

# Class field theory for nonmaximal orders (abstractly and explicitly)

Gene S. Kopp

Louisiana State University

University of Georgia  
April 17, 2024

## Abelian extensions of $\mathbb{Q}$

### Question

Fix  $K$  a number field. What are the abelian Galois extensions of  $K$ ?

### Theorem (Kronecker–Weber)

For  $K = \mathbb{Q}$ , every abelian Galois extension is contained in some  $\mathbb{Q}(\zeta_n)$ , where  $\zeta_n$  is a primitive  $n$ -th root of 1.

### Example (quadratic extensions of $\mathbb{Q}$ )

$$\sqrt{2} = \zeta_8 + \zeta_8^{-1}, \quad \text{so } \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\zeta_8).$$

$$\sqrt{-7} = 1 + 2\zeta_7 + 2\zeta_7^2 + 2\zeta_7^4, \quad \text{so } \mathbb{Q}(\sqrt{-7}) \subset \mathbb{Q}(\zeta_7).$$

### Example (non-abelian extension of $\mathbb{Q}$ )

For all  $n \in \mathbb{N}$ ,  $\sqrt[3]{2} \notin \mathbb{Q}(\zeta_n)$ .

## Abelian extensions of an imaginary quadratic field, unramified case

Fix  $K$  an imaginary quadratic field of discriminant  $\Delta$ .

Then  $\mathcal{O}_K = \mathbb{Z}[\omega] = \mathbb{Z} + \omega\mathbb{Z}$  where  $\omega = \frac{\Delta + \sqrt{\Delta}}{2}$ .

### Theorem (Weber, Hilbert)

Let  $K^{\text{ur}}$  be the maximal unramified abelian extension of  $K$ . Then  $K^{\text{ur}}/K$  is a finite extension of degree  $h_K = |\text{Cl}(K)|$ , it is the minimal extension such that there exists an elliptic curve

$E = \{y^2 = x^3 + ax + b\}$  with  $a, b \in K^{\text{ur}}$  and  $E(\mathbb{C}) \cong \mathbb{C}/(\mathbb{Z} + \omega\mathbb{Z})$ .

### Example ( $\mathbb{Q}(\frac{1+\sqrt{-7}}{2})^{\text{ur}} = \mathbb{Q}(\frac{1+\sqrt{-7}}{2})$ )

$E(\mathbb{C}) \cong \mathbb{C}/(\mathbb{Z} + \frac{1+\sqrt{-7}}{2}\mathbb{Z})$  for  $E = \{y^2 = x^3 - 140x - 784\}$ .

### Example ( $\mathbb{Q}(\sqrt{-6})^{\text{ur}} = \mathbb{Q}(\sqrt{-3}, \sqrt{2})$ )

$E(\mathbb{C}) \cong \frac{\mathbb{C}}{\mathbb{Z} + \sqrt{-6}\mathbb{Z}}$  for  $E = \{y^2 = x^3 - 3(95 + 4\sqrt{2})x + 46(7 + 17\sqrt{2})\}$ .

## Abelian extensions of an imaginary quadratic field, general case

Fix  $K$  an imaginary quadratic field of discriminant  $\Delta$ .

Then  $\mathcal{O}_K = \mathbb{Z}[\omega] = \mathbb{Z} + \omega\mathbb{Z}$  where  $\omega = \frac{\Delta + \sqrt{\Delta}}{2}$ .

### Theorem (Weber, others)

Consider the complex torus  $\mathbb{C}/(\mathbb{Z} + \omega\mathbb{Z})$ . Let  $H_m$  be the minimum field extension of  $K$  such that there exists an elliptic curve

$E$  with  $m$ -torsion points in  $H_m$  and  $E(\mathbb{C}) \cong \mathbb{C}/(\mathbb{Z} + \omega\mathbb{Z})$ .

Then any abelian extension of  $K$  is contained in some  $H_m$ .

