))^2}{2\sigma(\beta)} = c\frac{ad+ac\sqrt{d}}{\sqrt{ad+ab\sqrt{d}}} = c\sigma(\beta) + (c-b)\beta.$$

Therefore $\beta\sqrt{d} = c\sigma(\beta) - b\beta$. □

Lemma 2.9. *Let a, b, c, d, F, β in (2) and p be a prime number. Then:*

i) If $p \mid d$ then $p\mathcal{O}_F = P^4$ where $P = \langle p, \beta\rangle$ is the unique prime ideal of $\mathcal{O}_F$ above p.

ii) Assume that p is odd, $p \nmid abcd$ and d is not a quadratic residue modulo p. Then $p\mathcal{O}_F$ is inert in F.

iii) Assume that p is odd, $p \nmid abcd$ and d is a quadratic residue modulo p where z is such that $d \equiv z^2 \pmod{p}$.

If $ad + abz, ad - abz$ are quadratic residues modulo p with

$$ad + abz \equiv t_1^2, \quad ad - abz \equiv t_2^2 \pmod{p},$$

then $p\mathcal{O}_F$ totally splits in F, i.e, $p\mathcal{O}_F = P_1P_2P_3P_4$ where

$$P_1 = \langle p, \beta + t_1\rangle,\ P_2 = \langle p, \beta - t_1\rangle,\ P_3 = \langle p, \beta + t_2\rangle,\ P_4 = \langle p, \beta - t_2\rangle$$

are all prime ideals of $\mathcal{O}_F$ above p. Otherwise, $p\mathcal{O}_F = P_1P_2$ where

$$P_1 = \langle p, abz + ab\sqrt{d}\rangle,\ P_2 = \langle p, abz - ab\sqrt{d}\rangle$$

are all prime ideals above p.

Proof. In all the above cases, the prime p is not a divisor of index id_4 (see (5)). By using the result on the decomposition of primes [2, Theorem 4.8.13], the prime composition of $p\mathcal{O}_F$ can be obtained by factorizing $df(x)$ over $\mathbb{Z}_p$. Note that $df(x) = (x^2 - ad)^2 - a^2b^2d$.

i) If $p \mid d$, then $df(x) \equiv x^4 \pmod p$ and thus $p\mathcal{O}_F = P^4$ where $P = \langle p, \beta\rangle$ and P is a unique prime ideal above p.

ii) To prove ii, it is sufficient to prove $df(x)$ is irreducible in $\mathbb{Z}_p[x]$. By contradiction, suppose that the polynomial $df(x)$ is reducible over the field F_p. Since d is not a quadratic residue modulo p, $df(x)$ has no root in $\mathbb{Z}_p$. We now claim that $df(x)$ cannot be decomposed into the product of two quadratic polynomials. Indeed, if

$$df(x) \equiv \left(x^2 + Ax + B\right)\left(x^2 + Cx + D\right) \pmod p,$$

then

$$A + C \equiv 0,\ B + D + AC \equiv 2ad,\ AC + BD \equiv 0,\ BD \equiv a^2c^2d \pmod p.$$

This implies that

$$A \equiv -C,\ C\left(B - D\right) \equiv 0,\ BD \equiv a^2c^2d \pmod p.$$

The integer C must be nonzero because otherwise $BD = 0 = a^2c^2d$ and thus $p \mid acd$, contradicting the assumption that $p \nmid abcd$.

From $A \equiv -C \pmod p$, $C\left(B - D\right) \equiv 0 \pmod p$ and C being nonzero, one obtains $B \equiv D \pmod p$ and thus $D^2 \equiv BD \equiv a^2c^2d \pmod p$, which also contradicts the fact that d is a quadratic non-residue modulo p. This means $df(x)$ is irreducible over $\mathbb{Z}_p$ and hence $p\mathcal{O}_F$ is prime.

iii) One has

$$df(x) \equiv \left(x^2 - ad\right)^2 - a^2b^2z^2 \equiv \left(x^2 - (ad - abz)\right)\left(x^2 - (ad + abz)\right) \pmod p.$$

If $x^2 - (ad - abz)$ and $x^2 - (ad + abz)$ are irreducible over F_p, then $p\mathcal{O}_F = P_1P_2$ where $P_1 = \langle p, abz + ab\sqrt{d}\rangle, P_2 = \langle p, abz - ab\sqrt{d}\rangle$. Otherwise,

$$df(x) \equiv (x - t_1)(x + t_1)(x - t_2)(x + t_2) \pmod p.$$

Thus, $p\mathcal{O}_F = P_1P_2P_3P_4$ where

$$P_1 = \langle p, \beta + t_1\rangle,\ P_2 = \langle p, \beta - t_1\rangle,\ P_3 = \langle p, \beta + t_2\rangle,\ P_4 = \langle p, \beta - t_2\rangle$$

are all prime ideals of $\mathcal{O}_F$ above p.

□

In the Lemmas 2.10 and 2.11, we will consider prime divisors of the index of the field. In these cases, we cannot apply the result on the decomposition of primes [2, Theorem 4.8.13], instead, we can apply [2, Proposition 6.2.1].

Lemma 2.10. *Let a, b, c, d, F, K, β be as in (2) and p be a prime number. Then:*

i) Assume $p \mid a$. If d is a quadratic non-residue modulo p, then there is a unique prime ideal P above p and $p\mathcal{O}_F = P^2$. If d is a quadratic residue modulo p then there are exactly two prime ideals P_1, P_2 above p and $p\mathcal{O}_F = P_1^2 P_2^2$.

ii) Assume $p \mid c$ and $p \nmid a$. If $2a$ is a quadratic non-residue modulo p, then there are exactly two prime ideals P_1, P_2 above p and $p\mathcal{O}_F = P_1P_2$. In this case, $P_1 = \langle p, ad - ab\sqrt{d}\rangle$ and $P_2 = \langle p, ad + ab\sqrt{d}\rangle$. Otherwise, let $2a \equiv l^2 \pmod p$. Then $p\mathcal{O}_F = P_1P_2P_3P_4$ where P_1, P_2, P_3, P_4 are all prime ideals of $\mathcal{O}_F$ above p, with

$$P_1 = \langle p, \beta - lb\rangle,\ P_2 = \langle p, \beta + lb\rangle,\ P_3P_4 = \langle p, \beta^2\rangle,$$

and each ideal P_3 and P_4 is coprime with the ideals P_1 and P_2.

Proof. i) We have $p|a$, hence $p|\Delta_F$ by (4). Thus, p is ramified in F, i.e., one has that the prime decomposition of $p\mathcal{O}_F$ is of the form P^4, $P_1^2 Q P_2^2$ or P^2 where P, P_1, P_2 are prime ideals above p of $\mathcal{O}_F$ since F is Galois. On the other hand, we have $\gcd(a, d) = 1$, so $p \nmid d$ and $\left(\frac{d}{p}\right) \neq 0$ and therefore p is unramified in $K = \mathbb{Q}(\sqrt{d})$. As a result, $p\mathcal{O}_F$ is not of the form P^4 but instead $p\mathcal{O}_F = P_1^2P_2^2$ or $p\mathcal{O}_F = P^2$. Now, if d is a quadratic residue modulo p, it implies that p splits in K. It follows that $p\mathcal{O}_F = P_1^2P_2^2$. In the other cases, d is not a quadratic residue modulo p, which implies p is inert in K and hence $p\mathcal{O}_F = P^2$.

ii) If $p \mid c$ then $d \equiv b^2 \pmod p, b \not\equiv 0 \pmod p$ and thus $df(x) \equiv x^2\,(x^2 - 2ad) \pmod p$. If $2a$ is a quadratic non-residue modulo p, then $x^2 - 2ad$ is irreducible modulo p. By [2, Proposition 6.2.1], we have $p\mathcal{O}_F = P_1P_2$ where $P_1 = \langle p, \beta^2\rangle$, $P_2 = \langle p, \beta^2 - 2ad\rangle$ and P_1, P_2 are co-prime. Since $x^2 - 2ad$ is irreducible, P_2 is prime, and thus P_1 is also prime as F is Galois. Hence, there are only two prime ideals of $\mathcal{O}_F$ above p, namely P_1 and P_2. Similarly, considering the remaining case and by [2, Proposition 6.2.1], one has that $df(x) = (x - lb)\,(x + lb)\,x^2$ and $p\mathcal{O}_F = P_1P_2A$ where $P_1 = \langle p, \beta - lb\rangle, P_2 = \langle p, \beta + lb\rangle$, $A = \langle p, \beta^2\rangle$. Moreover, [2, Proposition 6.2.1] also yields that P_1, P_2 are prime and due to the Galois property of F, $A = P_3P_4$.

□

Lemma 2.11. *Let a, b, c, d, F, K, β be as in (2) and p be an odd prime divisor of b such that $p \nmid a$. Then:*

i) If a is a quadratic non-residue modulo p, then there are at most two prime ideals above p in $\mathcal{O}_F$ and $p\mathcal{O}_F$ is equal to the product of these prime ideals.

ii) If a is a quadratic residue modulo p, then there are at least two prime ideals above p in $\mathcal{O}_F$ and $p\mathcal{O}_F$ is equal to the product of these prime ideals.

Proof. One has $df(x) \equiv (x^2 - ad)^2 \pmod p$. We consider the first case in which $x^2 - ad$ is irreducible. According to [2, Proposition 6.2.1], if P is a prime ideal such that $P \mid p\mathcal{O}_F$, then $\mathbb{N}\,(P) = p^m$ where $m \geq 2$. This implies that $p\mathcal{O}_F$ is a product of at most two prime ideals. In the remaining case, $df(x)$ is the square of the product of two linear polynomials. By using [2, Proposition 6.2.1], $p\mathcal{O}_F$ is a product of two nontrivial coprime ideals. Hence, there are at least two prime ideals in the prime decomposition of $p\mathcal{O}_F$. □

The following lemma tells us the factorization of $2\mathcal{O}_F$ when Δ_F is even. In the case where Δ_F is odd, the factorization of $2\mathcal{O}_F$ will have one of the three forms: P, P_1P_2, or $P_1P_2P_3P_4$.

Lemma 2.12. *Assume that $2 \mid \Delta_F$. Then:*

i) If d is even, then there exists a unique prime ideal P_0 above 2 and $\mathbb{N}(P_0) = 2$.

ii) If $d \equiv 5 \pmod 8$, then there exists a unique prime ideal P_0 above 2 and $\mathbb{N}(P_0) = 4$.

iii) If $d \equiv 1 \pmod 8$, then $2\mathcal{O}_F = P_1^2P_2^2$, where P_1, P_2 are two distinct prime ideals and $\mathbb{N}(P_1) = \mathbb{N}(P_2) = 2$.

Proof. If d is even, then by Lemma 2.9.i), one has that $P_0 = \langle 2, \beta\rangle$ is a unique prime ideal above 2. If $d \equiv 1, 5 \pmod 8$, then 2 ramifies in F since $2 \mid \Delta_F$. Thus, the factorization of $2\mathcal{O}_F$ has one of the forms $R^4, R_1^2R_2^2, R^2$ for some prime ideals R, R_1, R_2 above 2 (since F is Galois). Let $K = \mathbb{Q}\left(\sqrt{d}\right)$. Then

$$df_K(x) = x^2 - x - \frac{d-1}{4}$$

is a defining polynomial of K and 2 does not ramify in K. Hence $2\mathcal{O}_F \neq R^4$. In the case where $d \equiv 5 \pmod 8$, $df_K(x)$ is irreducible modulo 2 and thus 2 is inert in K. Hence $2\mathcal{O}_F = R^2$. If $d \equiv 1 \pmod 8$ then $df_K(x)$ is reducible modulo 2 and thus 2 splits in K. Hence $2\mathcal{O}_F = P_1^2P_2^2$. □

3 Well-rounded ideal lattices of cyclic cubic fields

Let F be a cyclic cubic field with conductor m. In this section, we will find WR ideals of F and compute minimal bases of these ideals.

We denote by P_i the unique prime ideal above the prime $p_i \mid m$ for each $i \geq 0$ and α a root of the defining polynomial $df(x)$ as in (2). We will fix these notations for the whole section.

3.1 The case $9 \nmid m$

Let $m = p_1 \cdots p_r$ with $7 \leq p_1 < p_2 \cdots < p_r$, and $p_i \equiv 1 \pmod 3$ for all i and $r \geq 1$. In this section, we will show that:

1) the ideal $(P_1 \cdots P_r)^2$ is orthogonal and WR – this result has not been proven before; and

2) if $I \subset \{1, \ldots, r\}$, then $\prod_{i\in I} P_i$ is WR if and only if $\frac{m}{4} \leq \left(\prod_{i\in I} p_i\right)^2 \leq 4m$.

Lemma 3.1. *The sets* $\{\alpha, \sigma(\alpha), \sigma^2(\alpha)\}$ *and* $\{1, \alpha, \sigma(\alpha)\}$ *are two integral bases of* $\mathcal{O}_F$.

From now on, we will use one of the integral bases as mentioned in Lemma 3.1 depending on which one is convenient for our calculation.

By [24, page 166], also [9, page 2] and by [20], we obtain Lemma 3.2.

Lemma 3.2. *Let* $z = z_1\alpha + z_2\sigma(\alpha) + z_3\sigma^2(\alpha) \in \mathcal{O}_F$ *where* $z_i \in \mathbb{Z}, 1 \le i \le 3$. *Then*

$$\|z\|^2 = Tr(z^2) = m(z_1^2 + z_2^2 + z_3^2) + \frac{(1-m)(z_1+z_2+z_3)^2}{3}.$$

Moreover, one can rewrite this expression as

$$\|z\|^2 = \frac{m}{3}\left((z_1-z_2)^2 + (z_2-z_3)^2 + (z_3-z_1)^2\right) + \frac{1}{3}(z_1+z_2+z_3)^2.$$

Since α is a root of the defining polynomial $df(x)$ (see (2)), using [29, Proposition 2.2], one can show that $\mathrm{Tr}(\alpha) = 1$ and α is a shortest vector in $\mathcal{O}_F \backslash \mathbb{Z}$ with $\|\alpha\|^2 = \frac{2m+1}{3}$.

For $\ell \in \mathbb{Z}$ and $\ell > 0$, as in [8], we define

$$M_\ell = \{z = z_1\alpha + z_2\sigma(\alpha) + z_3\sigma^2(\alpha) \in \mathcal{O}_F : z_1 + z_2 + z_3 \equiv 0 \pmod{\ell}\}.$$

For all ℓ, the set M_ℓ is a $\mathbb{Z}$-module.

We remark that in [8], it is proved that the sublattice M_ℓ of $\mathcal{O}_F$ has index ℓ and it is WR if $\ell \equiv 1 \pmod 3$ and $\sqrt{\frac{m}{4}} \le \ell \le \sqrt{4m}$. Thus, if an ideal of $\mathcal{O}_F$ of norm satisfies these conditions, then that ideal is also WR. We prove the following.

Lemma 3.3. *The set* M_ℓ *is an ideal of* $\mathcal{O}_F$ *if and only if* $\ell | m$.

Proof. See Appendix A. □

Lemma 3.4. *Assume that* $p_i = 3n_i + 1$. *Then* $p_i\mathcal{O}_F = P_i^3$, *where* $P_i = \langle p_i, \alpha + n_i\rangle$ *is the unique prime ideal above* p_i. *Moreover, one has* $-\alpha + \sigma(\alpha) \in P_i$, $\|-\alpha + \sigma(\alpha)\|^2 = 2m$ *and* $\|\alpha + n_i\|^2 = \frac{2m+p_i^2}{3}$.

Proof. See Appendix A. □

Lemma 3.5. *We have* $M_{p_i} = P_i$. *As a consequence,* $p_i | Tr(z)$ *for all* $z \in P_i$.

Proof. When $p_i \mid m$, by Lemma (3.3), M_{p_i} is an ideal. Moreover, it is a prime ideal above p_i as its index is p_i. Therefore $M_{p_i} = P_i$. □

Lemma 3.6. *Let* $m = p_1 \cdots p_r$ $(r \ge 1)$ *and* $9 \nmid m$. *Let* $\rho = \alpha - \sigma(\alpha)$. *Then* $\rho \in P_i$ *for all* $i = 1, \ldots, r$ *and* $\|\rho^2\|^2 = Tr(\rho^4) = 2m^2$.

Proof. By Lemma 3.5, we have $P_i = \langle p_i, \alpha - n_i\rangle$. The statement $g \in P_i$ is implied from the equalities $\alpha - \sigma(\alpha) = (\alpha - n_i) + (\sigma(\alpha) - n_i)$ and $\sigma(P_i) = P_i$, $\forall i = 1, \ldots, r$.

