Alberta Number Theory Day 2024

Well-rounded ideal lattices of cyclic cubic and quartic fields

Ha Tran

Concordia University of Edmonton
joint work with Nam Le and Dat Tran

Content

Notations

- Let F be a number field with degree n, discriminant Δ and the ring of integers O_F. For simplicity, assume that F is totally real.

Notations

- Let F be a number field with degree n, discriminant Δ and the ring of integers O_F. For simplicity, assume that F is totally real.
- Let $\sigma_1, \ldots, \sigma_n$ be n embeddings of F.

Notations

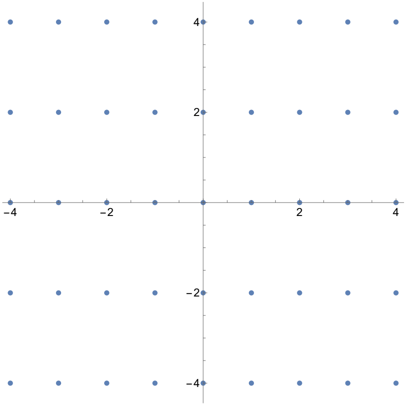
- Let F be a number field with degree n, discriminant Δ and the ring of integers O_F. For simplicity, assume that F is totally real.
- Let $\sigma_1, \ldots, \sigma_n$ be n embeddings of F.
- Denote by $\Phi = (\sigma_1, ..., \sigma_n)$. Then

$$\Phi : F \hookrightarrow \mathbb{R}^n \text{ takes } x \in F \text{ to } (\sigma_i(x))_i.$$

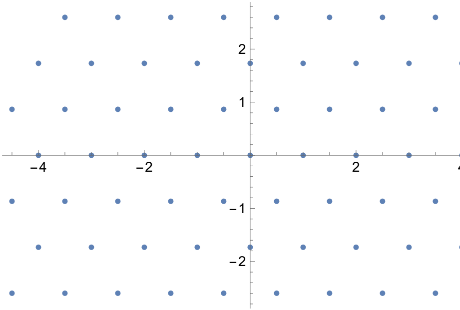
Lattices

Let $\mathcal{B} = \{v_1, v_2, ..., v_m\}$ be a linearly independent set of vectors in $\mathbb{R}^n$.

- $L = \{\sum_{i=1}^{m} a_i v_i | a_i \in \mathbb{Z}\}$ is called a lattice in $\mathbb{R}^n$ of rank m.
- $\mathcal{B}$ is said to be a basis of L, we write $L = \langle \mathcal{B} \rangle$.
- In case $m = n$, we say that L is full rank.



$L = \langle (1,0), (0,2) \rangle$.



The hexagonal lattice
$H = \left\langle (1,0), (1/2, \sqrt{3}/2) \right\rangle$.

Ideal lattices

Ex: $F = \mathbb{Q}(\sqrt{3})$ has 2 embeddings:
$\sigma_1(a + b\sqrt{3}) = a + b\sqrt{3}$ and
$\sigma_2(a + b\sqrt{3}) = a - b\sqrt{3}$.

[1] It can be defined more general.

Ideal lattices

Ex: $F = \mathbb{Q}(\sqrt{3})$ has 2 embeddings:
$\sigma_1(a + b\sqrt{3}) = a + b\sqrt{3}$ and
$\sigma_2(a + b\sqrt{3}) = a - b\sqrt{3}$.
The ideal $I = \langle 2, 1 - \sqrt{3} \rangle_{\mathbb{Z}}$.

[1] It can be defined more general.

Ideal lattices

Ex: $F = \mathbb{Q}(\sqrt{3})$ has 2 embeddings:
$\sigma_1(a + b\sqrt{3}) = a + b\sqrt{3}$ and
$\sigma_2(a + b\sqrt{3}) = a - b\sqrt{3}$.
The ideal $I = \langle 2, 1 - \sqrt{3} \rangle_{\mathbb{Z}}$.
$b_1 = \Phi(2) = (2, 2)$,
$b_2 = \Phi(1 - \sqrt{3}) = (1 - \sqrt{3}, 1 + \sqrt{3})$.

[1] It can be defined more general.