### Observation (Weber, Söhngen)

The above theorem remains true if  $\mathbb{C}/(\mathbb{Z} + \omega\mathbb{Z})$  is replaced with  $\mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z})$  for any  $\tau \in K$ . However, the  $H_m$  are replaced by larger fields  $H_m^{\mathcal{O}}$  depending on the **multiplier ring**

$$\mathcal{O} = \text{ord}(\mathbb{Z} + \tau\mathbb{Z}) = \{\alpha \in K : \alpha(\mathbb{Z} + \tau\mathbb{Z}) \subseteq \mathbb{Z} + \tau\mathbb{Z}\}.$$

## Abelian extensions of an arbitrary number field

Class field theory (early 20th century work of Artin, Furtwängler, Hasse, Hilbert, Takagi, Weber, ...) establishes, for any number field  $K$ :

- Ray class groups  $\text{Cl}_{m,\Sigma}(K)$  defined as refined quotients of ideal groups.
- Ray class fields  $H_{m,\Sigma}$  having the properties:
  - $\text{Gal}(H_{m,\Sigma}/K) \cong \text{Cl}_{m,\Sigma}(K)$ .
  - $H_{m,\Sigma}$  may be specified using prime splitting conditions.
  - Every abelian extension of  $K$  is contained in some  $H_{m,\Sigma}$ .

These generalize the fields  $H_m$  in the imaginary quadratic case.

### Remark

The ray class fields are not defined “explicitly” and are difficult to calculate computationally.

## Class field theory for orders of an arbitrary number field

This talk (work of K and Lagarias) will present an approach to class field theory based on more general class groups and class fields:

- Ray class groups of orders  $\text{Cl}_{m,\Sigma}(\mathcal{O})$  defined as refined quotients of **invertible** ideal groups.
- Ray class fields  $H_{m,\Sigma}^{\mathcal{O}}$  having the properties:
  - $\text{Gal}(H_{m,\Sigma}^{\mathcal{O}}/K) \cong \text{Cl}_{m,\Sigma}(\mathcal{O})$ .
  - $H_{m,\Sigma}^{\mathcal{O}}$  may be specified using splitting conditions of **prime ideals** of  $\mathcal{O}$ .
  - Every abelian extension of  $K$  is contained in some  $H_{m,\Sigma}^{\mathcal{O}}$ .

These generalize the fields  $H_m^{\mathcal{O}}$  in the imaginary quadratic case. The approach complements an idélic approach to “ray class fields for orders” by independent work of Campagna and Pengo (2021).

## Orders of number fields and fractional ideals

### Definition

Let  $K$  be a number field. An **order**  $\mathcal{O} \subset K$  is a subring for which

- $\mathcal{O}$  has finite rank as a  $\mathbb{Z}$ -module. (Excludes, e.g.,  $\mathbb{Z}[\frac{1}{2}]$  in  $\mathbb{Q}$ .)
- $\mathbb{Q}\mathcal{O} = K$ . (Excludes, e.g.,  $\mathbb{Z}$  in  $\mathbb{Q}(i)$ .)

The ring of integers  $\mathcal{O}_K$  is the maximal order. Examples of nonmaximal orders include  $\mathbb{Z}[\sqrt{5}]$  in  $\mathbb{Q}(\sqrt{5})$  and  $\mathbb{Z}[3i]$  in  $\mathbb{Q}(i)$ .

### Definition

A **fractional ideal**  $\mathfrak{a}$  of  $\mathcal{O}$  is a finite rank  $\mathcal{O}$ -submodule of  $K$ .  
(Equivalently, some integer multiple  $n\mathfrak{a}$  is in integral ideal of  $\mathcal{O}$ .)

Any lattice  $\Lambda \subset K$  is a fractional ideal of its **multiplier ring**

$$\text{ord}(\Lambda) = \{\alpha \in K : \alpha\Lambda \subseteq \Lambda\}.$$

## Invertible fractional ideals

Let  $\mathcal{O}$  be an order in a number field  $K$ .

