An alternative ordering on real quadratic fields and a connection to complex equiangular lines

Gene S. Kopp

Louisiana State University

Purdue University Automorphic Forms and Representation Theory and PANTHA Joint Seminar
April 3, 2025

Orders in quadratic fields

An order $\mathcal{O}$ in a field F is a subring such that

- $\mathcal{O}$ has finite rank as an additive group, and
- $\mathbb{Q}\mathcal{O} = F$.

Proposition

If $\mathcal{O}$ is an order in a quadratic field F with $\Delta_F = \Delta$, then

$$\mathcal{O} = \mathbb{Z} + f\frac{\Delta + \sqrt{\Delta}}{2}\mathbb{Z}$$

for some $f \in \mathbb{N}$.

The number f is called the conductor of $\mathcal{O}$.

Unit-generated orders in quadratic fields

We call an order $\mathcal{O}$ unit-generated if it is generated as an abelian group by $\mathcal{O}^\times$.

Proposition

If $\mathcal{O}$ is a unit-generated order in a quadratic field, then for some $n \in \mathbb{Z}_{\geq 0}$, either

(1) $\mathcal{O} = \mathcal{O}_n^+ = \mathbb{Z} + \varepsilon_n^+\mathbb{Z}$ for $\varepsilon_n^+ = \dfrac{n+\sqrt{n^2-4}}{2}$, or

(2) $\mathcal{O} = \mathcal{O}_n^- = \mathbb{Z} + \varepsilon_n^-\mathbb{Z}$ for $\varepsilon_n^- = \dfrac{n+\sqrt{n^2+4}}{2}$.

Here, $\mathrm{Nm}(\varepsilon_n^+) = 1$ and $\mathrm{Nm}(\varepsilon_n^-) = -1$.

We will focus on (1) and set $\mathcal{O}_n := \mathcal{O}_n^+$ and $F_n = \mathbb{Q}(\sqrt{n^2-4})$ its fraction field.

The unit ordering on real quadratic fields

Every real quadratic field contains some $\mathcal{O}_n = \mathbb{Z} + \varepsilon_n^+ \mathbb{Z}$.

n	ε_n^+	F_n	f	j
0	$\frac{1+\sqrt{-3}}{2}$	$\mathbb{Q}(\sqrt{-3})$	1	1
1	$\sqrt{-1}$	$\mathbb{Q}(\sqrt{-1})$	1	1
2	1	$\mathbb{Q}$	1	1
3	$\frac{3+\sqrt{5}}{2}$	$\mathbb{Q}(\sqrt{5})$	1	1
4	$2+\sqrt{3}$	$\mathbb{Q}(\sqrt{3})$	1	1
5	$\frac{5+\sqrt{21}}{2}$	$\mathbb{Q}(\sqrt{21})$	1	1
6	$3+2\sqrt{2}$	$\mathbb{Q}(\sqrt{2})$	2	1
7	$\frac{7+3\sqrt{5}}{2}$	$\mathbb{Q}(\sqrt{5})$	3	2
8	$4+\sqrt{15}$	$\mathbb{Q}(\sqrt{15})$	1	1

- f = conductor
- j = height = number of times F_n has appeared, and $\varepsilon_n^+ = (\varepsilon_{F_n}^+)^j$.

Repetitions are sparse

$\mathbb{Q}(\sqrt{5})$, $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{21})$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{5})$, $\mathbb{Q}(\sqrt{15})$, $\mathbb{Q}(\sqrt{77})$, $\mathbb{Q}(\sqrt{6})$, $\mathbb{Q}(\sqrt{13})$, $\mathbb{Q}(\sqrt{35})$, $\mathbb{Q}(\sqrt{165})$, $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{221})$, $\mathbb{Q}(\sqrt{7})$, $\mathbb{Q}(\sqrt{285})$, $\mathbb{Q}(\sqrt{5})$, $\mathbb{Q}(\sqrt{357})$, $\mathbb{Q}(\sqrt{11})$, $\ldots$