Now, we compute $\|\rho^2\|^2$. First, one has

$$\|\rho^2\|^2 = (\alpha - \sigma(\alpha))^4 + (\sigma(\alpha) - \sigma^2(\alpha))^4 + (\sigma^2(\alpha) - \alpha)^4. \tag{11}$$

The right side of (11) is a symmetric polynomial in the variables

$$\delta_1 = \alpha + \sigma(\alpha) + \sigma^2(\alpha) = 1,$$
$$\delta_2 = \alpha\sigma(\alpha) + \sigma(\alpha)\sigma^2(\alpha) + \sigma^2(\alpha)\alpha = \frac{1-m}{3},$$
$$\delta_3 = \alpha\sigma(\alpha)\sigma^2(\alpha) = \frac{m(a-3)+1}{27}.$$

Expressing it in terms of these, one deduces $\|\rho^2\|^2 = 2m^2$. □

The following result is new and has not been studied before. We remark that our WR lattice P in Proposition 3.7 is not one of the sublattices mentioned in [7, Theorem 4.9] since its norm is m^2.

Proposition 3.7. *Let $m = p_1 \cdots p_r$ where $r \geq 1$ and let $P = P_1 \cdots P_r$. Then P^2 is an orthogonal WR ideal lattice with a minimal basis $\{\kappa, \sigma(\kappa), \sigma^2(\kappa)\}$, where the element $\kappa = m - (\alpha - \sigma(\alpha))^2$.*

Proof. One has $Tr(\kappa) = m$ and $\|\kappa\|^2 = m^2$. By Lemma 2.5, the set $\{\kappa, \sigma(\kappa), \sigma^2(\kappa)\}$ is $\mathbb{R}-$linearly independent. It is clear $m \in P^2$ and thus $\kappa \in P^2$ by Lemma 3.4.

Now, we prove κ is a shortest vector in P^2. First, consider the sublattice of P^2 defined as $L = \mathbb{Z}\kappa + \mathbb{Z}\sigma(\kappa) + \mathbb{Z}\sigma^2(\kappa)\mathbb{Z}$. We remark that $\kappa + \sigma(\kappa) = \mathrm{Tr}(\kappa) - \sigma^2(\kappa) = (\alpha - \sigma^2(\alpha))^2$. It leads to

$$\|\kappa\|^2 + \|\sigma(\kappa)\|^2 + 2\mathrm{Tr}(\kappa\sigma(\kappa)) = \|(\alpha - \sigma^2(\alpha))^2\| = 2m^2 \tag{12}$$

by Lemma 3.6. Since $\|\kappa\|^2 = \|\sigma(\kappa)\|^2 = m^2$, the equality in equation (12) implies that $\mathrm{Tr}(\kappa\sigma(\kappa)) = 0$. It follows that $\kappa, \sigma(\kappa), \sigma^2(\kappa)$ are pairwise orthogonal. As a consequence, $\det(L) = m^3 = \det(P^2)$ and κ is a shortest vector of L. By Lemma 2.3, one has $L = P^2$. Thus, P^2 is an orthogonal WR ideal lattice with a minimal basis $\{\kappa, \sigma(\kappa), \sigma^2(\kappa)\}$. □

Let I be a non-empty subset of set $\{1, \ldots, r\}$, $p_I = \prod_{i\in I} p_i$ and $P_I = \prod_{i\in I} P_i$. As a consequence of Lemma 3.5, $P_I = M_{p_I}$. By [9, Theorem 4.1], if $p_I \in \left[\frac{\sqrt{m}}{2}, 2\sqrt{m}\right]$ then P_I is WR. Moreover, by using a different technique, independent of the proof of [9, Theorem 4.1], we can prove a stronger result: the condition $p_I \in \left[\frac{\sqrt{m}}{2}, 2\sqrt{m}\right]$ is not only necessary but also sufficient for P_I to be WR.

Proposition 3.8. *Let $m = p_1 \cdots p_r$ be the conductor of F and let P_i be the prime ideals above p_i for all $i = 1, \ldots, r$. For each nonempty subset I of $\{1, \ldots, r\}$, let $P_I = \prod_{i\in I} P_i$, $p_I = \prod_{i\in I} p_i$ and $n_I = \frac{p_I - 1}{3}$. Then P_I is WR if and only if $\frac{m}{4} \leq p_I^2 \leq 4m$. In this case, P_I has a minimal basis $\alpha + n_I, \sigma(\alpha) + n_I, \sigma^2(\alpha) + n_I$.*

Proof. By Lemma 3.4, $P_i = \langle p_i, \alpha + n_i \rangle$ where $n_i = \frac{p_i - 1}{3}$ for all $i \in I$. This implies that

$$\mathbb{Z}\left(\alpha + n_I\right) + \mathbb{Z}\left(\sigma(\alpha) + n_I\right) + \mathbb{Z}\left(\sigma^2(\alpha) + n_I\right) \subset P_I.$$

Moreover, this sublattice of P_I and P_I have the same indices in $\mathcal{O}_F$ and thus

$$P_I = \mathbb{Z}\left(\alpha + n_I\right) + \mathbb{Z}\left(\sigma(\alpha) + n_I\right) + \mathbb{Z}\left(\sigma^2(\alpha) + n_I\right).$$

Let δ be a nonzero vector of P_I. There exist integers x_1, x_2, x_3 such that

$$\delta = x_1\left(\alpha + n_I\right) + x_2\left(\sigma(\alpha) + n_I\right) + x_3\left(\sigma^2(\alpha) + n_I\right).$$

By Lemma 3.2, we have

$$\|\delta\|^2 = \frac{m}{3}\left((x_1 - x_2)^2 + (x_2 - x_3)^2 + (x_3 - x_1)^2\right) + \frac{(3n_I + 1)^2}{3}\left(x_1 + x_2 + x_3\right)^2.$$

Now, we will find the minimum value of $\|\delta\|^2$ when $\delta \neq 0$. Note that $z_1 z_2 z_3 \neq 0$. We consider all cases as below.

(i) If $z_1 + z_2 + z_3 = 0$, then

$$(z_1 - z_2)^2 + (z_2 - z_3)^2 + (z_3 - z_1)^2 \geq 2.$$

Here $(z_1 - z_2)^2 + (z_2 - z_3)^2 + (z_3 - z_1)^2$ is an even non-negative integer. If

$$(z_1 - z_2)^2 + (z_2 - z_3)^2 + (z_3 - z_1)^2 \in \{2, 4\},$$

then two of the three numbers z_1, z_2, z_3 are zero. Without loss of generality, we can assume $z_1 = z_2$. This implies that $z_3 = -2z_1$ and thus $(z_1 - z_2)^2 + (z_2 - z_3)^2 + (z_3 - z_1)^2$ is a multiple of 9. Hence,

$$(z_1 - z_2)^2 + (z_2 - z_3)^2 + (z_3 - z_1)^2 \geq 6,$$

and therefore, $\|\delta\|^2 \geq 2m$ in this case. The equality occurs if and only if

$$\delta \in \{\pm\left(\alpha - \sigma(\alpha)\right), \pm\left(\sigma(\alpha) - \sigma^2(\alpha)\right), \pm\left(\sigma^2(\alpha) - \alpha\right)\}.$$

(ii) If $(z_1 - z_2)^2 + (z_2 - z_3)^2 + (z_3 - z_1)^2 = 0$, then $z_1 = z_2 = z_3 = z \in \mathbb{Z}$ and thus $\delta = 3zp_I$. Hence $\|\delta\|^2 \geq 3p_I^2$. The equality occurs if and only if $\delta \in \{\pm p_I\}$.

(iii) If $z_1 + z_2 + z_3 \neq 0$ and $(z_1 - z_2)^2 + (z_2 - z_3)^2 + (z_3 - z_1)^2 \neq 0$, then $(z_1 + z_2 + z_3)^2 \geq 1$ and $(z_1 - z_2)^2 + (z_2 - z_3)^2 + (z_3 - z_1)^2 \geq 2$. Thus $\|\delta\|^2 \geq \frac{p_I^2 + 2m}{3}$. The equality occurs if and only if

$$\delta \in \{\pm\left(\alpha + n_I\right), \pm\left(\sigma(\alpha) + n_I\right), \pm\left(\sigma^2(\alpha) + n_I\right)\}.$$

Therefore, we conclude that P_I is WR if and only if $\frac{2m + p_I^2}{3} \leq \min\{2m, 3p_I^2\}$, which is equivalent to $\frac{m}{4} \leq p_I^2 \leq 4m$. □

3.2 The case $9 \mid m$

Let $m = p_0^2 p_1 \cdots p_r$ where $3 = p_0 < p_1 < p_2 \cdots < p_r$ and $r \geq 0$. For each nonempty subset I of $\{1 \cdots, r\}$, we denote $P_I = \prod_{i \in I} P_i$. In this section, we will show that:

i) if $m = 9$, then P_0 is WR;

ii) the ideal $P_0(P_1 \cdots P_r)^2$ is orthogonal and WR;

iii) if I is a nonempty subset of $\{1, 2, \cdots, r\}$, then $P_0 P_I$ is WR if and only if $\frac{m}{36} \leq p_I^2 \leq \frac{4m}{9}$; and

iv) if $r \geq 2$ and I, J are two nonempty and disjoint subsets of $\{1, 2, \cdots, r\}$, then $P_0 P_I^2 P_J$ is WR if and only if $\frac{m}{36} \leq p_I p_J^2 \leq \frac{4m}{9}$. The field F is not tame, and hence is not studied in [7] and [8]. Indeed, all of our results in this subsection are new and have not been investigated before.

By [20], one has $\{1, \alpha, \sigma(\alpha)\}$ is an integral basis. It can be easily verified that α satisfies $\|\alpha\|^2 = \frac{2m}{3}$ and thus it is a shortest vector in $\mathcal{O}_F \backslash \mathbb{Z}$ (see [29] for more details).

Lemma 3.9. *Let $m = 9p_1 \cdots p_r$ where $r \geq 0$. Then $p_i \mathcal{O}_F = P_i^3$ where P_i is the unique prime ideal above p_i. Moreover, $P_0 = \langle 3, \alpha - 1 \rangle$ and $P_i = \langle p_i, \alpha \rangle$ for all $1 \leq i \leq r$.*

Proof. To compute generators for P_i we can apply the decomposition of primes [2, Theorem 4.8.13] since Lemma 2.4 says that p_i does not divide the index $[\mathcal{O}_F : \mathbb{Z}[\alpha]]$. In other words, the result is obtained by factoring the defining polynomial $df(x)$ over the finite field F_{p_i} and by using the fact that $p_i | m$, and $a \equiv 6 \pmod 9$. □

In case $m > 9$, using Lemma 3.9 and the fact that $\frac{2m}{3} > 27 = \|3\|^2$ leads to the following.

Corollary 3.10. *Let $m > 9$. Then the vector α is a shortest vector in the set $P_i \backslash \mathbb{Z}$ for all $1 \leq i \leq r$, and $\|\alpha\|^2 = \frac{2m}{3}$. In the ideal P_0, the element p_0 is shortest and $\|p_0\|^2 = 27$.*

Proposition 3.11. *Let $m = 9$. Then P_0 is orthogonal and WR with a minimal basis $\{\alpha - 1, \sigma(\alpha) - 1, \sigma^2(\alpha) - 1\}$.*

Proof. Note that $\alpha - 1 \in P_0$ and this element has trace -3 since $\mathrm{Tr}(\alpha) = 0$, thus the three elements $\alpha - 1$, $\sigma(\alpha) - 1$ and $\sigma^2(\alpha) - 1$ are all in P_0 and are linearly independent by Lemma 2.5. To show that P_0 is WR, it is sufficient to show that $\alpha - 1$ is shortest in P_0.

We have that $\|\alpha - 1\|^2 = \|\alpha\|^2 + \|-1\|^2 = \frac{2m}{3} + 3 = 9$ because α has trace 0. One can easily compute all the shortest vectors of the ideal lattice P_0 (see the Fincke–Pohst algorithm – Algorithm 2.12 in [10]) and verify that $\alpha - 1$ is indeed shortest in P_0. □

Lemma 3.2 cannot be applied to the case $9 \mid m$. Therefore, we recalculate the length of vectors in $\mathcal{O}_F$ in this case as follows.

Lemma 3.12. *Let* $\delta = m_1 + m_2\alpha + m_3\sigma(\alpha) \in \mathcal{O}_F$. *Then*

$$\|\delta\|^2 = 3m_1^2 + \frac{2m}{3}(m_2^2 + m_3^2 - m_2m_3).$$

Proof. See Appendix A. □

Next, we claim that P_0P^2 is an orthogonal and WR lattice where $P = P_1 \cdots P_r$ and $r \geq 1$. To prove that, we need some Lemmas below.

Lemma 3.13. *For all* $1 \leq i \leq r$, *we have* $P_i = \mathbb{Z}p_i \oplus \mathbb{Z}\alpha \oplus \mathbb{Z}\sigma(\alpha)$.

Proof. It is clear that $L_i = \mathbb{Z}p_i \oplus \mathbb{Z}\alpha \oplus \mathbb{Z}\sigma(\alpha)$ is the sublattice of P_i and $\det(L_i) = \det(P_i)$. Therefore $P_i = L_i$ by Lemma 2.3. □

By using the same technique as in the proof of Lemma 3.13, one has the following result.

Corollary 3.14. *Let* I *be a subset of* $\{1, \dots, r\}$. *Then* $P_I = \mathbb{Z}p_I + \mathbb{Z}\alpha + \mathbb{Z}\sigma(\alpha)$. *In particular,* $P_1 \cdots P_r = \mathbb{Z}\frac{m}{9} \oplus \mathbb{Z}\alpha \oplus \mathbb{Z}\sigma(\alpha)$.

Proposition 3.15. *Let* I *be a subset of* $\{1, \dots, r\}$. *Then* P_I *is not WR.*

Proof. By Corollary 3.14, we have $P_I = \mathbb{Z}p_I + \mathbb{Z}\alpha + \mathbb{Z}\sigma(\alpha)$. If we let $\delta \in P_I$, then $\delta = z_1p_I + z_2\alpha + z_3\sigma(\alpha)$ where $z_1, z_2, z_3 \in \mathbb{Z}$. By applying Lemma 3.12, one obtains

$$\|\delta\|^2 = 3z_1^2p_I^2 + \frac{2m}{3}(z_2^2 + z_3^2 - z_2z_3).$$

Now, we will find the minimum value of $\|\delta\|^2$ when $\delta \neq 0$. We consider all cases as below.

1. If $z_1 = 0$, then $\|\delta\|^2 \geq \frac{2m}{3}$ (since $z_2^2 + z_3^2 - z_2z_3 \geq 1$), here the equality occurs when $z_2 = 1, z_3 = 0$ or $z_2 = 0, z_3 = 1$, therefore $\delta \in \{\alpha, \sigma(\alpha)\}$.
2. If $z_1 \neq 0$, then $\|\delta\|^2 \geq 3z_1^2p_I^2 + \frac{2m}{3}(z_2^2 + z_3^2 - z_2z_3) \geq 3z_1^2p_I^2 \geq 3p_I^2$, here the equality occurs when $z_2 = z_3 = 0, z_1 = 1$ and thus $\delta = p_I$.

In conclusion, $\min_{\delta\neq 0} \|\delta\| \in \{\|\alpha\|^2, \|p_I\|^2\} = \left\{\frac{2m}{3}, 3p_I^2\right\}$. Note that $\frac{2m}{3} \neq 3p_I^2$, so in the case $\|p_I\|^2 < \|\alpha\|^2$, we have $\pm p_I$ are the only two shortest vectors in P_I. Therefore, P_I is not WR. In another case $\|p_I\|^2 > \|\alpha\|^2$ and hence α is shortest in P_I.