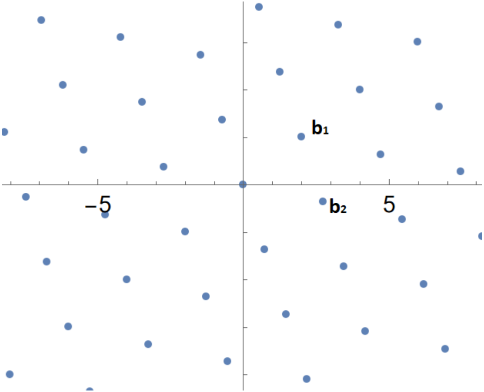
Ideal lattices

Ex: $F = \mathbb{Q}(\sqrt{3})$ has 2 embeddings:
$\sigma_1(a + b\sqrt{3}) = a + b\sqrt{3}$ and
$\sigma_2(a + b\sqrt{3}) = a - b\sqrt{3}$.
The ideal $I = \langle 2, 1 - \sqrt{3} \rangle_{\mathbb{Z}}$.
$b_1 = \Phi(2) = (2, 2)$,
$b_2 = \Phi(1 - \sqrt{3}) = (1 - \sqrt{3}, 1 + \sqrt{3})$.
Then $\Phi(I) = \langle b_1, b_2 \rangle_{\mathbb{Z}}$ is a lattice in R^2.

[1] It can be defined more general.

Ideal lattices

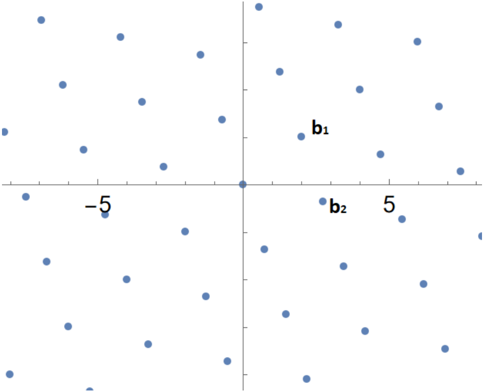
Ex: $F = \mathbb{Q}(\sqrt{3})$ has 2 embeddings:
$\sigma_1(a + b\sqrt{3}) = a + b\sqrt{3}$ and
$\sigma_2(a + b\sqrt{3}) = a - b\sqrt{3}$.
The ideal $I = \langle 2, 1 - \sqrt{3} \rangle_{\mathbb{Z}}$.
$b_1 = \Phi(2) = (2, 2)$,
$b_2 = \Phi(1 - \sqrt{3}) = (1 - \sqrt{3}, 1 + \sqrt{3})$.
Then $\Phi(I) = \langle b_1, b_2 \rangle_{\mathbb{Z}}$ is a lattice in R^2.



[1] It can be defined more general.

Ideal lattices

Ex: $F = \mathbb{Q}(\sqrt{3})$ has 2 embeddings:
$\sigma_1(a + b\sqrt{3}) = a + b\sqrt{3}$ and
$\sigma_2(a + b\sqrt{3}) = a - b\sqrt{3}$.
The ideal $I = \langle 2, 1 - \sqrt{3} \rangle_{\mathbb{Z}}$.
$b_1 = \Phi(2) = (2, 2)$,
$b_2 = \Phi(1 - \sqrt{3}) = (1 - \sqrt{3}, 1 + \sqrt{3})$.
Then $\Phi(I) = \langle b_1, b_2 \rangle_{\mathbb{Z}}$ is a lattice in R^2.



Proposition

Let I be a factional ideal of F. Then $\Phi(I)$ is a lattice in $\mathbb{R}^n$.

We call I an ideal lattice[1] of F.

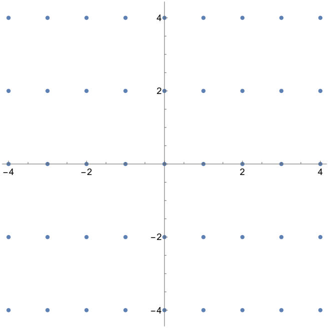
[1] It can be defined more general.