Repetitions occur when $\varepsilon_n^+ = (\varepsilon_{F_n}^+)^j$ for $j \geq 2$, that is, when $n = \mathrm{Tr}((\varepsilon_{n_1}^+)^j) =: T_j^*(n_1)$.

j	$n = T_j^*(n_1)$
2	$n_1^2 - 2$
3	$n_1^3 - 3n_1$
4	$n_1^4 - 4n_1^2 + 2$
5	$n_1^5 - 5n_1^3 + 5n_1$
6	$n_1^6 - 6n_1^4 + 9n_1^2 - 2$

As $X \to \infty$,

$$\{3 \leq n \leq X : n = T_j^*(n_1),\ n_1 \geq 3,\ j \geq 2\} << \sqrt{X}.$$

Philosophy of the unit ordering

- A serious computation about a real quadratic field probably involves computing the fundamental unit.
- The unit ordering builds in the complexity of fundamental unit into the parameter n.
- Class number formula says

$$h_F \log \varepsilon_F \approx \sqrt{\Delta_F}.$$

  In the unit ordering, the regulator is usually small, so the class number is usually large.
- Class numbers h_{F_n} should behave somewhat like class numbers of imaginary quadratic fields.

Class monoids and class groups of orders

For any order $\mathcal{O}$ in a field K, the class monoid is

$$\mathrm{Clm}(\mathcal{O}) = \frac{\{\text{nonzero fractional ideals of } \mathcal{O}\}}{\{\text{nonzero principal fractional ideals of } \mathcal{O}\}}.$$

The class group is

$$\mathrm{Cl}(\mathcal{O}) = \frac{\{\text{nonzero invertible fractional ideals of } \mathcal{O}\}}{\{\text{nonzero principal fractional ideals of } \mathcal{O}\}}.$$

Example (Class monoid of $\mathcal{O}_{10} = \mathbb{Z}[2\sqrt{6}]$)

$\times$	(1)	$(3, 2\sqrt{6})$	$(2, 2\sqrt{6})$
(1)	(1)	$(3, 2\sqrt{6})$	$(2, 2\sqrt{6})$
$(3, 2\sqrt{6})$	$(3, 2\sqrt{6})$	(1)	$(2, 2\sqrt{6})$
$(2, 2\sqrt{6})$	$(2, 2\sqrt{6})$	$(2, 2\sqrt{6})$	$(2, 2\sqrt{6})$

Class monoids and class groups of quadratic orders

If $\mathcal{O}$ is a quadratic order, there are canonical bijections between the following sets.

(0) $\mathrm{Clm}(\mathcal{O})$

(1) $\displaystyle\bigsqcup_{\mathcal{O}' \supseteq \mathcal{O}} \mathrm{Cl}(\mathcal{O}')$

(2) $\mathrm{GL}_2(\mathbb{Z}) \backslash \{Q(x,y) = ax^2 + bxy + cy^2 : b^2 - 4ac = f^2 \Delta_F\}$

(3) If $\mathcal{O} = \mathcal{O}_n$, the set of $\mathrm{GL}_2(\mathbb{Z})$ conj. classes in $\mathrm{SL}_2(\mathbb{Z})$ of trace n.

There are compatible canonical bijections between

(1') $\mathrm{Cl}(\mathcal{O})$

(2') $\mathrm{GL}_2(\mathbb{Z}) \Big\backslash \left\{ Q(x,y) = ax^2 + bxy + cy^2 : \begin{array}{l} b^2 - 4ac = f^2 \Delta_F, \\ \gcd(a,b,c) = 1 \end{array} \right\}$.

(3') If $\mathcal{O} = \mathcal{O}_n$, the set of $\mathrm{GL}_2(\mathbb{Z})$ conj. classes in $\mathrm{SL}_2(\mathbb{Z})$ of trace n that can't be written as nontrivial perfect powers.