We will next compute the set of all shortest vectors L of P_I. Let $\delta \in \mathcal{O}_F$ such that $\|\delta\| = \|\alpha\|$. Since $\mathcal{O}_F = \mathbb{Z} \oplus \mathbb{Z}[\sigma] \cdot \alpha$ (see [29, Proposition 2.2 and Proposition 2.3]), we can show easily that $\delta \in L = \{\pm\alpha, \pm\sigma(\alpha), \pm\sigma^2(\alpha)\}$. Moreover, one can observe that $\mathrm{Tr}(\alpha) = \alpha + \sigma(\alpha) + \sigma^2(\alpha) = 0$ and $\{\alpha, \sigma(\alpha), \alpha^2(\alpha)\}$ linearly dependent. Therefore, there does not exist three independent vectors from L. In other words, P_I is not WR. □

Lemma 3.16. *There exist integers* A, B *such that*

$$A^2 - AB + B^2 = \frac{m}{9}, \text{ and } \alpha^2 = \frac{2m}{9} + A\alpha + B\sigma(\alpha).$$

Proof. See Appendix A. □

Lemma 3.17. *Let α, A, B be in Lemma 3.16 and let $\kappa = \frac{m}{9} + A\alpha + B\sigma(\alpha)$. Then $P_0(P_1 \cdots P_r)^2 = \mathbb{Z}\kappa \oplus \mathbb{Z}\sigma(\kappa) \oplus \mathbb{Z}\sigma^2(\kappa)$.*

Proof. It is clear that the two lattices $P_0(P_1 \cdots P_r)$ and $\mathbb{Z}\kappa \oplus \mathbb{Z}\sigma(\kappa) \oplus \mathbb{Z}\sigma^2(\kappa)$ have the same index in $\mathcal{O}_F$ and thus it is sufficient to prove that $\mathbb{Z}\kappa \oplus \mathbb{Z}\sigma(\kappa) \oplus \mathbb{Z}\sigma^2(\kappa)$ is a sublattice of $P_0(P_1 \cdots P_r)$. It is obvious that $\frac{m}{9} \in (P_1 \cdots P_r)^2$. Since $\kappa = \alpha^2 - \frac{m}{9}$, one has $\kappa \in (P_1 \cdots P_r)^2$. Moreover,

$$\kappa = \alpha^2 - \frac{m}{9} = (\alpha - 1)(\alpha + 1) + (p_1 \cdots p_r - 1) \in P_0$$

as $P_0 = \langle 3, \alpha - 1 \rangle$ and $p_1 \equiv 1 \pmod 3$. Hence, $\kappa \in P_0(P_1 \cdots P_r)^2$. As a consequence, $\sigma(\kappa), \sigma^2(\kappa) \in P_0(P_1 \cdots P_r)^2$. □

Lemma 3.17 gives us an integral basis of $P_0(P_1 \cdots P_r)^2$. Let

$$\delta = z_1\kappa + z_2\sigma(\kappa) + z_3\sigma^2(\kappa) \in P_0(P_1 \cdots P_r)^2.$$

One has

$$\delta = \frac{m}{9}(z_1 + z_2 + z_3) + (Az_1 - Bz_2 + (B - A)z_3)\alpha + (Bz_1 + (A - B)z_2 - Az_3)\sigma(\alpha).$$

We then apply Lemma 3.12, to obtain that

$$\|\delta\|^2 = \frac{m^2}{27}(z_1 + z_2 + z_3)^2 + \frac{2m}{3}(A^2 - AB + B^2)(z_1^2 + z_2^2 + z_3^2 - z_1z_2 - z_1z_3 - z_2z_3). \quad (13)$$

Since $\frac{m}{9} = A^2 - AB + B^2$, the following result follows.

Proposition 3.18. *The ideal $P_0(P_1 \cdots P_r)^2$ is orthogonal and WR with a minimal basis $\{\kappa, \sigma(\kappa), \sigma^2(\kappa)\}$ with κ as in Lemma 3.17.*

Proof. Let $\delta \in P_0(P_1 \cdots P_r)^2$. Then there exist integers z_1, z_2, z_3 such that we can express δ as $\delta = z_1\kappa + z_2\sigma(\kappa) + z_3\sigma^2(\kappa)$ by Lemma 3.17. Since $\frac{m}{9} = A^2 - AB + B^2$, the equality in (13) implies that

$$\|\delta\|^2 = \frac{m}{9}(z_1^2 + z_2^2 + z_3^2).$$

When $\delta \neq 0$, it is clear that $\|\delta\|^2 \geq \frac{m^2}{9}$ as at least one of z_1, z_2, z_3 is a nonzero integer. Equality holds if and only if $\delta \in \{\pm\kappa, \pm\sigma(\kappa), \pm\sigma^2(\kappa)\}$. Hence $\{\pm\kappa, \pm\sigma(\kappa), \pm\sigma^2(\kappa)\}$ is the set of all shortest vectors of $P_0(P_1 \cdots P_r)^2$. Therefore, $P_0(P_1 \cdots P_r)^2$ is WR. Moreover, we can verify that $\mathrm{Tr}\,(\kappa\sigma\,(\kappa)) = 0$ and thus $P_0(P_1 \cdots P_r)^2$ is also orthogonal. □

From now on, for each nonempty subset I of $\{1, 2, \cdots, r\}$, we denote by $p_I = \prod_{i \in I} p_i$ and $P_I = \prod_{i \in I} P_i$.

For each $i \in \{1, \ldots, r\}$, let $\rho_i = p_i + \alpha + \sigma(\alpha)$. Since

$$\rho_i = (p_i - 1) + (\alpha - 1) + (\sigma(\alpha) - 1) \in P_0$$

and clearly $p_i \in P_i$, then $\rho_i \in P_0 P_i$. Hence $\mathbb{Z}\rho_i + \mathbb{Z}\sigma(\rho_i) + \mathbb{Z}\sigma^2(\rho_i)$ is a sublattice of $P_0 P_i$ and this sublattice has the same determinant as the one of $P_0 P_i$. Therefore, we have that $\mathbb{Z}\rho_i + \mathbb{Z}\sigma(\rho_i) + \mathbb{Z}\sigma^2(\rho_i) = P_0 P_i$.

By using the same argument, we can prove the following lemma.

Lemma 3.19. *Let $r \geq 1$ and I be a nonempty subset of $\{1, \ldots, r\}$ and let $\rho_I = p_I + \alpha + \sigma(\alpha)$. Then $P_I = \mathbb{Z}\rho_I \oplus \mathbb{Z}\sigma(\rho_I) \oplus \mathbb{Z}\sigma^2(\rho_I)$. In particular, $P_0 P_1 \cdots P_r = \mathbb{Z}\rho \oplus \mathbb{Z}\sigma(\rho) \oplus \mathbb{Z}\sigma^2(\rho)$ where $\rho = \frac{m}{9} + \alpha + \sigma(\alpha)$.*

The following proposition shows the necessary and sufficient conditions for the ideal $P_0 P_I^2$ of a given subset I of $\{1, 2, \cdots, r\}$ to be a WR lattice.

Proposition 3.20. *Let I be a nonempty subset of $\{1, 2 \cdots, r\}$. The ideal $P_0 P_I$ is WR if and only if $\frac{m}{36} \leq p_I^2 \leq \frac{4m}{9}$. In this case, a minimal basis of $P_0 P_I$ is $\{\rho_I, \sigma(\rho_I), \sigma^2(\rho_I)\}$ where $\rho_I = p_I + \alpha + \sigma(\alpha)$.*

Proof. By Lemma 3.19, $P_I = \mathbb{Z}\rho_I \oplus \mathbb{Z}\sigma(\rho_I) \oplus \mathbb{Z}\sigma^2(\rho_I)$. Let $\delta = z_1\rho_I + z_2\sigma(\rho_I) + z_3\sigma^2(\rho_I)$. Lemma 3.12 states that

$$\|\delta\|^2 = 3p_I^2(z_1 + z_2 + z_3)^2 + \frac{m}{3}\left((z_1 - z_2)^2 + (z_2 - z_3)^2 + (z_3 - z_1)^2\right).$$

Now, we will find the minimum value of $\|\delta\|^2$ when $\delta \neq 0$. We consider all cases as below.

(i) If $z_1 + z_2 + z_3 = 0$, then

$$(z_1 - z_2)^2 + (z_2 - z_3)^2 + (z_3 - z_1)^2 \geq 2.$$

Note that the expression on the left hand side is an even positive integer. If

$$(z_1 - z_2)^2 + (z_2 - z_3)^2 + (z_3 - z_1)^2 \in \{2, 4\},$$

then two of the three numbers z_1, z_2, z_3 are zero. Without loss of generality, we can assume $z_1 = z_2$. This implies that $z_3 = -2z_1$ and thus the expression is a multiple of 9. Hence

$$(z_1 - z_2)^2 + (z_2 - z_3)^2 + (z_3 - z_1)^2 \geq 6.$$

Therefore, $\|\delta\| \geq 2m$ in this case. The equality occurs if and only if

$$\delta \in \{\pm(\alpha - \sigma(\alpha)), \pm(\alpha - \sigma^2(\alpha)), \pm(\sigma(\alpha) - \sigma^2(\alpha))\}$$

(ii) If $(z_1 - z_2)^2 + (z_2 - z_3)^2 + (z_3 - z_1)^2 = 0$, then $z_1 = z_2 = z_3 = z \in \mathbb{Z}$ and thus $\delta = 3zp_I$. Hence $\|\delta\|^2 \geq 27p_I^2$. The equality occurs if and only if $\delta \in \{\pm 3p_I\}$.

(iii) If $z_1+z_2+z_3 \neq 0$ and $(z_1-z_2)^2+(z_2-z_3)^2+(z_3-z_1)^2 \neq 0$, then $(z_1+z_2+z_3)^2 \geq 1$ and

$$(z_1-z_2)^2+(z_2-z_3)^2+(z_3-z_1)^2 \geq 2.$$

Thus $\|\delta\|^2 \geq 3p_I^2+\frac{2m}{3}$. The equality occurs if and only if $\delta \in \{\pm g_I, \pm\sigma(g_I), \pm\sigma^2(g_I)\}$.

This implies that $\min_{\delta\neq 0}\|g\|^2 = \min\left\{2m, 27p_I^2, 3p_I^2+\frac{2m}{3}\right\}$. Since $\mathrm{Tr}(\rho_I) \neq 0$, the ideal P_0P_I is WR if and only if $\min_{\delta\neq 0}\|\delta\|^2 = 3p_I^2+\frac{2m}{3}$. It is equivalent to the statement $3p_I^2+\frac{2m}{3} \leq 2m$ and $3p_I^2 \leq 27p_I^2$. These inequalities occur if and only if $\frac{m}{36} \leq p_I^2 \leq \frac{4m}{9}$. □

Using Proposition 3.20 for $I=\{1,\cdots,r\}$, we have the following result.

Corollary 3.21. *Let $r \geq 1$. Then the ideal $P_0P_1\cdots P_r$ is not WR.*

Let I, J be two disjoint nonempty subsets of $\{1,2,\cdots,r\}$. Now, we show the necessary and sufficient condition for $P_0P_I^2P_J$ to be a WR lattice (Proposition 3.25).

Let $\xi_3 = \frac{-1-\sqrt{-3}}{2}$ be a primitive cube root of 1 and $K' = \mathbb{Q}(\xi_3)$. The minimal polynomial of ξ_3 is x^2+x+1. For each $i \in \{1,\ldots,r\}$, the polynomial x^2+x+1 has a root modulo p_i. It means $\mathcal{O}_{K'}$ has an ideal $\mathcal{P}_i$ of $\mathcal{O}_{K'}$ of norm p_i. For each subset I of $\{1,\ldots,r\}$, let $\mathcal{P}_I = \prod_{i\in I}\mathcal{P}_i$. Then $\mathcal{P}_I$ is an ideal of $\mathcal{O}_{K'}$ norm p_I. Moreover, since $\mathcal{O}_{K'}$ is a PID, then there exist integers x_I, y_I such that $\mathcal{P}_I = \langle x_I+y_I\xi_3\rangle$ and thus $p_I = \mathbb{N}(x_I+y_I\xi_3) = x_I^2-x_Iy_I+y_I^2$. In other words, the following result has been deduced.

Lemma 3.22. *For each nonempty subset I of $\{1,\ldots,r\}$, there exist integers x_I, y_I such that $x_I+y_I+1 \equiv 0 \pmod 3$ and $p_I = x_I^2-x_Iy_I+y_I^2$.*

Lemma 3.23. *Let $r \geq 2$ and $N = p_1\cdots p_r$ where p_i is a prime such that $p_i \equiv 1 \pmod 3$ for each $i \in \{1,\ldots,r\}$. Assume that $N = A^2-AB+B^2$ where A, B are integers that $A+B+1 \equiv 0 \pmod 3$. For each nonempty subset I of $\{1,\ldots,r\}$, let $p_I = \prod_{i\in I}p_i$. Then there exist integers x_I, y_I such that*

$$x_I+y_I+1 \equiv 0 \pmod 3, \quad p_I = x_I^2-x_Iy_I+y_I^2$$
$$p_I \mid (Ax_I-By_I-Ay_I), \quad p_I \mid (Bx_I-Ay_I).$$

Proof. See Appendix A. □

Lemma 3.24. *Let $N = \frac{m}{9} = p_1\cdots p_r = A^2-AB+B^2$ where A and B as in Lemma 3.16. With the notation in Lemma 3.23, one has $p_I^2 \mid \mathbb{N}_{K/\mathbb{Q}}(x_I\alpha+y_I\sigma(\alpha))$. In particular, $x_I\alpha+y_I\sigma(\alpha) \in P_I^2$.*

Proof. See Appendix A. □

Proposition 3.25. *Let $r \geq 2$ and I, J be two disjoint nonempty subsets of $\{1,2,\cdots,r\}$. The ideal $P_0P_I^2P_J$ is WR if and only if $\frac{m}{36} \leq p_I^2p_J \leq \frac{4m}{9}$. In this case, $P_0P_IP_J^2$ has a minimal basis $\{\kappa_{IJ}, \sigma(\kappa_{IJ}), \sigma^2(\kappa_{IJ}\}$ where $\kappa_{IJ} = p_{IJ}+x_I+y_I$ and x_I and y_I are given in Lemma 3.23.*

Proof. With x_I, y_I in Lemma 3.24, one has $x_I\alpha + y_I\sigma(\alpha) \in P_I^2$. By Corollary 3.14, we have $x_I\alpha + y_I\sigma(\alpha) \in P_J$. Thus $\kappa_{IJ} \in P_I^2 P_J$ as I, J are disjoint. Moreover, $\kappa_{IJ} \in P_0$ as

$$\kappa_{IJ} = (p_I p_J - 1) + (\alpha - 1)x_I + (\sigma(\alpha) - 1)y_I + (x_I + y_I + 1)$$

and $P_0 = \langle 3, \alpha - 1\rangle, \sigma(P_0) = P_0$ and $3 \mid (x_I + y_I + 1)$ by Lemma 3.23. Hence $\kappa_{IJ} \in P_0 P_I^2 P_J$ and thus $L_{IJ} = \mathbb{Z}\kappa_{IJ} \oplus \mathbb{Z}\sigma(\kappa_{IJ}) \oplus \mathbb{Z}\sigma^2(h_{IJ})$ is a sublattice of $P_0 P_I^2 P_J$. It is easy to verify that $\det(L_{IJ}) = \det(P_0 P_I^2 P_J)$ and thus $L_{IJ} = P_0 P_I^2 P_J$ by Lemma 2.3.

Let $\delta = z_1\kappa_{IJ} + z_2\sigma(\kappa_{IJ}) + z_3\sigma^2(\kappa_{IJ})$ be a nonzero vector of $P_0 P_I^2 P_J$. We can write

$$\begin{aligned}\delta = p_I p_J \left(z_1 + z_2 + z_3\right) + \left(x_I z_1 - y_I z_2 + \left(y_I - x_I\right) z_3\right) \alpha \\ + \left(y_I z_1 + \left(x_I - y_I\right) z_2 - x_I z_3\right) \sigma(\alpha)\end{aligned}$$

and hence by Lemma 3.12

$$\|\delta\|^2 = 3p_I^2 p_J^2 \left(z_1 + z_2 + z_3\right)^2 + \frac{2m}{3} \prod_{i \in I} p_i \left(z_1^2 + z_2^2 + z_3^2 - z_1 z_2 - z_2 z_3 - z_1 z_3\right).$$

By using a similar argument as the one in the proof of Proposition 3.20, one has

$$\min_{\delta \neq 0} \|\delta\|^2 = \min \left\{27 p_I^2 p_J^2, 2m p_I, 3p_I^2 p_J^2 + \frac{2m}{3} p_I\right\},$$

and the lattice $P_0 P_I^2 P_J$ is WR if and only if $\min_{\delta \neq 0} \|\delta\|^2 = 3p_I^2 p_J^2 + \frac{2m}{3} p_I$. It is equivalent to the statement

$$3p_I^2 p_J^2 + \frac{2m}{3} p_I \leq 27 p_I^2 p_J^2 \text{ and } 3p_I^2 p_J^2 + \frac{2m}{3} p_I \leq 2m p_I.$$

In other words, $P_0 P_I^2 P_J$ is WR if and only if $\frac{m}{36} \leq p_I p_J^2 \leq \frac{4m}{9}$. □

4 Well-rounded ideal lattices of cyclic quartic fields

In this section, we denote by F a cyclic quartic field defined by (a, b, c, d) as in Section 2.3. We fix the notation where $d = b^2 + c^2$, $\gcd(a, d) = 1$ and a, d are squarefree. Let $d = p_1 \cdots p_r$ and $a = sign(a) q_1 \cdots q_s$ be the factorizations of d and a where $sign(a) = 1$ if $a > 0$ and $sign(a) = -1$ otherwise. Note that all p_i and q_j are distinct since a and d are squarefree and $\gcd(a, d) = 1$. For each subset I of $\{1, \ldots, r\}$, let $p_I = \prod_{i \in I} p_i$ and $P_I = \prod_{i \in I} P_I$ where P_i is the unique prime ideal of $\mathcal{O}_F$ above p_i by Lemma 2.9, i) for all $i \in I$. In the case $I = \emptyset$, we define $p_I = 1$ and $P_I = \mathcal{O}_K$. If J is a subset of $\{1, \ldots, s\}$, we denote $q_J = \prod_{j \in J} q_j$. Let J be any subset of $\{1, \ldots, s\}$ such that for each $j \in J$, there is a unique prime ideal Q_j above q_j. In that case, we denote by $Q_J = \prod_{j \in J} Q_j$.