### Definition

The fractional ideal  $\mathfrak{a}$  is **invertible** if there exists another fractional ideal  $\mathfrak{b}$  such that  $\mathfrak{a}\mathfrak{b} = \mathcal{O}$ .

### Example

$2\mathbb{Z} + 2i\mathbb{Z}$  is **not** invertible as a  $\mathbb{Z}[2i]$ -ideal but **is** invertible as a  $\mathbb{Z}[i]$ -ideal.

### Example

$\mathfrak{q} = 2\mathbb{Z} + 2\sqrt[3]{2}\mathbb{Z} + 4\sqrt[3]{4}$  is an ideal of  $\text{ord}(\mathfrak{q}) = \mathbb{Z} + 2\sqrt[3]{2}\mathbb{Z} + 2\sqrt[3]{4}$ , but it is **not** an invertible ideal of **any** order.

## Colons, conductors, and coprimality

### Definition

For any two fractional ideals  $\mathfrak{a}, \mathfrak{b}$  of orders in  $K$ , the **colon ideal** is

$$(\mathfrak{a} : \mathfrak{b}) = \{\alpha \in K : \alpha \mathfrak{b} \subseteq \mathfrak{a}\}.$$

Special cases are the **conductor ideal of an order**  $\mathfrak{f}(\mathcal{O}) = (\mathcal{O} : \mathcal{O}_K)$  and the **multiplier ring of an ideal**  $\text{ord}(\mathfrak{a}) = (\mathfrak{a} : \mathfrak{a})$ .

### Definition

A fractional  $\mathcal{O}$ -ideal  $\mathfrak{c}$  is **coprime** to an integral  $\mathcal{O}$ -ideal  $\mathfrak{m}$  if  $\mathfrak{c} = \mathfrak{a}\mathfrak{b}^{-1}$  where  $\mathfrak{b}$  is invertible,  $\mathfrak{a} + \mathfrak{m} = \mathcal{O}$ , and  $\mathfrak{b} + \mathfrak{m} = \mathcal{O}$ .

### Example

The fractional ideal  $\mathfrak{c} = i\mathbb{Z}[2i]$  is **not** coprime to the conductor  $\mathfrak{f}(\mathbb{Z}[2i]) = 2\mathbb{Z}[i]$  even though  $\mathfrak{c}^2 = \mathbb{Z}[2i]$ .

### Proposition

Fractional  $\mathcal{O}$ -ideals coprime to  $\mathfrak{f}(\mathcal{O})$  are invertible.

## Ray class groups of orders

Let  $\mathcal{O}$  be an order in a number field  $K$ . Fix

- $\mathfrak{m}$  an ideal of  $\mathcal{O}$ ;
- $\Sigma$  a subset of the real embeddings  $\{\rho : K \rightarrow \mathbb{R}\}$ .

### Definition (K and Lagarias 2022)

The **ray class group** is defined as a quotient group

$$\text{Cl}_{\mathfrak{m}, \Sigma}(\mathcal{O}) = \frac{\text{J}_{\mathfrak{m}}^*(\mathcal{O})}{\mathsf{P}_{\mathfrak{m}, \Sigma}(\mathcal{O})}$$

where

$$\begin{aligned}\text{J}_{\mathfrak{m}}^*(\mathcal{O}) &= \{\text{invertible fractional ideals of } \mathcal{O} \text{ coprime to } \mathfrak{m}\}, \text{ and} \\ \mathsf{P}_{\mathfrak{m}, \Sigma}(\mathcal{O}) &= \{\alpha\mathcal{O} : \alpha \in K^\times, \alpha \equiv 1 \pmod{\mathfrak{m}}, \rho(\alpha) > 0 \text{ for all } \rho \in \Sigma\}.\end{aligned}$$

## Change of modulus

We need to add further coprimality conditions to the definition of the ray class group to allow us to

- define maps between different ray class groups for the same order, and
- make the invertibility condition follow from the coprimality condition.