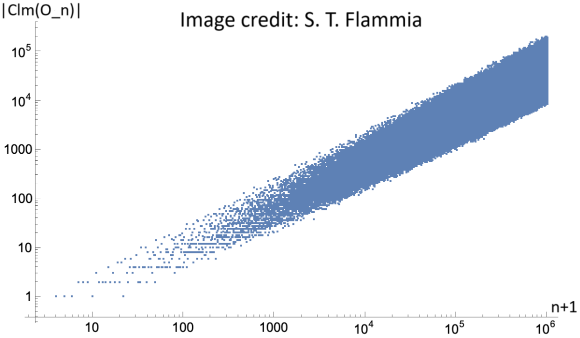
Growth of class numbers of $\mathcal{O}_n$

Theorem (K and Lagarias 2024)

As $n \to \infty$,

$$\log|\mathrm{Clm}(\mathcal{O}_n)| = \log|\mathrm{Cl}(\mathcal{O}_n)| + O\left(\frac{\log n}{\log\log n}\right) = \log n + o(\log n).$$

The implied constant in the $O\left(\frac{\log n}{\log\log n}\right)$ term is effective, but the $o(\log n)$ term is ineffective.



Proof sketch of growth of class numbers, part 1

Write $\mathcal{O}_n = \mathbb{Z}[f\frac{\Delta+\sqrt{\Delta}}{2}]$. For each $f'|f$, there is a surjection

$$\mathrm{Cl}(\mathbb{Z}[f\tfrac{\Delta+\sqrt{\Delta}}{2}]) \to \mathrm{Cl}(\mathbb{Z}[f'\tfrac{\Delta+\sqrt{\Delta}}{2}]).$$

Thus, $|\mathrm{Cl}(\mathcal{O}_n)| \leq |\mathrm{Clm}(\mathcal{O}_n)| \leq \sigma_0(f)\,|\mathrm{Cl}(\mathcal{O}_n)|$.

But $\log \sigma_0(f) << \frac{\log f}{\log\log f} << \frac{\log n}{\log\log n}$, so

$$\log|\mathrm{Clm}(\mathcal{O}_n)| = \log|\mathrm{Cl}(\mathcal{O}_n)| + O\left(\frac{\log n}{\log\log n}\right).$$

Proof sketch of growth of class numbers, part 2

Let $F = F_n$. There is an exact sequence

$$1 \to \frac{\mathcal{O}_F^\times}{\mathcal{O}_n^\times} \to \frac{(\mathcal{O}_F/f\mathcal{O}_F)^\times}{(\mathcal{O}_n/f\mathcal{O}_F)^\times} \to \mathrm{Cl}(\mathcal{O}_n) \to \mathrm{Cl}(\mathcal{O}_F) \to 1.$$

Thus, we have

$$\log|\mathrm{Cl}(\mathcal{O}_n)| = \log|\mathrm{Cl}(\mathcal{O}_F)| + \log\left|\frac{(\mathcal{O}_F/f\mathcal{O}_F)^\times}{(\mathcal{O}_n/f\mathcal{O}_F)^\times}\right| - \log\left|\frac{\mathcal{O}_F^\times}{\mathcal{O}_n^\times}\right|.$$

The term $\log\left|\frac{\mathcal{O}_F^\times}{\mathcal{O}_n^\times}\right| = \log j << \log\log\varepsilon_n^+ << \log\log n$ is negligible.