4.1 Prime decomposition of $p\mathcal{O}_F$ and integral bases of ideals of F

In this subsection, we provide a number of results concerning the prime factorization of the ideal $p\mathcal{O}_F$ for an arbitrary prime number p. Especially, we aim to classify all odd primes p based on the decomposition of $p\mathcal{O}_F$ (see Theorem 4.18). In addition, we construct integral bases for certain ideals of $\mathcal{O}_F$ which can be used to prove the well-roundness of ideals in Section 4.2.

By [3, Theorem 1.3], a prime p ramifies in F if and only if $p \mid \Delta_F$. In this case, by the Lemmas 2.9 and 2.10, the decomposition of $p\mathcal{O}_F$ is given as below.

- If $p \mid d$, then $p\mathcal{O}_F = P^4$ where P is a unique prime ideal of $\mathcal{O}_F$ above p.
- If $p \mid a$ and d is a quadratic non-residue modulo p, then $p\mathcal{O}_F = P^2$ where P is a unique prime ideal of $\mathcal{O}_F$ above p.
- If $p \mid a$ and d is a quadratic residue modulo p, then $p\mathcal{O}_F = P_1^2 P_2^2$ where P_1, P_2 are two distinct prime ideals of $\mathcal{O}_F$ above p.

Lemmas 2.9 and 2.10 show the prime decomposition of $p\mathcal{O}_F$ where $p \mid ac$. Furthermore, if $p \nmid abcd$, then the composition of $p\mathcal{O}_F$ is given as in 2.9.(iii). Eventually, to classify all odd primes p, we consider an odd prime divisor p of b such that $p \nmid a$. Lemma 4.13 is the key component that completes the classification of all odd prime numbers p.

By Lemmas 2.9.(i) and 2.10, there is a unique prime ideal P_i above a prime p_i for all $p_i \mid d$ and there exists a unique prime ideal Q_i above q_i for all $q_i \mid a$ if d is not a quadratic residue modulo q_i. We will identify necessary and sufficient conditions for a prime p such that $\mathcal{O}_F$ has a unique prime ideal above p (see Theorem 1.6).

Remark 4.1. Let $\delta \in \mathcal{O}_F$. Since P_i is the unique prime ideal above p_i, to show that $\delta \in P_I$ it is sufficient to show that $\delta \in P_i$ for all $i \in I$. By Lemma 2.10, Q_j is the unique prime ideal above q_j for all $j \in J$. As consequence, to show $\delta \in Q_J$, it is sufficient to show that $\delta \in Q_j$ for all $j \in J$. Moreover, to claim $\delta \in P_I Q_J$, it is sufficient to show that $\delta \in P_i$ and $\delta \in Q_j$ for all $i \in I, j \in J$.

When ($p \mid d$ or $p \mid a$) and d is a quadratic non-residue modulo p, an integral basis of the unique prime ideal above p is obtained as a consequence of Lemmas 4.2, 4.3, 4.4, 4.5 and 4.6.

Lemma 4.2. *Let $d \equiv 2 \pmod 4$. Then $P_I Q_J = \mathbb{Z}p_I q_J \oplus \mathbb{Z}q_J\sqrt{d} \oplus \mathbb{Z}\beta \oplus \mathbb{Z}\sigma(\beta)$.*

Proof. For each $i \in I$ and $j \in J$, since P_i is the unique prime ideal above p_i and Q_j is the unique prime ideal above q_j and by Lemma 2.8, one obtains that $\beta, \sigma(\beta) \in P_i$ and $\beta, \sigma(\beta) \in Q_j$. By Remark 4.1, one has $\beta, \sigma(\beta) \in P_I Q_J$. It is obvious to see that $p_I q_J \in P_I Q_J$ and $q_J\sqrt{d} \in Q_J$. Since $p_I \mid d^2 = \mathbb{N}(\sqrt{d})$ and P_i is the unique prime ideal above p_i, we have that $\sqrt{d} \in P_i$ for all $i \in I$ and thus $q_J\sqrt{d} \in P_I$ by Remark 4.1. This means that $q_J\sqrt{d} \in P_I Q_J$. This implies that $L_{IJ} = \mathbb{Z}p_I q_J \oplus \mathbb{Z}q_J\sqrt{d} \oplus \mathbb{Z}\beta \oplus \mathbb{Z}\sigma(\beta)$ is a sublattice of $P_I Q_J$. However, two lattices $P_I Q_J$ and L_{IJ} have the same indices in $\mathcal{O}_F$. Therefore $P_I Q_J = L_{IJ}$ by Lemma 2.3. □

Lemma 4.3. *If $d \equiv 1 \pmod 4$ and b is odd, then* $P_IQ_J = \mathbb{Z}p_Iq_J \oplus \mathbb{Z}\frac{q_I(p_I+\sqrt{d})}{2} \oplus \mathbb{Z}\beta \oplus \mathbb{Z}\sigma(\beta)$.

Proof. By Remark 2.6, $\frac{1+\sqrt{d}}{2} \in \mathcal{O}_F$ and thus we have $\frac{p_I+\sqrt{d}}{2} = \frac{p_I-1}{2} + \frac{1+\sqrt{d}}{2} \in \mathcal{O}_F$. Since $p_i \mid \left(\frac{p_I^2-d}{4}\right)^2 = \mathbb{N}\left(\frac{p_I+\sqrt{d}}{2}\right)$ and P_i is the unique prime ideal above p_i for all $i \in I$, we have $\frac{q_J(p_I+\sqrt{d})}{2} \in P_IQ_J$. By Lemma 2.8, $\beta, \sigma(\beta) \in P_i, Q_j$ for all $i \in I$ and $j \in J$. By Remark 4.1, we obtain $\beta, \sigma(\beta) \in P_IQ_J$. One can prove the result using a similar argument as in the proof of Lemma 4.2. □

Lemma 4.4. *Let $d \equiv 1 \pmod 4$, b be even and $a+b \equiv 3 \pmod 4$. Then*

$$P_IQ_J = \mathbb{Z}p_Iq_J \oplus \mathbb{Z}\frac{q_J\left(p_I+\sqrt{d}\right)}{2} \oplus \mathbb{Z}\frac{\beta+\sigma(\beta)}{2} \oplus \mathbb{Z}\frac{-\beta+\sigma(\beta)}{2}.$$

Next, we consider the case $d \equiv 1 \pmod 4$, $b \equiv 0 \pmod 2$, $a+b \equiv 1 \pmod 4$ and $a \equiv -c \pmod 4$. Let $\gamma_1', \gamma_2', \gamma_3', \gamma_4'$ be a integral basis of $\mathcal{O}_F$ as in Remark 2.6.iv. We define

$$\gamma_1 = \gamma_1',\ \gamma_2 = \gamma_2',\ \gamma_3 = -\gamma_4',\ \gamma_4 = \gamma_2' - \gamma_3'. \tag{14}$$

It is obvious to see that $\{\gamma_1, \gamma_2, \gamma_3, \gamma_4\}$ is a basis of $\mathcal{O}_F$ by 2.6.iv. One has the following result.

Lemma 4.5. *Let $d \equiv 1 \pmod 4$, b be even, $a+b \equiv 1 \pmod 4$ and $a \equiv -c \pmod 4$. Then*

$$P_IQ_J = \mathbb{Z}\rho_{IJ} \oplus \mathbb{Z}\sigma\left(\rho_{IJ}\right) \oplus \mathbb{Z}\sigma^2\left(\rho_{IJ}\right)\mathbb{Z}\sigma^3\left(\rho_{IJ}\right),$$

where $\rho_{IJ} = \frac{-p_Iq_J+q_J\sqrt{d}-\beta-\sigma(\beta)}{4}$.

Proof. By Remark 4.1, it is sufficient to prove $\rho_{IJ} \in P_i, Q_J$ for all $i \in I$ and $j \in J$. Let $\gamma_1, \gamma_2, \gamma_3, \gamma_4$ as in (14). Then

$$\rho_{IJ} = \frac{-p_Iq_J - q_J + 2}{4}\gamma_1 + \frac{q_J-1}{2}\gamma_2 + \gamma_4$$

and thus $\rho_{IJ} \in \mathcal{O}_F$. Moreover,

$$\mathbb{N}\left(\rho_{IJ}\right) = \frac{\left(p_Iq_J^2 + q_I^2d - 2ad\right)^2 - 2d\left(p_Iq_J^2 + |a|c\right)^2}{256}$$

and thus $\rho_{IJ} \in P_i, Q_j$ for all $i \in I$ and $j \in J$. As a result

$$\rho_{IJ},\ \sigma\left(\rho_{IJ}\right),\ \sigma\left(\rho_{IJ}\right),\ \sigma^3\left(\rho_{IJ}\right) \in P_IQ_J.$$

Hence $L_{IJ} = \mathbb{Z}\rho_{IJ} \oplus \mathbb{Z}\sigma\left(\rho_{IJ}\right) \oplus \mathbb{Z}\sigma^2\left(\rho_{IJ}\right)\mathbb{Z}\sigma^3\left(\rho_{IJ}\right)$ is a sublattice of P_IQ_J. Two lattices P_IQ_J and L_{IJ} have the same indices $p_Iq_J^2$ in $\mathcal{O}_F$. Therefore $P_IQ_J = L_{IJ}$. □

In the remaining case where $d \equiv 1 \pmod 4, b \equiv 0 \pmod 2, a+b \equiv 1 \pmod 4$ and $a \equiv c \pmod 4$, using a similar technique to the one in the proof of Lemma 4.5, one obtains the result as below.

Lemma 4.6. *Let* $d \equiv 1 \pmod 4$, $b \equiv 0 \pmod 2$, $a+b \equiv 1 \pmod 4$ *and* $a \equiv c \pmod 4$. *Then*

$$P_I Q_J = \mathbb{Z}\rho_{IJ} \oplus \mathbb{Z}\sigma(\rho_{IJ}) \oplus \mathbb{Z}\sigma^2(\rho_{IJ})\mathbb{Z}\sigma^3(\rho_{IJ}),$$

where $\rho_{IJ} = \dfrac{p_I q_J - q_J\sqrt{d} - \beta + \sigma(\beta)}{4}$.

Next, we will describe a prime ideal above q_i where $q_i \mid a$ and d is a quadratic residue modulo q_i. By Lemma 2.10, there exist exactly two prime ideals above q_i. Let z_1, z_2 be two positive integers such that $z_i^2 \equiv d \pmod{q_j}$. By the result on the decomposition of primes [2, Theorem 4.8.13], one has $q_j\mathcal{O}_K = \mathfrak{q}_{1j}\mathfrak{q}_{2j}$, where $K = [\sqrt{d}]$.

Before proceeding, we will outline a strategy to prove that a certain lattice is an ideal in Lemmas 4.8 to 4.16. The proofs can be seen in the Appendix B.

Remark 4.7. Let $\mathcal{O}_F = \mathbb{Z}\gamma'_1 \oplus \mathbb{Z}\gamma'_2 \oplus \mathbb{Z}\gamma'_3 \oplus \mathbb{Z}\gamma'_4$, where the γ'_i are as in Remark 2.6 and let $L = \mathbb{Z}\delta_1 \oplus \mathbb{Z}\delta_2 \oplus \mathbb{Z}\delta_3 \oplus \mathbb{Z}\delta_4$ where each $\delta_i \in \mathcal{O}_F$. To prove L is an ideal of $\mathcal{O}_F$, we will show that $\delta_i\gamma'_j \in L$ for all i, j. In other words, we perform the following steps for all $1 \leq i, j \leq 4$.

(1) Compute $\delta_i\gamma'_j$.

(2) Express $\delta_i\gamma'_j = z_1\delta'_1 + z_2\delta'_2 + z_3\delta'_3 + z_4\delta'_4$.

(3) Prove that all numbers z_1, z_2, z_3, z_4 are integers.

When d is even, $df_K(x) = x^2 - d$ is a defining polynomial of $K = \mathbb{Q}(\sqrt{d})$. Then

$$df_K(x) \equiv (x - z_i)(x - z_2) \pmod{p_j}. \tag{15}$$

By using the result on the decomposition of primes in [2, Theorem 4.8.13], one has $\mathfrak{q}_{kj} = \mathbb{Z}q_j \oplus \mathbb{Z}\left(z_i + \sqrt{d}\right)$. With z_1, z_2 as in (15), one has the result as follows.

Lemma 4.8. *If d is even and $q_i \mid a$ such that d is a quadratic residue modulo q_j, then there exist exactly two prime ideals Q_{1j}, Q_{2j} above q_j where*

$$Q_{kj} = \mathbb{Z}q_j \oplus \mathbb{Z}\left(z_k + \sqrt{d}\right) \oplus \mathbb{Z}\beta \oplus \mathbb{Z}\sigma(\beta).$$

When d is odd, $df_K(x) = x^2 - x + \frac{1-d}{4}$ is a defining polynomial of K. One has

$$4df_K(x) \equiv (2x-1)^2 - d \equiv (2x - 1 - z_1)(2x - 1 - z_2) \pmod{q_j}.$$

As $q \equiv 1 \pmod 4$, there exist integers t_1, t_2 such that $z_k = 4t_k - 1 \pmod{q_j}$ for $k = 1, 2$, and thus $df_K(x) \equiv (x - t_1)(x - t_2) \pmod{q_j}$.

Lemma 4.9. *If $d \equiv 1 \pmod 4$, $b \equiv 1 \pmod 2$ and $q_i \mid a$ such that d is a quadratic residue modulo q_j, then there exist exactly two prime ideals Q_{1i}, Q_{2i} above q_i where $k = 1, 2$ and*

$$Q_{kj} = \mathbb{Z}q_j \oplus \mathbb{Z}\left(\frac{4t_k - 1 + \sqrt{d}}{2}\right) \oplus \mathbb{Z}\beta \oplus \mathbb{Z}\sigma(\beta).$$

Lemma 4.10. *If $d \equiv 1 \pmod 4$, $b \equiv 0 \pmod 2$, $a + b \equiv 3 \pmod 4$ and $q_i \mid a$ such that d is a quadratic residue modulo q_j, then there exist exactly two prime ideals Q_{1i}, Q_{2i} above q_i where $k = 1, 2$ and*

$$Q_{kj} = \mathbb{Z}q_j \oplus \mathbb{Z}\left(\frac{4t_k - 1 + \sqrt{d}}{2}\right) \oplus \mathbb{Z}\frac{\beta + \sigma(\beta)}{2} \oplus \mathbb{Z}\frac{\beta - \sigma(\beta)}{2}.$$

Lemma 4.11. *If $d \equiv 1 \pmod 4$, $b \equiv 0 \pmod 2$, $a + b \equiv 1 \pmod 4$ and $a \equiv -c \pmod 4$ and $p_j \mid a$ such that d is a quadratic residue modulo q_j, then there are exactly two prime ideals Q_{1j}, Q_{2j} above q_j such that*

$$Q_{kj} = \mathbb{Z}q_j \oplus \mathbb{Z}\frac{4t_k - 1 + \sqrt{d}}{2} \oplus \mathbb{Z}\frac{4t_k - 1 + \sqrt{d} - \beta - \sigma(\beta)}{4} \oplus \mathbb{Z}\frac{2q_j + 4t_k - 1 + \sqrt{d} + \beta - \sigma(\beta)}{4}.$$

Lemma 4.12. *If $d \equiv 1 \pmod 4$, $b \equiv 0 \pmod 2$, $a + b \equiv 1 \pmod 4$ and $a \equiv c \pmod 4$ and $p_j \mid a$ such that d is a quadratic residue modulo q_j, then there exist integers t_1, t_2 and exactly two prime ideals Q_{1j}, Q_{2j} above q_j such that $q_j \nmid t_1 - t_2$, $d \equiv (4t_i - 1)^2 \pmod{q_j}$ and*

$$Q_{ij} = \mathbb{Z}q_j \oplus \mathbb{Z}\frac{4t_i - 1 + \sqrt{d}}{2} \oplus \mathbb{Z}\frac{4t_i - 1 + 2q_j + \sqrt{d} - \beta - \sigma(\beta)}{4} \oplus \mathbb{Z}\frac{4t_i - 1 + \sqrt{d} + \beta - \sigma(\beta)}{4}.$$

Now, consider a prime p such that $p \mid b$ and $p \nmid a$, Lemma 2.11 does not provide us the exact prime decomposition of $p\mathcal{O}_F$. To see this decomposition, it is sufficient to show that $\mathcal{O}_F$ has either a prime ideal of norm p^2 or a prime ideal of norm p.