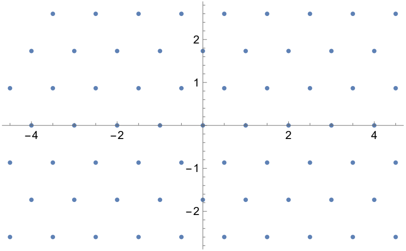
Well-rounded lattices

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

- $|L| = \min_{0\neq u\in L} \|u\|^2$ is called the minimum norm (length) of L.
- The set of shortest vectors of L is defined as

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



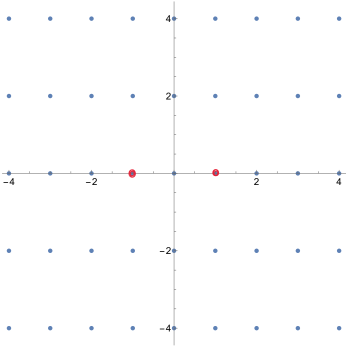


$L = \langle(1,0),(0,2)\rangle$.
$|L| =?$ $S(L) =?$

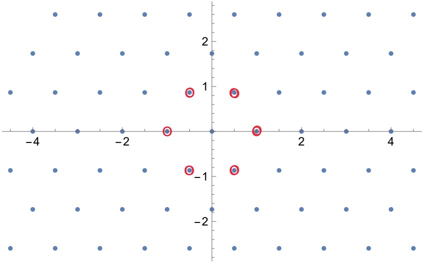
The hexagonal lattice
$H = \left\langle(1,0),(1/2,\sqrt{3}/2)\right\rangle$.
$|H| =?$ $S(H) =?$

Well-rounded lattices

- $|L| = \min_{0 \neq u \in L} \|u\|^2$
-
$$S(L) := \{u \in L : \|u\|^2 = |L|\}.$$



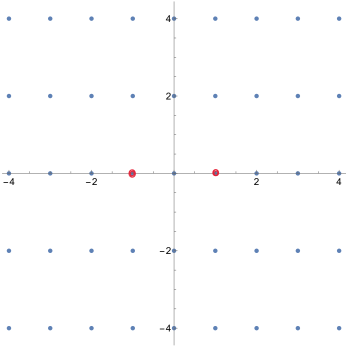
$L = \langle (1,0), (0,2) \rangle$.
$|L| = 1, S(L) = \{\pm(1,0)\}$.



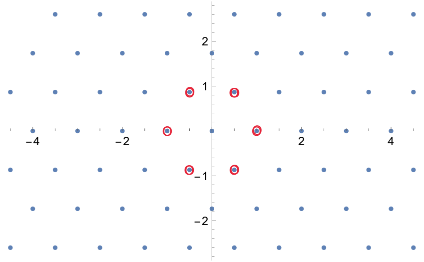
The hexagonal lattice
$H = \left\langle (1,0), (1/2, \sqrt{3}/2) \right\rangle$.

Well-rounded lattices

- $|L| = \min_{0 \neq u \in L} \|u\|^2$
- $$S(L) := \{u \in L : \|u\|^2 = |L|\}.$$



$L = \langle (1,0), (0,2) \rangle$.
$|L| = 1, S(L) = \{\pm(1,0)\}$.



The hexagonal lattice
$H = \left\langle (1,0), (1/2, \sqrt{3}/2) \right\rangle$.
$|L| = 1$,
S(L)= $\{\pm(1,0), (\pm 1/2, \pm\sqrt{3}/2)\}$.

Well-rounded lattices

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

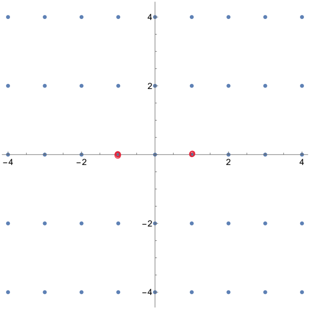
- L is well-rounded (WR) if $S(L)$ generates $\mathbb{R}^n$, that is, if $S(L)$ contains n linearly independent vectors.
- L is said strongly WR if $S(L)$ consists of a basis of L. We call this basis a minimal basis of L.

Well-rounded lattices

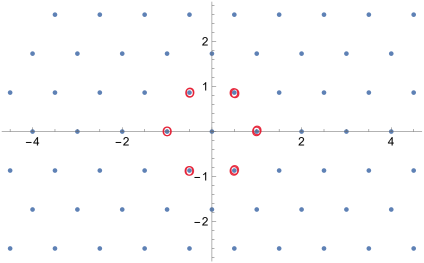
Let L be a lattice in $\mathbb{R}^n$.

- L is well-rounded (WR) if $S(L)$ generates $\mathbb{R}^n$, that is, if $S(L)$ contains n linearly independent vectors.
- L is said strongly WR if $S(L)$ consists of a basis of L. We call this basis a minimal basis of L.

When $n \leq 3$ WRness and strong WRness are equivalent.



$L = \langle (1,0), (0,2) \rangle$ is NOT WR.