### Proposition (K and Lagarias 2022)

For any  $\mathcal{O}$ -ideal  $\mathfrak{d} \subseteq \mathfrak{m}$ , the inclusion map  $J_{\mathfrak{d}}^*(\mathcal{O}) \subseteq J_{\mathfrak{m}}^*(\mathcal{O})$  induces an isomorphism

$$Cl_{\mathfrak{m}, \Sigma}(\mathcal{O}) \cong \frac{J_{\mathfrak{d}}^*(\mathcal{O})}{P_{\mathfrak{m}, \Sigma}^{\mathfrak{d}}(\mathcal{O})}$$

where

$J_{\mathfrak{d}}^*(\mathcal{O}) = \{\text{invertible fractional ideals of } \mathcal{O} \text{ coprime to } \mathfrak{d}\}$ , and

$P_{\mathfrak{m}, \Sigma}^{\mathfrak{d}}(\mathcal{O}) = \left\{ \alpha \mathcal{O} : \begin{array}{l} \alpha \in K^\times, \alpha \equiv 1 \pmod{\mathfrak{m}}, \rho(\alpha) > 0 \text{ for all } \rho \in \Sigma, \\ \text{and } \alpha \mathcal{O} \text{ is coprime to } \mathfrak{d} \end{array} \right\}.$

## Change of order

We also need to define maps between class groups for different orders. For  $\mathcal{O} \subseteq \mathcal{O}'$ , there are **extension** and **contraction** maps

$$\begin{aligned} \text{ext} : \{\mathcal{O}\text{-ideals}\} &\rightarrow \{\mathcal{O}'\text{-ideals}\} & \text{ext}(\mathfrak{a}) &= \mathfrak{a}\mathcal{O}, \\ \text{con} : \{\mathcal{O}'\text{-ideals}\} &\rightarrow \{\mathcal{O}\text{-ideals}\} & \text{con}(\mathfrak{a}') &= \mathfrak{a} \cap \mathcal{O}. \end{aligned}$$

The main technical result about extension and contraction maps is the following proposition.

### Proposition

Let  $\mathfrak{d}$  be an integral  $\mathcal{O}'$ -ideal with  $\mathfrak{d} \subseteq (\mathcal{O} : \mathcal{O}')$ . Then the extension and contraction maps extend uniquely to isomorphisms

$$\begin{aligned} \text{ext} : J_{\mathfrak{d}}(\mathcal{O}) &\rightarrow J_{\mathfrak{d}}(\mathcal{O}'), \\ \text{con} : J_{\mathfrak{d}}(\mathcal{O}') &\rightarrow J_{\mathfrak{d}}(\mathcal{O}). \end{aligned}$$

This is technically tricky because  $\text{con}$  is **not** a homomorphism on ideals not coprime to  $(\mathcal{O} : \mathcal{O}')$ .

## Change of modulus and order exact sequence

### Theorem (K and Lagarias 2022)

Let  $\mathfrak{m}$  be an ideal of  $\mathcal{O}$ ,  $\mathfrak{m}'$  an ideal of  $\mathcal{O}'$  such that  $\mathfrak{m}\mathcal{O}' \subseteq \mathfrak{m}'$ , and  $\Sigma' \subseteq \Sigma \subseteq \{\text{embeddings } K \hookrightarrow \mathbb{R}\}$ . Let  $\mathfrak{d}$  be any  $\mathcal{O}'$ -ideal such that  $\mathfrak{d} \subseteq (\mathfrak{m} : \mathcal{O}')$ . Let  $r = |\Sigma \setminus \Sigma'|$ . We have the following exact sequence.

$$1 \rightarrow \frac{U_{\mathfrak{m}', \Sigma'}(\mathcal{O}')}{U_{\mathfrak{m}, \Sigma}(\mathcal{O})} \rightarrow \frac{U_{\mathfrak{m}'}(\mathcal{O}'/\mathfrak{d})}{U_{\mathfrak{m}}(\mathcal{O}/\mathfrak{d})} \times \{\pm 1\}^r \rightarrow Cl_{\mathfrak{m}, \Sigma}(\mathcal{O}) \rightarrow Cl_{\mathfrak{m}', \Sigma'}(\mathcal{O}') \rightarrow 1.$$