Lemma 4.13. *Let $p \mid b$ and $p \nmid a$. One has the following.*

i) Assume $2 \mid d$. If a is a quadratic non-residue modulo p, then $p\mathcal{O}_F = P_1P_2$ where

$$P_1 = \mathbb{Z}p \oplus \mathbb{Z}\left(c + \sqrt{d}\right) \oplus \mathbb{Z}p\sigma(\beta) \oplus \mathbb{Z}\left(\beta + \sigma(\beta)\right), \text{ and}$$
$$P_2 = \mathbb{Z}p \oplus \mathbb{Z}\left(-c + \sqrt{d}\right) \oplus \mathbb{Z}p\sigma(\beta) \oplus \mathbb{Z}\left(\beta - \sigma(\beta)\right)$$

are all prime ideals of $\mathcal{O}_F$ *above* p.

If a *is a quadratic residue modulo* p *and we write* $a \equiv l^2 \pmod{p}$, *then we have* $p\mathcal{O}_F = P_1P_2P_3P_4$ *where*

$$\begin{aligned}
P_1 &= \mathbb{Z}p \oplus \mathbb{Z}\left(c+\sqrt{d}\right) \oplus \mathbb{Z}\left(lc-\sigma(\beta)\right) \oplus \mathbb{Z}\left(lc+\beta\right),\\
P_2 &= \mathbb{Z}p \oplus \mathbb{Z}\left(c+\sqrt{d}\right) \oplus \mathbb{Z}\left(lc+\sigma(\beta)\right) \oplus \mathbb{Z}\left(-lc+\beta\right),\\
P_3 &= \mathbb{Z}p \oplus \mathbb{Z}\left(-c+\sqrt{d}\right) \oplus \mathbb{Z}\left(lc-\sigma(\beta)\right) \oplus \mathbb{Z}\left(lc-\beta\right), \text{ and}\\
P_4 &= \mathbb{Z}p \oplus \mathbb{Z}\left(-c+\sqrt{d}\right) \oplus \mathbb{Z}\left(lc+\sigma(\beta)\right) \oplus \mathbb{Z}\left(lc+\beta\right)
\end{aligned}$$

are all prime ideals of $\mathcal{O}_F$ *above* p.

ii) Assume $d \equiv 1 \pmod{4}$ *and* $b \equiv 1 \pmod{2}$. *If* a *is a quadratic non-residue modulo* p, *then* $p\mathcal{O}_F = P_1P_2$ *where*

$$\begin{aligned}
P_1 &= \mathbb{Z}p \oplus \mathbb{Z}\frac{p+c+\sqrt{d}}{2} \oplus \mathbb{Z}p\sigma\left(\beta\right) \oplus \mathbb{Z}\left(\beta+\sigma(\beta)\right), \text{ and}\\
P_2 &= \mathbb{Z}p \oplus \mathbb{Z}\frac{p-c+\sqrt{d}}{2} \oplus \mathbb{Z}p\sigma\left(\beta\right) \oplus \mathbb{Z}\left(\beta-\sigma(\beta)\right)
\end{aligned}$$

are all prime ideals of $\mathcal{O}_F$ *above* p.

If a *is a quadratic residue modulo* p *and we write* $a \equiv l^2 \pmod{p}$, *then we have* $p\mathcal{O}_F = P_1P_2P_3P_4$ *where*

$$\begin{aligned}
P_1 &= \mathbb{Z}p \oplus \mathbb{Z}\frac{p-c+\sqrt{d}}{2} \oplus \mathbb{Z}\left(lc-\sigma(\beta)\right) \oplus \mathbb{Z}\left(lc+\beta\right),\\
P_2 &= \mathbb{Z}p \oplus \mathbb{Z}\frac{p-c+\sqrt{d}}{2} \oplus \mathbb{Z}\left(lc+\sigma(\beta)\right) \oplus \mathbb{Z}\left(-lc+\beta\right),\\
P_3 &= \mathbb{Z}p \oplus \mathbb{Z}\frac{p+c+\sqrt{d}}{2} \oplus \mathbb{Z}\left(lc-\sigma(\beta)\right) \oplus \mathbb{Z}\left(lc-\beta\right), \text{ and}\\
P_4 &= \mathbb{Z}p \oplus \mathbb{Z}\frac{p+c+\sqrt{d}}{2} \oplus \mathbb{Z}\left(lc+\sigma(\beta)\right) \oplus \mathbb{Z}\left(lc+\beta\right)
\end{aligned}$$

are all prime ideals of $\mathcal{O}_F$ *above* p.

iii) Assume $d \equiv 1 \pmod{4}, b \equiv 0 \pmod{2}$ *and* $a+b \equiv 3 \pmod{4}$. *If* a *is a quadratic non-residue modulo* p, *then* $p\mathcal{O}_F = P_1P_2$ *where*

$$\begin{aligned}
P_1 &= \mathbb{Z}p \oplus \mathbb{Z}\frac{-c+\sqrt{d}}{2} \oplus \mathbb{Z}\frac{\sigma(\beta)-\beta}{2} \oplus \mathbb{Z}p\frac{\beta+\sigma(\beta)}{2}, \text{ and}\\
P_2 &= \mathbb{Z}p \oplus \mathbb{Z}\frac{c+\sqrt{d}}{2} \oplus \mathbb{Z}p\frac{\sigma(\beta)-\beta}{2} \oplus \mathbb{Z}\frac{\beta+\sigma(\beta)}{2}
\end{aligned}$$

are all prime ideals above p.

If a is a quadratic residue modulo p and we write $a \equiv l^2 \pmod p$, then we have $p\mathcal{O}_F = P_1P_2P_3P_4$ where

$$P_1 = \mathbb{Z}p \oplus \mathbb{Z}\frac{-c+\sqrt{d}}{2} \oplus \mathbb{Z}\frac{\sigma(\beta)-\beta}{2} \oplus \mathbb{Z}\left(lc - \frac{\beta+\sigma(\beta)}{2}\right),$$
$$P_2 = \mathbb{Z}p \oplus \mathbb{Z}\frac{-c+\sqrt{d}}{2} \oplus \mathbb{Z}\frac{\sigma(\beta)-\beta}{2} \oplus \mathbb{Z}\left(lc + \frac{\beta+\sigma(\beta)}{2}\right),$$
$$P_3 = \mathbb{Z}p \oplus \mathbb{Z}\frac{c+\sqrt{d}}{2} \oplus \mathbb{Z}\left(lc + \frac{\sigma(\beta)-\beta}{2}\right) \oplus \mathbb{Z}\frac{\beta+\sigma(\beta)}{2}, \text{ and}$$
$$P_4 = \mathbb{Z}p \oplus \mathbb{Z}\frac{c+\sqrt{d}}{2} \oplus \mathbb{Z}\left(lc - \frac{\sigma(\beta)-\beta}{2}\right) \oplus \mathbb{Z}\frac{\beta+\sigma(\beta)}{2}$$

are all primes ideals of $\mathcal{O}_F$ above p.

iv) *Assume $d \equiv 1 \pmod 4, b \equiv 2 \pmod 4, a+b \equiv 1 \pmod 4$ and $a \equiv -c \pmod 4$. If a is a quadratic non-residue modulo p, then $p\mathcal{O}_F = P_1P_2$ where*

$$P_1 = \mathbb{Z}p \oplus \mathbb{Z}\frac{-c+\sqrt{d}}{2} \oplus \mathbb{Z}\frac{b-c+\sqrt{d}-\beta+\sigma(\beta)}{4} \oplus \mathbb{Z}\frac{-p+p\sqrt{d}+p\beta+p\sigma(\beta)}{4}, \text{ and}$$
$$P_2 = \mathbb{Z}p \oplus \mathbb{Z}\frac{c+\sqrt{d}}{2} \oplus \mathbb{Z}\frac{p+p\sqrt{d}-p\beta+p\sigma(\beta)}{4} \oplus \mathbb{Z}\frac{b-c-\sqrt{d}-\beta-\sigma(\beta)}{4}$$

are all prime ideals of $\mathcal{O}_F$ above p.

If a is a quadratic residue modulo p and we write $a \equiv l^2 \pmod p$, then we have $p\mathcal{O}_F = P_1P_2P_3P_4$ where

$$P_1 = \mathbb{Z}p \oplus \mathbb{Z}\frac{c+\sqrt{d}}{2} \oplus \mathbb{Z}\frac{(-2l+1)\,c+\sqrt{d}-\beta+\sigma(\beta)}{4} \oplus \mathbb{Z}\frac{b-c-\sqrt{d}-\beta-\sigma(\beta)}{4},$$
$$P_2 = \mathbb{Z}p \oplus \mathbb{Z}\frac{-c+\sqrt{d}}{2} \oplus \mathbb{Z}\frac{b-c+\sqrt{d}-\beta+\sigma(\beta)}{4} \oplus \mathbb{Z}\frac{(2l+1)\,c-\sqrt{d}-\beta-\sigma(\beta)}{4},$$
$$P_3 = \mathbb{Z}p \oplus \mathbb{Z}\frac{c+\sqrt{d}}{2} \oplus \mathbb{Z}\frac{(2l+1)\,c+\sqrt{d}-\beta+\sigma(\beta)}{4} \oplus \mathbb{Z}\frac{b-c-\sqrt{d}-\beta-\sigma(\beta)}{4}, \text{ and}$$
$$P_4 = \mathbb{Z}p \oplus \mathbb{Z}\frac{-c+\sqrt{d}}{2} \oplus \mathbb{Z}\frac{b-c+\sqrt{d}-\beta+\sigma(\beta)}{4} \oplus \mathbb{Z}\frac{(-2l+1)\,c-\sqrt{d}-\beta-\sigma(\beta)}{4}$$

are all prime ideals of $\mathcal{O}_F$ above p.

v) *Assume $d \equiv 1 \pmod 4, b \equiv 2 \pmod 4, a+b \equiv 1 \pmod 4$ and $a \equiv c \pmod 4$. If a is a quadratic non-residue modulo p, then $p\mathcal{O}_F = P_1P_2$ where*

$$P_1 = \mathbb{Z}p \oplus \mathbb{Z}\frac{-c+\sqrt{d}}{2} \oplus \mathbb{Z}\frac{b-c+\sqrt{d}-\beta+\sigma(\beta)}{4} \oplus \mathbb{Z}\frac{p+p\sqrt{d}+p\beta+p\sigma(\beta)}{4}, \text{ and}$$
$$P_2 = \mathbb{Z}p \oplus \mathbb{Z}\frac{c+\sqrt{d}}{2} \oplus \mathbb{Z}\frac{-p+p\sqrt{d}-p\beta+p\sigma(\beta)}{4} \oplus \mathbb{Z}\frac{b-c-\sqrt{d}-\beta-\sigma(\beta)}{4}$$

are all prime ideals of $\mathcal{O}_F$ above p. If a is a quadratic residue modulo p and we write $a = l^2 \pmod p$, then $p\mathcal{O}_F = P_1P_2P_3P_4$ where

$$P_1 = \mathbb{Z}p \oplus \mathbb{Z}\frac{c+\sqrt{d}}{2} \oplus \mathbb{Z}\frac{(2l+1)\,c+\sqrt{d}-\beta+\sigma(\beta)}{4} \oplus \mathbb{Z}\frac{b-c-\sqrt{d}-\beta-\sigma(\beta)}{4},$$
$$P_2 = \mathbb{Z}p \oplus \mathbb{Z}\frac{-c+\sqrt{d}}{2} \oplus \mathbb{Z}\frac{b-c+\sqrt{d}-\beta+\sigma(\beta)}{4} \oplus \mathbb{Z}\frac{(2l+1)\,c-\sqrt{d}-\beta-\sigma(\beta)}{4},$$
$$P_3 = \mathbb{Z}p \oplus \mathbb{Z}\frac{c+\sqrt{d}}{2} \oplus \mathbb{Z}\frac{(-2l+1)\,c+\sqrt{d}-\beta+\sigma(\beta)}{4} \oplus \mathbb{Z}\frac{b-c-\sqrt{d}-\beta-\sigma(\beta)}{4}, \text{ and}$$
$$P_4 = \mathbb{Z}p \oplus \mathbb{Z}\frac{-c+\sqrt{d}}{2} \oplus \mathbb{Z}\frac{b-c+\sqrt{d}-\beta+\sigma(\beta)}{4} \oplus \mathbb{Z}\frac{(-2l+1)\,c-\sqrt{d}-\beta-\sigma(\beta)}{4}$$

are all prime ideals of $\mathcal{O}_F$ above p.

Proof. The given lattices are completely distinct, and we can prove that they are ideals by following the steps in Remark 4.7. □

Finally, we consider prime ideals above 2 when Δ_F is even. The following result is obtained from Lemma 2.9.(i).

Lemma 4.14. *Let d be even. Then there exists a unique prime ideal P_0 above $p_0 = 2$. Moreover, $P_0 = \langle 2, \beta\rangle$ and $\mathbb{N}(P_0) = 2$.*

Lemma 4.15. *Let $d \equiv 1 \pmod 4$ and b be odd.*

(i) If $d \equiv 5 \pmod 8$, then there is a unique prime ideal P_0 above $p_0 = 2$, where $\mathbb{N}(P_0) = 4$ and

$$P_0 = \mathbb{Z}2 \oplus \mathbb{Z}(1+\sqrt{d}) \oplus \mathbb{Z}\beta \oplus \mathbb{Z}\sigma(\beta).$$

(ii) If $d \equiv 1 \pmod 8$, then there are exactly two distinct prime ideals P_{01}, P_{02} above $p_0 = 2$, where $\mathbb{N}(P_{01}) = \mathbb{N}(P_{02}) = 2$ and

$$P_{01} = \mathbb{Z}2 \oplus \mathbb{Z}\left(\frac{-1+\sqrt{d}}{2}\right) \oplus \mathbb{Z}\beta \oplus \mathbb{Z}\sigma(\beta), \text{ and}$$
$$P_{02} = \mathbb{Z}2 \oplus \mathbb{Z}\left(\frac{1+\sqrt{d}}{2}\right) \oplus \mathbb{Z}\beta \oplus \mathbb{Z}\sigma(\beta).$$

Lemma 4.16. *Let $d \equiv 1 \pmod 4$ and $b \equiv 0 \pmod 2$ and $a+b \equiv 3 \pmod 4$.*

(i) If $d \equiv 5 \pmod 8$, then there is a unique prime ideal P_0 above $p_0 = 2$, where $\mathbb{N}(P_0) = 4$ and

$$P_0 = \mathbb{Z}2 \oplus \mathbb{Z}(1+\sqrt{d}) \oplus \mathbb{Z}\frac{-1+\sqrt{d}-\beta-\sigma(\beta)}{2} \oplus \mathbb{Z}\frac{1+\sqrt{d}+\beta-\sigma(\beta)}{2}.$$

(ii) If $d \equiv 1 \pmod 8$, then there are exactly two prime ideals P_{01}, P_{02} above $p_0 = 2$, where $\mathbb{N}(P_{01}) = \mathbb{N}(P_{02}) = 2$ and

$$P_{01} = \mathbb{Z}2 \oplus \mathbb{Z}\left(\frac{-1+\sqrt{d}}{2}\right) \oplus \mathbb{Z}\frac{2-\beta-\sigma(\beta)}{2} \oplus \mathbb{Z}\frac{\beta-\sigma(\beta)}{2}, \text{ and}$$
$$P_{02} = \mathbb{Z}2 \oplus \mathbb{Z}\left(\frac{1+\sqrt{d}}{2}\right) \oplus \mathbb{Z}\frac{\beta+\sigma(\beta)}{2} \oplus \mathbb{Z}\frac{2+\beta-\sigma(\beta)}{2}.$$

For the case of $p = 2$ and Δ_F odd, we have the following result.