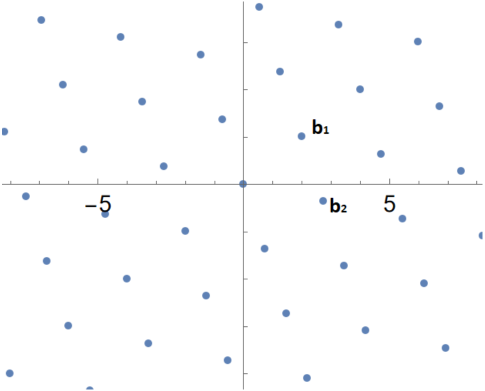


The hexagonal lattice is (strongly) WR.

Well-rounded ideal lattices

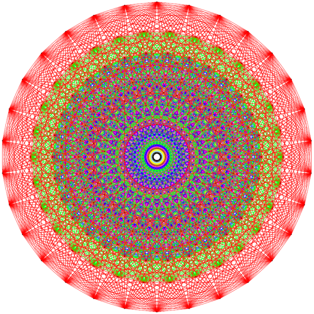
- An ideal I of a number field F is called WR if the lattice $\Phi(I)$ is WR.

Ex: $F = \mathbb{Q}(\sqrt{3})$. The ideal $I = \langle 2, 1-\sqrt{3}\rangle_{\mathbb{Z}}$ is WR since $\Phi(I) = \langle b_1, b_2\rangle_{\mathbb{Z}}$ is WR here
$b_1 = (2, 2)$,
$b_2 = (1-\sqrt{3}, 1+\sqrt{3})$.

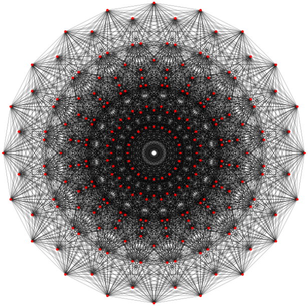


Why WR (ideal) lattices?

- Many well known lattices are WR: E_8, the Leech lattice, etc.
- WR ideal lattices can be used to investigate various problems:
  - the shortest vector problem,
  - kissing numbers,
  - sphere packing problems, etc.



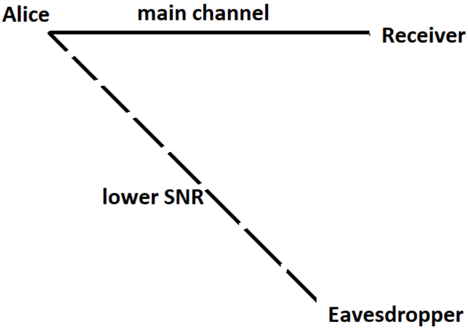
E_8 lattice (Peter McMullen)



The Leech lattice (Gro-Tsen)

Why WR (ideal) lattices?

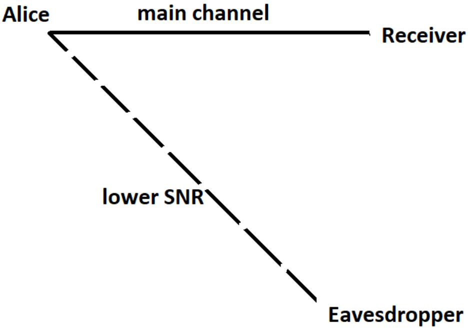
WR ideal lattices also offer a variety of applications to coding theory.



A wiretap fading channel.

Why WR (ideal) lattices?

WR ideal lattices also offer a variety of applications to coding theory.



A wiretap fading channel.

- WR ideal lattices can be used to reduce the value of the average probability of the correct decoding for the eavesdropper.

What have been done?

- Fukshanksy et al.: i) the ring of integer is WR if and only if the field is cyclotomic; ii) sufficient conditions for an ideal of quadratic fields to be WR, the necessary condition is then proven by Srinivasan.

What have been done?

- Fukshanksy et al.: i) the ring of integer is WR if and only if the field is cyclotomic; ii) sufficient conditions for an ideal of quadratic fields to be WR, the necessary condition is then proven by Srinivasan.
- Araujo and Costa: On WR lattices (but not necessarily for WR ideals) of cyclic fields with odd prime degrees.

What have been done?