Here, the “U-groups” are subgroups on unit groups defined by

$$U_{I, \Sigma}(R) := \{\alpha \in R^\times : \alpha \equiv 1 \pmod{I} \text{ and } \rho(\alpha) > 0 \text{ for } \rho \in \Sigma\}.$$

This theorem allows us to

- understand the kernel of the “extension and change of modulus map” between different ray class groups of orders;
- construct new maps (needed for class field construction);
- compute the sizes of ray class groups of orders.

## Construction of class field of orders

A surjective map from  $\psi : \text{Cl}_{(\mathfrak{m} : \mathcal{O}_K), \Sigma}(\mathcal{O}_K) \rightarrow \text{Cl}_{\mathfrak{m}, \Sigma}(\mathcal{O})$  is induced by the following diagram (and may also be described more explicitly using the contraction map).

$$\begin{array}{ccccccc}
 1 & \xrightarrow{\frac{\mathcal{O}_K^\times}{U_{(\mathfrak{m} : \mathcal{O}_K), \Sigma}(\mathcal{O}_K)}} & (\mathcal{O}_K / (\mathfrak{m} : \mathcal{O}_K))^\times \times \{\pm 1\}^{|\Sigma|} & \xrightarrow{\quad} & \text{Cl}_{(\mathfrak{m} : \mathcal{O}_K), \Sigma}(\mathcal{O}_K) & \xrightarrow{\quad} & \text{Cl}(\mathcal{O}_K) \rightarrow 1 \\
 & \downarrow \kappa & \downarrow \pi & & \downarrow \psi & & \parallel \text{id} \\
 1 & \xrightarrow{\frac{\mathcal{O}_K^\times}{U_{\mathfrak{m}, \Sigma}(\mathcal{O})}} & \frac{(\mathcal{O}_K / (\mathfrak{m} : \mathcal{O}_K))^\times}{U_{\mathfrak{m}}(\mathcal{O} / (\mathfrak{m} : \mathcal{O}_K))} \times \{\pm 1\}^{|\Sigma|} & \xrightarrow{\quad} & \text{Cl}_{\mathfrak{m}, \Sigma}(\mathcal{O}) & \xrightarrow{\quad} & \text{Cl}(\mathcal{O}_K) \rightarrow 1
 \end{array}$$

Then the Takagi existence theorem and Artin reciprocity (in standard class field theory) and the Galois correspondence defines a corresponding class field  $H_{\mathfrak{m}, \Sigma}^{\mathcal{O}}$  as a subfield of  $H_{(\mathfrak{m} : \mathcal{O}_K), \Sigma}$ .

## Theorem 1

The following theorem describes the ray class field of an order in terms of the splitting of primes.

## Theorem (K and Lagarias 2022)

The field  $H_{m,\Sigma}^{\mathcal{O}}$  is the unique abelian Galois extension of  $K$  with the property that:

a prime ideal  $\mathfrak{p}$  of  $\mathcal{O}_K$  that  
is coprime to  $(\mathfrak{m} : \mathcal{O}_K)$     $\iff$   
splits completely in  $H_{\mathfrak{m}, \Sigma}^{\mathcal{O}}$

$\mathfrak{p} \cap \mathcal{O} = \pi \mathcal{O}$ , a principal prime  $\mathcal{O}$ -ideal such that  $\pi \equiv 1 \pmod{\mathfrak{m}}$  and  $\rho(\pi) > 0$  for  $\rho \in \Sigma$ .

## Theorem 2

The following theorem relates the ray class field of an order to ray class fields of a larger order (such as the maximal order).