Lemma 4.17. *Assume that $d \equiv 1 \pmod 4$ and $a + b \equiv 1 \pmod 4$.*

i) If $d \equiv 1 \pmod 8$, then $2\mathcal{O}_F$ can be factored as one of the forms P_1P_2, and $P_1P_2P_3P_4$ where P_1, P_2, P_3, P_4 are prime ideals of $\mathcal{O}_F$ above 2.

ii) If $d \equiv 5 \pmod 8$, then $2\mathcal{O}_F$ is prime.

Proof. i) This is deduced directly from the fact that $p\mathcal{O}_K$ splits totally in $\mathcal{O}_K$ where $\mathcal{O}_K$ as in (6).

ii) See Appendix B.

□

The below theorem follows directly from the combination of Lemmas 2.9, 2.10,2.11 and 4.13.

Theorem 4.18. *Let F be a cyclic quartic field defined by a, b, c, d as in (2) and p be an odd prime. One has the following statements.*

i) The prime p is totally ramified if and only if $p \mid d$.

ii) The ideal $p\mathcal{O}_F$ is of the forms $p\mathcal{O}_F = P^2$ for P a unique prime ideal of $\mathcal{O}_F$ above p if and only if $p \mid a$ and d is a quadratic non-residue modulo p.

iii) The ideal $p\mathcal{O}_F$ is of the form $p\mathcal{O}_F = P_1^2P_2^2$ where P_1, P_2 are exactly two prime ideals of $\mathcal{O}_F$ above p if and only if $p \mid a$ and d is a quadratic residue modulo p.

iv) The prime p is inert if and only if $p \nmid abcd$ and d is a quadratic non-residue modulo p.

v) The prime p totally splits if and only if p satisfies one of the conditions listed below.

- *The prime $p \mid b$ and a is a quadratic residue modulo p.*
- *The prime $p \mid c$ and $2a$ is a quadratic residue modulo p.*
- *The prime $p \nmid abcd$, d is a quadratic residue modulo p, and if $d \equiv z^2 \pmod p$ then $ad + abz$ and $ad - abz$ are also quadratic residues modulo p.*

vi) The ideal $p\mathcal{O}_F$ is the product of two distinct prime ideals in all the remaining cases.

From Theorem 4.18 and Lemmas 4.14, 4.15, and 4.16, we obtain the necessary and sufficient conditions for a prime p for which $\mathcal{O}_F$ has a unique prime ideal P over p. In the next subsection, we will investigate the conditions for the unique prime ideals P mentioned above to be WR.

4.2 Well-rounded ideals of cyclic quartic fields

According to the first part of Theorem 1.6, there are three cases in which $\mathcal{O}_F$ has a unique prime ideal P over a prime number p. However, in the last case of the theorem, $P = p\mathcal{O}_F$ and it is not primitive. Therefore, we only investigate prime ideals P belonging to the first two cases of the theorem. In general, we will prove necessary and sufficient conditions for an ideal of the form $P_I Q_J$ to be WR, where I is a subset of $\{1, \ldots, r\}$ and J is a subset of $\{1, \ldots, s\}$ such that d is a non-quadratic residue modulo q_j for all $j \in J$.

Proposition 4.19. *Let $d \equiv 2 \pmod 4$. Then $P_I Q_J$ is not WR.*

Proof. Let $\delta \in P_I Q_J$ be a nonzero vector of $P_I Q_J$. By Lemma 4.2, there exist integers x_1, x_2, x_3, x_4 such that $\delta = x_1 p_I q_J + x_2 q_J \sqrt{d} + x_3 \beta + x_4 \sigma(\beta)$ and by (8), one obtains

$$\|\delta\|^2 = 4\left(x_1^2 p_I^2 q_J^2 + x_2^2 q_J^2 d + |a| d \left(x_3^2 + x_4^2\right)\right).$$

It is easy to verify that $\min_{\delta \neq 0} \|\delta\|^2 \in \min \mathcal{S}$, where $\mathcal{S} = \{4p_I^2 q_J^2, 4q_J^2 d, 4|a|d\}$. Each value in $\mathcal{S}$ corresponds to the squared length of at most two independent vectors. Thus, $P_I Q_J$ is not WR. □

Proposition 4.20. *Let $d \equiv 1 \pmod 4$ and b be odd. Then $P_I Q_J$ is not WR.*

Proof. Let $\delta \in P_I Q_J$ be a nonzero vector of $P_I Q_J$. By Lemma 4.2, there exist integers x_1, x_2, x_3, x_4 such that $\delta = x_1 p_I q_J + x_2 q_J \frac{p_I + \sqrt{d}}{2} + x_3 \beta + x_4 \sigma(\beta)$ and by (8), one obtains

$$\|\delta\|^2 = (2x_1 + x_2)^2 p_I^2 q_J^2 + x_2^2 q_J^2 d + 4|a|d\left(x_3^2 + x_4^2\right).$$

Since $2x_1 + x_2$ and x_2 have the same parity, it is easy to verify that $\min_{\delta \neq 0} \|\delta\|^2 \in \min \mathcal{S}$, where $\mathcal{S} = \{p_I^2 q_J^2 + q_J^2 d, 4|a|d\}$. Each value in $\mathcal{S}$ corresponds to the squared length of at most two independent vectors. Thus $P_I Q_J$ is not WR. □

Proposition 4.21. *Let $d \equiv 1 \pmod 4$, b be even and $a + b \equiv 3 \pmod 4$. Then $P_I Q_J$ is not WR.*

Proof. Let $\delta \in P_I Q_J$ be a nonzero vector of $P_I Q_J$. By Lemma 4.2, there exist integers x_1, x_2, x_3, x_4 such that $\delta = x_1 p_I q_J + x_2 q_J \frac{p_I + \sqrt{d}}{2} + x_3 \frac{\beta + \sigma(\beta)}{2} + x_4 \frac{-\beta + \sigma(\beta)}{2}$ and by (8), one obtains

$$\|\delta\|^2 = (2x_1 + x_2)^2 p_I^2 q_J^2 + x_2^2 q_J^2 d + 2|a|d\left(x_3^2 + x_4^2\right).$$

The result is then obtained using the same argument as in the proof of Proposition 4.20. □

Proposition 4.22. *Suppose that* $d \equiv 1 \pmod 4$, $b \equiv 0 \pmod 2$, $a+b \equiv 1 \pmod 4$ *and* $a \equiv -c \pmod 4$. *Then* $P_I Q_J$ *is WR if and only if* $p_I^2 q_J^2 + q_J^2 d + 2|a|d \le \min \mathcal{M}$, *where*

$$\mathcal{M} = \left\{16q_J^2 d, 8|a|d, 4q_I^2 d + 4|a|d, 16p_I^2 q_J^2, 4p_I^2 q_J^2 + 4|a|d, 4p_I^2 q_J^2 + 4q_J^2 d\right\}.$$

Proof. Let ρ_{IJ} be in Lemma 4.5 and δ be a nonzero vector of $P_I Q_J$. By Lemma 4.5, there exist integers x_1, x_2, x_3, x_4 such that $4\delta = S_1 p_I q_J + S_2 q_J \sqrt{d} + S_3 \beta + S_4 \sigma(\beta)$ where

$$S_1 = -x_1 - x_2 - x_3 - x_4, \quad S_2 = x_1 - x_2 + x_3 - x_4,$$
$$S_3 = -x_1 + x_2 + x_3 - x_4, \quad S_4 = -x_1 - x_2 + x_3 + x_4.$$

By (8), one has

$$4\|\delta\|^2 = S_1^2 p_I^2 q_J^2 + S_2^2 q_J^2 d + |a|d\left(S_3^2 + S_4^2\right).$$

It is easy to prove that $\min_{\delta \neq 0} \|4\delta\|^2 = \min \mathcal{S}$ where

$$\mathcal{S} = \left\{p_I^2 q_J^2 + q_I^2 d + 2|a|d,\ 16q_J^2 d,\ 8|a|d, 4q_I^2 d + 4|a|d,\ 16p_I^2 q_J^2, 4p_I^2 q_J^2 + 4|a|d,\ 4p_I^2 q_J^2 + 4q_I^2 d\right\}.$$

Among seven numbers in $\mathcal{S}$, the only one that is correspondent to the squared length of four linearly independent vectors in P_I is $p_I^2 q_J^2 + q_J^2 d + 2|a|d$. Therefore, the lattice $P_I Q_J$ is WR if and only if $\min_{\delta \neq 0} 4\|\delta\|^2 = p_I^2 q_J^2 + q_J^2 d + 2|a|d$. □

Proposition 4.23. *Suppose that* $d \equiv 1 \pmod 4, b \equiv 0 \pmod 2, a + b \equiv 1 \pmod 4$ *and* $a \equiv c \pmod 4$. *Then* $P_I Q_J$ *is WR if and only if* $p_I^2 q_J^2 + q_J^2 d + 2|a|d \le \min \mathcal{M}$ *where*

$$\mathcal{M} = \left\{16q_J^2 d, 8|a|d, 4q_J^2 d + 4|a|d, 16p_I^2 q_J^2, 4p_I^2 q_J^2 + 4|a|d, 4p_I^2 q_J^2 + 4q_J^2 d\right\}.$$

Proof. Let ρ_{IJ} be in Lemma 4.6 and δ be a nonzero vector of $P_I Q_J$. By Lemma 4.6, there exist integers x_1, x_2, x_3, x_4 such that $4\delta = S_1 p_I q_J + S_2 q_J \sqrt{d} + S_3 \beta + S_4 \sigma(\beta)$ where $S_1 = x_1 + x_2 + x_3 + x_4, S_2 = -x_1 + x_2 - x_3 + x_4, S_3 = -x_1 - x_2 + x_3 + x_4, S_4 = x_1 - x_2 - x_3 + x_4$. By (8), one has

$$4\|\delta\|^2 = S_1^2 p_I^2 q_J^2 + S_2^2 q_J^2 d + |a|d\left(S_3^2 + S_4^2\right).$$

It is not hard to verify that $\min_{\delta \neq 0} \|4\delta\|^2 = \min \mathcal{S}$ where

$$\mathcal{S} = \left\{p_I^2 q_J^2 + q_I^2 d + 2|a|d, 16q_J^2 d, 8|a|d, 4q_I^2 d + 4|a|d, 16p_I^2 q_J^2, 4p_I^2 q_J^2 + 4|a|d, 4p_I^2 q_J^2 + 4q_I^2 d\right\}.$$

Among seven numbers in $\mathcal{S}$, the only one that corresponds to the squared length of four linearly independent vectors in P_I is $p_I^2 q_J^2 + q_J^2 d + 2|a|d$. Therefore, the lattice $P_I Q_J$ is WR if and only if $\min_{\delta \neq 0} 4\|\delta\|^2 = p_I^2 q_J^2 + q_J^2 d + 2|a|d$. □

We now prove Theorem 1.5.

Proof of Theorem 1.5. i) By Propositions 4.19, 4.20, 4.21, 4.22 and 4.23, the ideal P_I is WR if and only if $d \equiv 1 \pmod 4$, $p \equiv 0 \pmod 2$, $a+b \equiv 1 \pmod 4$ and $p_I^2 + (2|a|+1)\, d \leq \min \mathcal{S}$, where

$$\mathcal{S} = \left\{16d, 8|a|d,\ 4d+4|a|d,\ 16p_I^2,\ 4p_I^2+4|a|d, 4p_I^2+4d\right\}.$$

The last inequality is equivalent to the statement

$$\begin{aligned}
p_I^2 + (2|a|+1)\, d &\leq 16d,\\
p_I^2 + (2|a|+1)\, d &\leq 4d+4|a|d,\\
p_I^2 + (2|a|+1)\, d &\leq 16p_I^2,\\
p_I^2 + (2|a|+1)\, d &\leq 4p_I^2+4d.
\end{aligned}$$

This means

$$\max\left\{\frac{(2|a|-3)d}{3}, \frac{(2|a|+1)d}{15}\right\} \leq p_I^2 \leq \min\left\{(15-2|a|)\, d, (2|a|+3)\, d\right\}. \tag{16}$$

The inequalities in (16) occur only if $2|a| \leq 15$ and thus $|a| \in \{1,3,5,7\}$.

- If $|a| = 1$, the inequalities in (16) become $\frac{d}{5} \leq p_I^2 \leq 5d$.
- If $|a| = 3$, the inequalities in (16) become $d \leq p_I^2 \leq 9d$.
- If $|a| = 5$, the inequalities in (16) become $\frac{7d}{3} \leq p_I^2 \leq 5d$.
- If $|a| = 7$, the inequalities in (16) lead to $\frac{11d}{3} \leq p_I^2 \leq d$, which is impossible.

ii) By Propositions 4.19, 4.20, 4.21, 4.22 and 4.23, one can show that Q_J is WR if and only if $d \equiv 1 \pmod 4$, $p \equiv 0 \pmod 2$, $a+b \equiv 1 \pmod 4$ and $q_J^2(d+1)+2|a|d \leq \min \mathcal{S}$, where

$$\mathcal{S} = \left\{16q_J^2 d,\ 8|a|d,\ 4q_J^2 d+4|a|d,\ 16q_J^2,\ 4q_J^2+4|a|d,\ 4q_J^2+4q_J^2 d\right\}.$$

The last inequality is equivalent to

$$\begin{aligned}
q_J^2(d+1) + 2|a|d &\leq 16q_J^2,\\
q_J^2(d+1) + 2|a|d &\leq 8|a|d,\\
q_J^2(d+1) + 2|a|d &\leq 16q_J^2,\\
q_J^2(d+1) + 2|a|d &\leq 4q_J^2+4d.
\end{aligned}$$

This means $d < 15$ and

$$\max\left\{\frac{2|a|d}{15-d}, \frac{2|a|d}{3\,(d+1)}\right\} \leq q_J^2 \leq \min\left\{\frac{6|a|d}{d+1}, \frac{2|a|d}{d-3}\right\}. \tag{17}$$

Since d is odd and squarefree, and $d < 15$, one must have $d \in \{5, 13\}$. If $d = 13$ then (17) becomes $13|a| \leq q_J^2 \leq \frac{13|a|}{5}$, which is impossible. Thus d must be 5 and the inequalities in (17) become $|a| \leq q_J^2 \leq 5|a|$.

□

Now we consider prime ideals above 2.

Lemma 4.24. *No prime ideal above* 2 *is WR if d is even or if d is odd and* $b \equiv 1 \pmod 2$.

Proof. When d is even, the result is directly implied from Proposition 4.19. The result in the remaining case can be obtained by using a similar argument to the proofs of Propositions 4.19 and 4.20. □

By employing the same methodology used to prove Propositions 4.19 and 4.20, we can establish the result of Lemma 4.25.

Lemma 4.25. *Let* $d \equiv 1 \pmod 8, b \equiv 0 \pmod 2$ *and* $a + b \equiv 3 \pmod 4$. *Then all prime ideals above* 2 *are not WR.*

Lemma 4.26. *Let* $d \equiv 5 \pmod 8, b \equiv 0 \pmod 2$ *and* $a + b \equiv 3 \pmod 4$. *Then $\mathcal{O}_F$ has a unique prime ideal P_0 above* 2. *Moreover, P_0 is WR if and only if* $a = 1, b = 2, c = 1, d = 5$.

Proof. By Lemma 4.16, there is a unique prime ideal P_0 above 2 and an integral basis of P_0 is given as in this lemma. Let $0 \neq \delta \in P_0$, there are integers z_1, z_2, z_3, z_4 such that

$$\delta = 2z_1 + z_2\left(1+\sqrt{d}\right) + z_3\frac{-1+\sqrt{d}-\beta-\sigma(\beta)}{2} + z_4\frac{1+\sqrt{d}+\beta-\sigma(\beta)}{2}$$

and by (8), one obtains $\|\delta\|^2 = S_1^2 + S_2^2 d + |a|d\left(S_3^2 + S_4^2\right)$, where

$$\begin{aligned} S_1 &= 4x_1 + 2z_2 - z_3 + z_4, \\ S_2 &= 2z_2 + z_3 + z_4, \\ S_3 &= -z_3 + z_4, \\ S_4 &= -z_3 - z_4. \end{aligned}$$

It is easy to prove that $\min_{\delta\neq 0} \|\delta\|^2 = \min\{16, 1 + d\,(2|a|+1)\}$ and P_0 is WR if and only if $16 \geq 1 + (2|a|+1)$. It occurs only if $a = 1, b = 2, c = 1$. □

Remark 4.27. If P is a ideal above 2, then $2 \in P$. Thus, if P is WR, then there exists $\delta \in P \setminus \mathbb{Q}(\sqrt{d})$ such that $\|\delta\|^2 \leq 16$.