- Fukshanksy et al.: i) the ring of integer is WR if and only if the field is cyclotomic; ii) sufficient conditions for an ideal of quadratic fields to be WR, the necessary condition is then proven by Srinivasan.
- Araujo and Costa: On WR lattices (but not necessarily for WR ideals) of cyclic fields with odd prime degrees.
- Damir and Mantilla-Soler: construct a parametric family of WR sub-lattices of a tame lattice with a Lagrangian basis.

What have been done?

- Fukshanksy et al.: i) the ring of integer is WR if and only if the field is cyclotomic; ii) sufficient conditions for an ideal of quadratic fields to be WR, the necessary condition is then proven by Srinivasan.
- Araujo and Costa: On WR lattices (but not necessarily for WR ideals) of cyclic fields with odd prime degrees.
- Damir and Mantilla-Soler: construct a parametric family of WR sub-lattices of a tame lattice with a Lagrangian basis.
- Solan: for any lattice L there exists a diagonal real matrix D (called a twist) with positive entries and $\det(D) = 1$ such that DL is WR.

What have been done?

- Fukshanksy et al.: i) the ring of integer is WR if and only if the field is cyclotomic; ii) sufficient conditions for an ideal of quadratic fields to be WR, the necessary condition is then proven by Srinivasan.
- Araujo and Costa: On WR lattices (but not necessarily for WR ideals) of cyclic fields with odd prime degrees.
- Damir and Mantilla-Soler: construct a parametric family of WR sub-lattices of a tame lattice with a Lagrangian basis.
- Solan: for any lattice L there exists a diagonal real matrix D (called a twist) with positive entries and $\det(D) = 1$ such that DL is WR.
- WR twists of ideal lattices of real quadratic fields are investigated by Damir and Karpuk, and of imaginary fields by Le, Tran and Tran.

What have been done?

- Fukshanksy et al.: i) the ring of integer is WR if and only if the field is cyclotomic; ii) sufficient conditions for an ideal of quadratic fields to be WR, the necessary condition is then proven by Srinivasan.
- Araujo and Costa: On WR lattices (but not necessarily for WR ideals) of cyclic fields with odd prime degrees.
- Damir and Mantilla-Soler: construct a parametric family of WR sub-lattices of a tame lattice with a Lagrangian basis.
- Solan: for any lattice L there exists a diagonal real matrix D (called a twist) with positive entries and $\det(D) = 1$ such that DL is WR.
- WR twists of ideal lattices of real quadratic fields are investigated by Damir and Karpuk, and of imaginary fields by Le, Tran and Tran.
- Gnilke et al. and Damir et al.: analyses of some WR lattices used in wiretap channels, and Damir et al.: use WR lattices to optimize coset codes for Gaussian and fading wiretap channels.

What have been done?

- Fukshanksy et al.: i) the ring of integer is WR if and only if the field is cyclotomic; ii) sufficient conditions for an ideal of quadratic fields to be WR, the necessary condition is then proven by Srinivasan.
- Araujo and Costa: On WR lattices (but not necessarily for WR ideals) of cyclic fields with odd prime degrees.
- Damir and Mantilla-Soler: construct a parametric family of WR sub-lattices of a tame lattice with a Lagrangian basis.
- Solan: for any lattice L there exists a diagonal real matrix D (called a twist) with positive entries and $\det(D) = 1$ such that DL is WR.
- WR twists of ideal lattices of real quadratic fields are investigated by Damir and Karpuk, and of imaginary fields by Le, Tran and Tran.
- Gnilke et al. and Damir et al.: analyses of some WR lattices used in wiretap channels, and Damir et al.: use WR lattices to optimize coset codes for Gaussian and fading wiretap channels.

This talk: WR ideal lattices for cyclic cubic and quartic fields.

Why cyclic cucbic and quartic fields?

Let F be a cyclic cubic field with discriminant Δ_F and Galois group $Gal(F) = \langle \sigma \rangle$.

- If a prime $p|\Delta_F$, then $pO_F = P^3$ 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 $\{\sigma^i(x) : 0 \leq i \leq 2\}$ is linearly independent then P is WR.

Why cyclic cucbic and quartic fields?

Let F be a cyclic cubic field with discriminant Δ_F and Galois group $Gal(F) = \langle\sigma\rangle$.

- If a prime $p|\Delta_F$, then $pO_F = P^3$ 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 $\{\sigma^i(x) : 0 \leq i \leq 2\}$ is linearly independent then P is WR.

Similar idea for:

- ideals of the form $\prod_i P_i^{m_i}$ where P_i is the unique ramified prime ideal above some prime p, and
- cyclic quartic fields with some modifications.