### Theorem (K and Lagarias 2022)

For any order  $\mathcal{O}' \supseteq \mathcal{O}$ , there are inclusions of ray class fields

$$H_{\mathfrak{m}\mathcal{O}',\Sigma}^{\mathcal{O}'} \subseteq H_{\mathfrak{m},\Sigma}^{\mathcal{O}} \subseteq H_{(\mathfrak{m}:\mathcal{O}'),\Sigma}^{\mathcal{O}'}$$

In particular, for  $\mathcal{O}' = \mathcal{O}_K$ ,

$$H_{\mathfrak{m}\mathcal{O}_K,\Sigma} \subseteq H_{\mathfrak{m},\Sigma}^{\mathcal{O}} \subseteq H_{(\mathfrak{m}:\mathcal{O}_K),\Sigma}^{\mathcal{O}'}$$

## Theorem 3

The following theorem is a generalization of the Artin reciprocity law to ray class fields of orders.

### Theorem (K and Lagarias 2022)

Let  $H_0 = H_{\mathfrak{m}, \Sigma}^{\mathcal{O}}$  and  $H_1 = H_{(\mathfrak{m} : \mathcal{O}_K), \Sigma}$ . There is an isomorphism

$$\text{Art}_{\mathcal{O}} : \text{Cl}_{\mathfrak{m}, \Sigma}(\mathcal{O}) \rightarrow \text{Gal}(H_0/K),$$

uniquely determined by the condition on prime ideals

$$\text{Art}_{\mathcal{O}}([\mathfrak{p}])(\alpha) \equiv \alpha^p \pmod{\mathfrak{P}}$$

where  $\mathfrak{P}$  is any prime of  $\mathcal{O}_{H_0}$  lying over  $\mathfrak{p}\mathcal{O}_K$ . Moreover, for any ideal  $\mathfrak{a}$  coprime to  $\mathfrak{f}(\mathcal{O}) \cap \mathfrak{m}$ ,

$$\text{Art}_{\mathcal{O}}([\mathfrak{a}]) = \text{Art}([\mathfrak{a}\mathcal{O}_K])|_{H_0},$$

where  $\text{Art} : \text{Cl}_{(\mathfrak{m} : \mathcal{O}_K), \Sigma}(\mathcal{O}_K) \rightarrow \text{Gal}(H_1/K)$  is the usual Artin map of class field theory.

## Explicit class field theory, overview

Hilbert's 12th Problem asks for analytic functions whose special values generate the abelian extensions of a number field  $F$ .

We really want:

- (1) analytic functions
- (2) a geometric explanation

Stark's conjecture provides a partial answer to (1) via  $L$ -functions. We still don't know much about (2).

I won't talk about:

- CM abelian varieties in  $\dim > 1$
- $p$ -adic solutions (Gross–Stark and Brumer–Stark conjectures; work of Dasgupta, Kakde, Silliman, Ventullo, Wang; work of Darmon, Pozzi, Vonk)

## Explicit class field theory, analytic approach

field $F$	analytic function values generating $H_{m\mathcal{O}, \Sigma}^{\mathcal{O}}$
$\mathbb{Q}$	$\exp\left(\frac{2\pi i}{m}\right)$
imaginary quadratic	complex multiplication values of modular functions (e.g., the Klein $j$ -function and Weber's functions/modular units) of level $m$
real quadratic	conjecturally, stable (RM) values $\mathfrak{w}^r[\beta]$ of the level $m$ Shintani–Faddeev modular cocycle [K 2024+; see also Stark 1976, Shintani 1977, Kurokawa 1991, Sczech 1993, ...]
complex cubic	conjecturally, at least for $\mathcal{O} = \mathcal{O}_F$ , stable values of a cocycle related to the elliptic gamma function [Bergeron, Charollois, García 2023]