Proof sketch of growth of class numbers, part 3

The Brauer–Siegel Theorem says that (ineffectively)

$$\begin{aligned}\log|\mathrm{Cl}(\mathcal{O}_F)| &= \tfrac{1}{2}\log\Delta + \log\log\varepsilon_F + o(\log\Delta)\\ &= \tfrac{1}{2}\log\Delta + O(\log\log n) + o(\log\Delta).\end{aligned}$$

We also have, taking $\omega = \frac{\Delta+\sqrt{\Delta}}{2}$,

$$\frac{(\mathcal{O}_F/f\mathcal{O}_F)^\times}{(\mathcal{O}_n/f\mathcal{O}_F)^\times} = \frac{((\mathbb{Z}+\omega\mathbb{Z})/(f\mathbb{Z}+f\omega\mathbb{Z}))^\times}{((\mathbb{Z}+f\omega\mathbb{Z})/(f\mathbb{Z}+f\omega\mathbb{Z}))^\times},$$

from which we can show $\log\left|\frac{(\mathcal{O}_F/f\mathcal{O}_F)^\times}{(\mathcal{O}_n/f\mathcal{O}_F)^\times}\right| = \log f + o(\log f)$ Thus (with some care),

$$\begin{aligned}\log|\mathrm{Cl}(\mathcal{O}_F)| &= \log\sqrt{f^2\Delta} + O(\log\log n) + o(\log\Delta) + o(\log f)\\ &= \log n + o(\log n),\end{aligned}$$

using $f^2\Delta = n^2 - 4$.

Class number one problem

The following theorem was previously a conjecture of Mollin.

Theorem (Byeon–Kim–Lee 2007)

Let $n \geq 0$, $n \neq 2$. If $\mathcal{O}_n = \mathcal{O}_{F_n}$, then

$$|\mathrm{Cl}(\mathcal{O}_n)| = 1 \iff n \in \{0, 1, 3, 4, 5, 9, 21\}.$$

The following extension to nonmaximal orders has been verified numerically for $n \leq 10^6$.

Conjecture (Kopp–Lagarias 2025)

Let $n \geq 0$, $n \neq 2$. Then

$$|\mathrm{Cl}(\mathcal{O}_n)| = 1 \iff n \in \{0, 1, 3, 4, 5, 6, 7, 9, 11, 21\}.$$

Units of negative norm

Contrast the unit ordering and the discriminant ordering.

Proposition (elementary)

The field F_n has a unit of negative norm if and only if $n = k^2 + 2$ or $n = T_j^*(n_1)$ for some $j \geq 2$ and $n_1 = k^2 + 2$.

Theorem (Fouvrey–Klüners 2010)

As $X \to \infty$,

$$\frac{c_1 + o(1)}{\sqrt{\log X}} \leq \frac{\{\text{fund. discs. } 0 < \Delta < X : \mathrm{Nm}(\varepsilon_{\mathbb{Q}(\Delta)}) = -1\}}{\{\text{fund. discs. } 0 < \Delta < X\}} \leq \frac{c_2 + o(1)}{\sqrt{\log X}}$$

for explicit positive constants c_1, c_2.

Units of odd trace

Contrast the unit ordering and the discriminant ordering.

Proposition (elementary)

The field F_n has a unit of odd trace if and only if n is odd or $n = T_j^*(n_1)$ for some $j \geq 2$ and n_1 odd.

Theorem (Appleby–Flammia–K 2025 using Taniguchi–Thorne 2013; special thanks to J. Wang)

As $X \to \infty$,

$$\frac{2}{27} + o(1) \leq \frac{\{\text{fund. discs. } 0 < \Delta < X : \operatorname{Tr}(\varepsilon_{\mathbb{Q}(\Delta)}) \text{ is odd}\}}{\{\text{fund. discs. } 0 < \Delta < X\}} \leq \frac{1}{3} + o(1).$$

SIC-POVMs

Definition

A SIC or SIC-POVM (symmetric, informationally complete, positive operator-valued measure) is (an set of quantum measurements equivalent) to d^2 equiangular lines in $\mathbb{C}^d$.