Lemma 4.28. *Let* $d \equiv 1 \pmod 4, b \equiv 0 \pmod 2$ *and* $a + b \equiv 1 \pmod 4$. *Then all prime ideals above* 2 *are not WR.*

Proof. If $d \equiv 5 \pmod 8$, then $2\mathcal{O}_F$ is prime (see Lemma 4.17) and not primitive. We now consider the case $d \equiv 1 \pmod 8$ here. Note that $d \geq 17$ as $d \equiv 1 \pmod 4$ and d is squarefree. We divide into two sub-cases: $a \equiv -c \pmod 4$ and $a \equiv c \pmod 4$. Since the techniques used in the proofs of the two cases are similar, we only consider the first. In this case, suppose that there exists a prime ideal P above 2 such that P is WR. Hence, by Remark 4.27, there exists $\delta \in P \setminus \mathbb{Q}(\sqrt{d})$ such that $\|\delta\|^2 \leq 16$. Let $\gamma_1', \gamma_2', \gamma_3', \gamma_4'$ be as in

Remark 2.6. There exist integers z_1, z_2, z_3, z_4 such that $\delta = z_1\gamma_1' + z_2\gamma_2' + z_3\gamma_3' + z_4\gamma_4'$ and thus

$$\|\delta\|^2 = \frac{1}{4}\left((4z_1 + 2z_2 + z_3 + z_4)^2 + d\,(2z_2 + z_3 - z_4) + 2|a|d\left(z_3^2 + z_4^2\right)\right).$$

Since $\delta \notin \mathbb{Q}(\sqrt{d})$, one has $z_3^2 + z_4^2 \geq 1$. Hence, $|a|d \leq \|\delta\|^2 \leq 32$ which occurs only if $|a| = 1$ and $d \leq 32$. This means $(a, d) \in \{(1, 17), (-1, 17)\}$ as $d \equiv 1 \pmod 8$ and d is squarefree. In both cases of (a, d), there are two prime ideals above 2 and we can verify that these prime ideals are not WR by using Pari/GP. Hence, all prime ideals above 2 are not WR when $d \equiv 1 \pmod 4), b \equiv 0 \pmod 2$ and $a + b \equiv 1 \pmod 4$. □

Combining Lemmas 4.24, 4.25, 4.26 and 4.28, we imply Proposition 4.29.

Proposition 4.29. *Let F, a, b, c, d be as in Section 2.3. Then a prime ideal above 2 of $\mathcal{O}_F$ is WR if and only if $a = 1, b = 2, c = 1, d = 5$. In this case, $\mathcal{O}_F$ has a unique prime ideal above 2.*

5 Conclusion and future research

This paper investigates WR ideals of cyclic and quartic fields. We show that all cyclic cubic fields have WR ideals. Moreover, we present families of cyclic cubic and quartic fields of which WR ideal lattices exist and also construct explicit minimal bases of these WR ideals.

We observe that all WR ideals obtained from our experiment have norms dividing the discriminant of the field if the discriminant is odd. Therefore, we form the following conjecture.

Conjecture: Let F be a cyclic cubic or cyclic quartic field with an odd discriminant. If a primitive integral ideal I of F is WR, then $N(I)$ divides the discriminant of F.

If this conjecture holds then there are only finitely many WR ideals from each of these fields.

Note that this conjecture agrees with the observation in [11] for real quadratic fields, and it was later proved for these fields [27]. In addition, for a cyclic quartic field F of odd discriminant, the conjecture holds for the case when the ideal I of F is the unique prime ideal above a prime number as a result of Theorem 1.6.

We also remark that the conjecture does not hold for cyclic quartic fields of even discriminant. That is, there exist cyclic quartic fields with even discriminant which have WR ideals of norms that do not divide the field discriminant. For example, the cyclic quartic field F defined by $(a, b, c, d) = (1, 2, 1, 5)$ has WR ideals with norms 484, 2420, 3364, and 3844 which do not divide $\Delta_F = 2000$. Another remark is that this is the only case in which a prime ideal above 2 is WR by Proposition 4.29.

Our future research will investigate the above conjecture and WR ideals of other number fields.

Acknowledgements

The authors would like to thank Amy Feaver for her help to improve the initial version of this manuscript and to thank the reviewer for their constructive comments that helped improve the manuscript. Ha T. N. Tran was supported by the Natural Sciences and Engineering Research Council of Canada (NSERC) (funding RGPIN-2019-04209 and DGECR-2019-00428).

References

[1] E. Bayer-Fluckiger. Lattices and number fields. *Algebraic Geometry: Hirzebruch 70*, 241, 1999.

[2] H. Cohen, H. Cohen, and H. Cohen. *A course in computational algebraic number theory*, volume 8. Springer-Verlag Berlin, 1993.

[3] K. Conrad. Discriminants and ramified primes. *Expository papers on algebraic number theory.*

[4] M. T. Damir, O. Gnilke, L. Amorós, and C. Hollanti. Analysis of some well-rounded lattices in wiretap channels. In *2018 IEEE 19th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, pages 1–5. IEEE, 2018.

[5] M. T. Damir and D. Karpuk. Well-rounded twists of ideal lattices from real quadratic fields. *Journal of Number Theory*, 196:168–196, 2019.

[6] M. T. Damir, A. Karrila, L. Amorós, O. W. Gnilke, D. Karpuk, and C. Hollanti. Well-rounded lattices: Towards optimal coset codes for gaussian and fading wiretap channels. *IEEE Transactions on Information Theory*, 67(6):3645–3663, 2021.

[7] M. T. Damir and G. Mantilla-Soler. Bases of minimal vectors in lagrangian lattices. *arXiv preprint arXiv:2006.16794*, 2020.

[8] R. R. de Araujo and S. I. Costa. Well-rounded algebraic lattices in odd prime dimension. *Archiv der Mathematik*, 112(2):139–148, 2019.

[9] E. L. De Oliveira, J. C. Interlando, T. P. Da Nobrega Neto, and J. O. D. Lopes. The integral trace form of cyclic extensions of odd prime degree. *Rocky Mountain Journal of Mathematics*, 47(4):1075–1088, 2017.

[10] U. Fincke and M. Pohst. Improved methods for calculating vectors of short length in a lattice, including a complexity analysis. *Mathematics of computation*, 44(170):463–471, 1985.

[11] L. Fukshansky, G. Henshaw, P. Liao, M. Prince, X. Sun, and S. Whitehead. On well-rounded ideal lattices ii. *Int. J. Number Theory*, 09(01):139–154, 2013.

[12] L. Fukshansky and K. Petersen. On well-rounded ideal lattices. *Int. J. Number Theory*, 8(1):189–206, 2012.

[13] O. W. Gnilke, A. Barreal, A. Karrila, H. T. N. Tran, D. A. Karpuk, and C. Hollanti. Well-rounded lattices for coset coding in mimo wiretap channels. In *Telecommunication Networks and Applications Conference (ITNAC), 2016 26th International*, pages 289–294. IEEE, 2016.

[14] O. W. Gnilke, H. T. N. Tran, A. Karrila, and C. Hollanti. Well-rounded lattices for reliability and security in rayleigh fading siso channels. In *Information Theory Workshop (ITW), 2016 IEEE*, pages 359–363. IEEE, 2016.

[15] H. Hasse. Arithmetische theorie der kubischen zahlkörper auf klassenkörpertheoretischer grundlage. *Mathematische Zeitschrift*, 31(1):565–582, 1930.

[16] R. Hudson and K. S. Williams. The integers of a cyclic quartic field. *The Rocky Mountain journal of mathematics*, pages 145–150, 1990.

[17] G. C. Jorge, A. A. de Andrade, S. I. Costa, and J. E. Strapasson. Algebraic constructions of densest lattices. *Journal of Algebra*, 429:218–235, 2015.

[18] G. C. Jorge, A. J. Ferrari, and S. I. Costa. Rotated dn-lattices. *Journal of Number Theory*, 132(11):2397–2406, 2012.

[19] N. H. Le, D. T. Tran, and H. T. Tran. Well-rounded twists of ideal lattices from imaginary quadratic fields. *Journal of Algebra and Its Applications*, 21(07):2250133, 2022.

[20] S. Mäki. *The determination of units in real cyclic sextic fields*, volume 797 of *Lecture Notes in Mathematics*. Springer, Berlin, 1980.

[21] J. Martinet. *Perfect lattices in Euclidean spaces*, volume 327. Springer Science & Business Media, 2013.

[22] C. McMullen. Minkowski's conjecture, well-rounded lattices and topological dimension. *Journal of the American Mathematical Society*, 18(3):711–734, 2005.

[23] J. S. Milne. *Algebraic number theory*. JS Milne, 2008.

[24] W. Narkiewicz. *Elementary and Analytic Theory of Algebraic Numbers*, volume 57. Springer, 1974.

[25] R. Schoof. Computing Arakelov class groups. In *Algorithmic number theory: lattices, number fields, curves and cryptography*, volume 44 of *Math. Sci. Res. Inst. Publ.*, pages 447–495. Cambridge Univ. Press, Cambridge, 2008.

[26] O. N. Solan. Stable and well-rounded lattices in diagonal orbits. *Israel Journal of Mathematics*, 234(2):501–519, 2019.

[27] A. Srinivasan. A complete classification of well-rounded real quadratic ideal lattices. *Journal of Number Theory*, 207:349–355, 2020.

[28] The PARI Group, Univ. Bordeaux. *PARI/GP version 2.13.4*, 2022. available from http://pari.math.u-bordeaux.fr/.

[29] H. T. N. Tran and P. Tian. The size function for cyclic cubic fields. *Int. J. Number Theory*, 14:399–415, 2018.

A Some results related to cyclic cubic fields

Proof of Lemma 3.12. Recall that $\mathrm{Tr}(\alpha) = \alpha + \sigma(\alpha) + \sigma^2(\alpha) = 0$. We have

$$\begin{aligned}\sigma^2(\delta) &= m_1 - m_3\sigma(\alpha) + (m_2 - m_3)(-\alpha - \sigma(\alpha)) \\ &= m_1 + (m_3 - m_2)\alpha - m_2\sigma(\alpha).\end{aligned}$$

Thus

$$\begin{aligned}\|\delta\|^2 &= \delta^2 + \sigma(\delta)^2 + (\sigma^2(\delta))^2 \\ &= 3m_1^2 + 2(m_2^2 + m_3^2 - m_2m_3)(\alpha^2 + \sigma(\alpha)^2 + \alpha\sigma(\alpha)) \\ &= 3m_1^2 + \frac{2m}{3}(m_2^2 + m_3^2 - m_2m_3).\end{aligned}$$

The last equality occurs because of the fact that

$$\begin{aligned}\alpha^2 + \sigma(\alpha)^2 + \alpha\sigma(\alpha) &= -\alpha\sigma(\alpha) + (\alpha + \sigma(\alpha))^2 \\ &= -\alpha\sigma(\alpha) - (\alpha + \sigma(\alpha))\sigma^2(\alpha) \\ &= \frac{m}{3}.\end{aligned}$$

□

Proof of Lemma 3.22. Let $P = P_1 \cdots P_r$. From Corollary 3.14 and from $\alpha^2 \in P^2$, there exists integers k, A, B such that $\alpha^2 = k\frac{m}{9} + A\alpha + B\sigma(\alpha)$. The value of k is 2 since $\mathrm{Tr}(\alpha) = \mathrm{Tr}(\sigma(\alpha)) = 0$ and $\mathrm{Tr}(\alpha^2) = \frac{2m}{3}$. By using Lemma 3.12, one deduces that

$$\|\alpha^2\|^2 = \frac{4m^2}{29} + \frac{2m}{3}(A^2 - AB + B^2).$$

It is easy to show that $\|\alpha\|^2 = \frac{2m^2}{9}$. Therefore $A^2 - AB + B^2 = \frac{m}{9}$. □

Proof of Lemma 3.3. By using the coefficients of the defining polynomial of F in (2), one has

$$\mathrm{Tr}(\alpha) = \mathrm{Tr}(\sigma(\alpha)) = 1, \mathrm{Tr}(\alpha^2) = \frac{2m+1}{3} \text{ and } \mathrm{Tr}(\alpha\sigma(\alpha)) = \frac{1-m}{3}. \tag{18}$$

Note that the set M_ℓ can be defined equivalently as $M_\ell = \{\delta \in \mathcal{O}_F : \mathrm{Tr}(\delta) \equiv 0 \pmod{\ell}\}$. Let $\delta = a_1\alpha + a_2\sigma(\alpha) + a_3\sigma^2(\alpha) \in M_\ell$. Then $a_1 + a_2 + a_3 \equiv 0 \pmod{\ell}$. By computation, we obtain

$$\begin{aligned}\mathrm{Tr}(\delta\alpha) &= \frac{1-m}{3}(a_1 + a_2 + a_3) + a_1m \\ \mathrm{Tr}(\delta\sigma(\alpha)) &= \frac{1-m}{3}(a_1 + a_2 + a_3) + a_2m \\ \mathrm{Tr}(\delta\sigma^2(\alpha)) &= \frac{1-m}{3}(a_1 + a_2 + a_3) + a_3m.\end{aligned}$$

If $\ell \mid m$, then $\mathrm{Tr}(\delta\alpha) = \mathrm{Tr}(\delta\sigma(\alpha)) = \mathrm{Tr}(\delta\sigma^2(\alpha)) \equiv 0 \pmod{\ell}$. Thus, all of $\delta\alpha$, $\delta\sigma(\alpha)$ and $\delta\sigma^2(\alpha)$ are in I. Since $\{\alpha, \sigma(\alpha), \sigma^2(\alpha)\}$ is a basis of $\mathcal{O}_F$ (Lemma 3.1), one has that M_ℓ is an ideal.

Conversely, assume that M_ℓ is ideal. Then the element $\alpha - \sigma(\alpha)$ has trace 0 and hence is in M_ℓ. Thus $\alpha(\alpha - \sigma(\alpha)) \in M_\ell$ since $\alpha \in \mathcal{O}_F$ and M_ℓ is an ideal. Therefore, by (18), $\mathrm{Tr}(\alpha(\alpha - \sigma(\alpha))) = \mathrm{Tr}(\alpha^2) - \mathrm{Tr}(\alpha\sigma(\alpha)) = m \equiv 0 \pmod{\ell}$. In other words, $\ell | m$. □

Proof of Lemma 3.4. By using the fact that $p_i | m$ and $n_i = -3^{-1} \pmod{p_i}$, one can factor $df(x)$ as $df(x) \equiv (\alpha + n_i)^3 \pmod{p_i}$. On the other hand, Lemma 2.4 says that p_i does not divide the index $[\mathcal{O}_F : \mathbb{Z}[\alpha]]$. Therefore, one has $P_i = \langle p_i, \alpha + n_i\rangle$ by using the result on the decomposition of primes [2, Theorem 4.8.13].

First, $-\alpha + \sigma(\alpha) = -(\alpha + n) + (\sigma(\alpha) + n) \in P_i$ since we have proved that $P_i = \langle p_i, \alpha + n_i\rangle$ and by the fact that $\sigma(P_i) = P_i$. The length of this element is easily computed by applying Lemma 3.2.