Why cyclic cucbic and quartic fields?

Let F be a cyclic cubic field with discriminant Δ_F and Galois group $Gal(F) = \langle \sigma \rangle$.

- If a prime $p | \Delta_F$, then $pO_F = P^3$ 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 $\{\sigma^i(x) : 0 \leq i \leq 2\}$ is linearly independent then P is WR.

Similar idea for:

- ideals of the form $\prod_i P_i^{m_i}$ where P_i is the unique ramified prime ideal obove some prime p, and
- cyclic quartic fields with some modifications.

On the other hand, there are only few defining polynomials of cyclic number fields of degree at least 5 are available.

Strategy

1. Find the defining polynomials of the field.

Strategy

1. Find the defining polynomials of the field.
2. Generate a list of all integral ideals of norms bounded by a certain number.

Strategy

1. Find the defining polynomials of the field.
2. Generate a list of all integral ideals of norms bounded by a certain number.
3. Test which ideals in the list are WR (using the function `qfminim` in Pari/GP).

Strategy

1. Find the defining polynomials of the field.
2. Generate a list of all integral ideals of norms bounded by a certain number.
3. Test which ideals in the list are WR (using the function `qfminim` in Pari/GP).
4. Examine properties of obtained WR ideals such as the geometry of integral bases, the coordinates of shortest vectors with respect to a given integral basis, etc.

Strategy

1. Find the defining polynomials of the field.
2. Generate a list of all integral ideals of norms bounded by a certain number.
3. Test which ideals in the list are WR (using the function `qfminim` in Pari/GP).
4. Examine properties of obtained WR ideals such as the geometry of integral bases, the coordinates of shortest vectors with respect to a given integral basis, etc.
5. Formulate conjectures.

Strategy

1. Find the defining polynomials of the field.
2. Generate a list of all integral ideals of norms bounded by a certain number.
3. Test which ideals in the list are WR (using the function `qfminim` in Pari/GP).
4. Examine properties of obtained WR ideals such as the geometry of integral bases, the coordinates of shortest vectors with respect to a given integral basis, etc.
5. Formulate conjectures.
6. Prove these conjectures.

Cyclic cubic fields

Let F be a cyclic cubic field with conductor m.

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

where $a, b \in \mathbb{Z}$ such that

$$\begin{aligned} a \equiv 2 \mod 3, b \equiv 0 \mod 3 \text{ and } b > 0 \text{ for } 3 \nmid m, \text{ and} \\ a \equiv 6 \mod 9, b \equiv 3 \text{ or } 6 \mod 9 \text{ and } b > 0 \text{ for } 3 | m. \end{aligned} \tag{2}$$

Cyclic cubic fields

Let F be a cyclic cubic field with conductor m.

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

where $a, b \in \mathbb{Z}$ such that

$$\begin{aligned} a \equiv 2 \mod 3, b \equiv 0 \mod 3 \text{ and } b > 0 \text{ for } 3 \nmid m, \text{ and} \\ a \equiv 6 \mod 9, b \equiv 3 \text{ or } 6 \mod 9 \text{ and } b > 0 \text{ for } 3 | m. \end{aligned} \tag{2}$$

The conductor m 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

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

Cyclic cubic fields

Let F be a cyclic cubic field with conductor m.

The discriminant of F is $\Delta_F = m^2$.

Cyclic cubic fields

Let F be a cyclic cubic field with conductor m.

The discriminant of F is $\Delta_F = m^2$. The following polynomial can be used to define F,

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

Cyclic cubic fields

Let F be a cyclic cubic field with conductor m.

The discriminant of F is $\Delta_F = m^2$. The following polynomial can be used to define F,

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

Let $m = p_1 \cdots p_r$ or $m = 9 \cdot p_1 \cdots p_r$ here all p_i are distinct prime numbers and $p_i \equiv 1 \mod 3$ for $i = 1, \cdots, r$ and $p_0 = 3$, $p_1 < p_2 < \cdots < p_r$.