Example (SIC for $d = 2$)

Vertecies of a regular tetrahedron in $\mathbb{P}^1(\mathbb{C})$:

$$\left\{ \left[1 : \frac{1+i}{1+\sqrt{3}} \right], \left[1 : \frac{-1-i}{1+\sqrt{3}} \right], \left[\frac{1+i}{1+\sqrt{3}} : 1 \right], \left[\frac{-1-i}{1+\sqrt{3}} : 1 \right] \right\}$$

Zauner's conjecture

Conjecture (Zauner 1999)

There is at least one SIC in every dimension $d \geq 1$.

- Zauner also conjectured that SICs could be constructed with certain symmetries related to a *d*-dimensional representation of the (Weyl–)Heisenberg group $\mathrm{WH}(\mathbb{Z}/d\mathbb{Z})$.
- Weyl–Heisenberg SICs are known in dimensions 1–53 and many other dimensions as large as $d = 1299$. Some involve algebraic numbers of huge degree (> 10000).
- Numerical (probable) SICs are known in dimension 1–193 and various higher dimensions. Most exact and numerical solutions have been found by Grassl and Scott.
- SICs are only known to exist in finitely many dimensions.

Example ($d = 5$)

The unique SIC in dimension 5 is given by equiangular lines

$$\{\mathbb{C}\mathbf{v}_1, \mathbb{C}\mathbf{v}_2, \ldots, \mathbb{C}\mathbf{v}_{25}\},$$

for unit vectors $\mathbf{v}_i$ whose inner products for $i \neq j$ are

$$\langle \mathbf{v}_i, \mathbf{v}_j \rangle = \frac{1}{\sqrt{6}} \eta_{ij},$$

where $|\eta_{ij}| = 1$, and the η_{ij}^2 are (up to multiplication by fifth roots of unity) the roots of the polynomial

$$\begin{aligned} x^8 &- (8 - 5\sqrt{3})x^7 + (53 - 30\sqrt{3})x^6 - (156 - 90\sqrt{3})x^5 \\ &+ (225 - 130\sqrt{3})x^4 - (156 - 90\sqrt{3})x^3 + (53 - 30\sqrt{3})x^2 \\ &- (8 - 5\sqrt{3})x + 1 = 0. \end{aligned}$$

SICs from ideal classes

Conjecture (K 2017; K–Lagarias 2024; Appleby–Flammia–K 2025)

There is a bijection

$$\mathrm{Cl}_{\mathrm{m}}(\mathcal{O}_{d-1}) \xrightarrow{\Phi} \left\{ \begin{array}{c} \text{projective unitary equivalence classes of} \\ \text{Weyl–Heisenberg SICs in dimension } d \end{array} \right\}.$$

This bijection is described by an explicit formula using refined Stark units produced by the Shintani–Faddeev modular cocycle (see A–F–K for details).

Under this bijection, the field of unitary invariants is a particular generalized ray class field (an abelian extension of F_{d-1})

$$F^{\mathrm{inv}}(\Phi([\mathfrak{a}])) = H^{\mathcal{O}'}_{d\infty_1\infty_2}$$

with $\mathcal{O}' = (\mathfrak{a} : \mathfrak{a}) = \mathbb{Z}[f' \frac{\Delta+\sqrt{\Delta}}{2}]$ for some $f'|f$.

r-SICs

Definition

An r-SIC (also called a maximal equichordal fusion frame) is a set $\{\Pi_1, \Pi_2, \ldots, \Pi_{d^2}\} \subset \mathrm{Mat}_{d\times d}(\mathbb{C})$ satisfying

(1) $\mathrm{Tr}(\Pi_i \Pi_j) = \begin{cases} r & \text{if } i = j, \\ \dfrac{r(d-r)}{d^2-1} & \text{if } i \neq j. \end{cases}$

(2) $\Pi_i^2 = \Pi_i$.

(3) $\Pi_1^\dagger = \Pi_i$.

An r-SIC is a set of rank-r Hermitian projections onto d^2 "equiangular" (really, equichordal) subspaces of $\mathbb{C}^d$.

Can be thought of as an "optimal code" on the Grassmannian $\mathrm{Gr}_r(\mathbb{C}^d)$ with the chordal metric.