## Spotlight: The Shintani–Faddeev modular cocycle

Let  $\mathbf{r} = \begin{pmatrix} r_1 \\ r_2 \end{pmatrix} \in \mathbb{Q}^2$  and  $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_{\mathbf{r}} = \{A \in \mathrm{SL}_2(\mathbb{Z}) : A\mathbf{r} - \mathbf{r} \in \mathbb{Z}^2\}$ .  
For  $\mathrm{Im}(\tau) > 0$ , define

$$\mathfrak{w}_A^{\mathbf{r}}(\tau) = \prod_{k=0}^{\infty} \frac{1 - e\left((k + r_2)\frac{a\tau + b}{c\tau + d} - r_1\right)}{1 - e((k + r_2)\tau - r_1)}, \text{ where } e(z) := e^{2\pi iz}.$$

### Theorem (Dimofte 2015; K 2024+)

The function  $\mathfrak{w}_A^{\mathbf{r}}(\tau)$  meromorphically continues (with some poles in  $\mathbb{Q}$ ) to  $U_A = \mathbb{C} \setminus \{\tau \in \mathbb{R} : c\tau + d \leq 0\}$ .

### Theorem (K 2024+)

Suppose  $\beta$  is real quadratic and  $\frac{a\beta + b}{c\beta + d} = \beta$ . Assuming the Stark conjectures, if  $\mathcal{O} = \mathrm{ord}(\beta\mathbb{Z} + \mathbb{Z})$  and  $\mathbf{r} \in \frac{1}{m}\mathbb{Z}^2$ , then

$$(\text{explicit } 12m\text{-th root of unity})(\mathfrak{w}_A^{\mathbf{r}}(\beta))^2 \in H_{m\mathcal{O}, \{\infty_2\}}^{\mathcal{O}}.$$

## Explicit class field theory, algebraic/geometric approach

field $F$	geometric object producing $H_{m\mathcal{O}, \Sigma}^{\mathcal{O}}$
$\mathbb{Q}$	$m$ -torsion points on the unit circle
imaginary quadratic	$m$ -torsion points on elliptic curve $E$ with $E(\mathbb{C}) \cong \mathbb{C}/\mathcal{O}$
real quadratic	conjecturally (for a restricted set of $m$ ), certain equichordal configurations of $m^2$ subspaces in $\mathbb{C}^m$ [Appleby, Flammia, K 2024+]
complex cubic	???

## Spotlight: Sample of Appleby–Flammia–K construction

Let  $F = \mathbb{Q}(\sqrt{5})$  and  $\varphi = \frac{1+\sqrt{5}}{2}$ .

- $H_{(4)\infty_1\infty_2}^{\mathbb{Z}[\varphi]} = H_{4\mathbb{Z}[\varphi],\{\infty_1,\infty_2\}}^{\mathbb{Z}[\varphi]}$  is generated by the unitary invariants of 16 equiangular lines in  $\mathbb{C}^4$ .
- $H_{(8)\infty_1\infty_2}^{\mathbb{Z}[\varphi]}$  and  $H_{(8)\infty_1\infty_2}^{\mathbb{Z}[2\varphi]}$  are generated by the unitary invariants of two different configurations of 64 equiangular lines in  $\mathbb{C}^8$ .
- $H_{(11)\infty_1\infty_2}^{\mathbb{Z}[\varphi]}$  is generated by the unitary invariants of 121 equichordal 3-dimensional subspaces in  $\mathbb{C}^{11}$ .
- Assuming the Stark conjectures and a (probably very difficult!) special value identity for  $\mathfrak{w}_A^r(\tau)$ , a cofinal set of class fields are obtained similarly.

## Other potential applications

- Complex multiplication of abelian varieties (non-Gorenstein orders cause difficulties; talk to Pete Clark)
- (Higher) composition laws (and arithmetic statistics)
- Modular-eque  $q$ -series  $\sum_{\mathcal{O}} c_{\mathcal{O}} q^{\pm \text{disc}(\mathcal{O})}$  built from ray class data over some family of orders (Beckwith and K work in progress)
- Lattice-based cryptography (some existing schemes use non-maximal orders)
- Computational algebraic number theory

Introduction  
○○○○○

Class groups of orders  
○○○○○○○

Class fields of orders  
○○○○

Explicit class field theory  
○○○○○●

**Thank you!**

Thank you for listening! Any questions?