Next, we compute the length of $\alpha + n_i$. By writing

$$\alpha + n_i = \alpha + n_i(\alpha + \sigma(\alpha) + \sigma^2(\alpha)) = (n_i + 1)\alpha + n_i\sigma(\alpha) + n_i\sigma^2(\alpha)$$

and applying Lemma 3.2, the result is obtained. □

Proof of Lemma 3.23. Let $F = \mathbb{Q}(\xi_3)$ and $\theta = A + B\xi_3$. Then $\mathbb{N}(\theta) = N$ and there exists an ideal $\mathcal{P}_1, \cdots \mathcal{P}_i$ such that $\mathbb{N}(\mathcal{P}_i) = p_i$ and

$$\theta\mathcal{O}_K = \mathcal{P}_1 \cdots \mathcal{P}_r = \prod_{i \in I} \mathcal{P}_i \prod_{j \notin I} \mathcal{P}_j.$$

Since $\mathcal{O}$ is a PID, then there exist elements $x_j + y_j\xi_3 \in \mathcal{O}_K$ and $x_I + y_I\xi_3 \in \mathcal{O}_K$ such that $x_j + y_j \equiv 1 \pmod 3$ for all $j \notin I, x_I + y_I \equiv 1 \pmod 3$ and $\mathcal{P}_i = \langle\delta_i\rangle, \mathcal{P}_I = \langle\delta_I\rangle$ whereas $\delta_i = x_i + y_i\xi_3$ and $\delta_I = x_I + y_I\xi_3$. It leads to the equality $\theta\mathcal{O}_K = \left(\delta_I \prod_{j \notin I} \delta_j\right) \mathcal{O}_K$ and thus there exists $\varepsilon \in \mathcal{O}_K^*$ such that $\theta\varepsilon = \delta_I \prod_{j \notin I} \delta_j$. Let $\sigma_F(\delta_I)$ be the conjugate of δ_I over F. One has $\delta_I\sigma_F(\delta_I) = p_I$ and thus

$$\theta\varepsilon\sigma_F(\delta_I) = \left(\prod_{j \notin I} \delta_j\right)(\delta_I\sigma_F(\delta_I)) = p_I\left(\prod_{j \neq i} \delta_j\right).$$

It means $\theta\sigma_F(\delta_I) \in p_I\mathcal{O}_K$. Moreover,

$$\theta\sigma_F(\delta_I) = Ax_I + By_I - Ay_I + (Bx_I - Ay_I)\xi_3$$

and thus $Bx_I - Ay_I, Ax_I + By_I - Ay_I$ are multiples of p_I. □

Proof of Lemma 3.24. Let $\gamma = x_I\alpha + y_I\sigma(\alpha)$. Remark that $\frac{m}{9} = A^2 - AB + B^2$ and $\alpha^2 = \frac{2m}{9} + A\alpha + B\sigma(\alpha)$. Since $\mathrm{Tr}(\alpha\sigma(\alpha)) = -\frac{n}{3}$, then we can write $\alpha\sigma(\alpha) = \frac{-m}{9} + C\alpha + D\sigma\alpha$

for some integers C, D. One has $\alpha^3 = \frac{m\alpha}{3} + \frac{am}{27}$ and $\alpha^3 = \frac{2m\alpha}{9} + A\alpha^2 + B\alpha\sigma\alpha$. This implies that

$$\frac{m\alpha}{3} + \frac{am}{27} = (AB + BD)\,\sigma(\alpha) + \left(\frac{2m}{9} + A^2 + BC\right)\alpha + \left(\frac{2mA}{9} - \frac{mB}{9}\right)$$

and thus $AB + BD = 0$, $\frac{2m}{9} + A^2 + BC = \frac{m}{3}$, $\frac{ma}{27} = \frac{2mA}{9} - \frac{mB}{9}$. Since B must be nonzero, $A = -D$ and it is easy to prove $C = B - A$.

One can easily verify that

$$\begin{aligned}\gamma\alpha &= \frac{m}{9}(2x_I - y_I) + (Ax_I + By_I - Ay_I)\,\alpha + (Bx_I - Ay_I)\,\sigma(\alpha),\\ \gamma\sigma(\alpha) &= \frac{m}{9}(-x_I + 2y_I) + (Bx_I - Ay_I - By_I)\,\alpha + (-Ax_I + Ay_I - By_I)\,\sigma\alpha.\end{aligned}$$

Let $M_\gamma = \begin{pmatrix} 0 & \frac{m}{9}(2x_I - y_I) & \frac{m}{9}(-x_I + 2y_I) \\ x_I & Ax_I - By_I - Ay_I & Bx_I - Ay_I - By_I \\ y_I & Bx_I - Ay_I & -Ax_I + Ay_I - By_I \end{pmatrix}$.

Since all the entries in the second and third columns are multiples of p_I, one has that $\det(M_\gamma)$ is a multiple of p_I^2. Hence, $p_I^2 \mid \mathbb{N}_{K/\mathbb{Q}}(\gamma)$ as $\mathbb{N}_{K/\mathbb{Q}}(\gamma) = \det(M_\gamma)$ by [23]. □

B Some results related to cyclic quartic fields

Proof of Lemma 4.8. First, we prove that that Q_{1i}, Q_{2i} are ideals. By Remark 2.6.(i), it is sufficient to show $(z_k + \sqrt{d})\beta \in Q_{kj}$. Indeed, one has

$$\begin{aligned}(z_k + \sqrt{d})\beta &= z_k\beta + \sqrt{d}\beta\\ &= z_k\beta + c\sigma(\beta) - b\beta\\ &= (z_k - b)\,\beta + c\sigma(\beta) \in Q_{kj}\end{aligned}$$

for $k = 1, 2$. Hence Q_{1j}, Q_{2j} are ideals of $\mathcal{O}_F$. These two ideals have norm q_j and thus they are prime ideals. Moreover, one has $\mathbb{Q} \leq K = \mathbb{Q}(\sqrt{d}) \leq F$ and $Q_{kj} \cap \mathcal{O}_K = \mathfrak{q}_{kj}$. Hence Q_{1j}, Q_{2j} are distinct. By Lemma 2.10, these ideals are the only prime ideals above q_j. □

Proof of Lemma 4.9. To prove Q_{1j}, Q_{2j} are ideals, it is sufficient to prove $\frac{4t_k - 1 + \sqrt{d}}{2}\beta \in Q_{kj}$ and $\frac{4t_k - 1 + \sqrt{d}}{2}\sigma(\beta) \in Q_{kj}$ for $k = 1, 2$. By using Lemma 2.8, we have

$$\begin{aligned}\frac{4t_k - 1 + \sqrt{d}}{2}\beta &= (2t_k - 1)\,\beta + \frac{\beta + \beta\sqrt{d}}{2}\\ &= (2t_k - 1)\beta + \frac{\beta + c\sigma(\beta) - b\beta}{2}\\ &= \left(2t_k - 1 + \frac{1 - b}{2}\right)\beta + \frac{c}{2}\sigma(\beta) \in Q_{kj},\\ \frac{4t_k - 1 + \sqrt{d}}{2}\sigma(\beta) &= (2t_k - 1)\sigma(\beta) + \frac{\sigma(\beta) + \sigma(\beta)\sqrt{d}}{2}\\ &= \left(2t_k - 1 + \frac{1 + b}{2}\right)\sigma(\beta) + \frac{c}{2}\beta \in Q_{kj},\end{aligned}$$

for $k = 1, 2$. Hence Q_{1j}, Q_{2j} are ideals and thus they are prime as their norms are q_j. Moreover, $Q_{kj} \cap \mathcal{O}_K = \mathfrak{q}_{kj}$. Hence these ideals are distinct. By Lemma 2.10, Q_{1j}, Q_{2j} are two only prime ideals of $\mathcal{O}_F$ above q_j. □

The proof of Lemma 4.10 is similar to Lemma 4.9.

Proof of Lemma 4.11. Let $\gamma_1, \gamma_2', \gamma_3', \gamma_4$ as in Remark 2.6,iv. Let $\rho_{kj} = \frac{4t_k-1+\sqrt{d}-\beta-\sigma(\beta)}{4}$ and $\psi_{kj} = \frac{2q_j+4t_k-1+\sqrt{d}+\beta-\sigma(\beta)}{4}$. First, we prove that Q_{kj} are ideals for all $k = 1, 2$. To do that, it is sufficient to prove that $q_j\gamma_i'$, $\frac{4t_k-1+\sqrt{d}}{2}\gamma_i'$, $\rho_{kj}\gamma_i'$, $\psi_{kj}\gamma_i' \in Q_{kj}$ for all $i = 1, 2, 3, 4$ and $k = 1, 2$. It is obvious that $q_j\gamma_i'$; $\frac{4t_k-1+\sqrt{d}}{2}\gamma_i'$, ρ_{kj}, $\psi_{kj} \in Q_{kj}$, for all $k = 1, 2$ and $i = 1, 2$. One has

$$\begin{aligned}
q_j\gamma_3' &= \frac{q_j+1-2t_k}{2}q_j + q_j\frac{4t_k-1+\sqrt{d}}{2} - q_j\psi_{kj}\\
q_j\gamma_4' &= t_kq_j - q_j\rho_{kj}\\
\frac{4t_k-1+\sqrt{d}}{2}\gamma_3' &= \frac{d-(4t_k-1)^2-2q_j\left(c+1-4t_k\right)}{8q_j}q_j + \frac{b-c-1+8t}{4}\frac{4t_k-1+\sqrt{d}}{2}\\
&\quad - \frac{b}{2}\rho_{kj} + \frac{c-1-4t_k}{2}\psi_{kj}\\
\frac{4t_k-1+\sqrt{d}}{2}\gamma_4' &= \frac{2bq_j-d+(4t_k-1)^2}{8q_j}q_j + \frac{b+c+1}{4}\frac{4t_k-1+\sqrt{d}}{2}\\
&\quad + \frac{-c+1-4t}{2}\rho_{kj} - \frac{b}{2}\psi_{kj}\\
\rho_{kj}\gamma_2' &= \frac{d-(4t_k-1)^2+2bq_j}{8q_j}q_j + \frac{-b-c+4t-1}{4}\frac{4t_k-1+\sqrt{d}}{2}\\
&\quad + \frac{c+1}{2}\rho_{kj} + \frac{b}{2}\psi_{kj}\\
\psi_{kj}\gamma_2' &= \frac{d-(4t_k-1)^2+2q_j\left(c+1-4t_k\right)}{8q_j}q_j\\
&\quad + \frac{-b+c-1+2q_j+4t_k}{4}\frac{4t_k-1+\sqrt{d}}{2} + \frac{b}{2}\rho_{kj} + \frac{1-c}{2}\psi_{kj}\\
\rho_{kj}\gamma_3' &= \frac{d-(4k_1-1)^2-2ab+8abt-2q\left(b+c+1+8t\right)}{16q_j}q_j\\
&\quad + \frac{4t-ab-c-1}{4}\frac{4t_k+1+\sqrt{d}}{2} + \frac{c-b+1}{4}\rho_{kj} + \frac{b+c+1-4t}{4}\psi_{kj}\\
\rho_{kj}\gamma_4' &= \frac{(4t_k-1)^2-d-2a\left(c+d-4ct\right)+4bq}{16q_j}q_j + \frac{b+c-ac}{4}\frac{4t_k+1-\sqrt{d}}{2}\\
&\quad + \frac{1-c-2t_k}{2}\rho_{kj} - \frac{b}{2}\psi_{kj}
\end{aligned}$$

$$\psi_{kj}\gamma_3' = \frac{2a\left(c-d-4ct_k\right)+4q_j^2+d-\left(4t_k-1\right)^2}{16q_j}q_j + \frac{ac+2q_j+4t_k-1}{4}\frac{4t_k-1+\sqrt{d}}{2} + \frac{-q_j-2t_k+1}{2}\psi_{kj}$$

$$\psi_{kj}\gamma_4' = \frac{(4t_k-1)^2-d-2ab\left(1-4t_k\right)+2q_j\left(b-c-1+4t_k\right)}{16q_j}q_j - \frac{ab-b}{4}\frac{4t_k-1+\sqrt{d}}{2} - \frac{b+c+2q_j-4t_k+1}{4}\rho_{kj} + \frac{-b+c+1}{4}\psi_{kj}.$$

It is not hard to prove all the coefficients of the above expressions are integers. Thus Q_{1j}, Q_{2j} are ideals. Moreover, $Q_{kj}\cap\mathcal{O}_K = \mathfrak{q}_{kj}$ and thus $Q_{1j}\neq Q_{2j}$ and they are all prime ideals of $\mathcal{O}_F$ above q_j. □

To prove Lemma 4.17.(ii), we again consider two cases, namely $a\equiv -c \pmod 4$ and $a\equiv c \pmod 4$. The proofs of both cases use the same technique, thus we only prove the first case here. The notations $\gamma_1',\gamma_2',\gamma_3',\gamma_4'$ are as defined in Remark 2.6. One has

$$\gamma_1'\cdot\gamma_i' = \gamma_i', \text{ for } i=1,2,3,4$$

$$\gamma_2'^2 = \frac{d-1}{4}\gamma_1' + \gamma_2'$$

$$\gamma_2'\cdot\gamma_3' = \frac{-2b+d-1}{8}\gamma_1' + \frac{b+c+1}{4}\gamma_2' + \frac{1-c}{2}\gamma_3' + \frac{b}{2}\gamma_4'$$

$$\gamma_2'\cdot\gamma_4' = \frac{-d-2c-1}{8}\gamma_1' + \frac{-b+c+1}{4}\gamma_2' + \frac{b}{2}\gamma_3' + \frac{c+1}{2}\gamma_4'$$

$$\gamma_3'^2 = \frac{-4b+2ac+2ad+d-1}{16}\gamma_1' + \frac{b+c-ac}{4}\gamma_2' + \frac{-c+1}{2}\gamma_3' + \frac{b}{2}\gamma_4'$$

$$\gamma_3'\cdot\gamma_4' = \frac{-2ab+2b-2c-d-1}{16}\gamma_1' + \frac{ab-b}{4}\gamma_2' + \frac{b+c+1}{4}\gamma_3' + \frac{-b+c+1}{4}\gamma_4'$$

$$\gamma_4'^2 = \frac{-2ac+4c+2ad+d-1}{16}\gamma_1' + \frac{b+ac-c}{4}\gamma_2' - \frac{b}{2}\gamma_3' + \frac{1-c}{2}\gamma_4'.$$

Let $\delta = z_1\gamma_1' + z_2\gamma_2 + z_3\gamma_3' + z_4\gamma_4'$ and $\psi = t_1\gamma_1' + t_2\gamma_2 + t_3\gamma_3' + t_4\gamma_4'$ be arbitrary elements of $\mathcal{O}_F$. Then

$$\delta\cdot\psi = S_1\gamma_1' + S_2\gamma_2' + S_3\gamma_3' + S_4\gamma_3'$$

where

$$\begin{aligned}
S_1 = {} & z_1t_1 + z_2t_2\frac{-2b+d-1}{4} + z_2t_3\frac{-2b+d-1}{8} + z_2t_4\frac{-d-2c-1}{8} + z_3t_2\frac{-b+d-1}{8} \\
& + z_3t_3\frac{-4b+2ac+2ad+d-1}{16} + z_3t_4\frac{-2ab+2b-2c-d-1}{16} + z_4t_2\frac{-d-2c-1}{8} \\
& + z_4t_3\frac{-2ab+2b-2c-d-1}{16} + z_4t_4\frac{-2ac+4c+2ad+d-1}{16} \\
S_2 = {} & z_1t_2 + z_2t_1 + z_2t_2 + z_2t_3\frac{b+c+1}{4} + z_2t_4\frac{-b+c+1}{4} + z_3t_2\frac{b+c+1}{4} + z_3t_3\frac{b+c-ac}{4} \\
& + z_3t_4\frac{ab-b}{4} + z_4t_2\frac{-b+c+1}{4} + z_4t_3\frac{ab-b}{4} + z_4t_4\frac{b+ac-c}{4} \\
S_3 = {} & z_1t_3 + z_2t_3\frac{1-c}{2} + z_2t_4\frac{b}{2} + z_3t_1 + z_3t_2\frac{1-c}{2} \\
& + z_3t_3\frac{1-c}{2} + z_3t_4\frac{b+c+1}{4} + z_4t_2\frac{b}{2} + z_4t_3\frac{b+c+1}{4} + z_4t_4\frac{-b}{2} \\
S_4 = {} & z_1t_4 + z_2t_3\frac{b}{2} + z_2t_4\frac{c+1}{2} + z_3t_2\frac{b}{2} \\
& + z_3t_3\frac{b}{2} + z_3t_4\frac{-b+c+1}{4} + z_4t_1 + z_4t_2\frac{c+1}{2} + z_4t_3\frac{-b+c+1}{4} + z_4t_4\frac{1-c}{2}
\end{aligned}$$

Proof of Lemma 4.17.(ii). To prove $2\mathcal{O}_F$ is prime, we claim that $\delta \cdot \psi \notin 2\mathcal{O}_F$ wherever $\delta \notin 2\mathcal{O}_F$ and $\psi \notin 2\mathcal{O}_F$. It is sufficient to claim that if the two tuples (t_1, t_2, t_3, t_4) and (z_1, z_2, z_3, z_4) are not simultaneously equal to $(0, 0, 0, 0)$ modulo 2, then S_1, S_2, S_3 and S_4 are also not simultaneously equal to $0 \pmod 2$. Since the largest denominator of S_1, S_2, S_3, S_4 is 16, one can prove this by considering the integers a, b, c, d modulo 32 and verify whether S_1, S_2, S_3, S_4 are all zero modulo 2 or not. It is done by using any programming language. □

Received: March 31, 2023
Accepted for publication: August 28, 2023
Communicated by: Camilla Hollanti and Lenny Fukshansky