The dimension and rank grids

All solutions to the Diophantine equation

$$\frac{r(d-r)}{d^2-1} = \frac{1}{k}$$

in positive integers (d, r, k) with $1 \leq r < \frac{d-1}{2}$ are given by...
$(d, r, k) = (d_{j,m}, r_{j,m}, k_j)$

$$d_{j,m} = \frac{\varepsilon^{j(m+1)} - \varepsilon^{-jm}}{\varepsilon^j - 1}, \qquad r_{j,m} = \frac{\varepsilon^{jm} - \varepsilon^{-jm}}{\varepsilon^j - \varepsilon^{-j}}, \qquad k_j = \varepsilon^j + 2 + \varepsilon^{-j},$$

where $\varepsilon = \varepsilon_F^+$ is a totally positive fundamental unit for a real quadratic field F. The grids of solutions for r and d indexed by (j, m) are called the dimension grid and rank grid for F, respectively.

Example of dimension and rank grids

For $F = \mathbb{Q}(\sqrt{5})$ and $\varepsilon_F^+ = \frac{3+\sqrt{5}}{2}$, we have:

$$d_{j,m} = \begin{matrix} \vdots & \vdots & \vdots & \vdots & \\ 48 & 2\,255 & 105\,937 & 4\,976\,784 & \dots \\ 19 & 341 & 6\,119 & 109\,801 & \dots \\ 8 & 55 & 377 & 2\,584 & \dots \\ 4 & 11 & 29 & 76 & \dots \end{matrix}$$

$$r_{j,m} = \begin{matrix} \vdots & \vdots & \vdots & \vdots & \\ 1 & 47 & 2\,208 & 103\,729 & \dots \\ 1 & 18 & 323 & 5\,796 & \dots \\ 1 & 7 & 48 & 329 & \dots \\ 1 & 3 & 8 & 21 & \dots \end{matrix}$$

r-SICs from ideal classes

Conjecture (Appleby–Flammia–K 2025)

For each real quadratic field F and each pair of positive integers (j, m), there is an injective map

$$\mathrm{Clm}(\mathcal{O}_{k_j-2}) \xrightarrow{\Phi} \left\{ \begin{array}{c} \text{projective unitary equivalence classes of} \\ \text{Weyl–Heisenberg } r_{j,m}\text{-SICs in dimension } d_{j,m} \end{array} \right\}.$$

This bijection is described by an explicit formula using refined Stark units produced by the Shintani–Faddeev modular cocycle (see A–F–K for details).

Under this map, the field of unitary invariants is a particular generalized ray class field (an abelian extension of F)

$$F^{\mathrm{inv}}(\Phi([\mathfrak{a}])) = H^{\mathcal{O}'}_{d_{j,m}\infty_1\infty_2}$$

with $\mathcal{O}' = (\mathfrak{a} : \mathfrak{a}) = \mathbb{Z}[f' \frac{\Delta+\sqrt{\Delta}}{2}]$ for some $f'|f$.

Implications for explicit class field theory over real quadratic fields

Theorem (Appleby–Flammia–K 2025)

Let F be a real quadratic field.

(1) If F has a unit of odd trace, then every abelian extension of F is contained in one of the fields $H^{\mathcal{O}_F}_{d_{j,m}\infty_1\infty_2}$.

(2) If F does not have a unit of odd trace, then every abelian extension of F not ramified at 2 is contained in one of the fields $H^{\mathcal{O}_F}_{d_{j,m}\infty_1\infty_2}$.

Thus, conjecturally, unitary invariants of r-SICs generate all the abelian extensions of a positive proportion of real quadratic fields.

As a long-term research goal, I hope to prove these conjectures and develop the theory of r-SICs to a level on par with the theory of elliptic curves with complex multiplication (which describes explicit class field theory over imaginary quadratic fields).

Thank you!

Thank you for listening! Any questions?