Our results: cyclic cubic fields

Theorem 1

Every cyclic cubic field F has orthogonal and WR ideal lattices. In particular, let m be the conductor of F. Then 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.*

Our results: cyclic cubic fields

Theorem 1

Every cyclic cubic field F has orthogonal and WR ideal lattices. In particular, let m be the conductor of F. Then 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 $\dfrac{m^2}{27}$ is orthogonal and WR.*

Theorem 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 O_F such that $\mathcal{N}(Q) = q$. In this case, Q is WR if and only if $\left(\dfrac{m}{4} \leq q^2 \leq 4m \text{ when } 3 \nmid m\right)$ and $\left(3 \mid q, \dfrac{m}{4} \leq q^2 \leq 4m \text{ when } 3 \mid m\right)$.

Our results: cyclic cubic fields

Theorem 3

Let $m = 9p_1p_2\cdots p_r (r \geq 2)$ *be the conductor* m *of a cyclic cubic field* F *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* $\frac{m}{36} \leq qq'^2 \leq \frac{4m}{9}$.

Cyclic quartic fields

A cyclic quartic field has the form $F = \mathbb{Q}(\beta)$ where $a, b, c, d \in \mathbb{Z}$, a is squarefree and odd, $d = b^2 + c^2$ is squarefree, $b > 0, c > 0$, $\gcd(a, d) = 1$ and $\beta = \sqrt{a(d - b\sqrt{d})}$.

Cyclic quartic fields

A cyclic quartic field has the form $F = \mathbb{Q}(\beta)$ where $a, b, c, d \in \mathbb{Z}$, 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 totally real, and if $a < 0$ then F is totally imaginary.

Cyclic quartic fields

A cyclic quartic field has the form $F = \mathbb{Q}(\beta)$ where $a, b, c, d \in \mathbb{Z}$, 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 totally real, and if $a < 0$ then F is totally imaginary.

A defining polynomial of F is

$$df(x) = x^4 - 2adx^2 + a^2c^2d.$$

Cyclic quartic fields

A cyclic quartic field has the form $F = \mathbb{Q}(\beta)$ where $a, b, c, d \in \mathbb{Z}$, 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 totally real, and if $a < 0$ then F is totally imaginary.

A defining polynomial of F is

$$df(x) = x^4 - 2adx^2 + a^2c^2d.$$

The discriminant of F is

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

Our results: cyclic quartic fields

Theorem 4

Let F be a cyclic quartic field defined by a, b, c, d and $D \mid d$, $A \mid a$ such that d is a quadratic non-residue $\pmod{q}$ for each prime divisor q of A. Then there are unique ideals of norm D and A, denoted by P_D and Q_A respectively. Let

$$\mathcal{M} = \{16A^2d, 8|a|d, 4D^2d+4|a|d, 16D^2A^2, 4D^2A^2+4|a|d, 4D^2Q_A^2+4A^2d\}.$$

Then the ideal P_DQ_A is WR if and only if $d \equiv 1 \pmod{4}$, $b \equiv 1 \pmod{2}$, $a + b \equiv 1 \pmod{4}$ and $D^2A^2 + A^2d + 2|a|d \leq \min \mathcal{M}$.

Our results: cyclic quartic fields

Theorem 5

With the notation given in Theorem 4, the following hold.

i) *The ideal* P_D *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* $\frac{1}{5}d \leq D^2 \leq 5d$,
   - $|a| = 3$ *and* $d \leq D^2 \leq 9d$,
   - $|a| = 5$ *and* $\frac{7}{3}d \leq D^2 \leq 5d$.

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

Our results: cyclic quartic fields

Theorem 6

Let F be a cyclic quartic field defined by a, b, c, d 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) $p \mid d$.

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

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

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 5 are satisfied.

Our 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.

Our 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 these fields.

Our 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 these fields.
- This conjecture agrees with the observation in Fukshansky et al. for real quadratic fields and was later proved by Srinivasan.

Our 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 these fields.
- This conjecture agrees with the observation in Fukshansky et al. for real quadratic fields and was later proved by Srinivasan.
- 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.

Our 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 these fields.
- This conjecture agrees with the observation in Fukshansky et al. for real quadratic fields and was later proved by Srinivasan.
- 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.
- The conjecture does not hold for cyclic quartic fields of even discriminant.

Conclusion

- We establish the conditions for the existence of WR ideal lattices in cyclic number fields of degrees 3 and 4.
- We show that every cyclic cubic field has orthogonal and WR ideal lattices.
- For cyclic quartic fields, we consider WR ideals of both the real and complex cases. This is the first time such results are obtained for these classes of number fields.
- We give families of cyclic cubic and cyclic quartic fields that admit WR ideals and explicitly construct minimal integral bases of these ideals.

Thank you so much for your attention!